The 72-Hour Family Office

A crisis operating plan for authority, liquidity, people, data and custody when normal arrangements fail

Authored by Chennakeshav Adya
Independent Researcher
August 2026

ABSTRACT

Background. A family office can remain economically solvent while losing the authority, access, people, data or provider capacity required to meet its obligations.

Objective. This paper develops a 72-hour crisis operating plan for delegated authority, liquidity access, staff safety, data continuity and alternative custody.

Approach. The framework adapts current official UAE, UK and international operational-resilience, business-continuity, cyber, custody and financial-crime sources to a proportionate family-office command model.

Findings. Resilience depends on service-level tolerances, function-specific succession, dual control, verified liquidity, reconstructed custody data, clean communication and tested recovery routes.

Implications. The office should activate against service impairment, operate through six control windows, preserve evidence and move from temporary command to governed recovery at hour seventy-two.

Practical priorities

1. Approve function-specific deputies, limits and dual-control requirements before activation.
2. Maintain a verified 72-hour liquidity ladder, minimum custody data set and clean recovery pack.
3. Exercise people safety, payment, identity, data and provider failure as one integrated operating system.

JEL Classification: G23, G32, G21, G28, M10, M15

Keywords: family office, operational resilience, crisis management, delegated authority, liquidity access, custody continuity, cyber recovery, staff safety, business continuity

Research paper only. This document provides general information and is not legal, tax, accounting, investment, regulatory, cyber, employment, insurance or security advice. Every worked scenario, threshold and value is hypothetical and simplified. Current fact-specific professional advice and official guidance are essential.

1. INTRODUCTION

A family office is most vulnerable when an ordinary operating problem becomes a decision problem. A bank portal fails while a payroll file is due. The principal is travelling when a payment requires approval. A cyber incident makes the document repository unavailable. Staff cannot reach the office. A custodian restricts an access channel while markets are moving. Each event can be manageable on its own. The combined event can expose a family to missed obligations, unsafe work, uncontrolled instructions and avoidable loss.

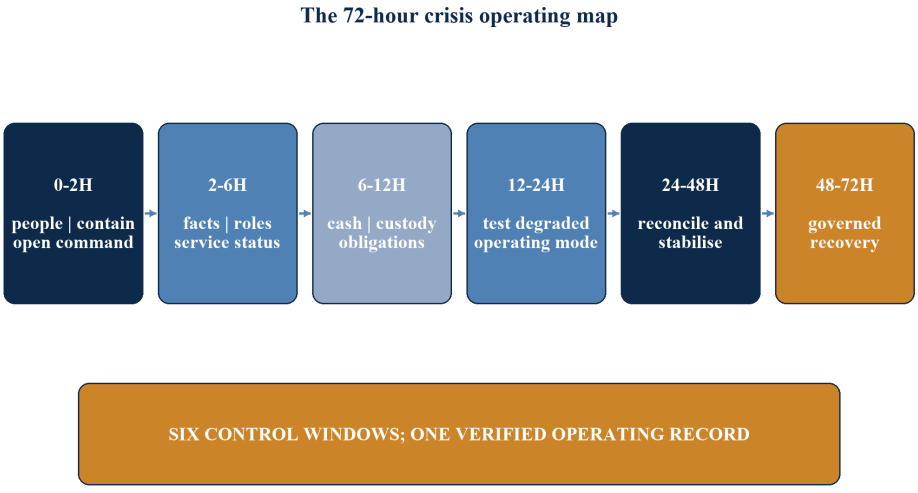
This paper develops a 72-hour crisis operating plan for a family office. The period is divided into six control windows: the first two hours, hours two to six, hours six to twelve, hours twelve to twenty-four, day two and day three. Each window has a defined purpose. The first window protects people, accounts and evidence. The second establishes command and a reliable fact base. The third secures liquidity and critical service continuity. The fourth validates alternative routes. Day two stabilises the operating model. Day three prepares a controlled transition to a longer recovery plan.

The framework begins with services rather than assets. A portfolio can remain economically sound while the office loses access to payment instructions, custody records, delegated authorities, identity documents or communication channels. Operational resilience therefore asks which outcomes must continue, how long disruption can be tolerated, which people and systems support each outcome, and which safe degraded mode can operate while the primary route is unavailable [1-11].

The plan covers five linked control domains. Delegated authority determines who may decide and who may execute when the usual approver is unavailable. Liquidity access matches cash sources to obligations and payment rails. Staff safety provides a verified welfare and location process. Data continuity protects critical records and establishes clean recovery routes. Alternative custody separates asset ownership, safekeeping, access, trading and settlement so that a failure in one layer is not misdiagnosed as a loss of the asset itself [3-9,12-19].

The analysis is general research. It does not determine any family's legal, tax, regulatory, investment, cyber, employment, insurance or security requirements. Every scenario, threshold and value is hypothetical and simplified. The relevant governing documents, provider terms, official guidance and fact-specific professional advice remain decisive.

Figure 1. The 72-hour crisis operating map.



2. THE 72-HOUR OPERATING DOCTRINE

2.1 Preserve life, authority, access and evidence

The operating doctrine has four priorities in order. First, confirm the safety of family members, staff and essential contractors. Second, prevent unauthorised or irreversible actions. Third, preserve access to essential liquidity, custody information and communication. Fourth, record the facts, decisions and evidence required for recovery. A plan that starts with portfolio views before these controls are stable risks making financially consequential decisions on an unreliable operating base.

NCEMA's business-continuity framework emphasises essential functions, incident management, crisis roles, recovery planning and exercises. CBUAE standards require regulated institutions to identify critical operations, roles, recovery objectives, communication plans and disruption scenarios. Basel and FCA resilience frameworks similarly focus on important services, impact tolerances, dependencies, testing and learning [1-10]. A family office can adapt those disciplines proportionately without presenting itself as a regulated bank.

The office should publish a one-page activation card. It states the trigger, crisis level, command lead, deputy, staff-safety lead, treasury lead, technology lead, legal and compliance contact, approved communication channels and time of the next update. It also states what is temporarily prohibited: new beneficiaries, new custody instructions, changes to bank mandates, payments outside the approved queue, use of unverified personal messaging and destruction or alteration of records.

2.2 The plan operates in windows

The first 72 hours are short enough to require discipline and long enough to expose weak dependencies. The operating windows should be measured from activation, not from the time an event first occurred. The activation record therefore carries two timestamps: the earliest known event time and the formal activation time.

Window	Primary purpose	Required output	Decision gate
0 to 2 hours	protect people and contain authority	verified roll call, frozen change queue, incident owner	has immediate harm been contained?
2 to 6 hours	establish command and facts	situation report, service status, decision log	is the fact base reliable enough to act?
6 to 12 hours	secure obligations and access	liquidity ladder, payment queue, custody status	can critical obligations be met safely?
12 to 24 hours	validate alternative routes	tested degraded modes and provider escalations	can day-two operations proceed within tolerance?
24 to 48 hours	stabilise and reconcile	reconciled balances, access review, staff plan	is the crisis operating model controlled?
48 to 72 hours	transition to recovery	board or family report, remediation owner, