Key-Person Risk inside the Family Office

Institutional Continuity beyond the Trusted Adviser

Authored by Chennakeshav Adya
Independent Researcher
August 2026

Abstract

A family office can appear institutionally sophisticated while remaining dependent on one trusted adviser. That person can hold the investment history, family context, bank relationships, password-recovery path, payment knowledge, document map and informal authority needed to turn a decision into action. Illness, incapacity, departure, conflict, cyber compromise or death can therefore interrupt more than a role. The event can suspend liquidity, delay a capital call, weaken investment challenge, expose confidential information, impair entity governance and leave the family unable to determine who may act.

This paper develops a key-person continuity framework for family offices, private investment companies and related family structures. It begins with the decisions and services that must continue, maps each dependency across people, authority, process, systems, evidence and external providers, and distinguishes temporary unavailability from permanent succession. The framework draws on ISO 22301 business-continuity principles, NIST contingency-planning and cybersecurity guidance, FINRA's business-continuity rule and observations within their broker-dealer scope, the SEC's expressly identified 2016 adviser proposal, ILPA's key-person guidance within private funds, and current DIFC and ADGM family-governance materials.

Six figures show the dependency architecture, critical-capability map, recoverability matrix, entity-aware liquidity ladder, incident decision tree and continuity dashboard. Six tables specify the key-person register, authority-and-alternate matrix, process recovery controls, data and provider continuity, scenario exercise and 100-day implementation. A hypothetical UAE family office demonstrates how a board can convert informal reliance into measured institutional continuity. Every number and circumstance in the example is a management assumption created solely to explain the method.

The applicable legal, fiduciary, employment, succession, tax, accounting, regulatory, privacy, cybersecurity and governance treatment depends on the family, entities, jurisdictions, documents and facts. This paper provides general information for professional audiences and does not provide legal, tax, accounting, regulatory, cybersecurity, medical or investment advice.

JEL Classification: D81, G11, G23, G32, G34, M12, M15

Keywords: family office, key-person risk, business continuity, succession planning, delegated authority, investment governance, treasury controls, knowledge management, operational resilience, family governance

1. The trusted-adviser paradox

Trust is central to a family office. The governing family needs people who understand its history, preferences, entities, investments and private circumstances. Concentrating that understanding in one adviser can also concentrate operational risk. The office may have investment policies, bank mandates and board minutes while one person still knows how the system actually works.

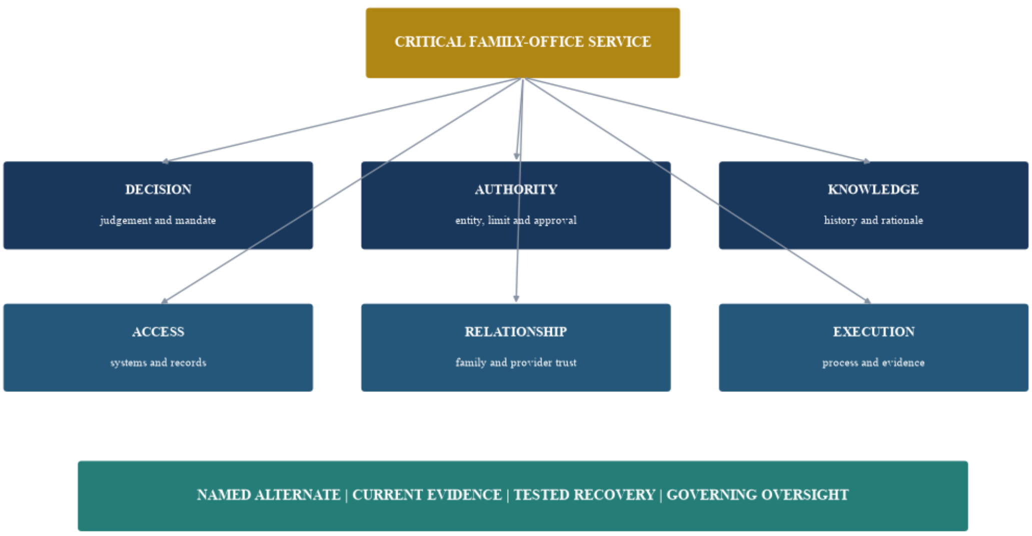
The dependency often becomes visible during an absence. A bank asks for an authority document that only one adviser can locate. A capital call arrives and the payment preparer lacks verified instructions. An investment committee can see the proposed transaction, yet cannot reconstruct the prior negotiation or portfolio constraint. An external manager will speak only with the established relationship owner. A family member asks why an exception was accepted and the rationale sits in private messages.

Key-person risk therefore concerns more than succession to a job title. It concerns continuity of a capability. The capability may require a combination of legal authority, judgement, information, system access, provider cooperation, family confidence and current evidence. Naming a deputy addresses only one component.

The control objective is practical: the office should continue priority services at an approved level when a critical person becomes unavailable. It should also preserve segregation of duties, confidentiality and lawful authority during the response. A continuity arrangement that gives one alternate unrestricted access can create a second concentration of risk.

ISO 22301:2019 provides a general business-continuity management framework for organisations of different sizes.[1] NIST SP 800-34 Rev. 1 describes the evaluation of systems and operations to determine contingency requirements and priorities.[2] These references support an operating discipline built around critical activities, impact, recovery, testing and maintenance. They do not determine the family office's legal structure or succession rights.

Figure 1. Key-person dependency architecture inside a family office



Author framework. Continuity requires capability, authority, access, evidence and communication to remain aligned.

2. Define continuity before naming a successor

The governing body should first identify the services that require continuity. Typical priorities include cash visibility, payments, capital calls, debt service, investment monitoring, investment approvals, entity actions, tax and regulatory deadlines, payroll, document access, insurance notifications, cyber response and family communications. The list should state the minimum acceptable service during disruption.

Each service receives a maximum tolerable period of disruption and a target recovery time. A same-day capital-call payment may need immediate triage, while a quarterly asset-allocation review may tolerate a short delay. The office also identifies a recovery point for information. Daily cash data may require a recent snapshot; a legal authority schedule must reflect the current executed instrument.

The criticality decision should consider value, time, legal consequence, liquidity, confidentiality and reversibility. A low-value payment can be critical when it keeps an entity in good standing. A large proposed investment can wait when the committee lacks adequate evidence. A family communication can become urgent when silence creates conflicting instructions.

The continuity charter names the governing sponsor, incident authority, scope, thresholds, escalation route and review frequency. It distinguishes service continuity from succession. Service continuity keeps priority activities operating through a disruption. Succession transfers a role or relationship for a longer period under the applicable legal and governance process.

The charter should state which services may pause. A controlled pause can be safer than improvisation when authority, evidence or segregation is incomplete. The decision and rationale should be recorded.

3. Build the critical-capability register

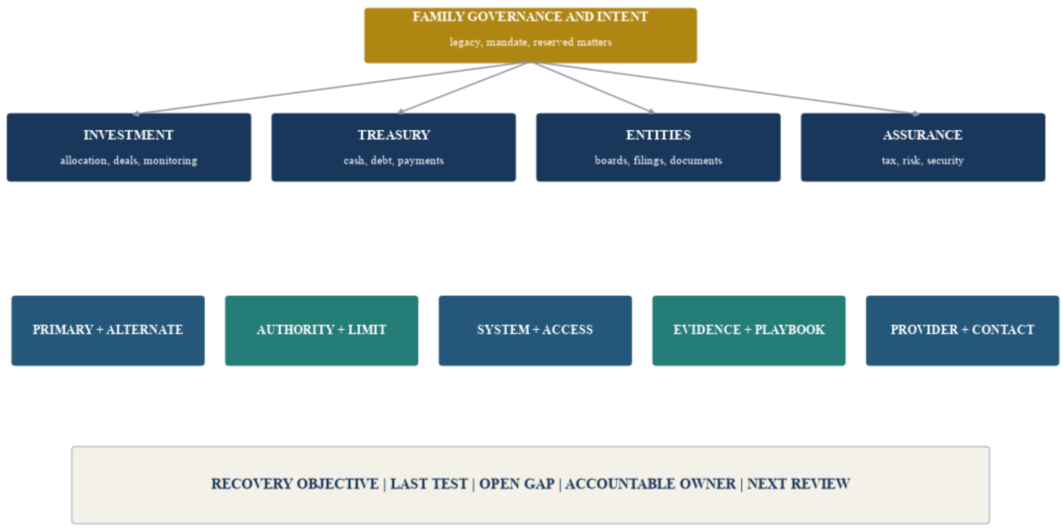
A job description rarely captures the full dependency. The office should observe the work, review recent decisions, inspect calendars and correspondence, and ask providers how instructions are received. This produces a critical-capability register organised around outcomes.

For every capability, the register identifies the primary person, alternate, legal entity, decision owner, process, system, credential path, evidence, provider and family relationship. It records frequency, deadline, disruption impact, recovery objective and current test status. A capability can have several key people. One adviser may frame an investment, another may challenge it, and two directors may approve the correct entity action.

Concentration can be hidden in informal work. Examples include interpreting the founder's intent, knowing why an asset is held through a particular structure, recalling a side-letter right, understanding a bank's operational practice, locating a signed guarantee, recognising a fraudulent payment request or knowing which family members should receive sensitive information.

The register should also capture negative knowledge: transactions the family has declined, conflicts that have occurred, providers whose scope is limited, and exceptions that require renewed approval. Continuity requires enough context to avoid repeating a settled mistake.

Figure 2. Critical-capability map from family governance to authorised execution



Author framework. The map links each outcome to people, evidence and operating dependencies.

Table 1. Minimum key-person and critical-capability register

Field	Required record	Control question	Evidence
Critical service	outcome, legal entity, frequency and deadline	what must continue and for whom?	approved continuity charter
Primary dependency	person, role and specific contribution	what fails when this person is unavailable?	observed process and decision history
Alternate	person, readiness and permitted scope	can the alternate perform at the required level?	assessment, training and exercise result
Authority	instrument, entity, action, limit and validity	may the person lawfully approve or execute?	mandate, resolution, power or governing document
Process	steps, inputs, controls and handoffs	can another person reproduce the activity?	current procedure and completed example
Systems and access	application, role, authentication and recovery	can authorised access be obtained without sharing credentials?	access register and tested recovery
Information	source, location, owner, date and sensitivity	is the required evidence current and available?	controlled repository and index
Provider	institution, service, contact and escalation	will the provider recognise the alternate?	contract, mandate and relationship confirmation
Recovery	target time, minimum service and last exercise	has recoverability been demonstrated?	exercise record and remediation log

Every record should link to current evidence and an accountable review owner.

4. Separate authority, capability and access

Continuity fails when an office treats authority, capability and access as interchangeable. A person can understand the portfolio while lacking authority to instruct a bank. A director can possess legal authority while lacking current investment information. An administrator can access a system while lacking approval rights. All three conditions should be tested separately.

The authority matrix should identify each legal entity, governing body, committee, bank account, custody account, contract and filing. For each action it records the decision maker, preparer, reviewer, signatory, release authority, financial limit, quorum, dual-control rule and fallback route. It also records the source instrument and effective date.

Incapacity and death can affect authority differently across entities and documents. The family should obtain current jurisdiction-specific advice on powers of attorney, directorships, foundation councils, guardians, trustees, executors, protectors, authorised signatories and employment delegations. An internal continuity plan cannot create a legal power that the relevant instrument or law does not provide.

DIFC's Family Arrangements Regulations provide a current framework for family businesses and entities controlled by families holding assets and operating in or from DIFC.[3] ADGM describes its foundation as a distinct legal person with a Foundation Council and guardian oversight, and its official materials identify perpetual existence after the founder's lifetime.[4] The specific effect of a structure depends on its governing documents and current law. These regimes illustrate why institutional continuity should be built into entities and authority rather than resting only on a personal relationship.

Capability requires knowledge, judgement and practice. The alternate should complete the task under supervision before an incident. Access should use individual identities, least privilege, strong authentication and controlled recovery. Shared credentials weaken accountability and can prevent rapid revocation after a departure or compromise.

Table 2. Authority-and-alternate matrix

Action	Primary role	Alternate role	Authority evidence	Capability evidence	Access gate
View consolidated cash	treasury lead	finance controller	approved role schedule	recent reconciled cash pack	individual read access and strong authentication
Prepare payment	treasury operations	trained finance alternate	workflow delegation	observed preparation and fraud checks	maker-only bank entitlement
Approve payment	authorised signatories	documented alternate signatories	current bank mandate and entity resolution	limit and entity training	checker entitlement with dual control
Approve investment	investment committee	permitted alternate quorum	committee terms and delegation	completed decision exercise	approved committee repository
Sign transaction document	entity director or attorney	valid alternate officer or attorney	constitutional document, resolution or power	transaction briefing and advice	controlled signature process
Instruct custodian	authorised investment or operations role	registered alternate	custody mandate	tested instruction and settlement process	named user and approved channel
File entity return	company secretary or provider	nominated alternate	engagement and filing authority	deadline and evidence review	portal role and recovery path
Communicate with family	designated relationship lead	approved family liaison	family communication protocol	confidentiality and escalation training	need-to-know information set

Legal and regulatory conclusions require current advice for the relevant entity, jurisdiction and instrument.

5. Design for temporary absence and permanent succession

Temporary and permanent events require different response paths. Temporary unavailability can arise from travel disruption, illness, cyber lockout, communications failure, conflict or an urgent family matter. The office may preserve the person's role while activating limited alternates. Permanent unavailability can require appointment, removal, probate, board action, contract transition, long-term recruitment and transfer of relationships.

The plan should define activation thresholds. A short communication delay may require monitoring. A missed capital-call deadline or inability to confirm authority may require immediate escalation. A suspected credential compromise requires security response even if the person remains available. A conflict allegation can require recusal and independent review.

The SEC's 2016 proposed adviser business-continuity and transition rule expressly discussed temporary and permanent loss of key personnel, short-term role coverage and long-term succession.[5] The proposal was not adopted as a final rule. Its structure provides a useful design reference for distinguishing service continuity from business transition.

ILPA Principles 3.0 address key-person provisions within private-fund partnerships. ILPA links key people to investment outcomes, calls for orderly planned and unplanned transitions, and discusses notification and suspension mechanisms following a trigger.[6] A family office investing as an LP should understand each fund's contractual provisions. Inside the family office, the same logic supports explicit triggers, affected decisions, interim limits and governing review.

Every activation should state duration, scope and conditions. An interim investment lead may monitor existing assets and close previously approved matters while new commitments remain paused. An alternate signatory may make priority payments within a reduced limit. Permanent succession should follow the relevant appointment and approval process.

6. Protect investment judgement and institutional memory

Investment continuity requires more than an asset list. The office should preserve the thesis, downside case, valuation basis, ownership rights, governance obligations, expected milestones, conflicts, tax or legal dependencies and exit conditions for every material position.

The investment record should explain why an asset was acquired, what evidence would invalidate the thesis and what the governing body approved. It should link committee papers, advice, signed documents, cash flows, monitoring reports and post-investment actions. A relationship history records manager interactions, negotiated rights, unresolved requests and communication commitments.

Portfolio memory also includes rejected decisions. A proposal can return under a different name after the adviser who rejected it departs. A concise decision log lets the committee review the previous evidence and determine whether facts have changed.

Knowledge transfer works best through operating artefacts. The alternate should prepare a committee pack, challenge a valuation, reconcile a capital account, attend a manager meeting and document the result. Interviews and written handovers support the transfer, while observed performance demonstrates capability.

The office should avoid creating an uncontrolled personal archive. Current documents, notes and correspondence should sit within approved repositories, retention rules and access permissions. Sensitive family context should be separated from operational facts and limited to people with a legitimate need.

7. Preserve treasury and payment continuity

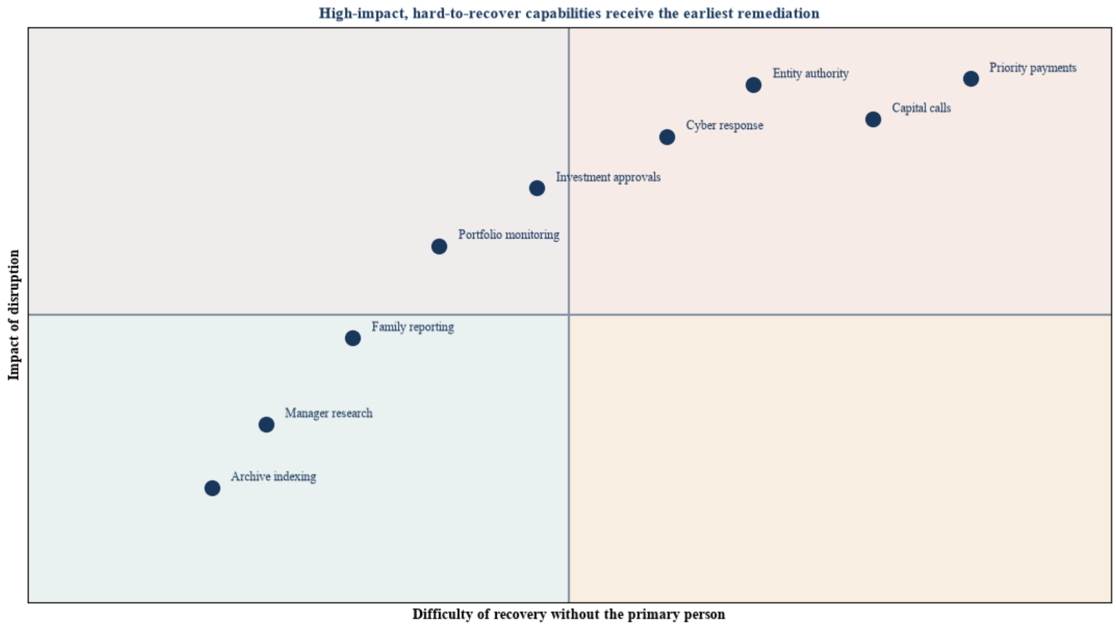
Treasury becomes critical because deadlines continue during an absence. The office needs a daily or appropriately frequent cash view by legal entity, account and currency. It should distinguish available, restricted, pledged and reserved cash, then connect upcoming uses to the entity that must pay.

The continuity pack identifies payroll, debt service, tax, insurance, capital calls, contractual payments and approved family distributions. Each item includes due date, amount, currency, legal owner, verified instructions, preparation route, approval requirement and evidence. Expected receipts remain separate from available cash.

Payment continuity should preserve dual control. Emergency access should not combine preparation, approval and release in one person. Alternate signatories should be established in advance and validated with the institution. The office should independently verify new or changed payment instructions through a known channel.

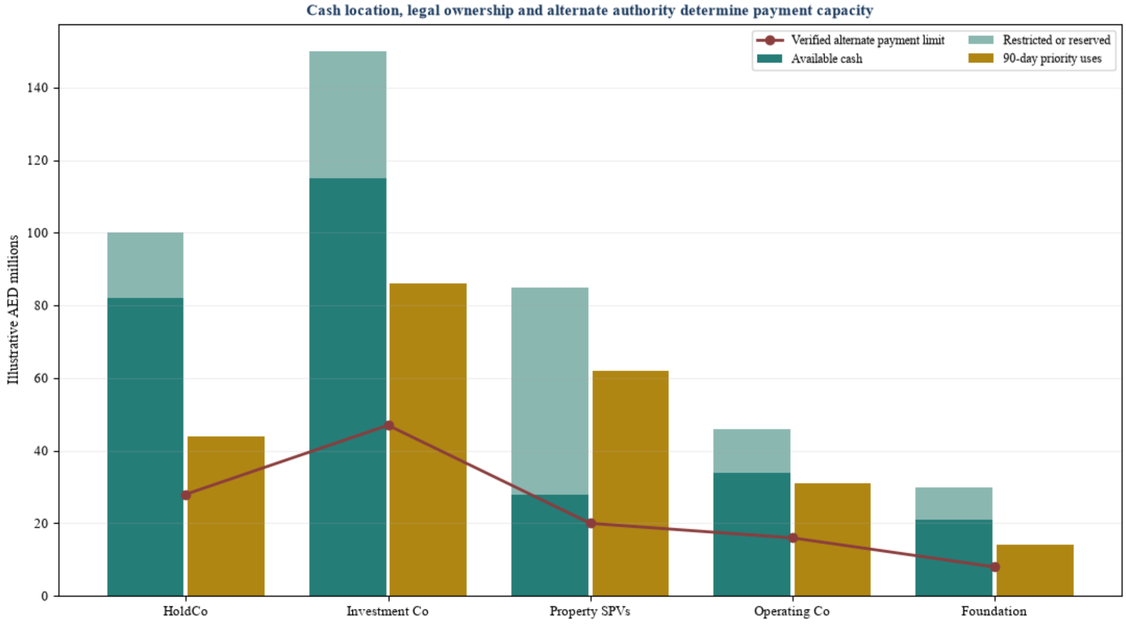
FINRA Rule 4370 requires members within its scope to maintain written business-continuity plans addressing areas including backup and recovery, mission-critical systems, financial and operational assessments, alternate communications, critical banks and counterparties, and customer access to funds and securities.[7] It also requires senior management approval, annual review and two emergency contacts. A family office outside FINRA's perimeter is not subject to that rule solely because it uses these topics. The categories offer a rigorous checklist for treasury continuity.

Figure 3. Criticality and recoverability matrix for family-office capabilities



Illustrative placement. Each office should approve its own impact and recoverability assessment.

Figure 4. Entity-aware liquidity ladder during a key-person disruption



Values are illustrative management assumptions used solely to demonstrate continuity analysis.

8. Keep entity governance current

Entities continue to face deadlines and governance requirements during a disruption. The office should maintain a current map of directors, officers, council members, guardians, trustees, protectors, secretaries, authorised representatives, beneficial owners and advisers. It should identify vacancies, conflicts, expiry dates, quorum and reserved matters.

The entity pack contains the constitutional document, governing regulations, shareholder or partnership agreement, trust deed or foundation charter and by-laws where applicable, current registers, delegations, powers, mandates, licences, insurance and filing calendar. The pack records the authoritative location and the adviser responsible for current legal interpretation.

An entity action should follow the correct chain. The investment committee may recommend a transaction while the entity board or authorised signatory approves and executes it. Continuity planning should preserve that distinction. A family consensus cannot automatically substitute for a required corporate, trust or foundation act.

ADGM's official foundations material describes guardian supervision of the Foundation Council and provides for a distinct legal personality and perpetual existence.[4] DIFC's family arrangements materials support family and legacy planning through defined structures.[3] These are jurisdiction-specific frameworks. Their relevance to any family requires current professional advice and review of the actual governing instruments.

9. Control data, credentials and recovery

The office should know which systems support every critical service. The inventory includes banking, custody, portfolio reporting, accounting, document management, communication, identity, payroll, tax, entity administration and cybersecurity tools. It names the system owner, vendor, administrator, authentication method, recovery route, backup, data export and service dependency.

NIST Cybersecurity Framework 2.0 organises cybersecurity outcomes around Govern, Identify, Protect, Detect, Respond and Recover.[8] Its Govern function emphasises strategy, expectations and policy. A family office can use these functions to align identity, data protection, monitoring, incident response and recovery with its continuity programme.

Every critical system should have at least two authorised administrative paths under separation of duties. Recovery should avoid dependence on the unavailable person's phone, personal email or private device. Emergency credentials can be held through a controlled vault with dual approval, logging and periodic testing. Individual accounts should remain attributable.

Backups need restoration tests. A successful backup job does not demonstrate that the office can recover current records, permissions and workflows. The test should restore a defined data set, validate completeness, confirm authorised access and record elapsed time.

Departure controls require immediate access review, credential revocation, device recovery, forwarding rules review, provider notification and preservation of business records under applicable law and policy. A suspected compromise follows the cyber incident process and may require a broader response than a normal departure.

Table 3. Critical-process recovery controls

Process	Minimum service during disruption	Recovery input	Alternate control	Evidence of recovery
Cash position	available cash by entity, account and currency	bank or custodian source and prior reconciliation	treasury alternate prepares; controller reviews	dated cash pack and exception list
Priority payments	verified obligations paid by due date	invoice, notice, mandate and cash	maker-checker-release separation	bank confirmation and post-payment match
Capital calls	notice validated, liquidity reserved and payment controlled	LPA data, administrator notice and verified instructions	fund-operations alternate plus signatories	notice checklist, approval and settlement
Investment monitoring	material events and covenant or milestone exceptions identified	company, manager and provider reports	secondary deal owner reviews	updated monitoring record and escalation
Investment decision	decision pack, authority, conflict and funding complete	source evidence and current portfolio view	alternate chair or quorum under terms	minutes, conditions and authority record
Entity governance	deadlines, quorum and authorised actions maintained	governing documents and calendar	company secretary and alternate officer	filing receipt, resolution or register update
Cyber incident	affected identities isolated and critical services protected	logs, asset inventory and response plan	security lead and external incident provider	incident record, containment and recovery test
Family communication	accurate need-to-know update delivered	approved facts and communication protocol	designated family liaison	approved message and recipient record

Recovery objectives and minimum service levels require governing approval.

10. Govern external providers and relationship ownership

A family office depends on banks, custodians, administrators, investment managers, lawyers, tax advisers, accountants, company secretaries, technology vendors, insurers and specialist consultants. The internal key person can become the only bridge to these providers.

The provider register records service, entity, contract, relationship owner, operational contact, escalation contact, instruction method, authority requirement, data delivery, critical dependency, termination assistance and current alternate. The office should verify that the provider recognises the alternate and holds current mandates.

The contract review should examine service continuity, notification, data access, portability, subcontractors, security, incident support, exit and record retention. Actual rights depend on the executed contract. A vendor marketing statement does not establish an enforceable recovery commitment.

Provider concentration also matters. Several family-office services can depend on the same cloud, identity provider, administrator group or adviser. The dependency map should look through branded services where evidence is available. A fallback provider requires onboarding, data and authority before it becomes operationally useful.

FINRA's 2019 examination observations within its member-firm scope highlighted testing of mission-critical systems, key-person availability and vendor relationships.[9] The general lesson is measurable: the family office should test its own role and the provider's expected response together.

Table 4. Data, credential and provider continuity register

Dependency	Primary path	Alternate path	Control	Test evidence
Identity	named corporate account and strong authentication	approved recovery administrator	dual approval, logging and periodic access review	recovery exercise without primary device
Bank access	individual maker, checker and release roles	registered alternate users and signatories	entity and limit controls	low-risk test or institution confirmation
Documents	controlled repository with indexed current versions	encrypted tested backup and authorised custodian	classification, retention and immutable audit where used	sampled restore and document reconciliation
Portfolio data	administrator, custodian and approved internal records	controlled export and manual priority template	source, date, owner and reconciliation	reconstructed priority portfolio view
Communications	corporate channels and contact directory	approved alternate channel and family protocol	need-to-know scope and message approval	call-tree exercise
External provider	relationship owner and operating contact	named escalation and substitute relationship owner	current contract, mandate and service level	provider acknowledgement or joint exercise
Emergency secrets	controlled enterprise vault	dual-authorised recovery procedure	sealed access, logging and immediate rotation	witnessed recovery and revocation test
Physical records	secure indexed location	approved off-site or digital copy	access register and environmental protection	retrieval exercise

Provider capabilities and contractual rights should be confirmed directly and periodically.

11. Preserve family confidentiality and decision legitimacy

Continuity can widen information access at the moment when discretion matters most. The office should classify family information by purpose and recipient. Investment facts, personal information, ownership records, health information, disputes, estate plans and security details may require different access.

The alternate receives the minimum information required for the activated service. Sensitive context can be released in stages by an authorised information owner. Logs should record access to emergency repositories and critical documents. Data-protection and privilege questions require current professional advice.

Decision legitimacy also matters. A crisis can lead to conflicting instructions from family members, advisers and entity representatives. The continuity plan should identify who speaks for each legal person, who represents the family in communications, who resolves a conflict and which decisions remain reserved.

The office should communicate known facts, activated controls, affected services, decisions required and next update. It should avoid circulating medical or personal detail beyond legitimate need. A permanent succession announcement follows the relevant family and entity approval process.

12. Maintain challenge, conflicts and segregation

An unavailable key person can remove an important source of challenge. The office should identify whether the person serves as adviser, gatekeeper, controller, committee chair, signatory or relationship owner. An alternate operating model should recreate the needed challenge through defined roles.

Investment preparation, independent review and approval should remain distinct. Treasury preparation and release should remain separated. Valuation input and approval should use different roles where practicable. A related-party matter should preserve disclosure, recusal and authorised decision making.

Conflicts can also cause the event. A suspended adviser should not control the investigation, evidence or access response. The plan should include an independent escalation route to the board, family governance body, external counsel or other authorised function as applicable.

An emergency override needs a defined authority, narrow scope, reason, expiry and retrospective review. Repeated overrides indicate a structural weakness that requires remediation.

13. Exercise the plan through realistic scenarios

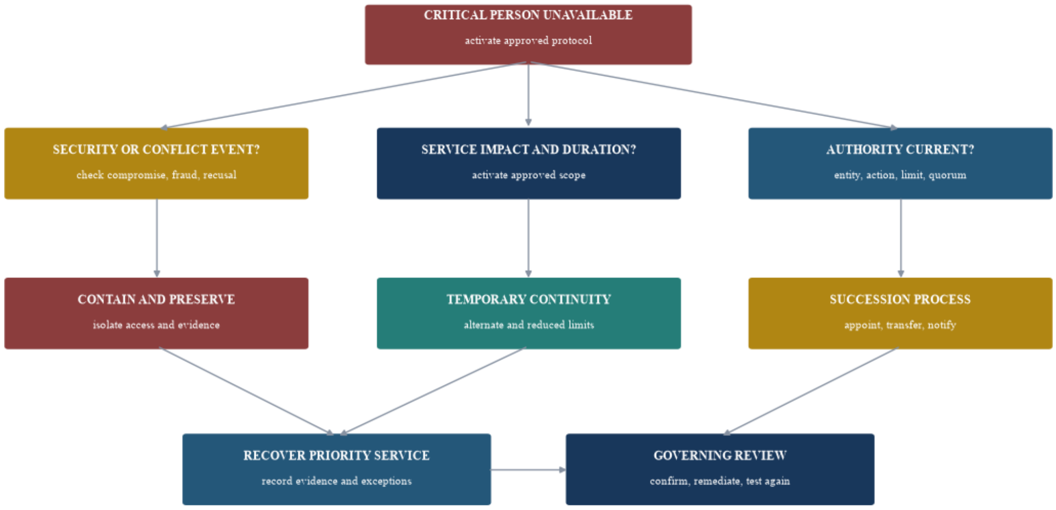
A continuity document has limited value until people perform the work. Exercises should test an end-to-end outcome through the real systems, evidence, providers and approvals used in normal operations. They can begin with a tabletop discussion and progress to parallel execution or controlled live tests.

Scenarios should cover sudden illness, extended incapacity, resignation, death, conflict, suspected fraud, credential compromise, provider outage and simultaneous disruption. The office should include an event that arrives during the absence, such as a capital call, covenant notice, time-sensitive acquisition or urgent entity filing.

The exercise measures detection time, activation time, service recovery, authority validation, evidence retrieval, provider response, decision quality, communication and exception closure. Observers record workarounds and control failures. Each issue receives an owner, deadline and consequence.

FINRA guidance within its scope explains that annual review may include testing specific functions, backup technology or an emergency personnel team.[10] The joint FINRA, SEC and CFTC advisory following Hurricane Sandy also encouraged business-continuity training and exercises.[11] A family office can adopt the discipline without implying regulatory coverage.

Figure 5. Incident decision tree for key-person unavailability



Author framework. Governing documents and current professional advice determine transaction-specific authority.

Table 5. Key-person continuity exercise design

Scenario	Inject	Required outcome	Measures	Typical remediation
Sudden 48-hour illness	capital call due next business day	validate notice, reserve cash and complete authorised payment	activation, evidence retrieval, dual control and settlement	alternate training, mandate or document-index update
Extended incapacity	primary investment lead unavailable for eight weeks	monitor assets and conduct a permitted committee decision	quorum, pack quality, conflicts and decision time	shadow ownership and committee terms update
Immediate departure	relationship owner loses access	preserve records, revoke access and transition providers	revocation time, provider acceptance and record completeness	offboarding playbook and alternate contacts
Credential compromise	primary user's device and email suspected	contain access and recover critical services securely	detection, isolation, secret rotation and restoration	identity architecture and logging improvements
Death of office principal	permanent role and authority transition required	activate family, entity and provider succession processes	valid appointments, communications and service continuity	governing-document and succession review
Provider outage	portfolio platform unavailable during board cycle	reconstruct priority view from controlled exports	recovery point, reconciliation and reporting delay	export cadence, backup and alternative process
Conflict allegation	key adviser must recuse immediately	preserve evidence and maintain independent decision path	access scope, recusal, escalation and legitimacy	independent escalation and role redesign

Exercise scope should be approved to avoid unauthorised transactions or disclosure.

14. Demonstrate the framework with a hypothetical family office

Consider a hypothetical UAE family office with management-estimated gross assets of AED 4.8 billion, 14 legal entities, five banks, three custodians, 21 private funds, six direct investments and four property SPVs. It employs nine people and uses 11 material external providers. Every number and circumstance is a management assumption created solely to demonstrate the framework. It does not describe a client or market observation.

The initial review finds that the chief investment adviser is the primary relationship owner for 17 managers and all six direct investments. The adviser chairs the investment committee, retains the narrative history for most decisions and administers the office's document workspace. The finance controller can access bank balances but cannot reconstruct the 12-month commitment forecast. Two family members are bank signatories, while the current mandate for one investment company remains incomplete in the central file.

The office identifies 46 critical capabilities. Twelve have no named alternate. Nine have a named alternate who has never completed the activity. Seven depend on a password-recovery route linked to the chief adviser's device. These conditions are illustrative.

The governing body sets recovery targets. Priority cash visibility and payment triage should recover within four hours. Capital-call processing should recover within one business day. Material investment monitoring should recover within two business days. New investment approvals can pause until valid quorum, evidence and challenge are available.

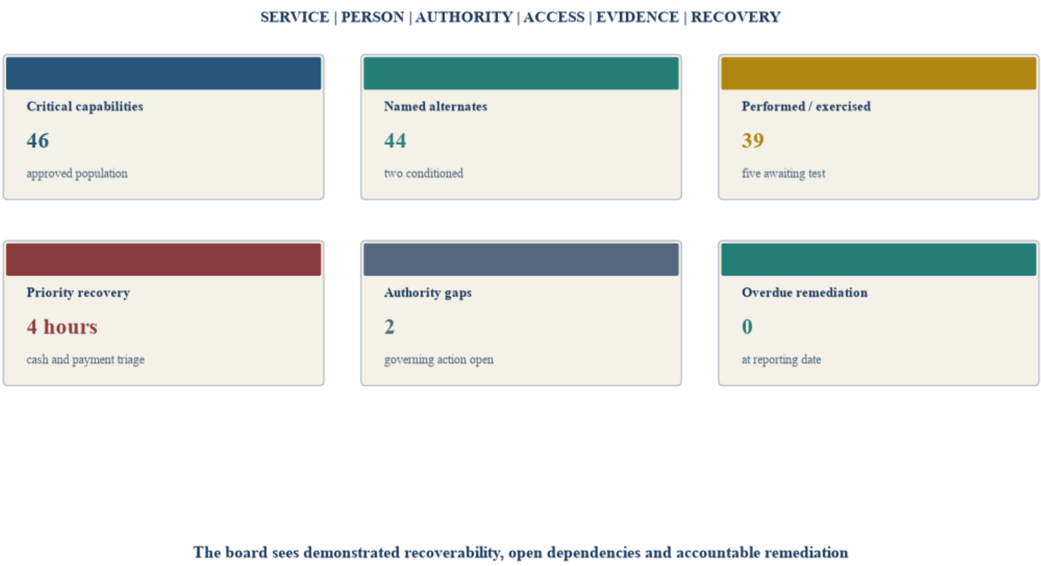
The hypothetical 90-day liquidity ladder shows AED 280 million of available cash and AED 131 million of restricted or reserved cash. Priority uses total AED 237 million. Existing alternates have verified authority to release only AED 119 million across the correct entities. Aggregate liquidity therefore appears adequate, yet operationally available authority is insufficient for the full schedule. The office arranges properly reviewed mandates and tests dual-controlled access before treating the gap as closed.

The first exercise presents an AED 38 million capital call due the next business day. The alternate finds the notice, validates the fund and commitment, confirms instructions through the administrator's known channel, reserves cash in the correct investment entity and prepares the payment. The exercise stops before a live transfer. It reveals that the administrator's escalation contact and the latest bank mandate were missing from the controlled repository.

The second exercise tests a direct-investment board issue. The alternate can locate the shareholder agreement and latest board pack, yet the decision log lacks the reason for a prior consent condition. The office creates a governed investment memory pack containing thesis, rights, milestones, conflicts, past decisions and current actions.

After remediation, 44 of the 46 critical capabilities have named alternates and current evidence. Thirty-nine have been performed or exercised. Two capabilities remain dependent on specialist external advice and are reported as conditioned. The dashboard keeps those gaps visible. This result is an illustrative management assumption and does not predict an outcome.

Figure 6. Hypothetical family-office key-person continuity dashboard



Every displayed value is an illustrative management assumption used solely to demonstrate dashboard design.

15. Measure continuity as an operating capability

The board dashboard should report coverage, readiness and observed performance. Coverage measures critical capabilities with an approved primary, alternate, authority record, playbook, system path and provider contact. Readiness measures training, evidence currency and successful exercises. Recovery performance measures elapsed time and minimum service achieved.

Useful indicators include single-person dependencies, alternate vacancy, expired authority, untested access, overdue knowledge packs, provider contacts awaiting confirmation, failed restorations, exercise findings, overdue remediation and emergency overrides. The dashboard should separate a documented control from a demonstrated control.

Quality matters alongside speed. A recovered investment process should preserve evidence, challenge, conflicts and authority. A payment completed quickly through shared credentials is a control failure. A delayed decision can be the approved outcome when the evidence is incomplete.

The risk appetite can define escalation thresholds. A priority service without a tested alternate may require board action. A high-impact authority gap can restrict new commitments. A provider dependency without an accessible data export can require contractual or operating remediation.

The register should be reviewed after personnel, entity, mandate, provider, system or portfolio changes. Annual review alone may be insufficient for an office experiencing active transactions or rapid team change.

16. Implement institutional continuity in 100 days

Days one to 20 establish sponsorship, service scope, impact criteria and a preliminary dependency inventory. The team reviews recent decisions and operating events to find informal work that job descriptions omit.

Days 21 to 40 validate the critical-capability register, authority matrix, systems, credentials, documents and providers. The office separates observed evidence from management assumptions and records every gap.

Days 41 to 60 appoint alternates, update role descriptions, create knowledge packs and begin supervised performance. Current legal and governance advice is obtained for authority, incapacity and succession arrangements where required.

Days 61 to 80 implement secure access, backups, provider confirmations, liquidity continuity, decision logs and incident communications. The office avoids granting broad emergency privileges without segregation and review.

Days 81 to 100 run scenario exercises, close priority findings, approve the dashboard and establish ongoing governance. Unresolved dependencies remain visible with owners, dates and consequences. Launch signifies an approved operating scope, not the absence of residual risk.

Table 6. One-hundred-day key-person continuity programme

Days	Workstream	Controlled deliverable	Gate
1 to 10	charter	critical services, impact criteria, sponsor and incident authority	governing sponsor approves scope
11 to 20	discovery	people, decisions, processes, systems, providers and informal dependencies	preliminary register reviewed with operators
21 to 30	authority	entity actions, mandates, limits, quorum and delegations	current evidence linked; legal gaps escalated
31 to 40	recovery design	targets, minimum service, alternates and activation thresholds	priority service design approved
41 to 50	knowledge	investment memory, process guides, contacts and document index	alternate can retrieve representative evidence
51 to 60	capability	supervised performance, training and role confirmation	alternates demonstrate priority tasks
61 to 70	technology	identity, access, vault, backup, logging and recovery	authorised recovery succeeds without primary device
71 to 80	providers	mandates, escalation, data access and relationship transfer	material providers acknowledge approved alternates
81 to 90	exercises	temporary absence, departure, cyber and succession scenarios	findings assigned and critical failures contained
91 to 100	governance	dashboard, remediation, review cycle and board approval	controlled production scope approved

Timing depends on entity complexity, provider cooperation, legal review, technology and team capacity.

17. Limitations and decision boundaries

Family structures differ materially. The validity and effect of a delegation, power, directorship, foundation role, trust role, bank mandate or succession mechanism depend on the governing instrument, jurisdiction, facts and current law. Professional advice should address each structure.

ISO 22301 provides a general business-continuity framework.[1] NIST SP 800-34 focuses on contingency planning for federal information systems and provides useful analytical methods within that scope.[2] NIST CSF 2.0 is an outcome-based cybersecurity framework.[8] These sources support design; they do not certify a family office's legal authority or operational readiness.

FINRA Rule 4370 and related observations apply within the stated member-firm perimeter.[7][9][10][11] The SEC source discussed in this paper was a 2016 proposal and should not be described as a final adviser rule.[5] ILPA Principles are industry guidance for private-fund relationships.[6]

DIFC and ADGM materials describe jurisdiction-specific family and foundation frameworks.[3][4] The actual constitution, appointments, mandates, regulatory status and family facts determine the relevant treatment.

Exercises can establish performance under the tested conditions. They cannot reproduce every event. A person, provider, cyber incident, legal dispute and family circumstance can fail simultaneously. The programme should use several scenarios and update them after changes.

The hypothetical example contains management assumptions solely for framework demonstration. It does not describe a client, expected result, provider capability or investment recommendation.

18. Conclusion

Key-person risk becomes manageable when the family office defines continuity as an institutional capability. The office identifies priority services, maps dependencies beyond the job title, separates authority from capability and access, prepares for temporary and permanent events, preserves investment memory, protects treasury, controls providers and demonstrates recovery through exercises.

The governing body should be able to answer five questions at any time. Which services must continue? Which people and providers support them? Who may act for the correct entity? Where is the current evidence? When was the alternate path last demonstrated?

A trusted adviser can remain central to the family while institutional continuity grows around that relationship. Clear authority, documented judgement, trained alternates, controlled access and current evidence let the office preserve its service, privacy and decision legitimacy through change.

The resulting operating model gives the board a measured view of critical capabilities, alternate readiness, authority gaps, recovery performance and remediation. It supports continuity through illness, departure, conflict, compromise and succession while preserving the governance required for family capital.

References

[1] International Organization for Standardization, ISO 22301:2019, Security and resilience, Business continuity management systems, Requirements, published October 2019, accessed 13 August 2026. https://www.iso.org/standard/75106.html

[2] National Institute of Standards and Technology, SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, updated November 2010, accessed 13 August 2026. https://doi.org/10.6028/NIST.SP.800-34r1

[3] Dubai International Financial Centre, Family Arrangements Regulations 2023 and enactment announcement, accessed 13 August 2026. https://www.difc.com/whats-on/news/difc-announces-enactment-new-difc-family-arrangements-regulations-1

[4] Abu Dhabi Global Market, Foundations regime and setting-up guidance, accessed 13 August 2026. https://www.adgm.com/faqs/setting-up

[5] U.S. Securities and Exchange Commission, Proposed Rule, Adviser Business Continuity and Transition Plans, Release No. IA-4439, 28 June 2016. https://www.sec.gov/files/rules/proposed/2016/ia-4439.pdf

[6] Institutional Limited Partners Association, ILPA Principles 3.0, including Key Person guidance, June 2019. https://ilpa.org/wp-content/uploads/2019/06/ILPA-Principles-3.0_2019.pdf

[7] Financial Industry Regulatory Authority, Rule 4370, Business Continuity Plans and Emergency Contact Information, accessed 13 August 2026. https://www.finra.org/rules-guidance/rulebooks/finra-rules/4370

[8] National Institute of Standards and Technology, The NIST Cybersecurity Framework 2.0, 26 February 2024. https://doi.org/10.6028/NIST.CSWP.29

[9] Financial Industry Regulatory Authority, 2019 Report on Examination Findings and Observations, Business Continuity Plans, 16 October 2019. https://www.finra.org/rules-guidance/guidance/reports/2019-report-exam-findings-and-observations/business-continuity-planning

[10] Financial Industry Regulatory Authority, Business Continuity Planning FAQ, accessed 13 August 2026. https://www.finra.org/rules-guidance/key-topics/business-continuity-planning/faq

[11] Financial Industry Regulatory Authority, Regulatory Notice 13-25, FINRA, the SEC and CFTC Issue Joint Advisory on Business Continuity Planning, 16 August 2013. https://www.finra.org/rules-guidance/notices/13-25

About the Author

Chennakeshav Adya is an independent researcher and Managing Partner of Matchpoint Partners. His research focuses on investment strategy, capital formation, transaction execution, governance and operating-model design across the Gulf and international markets.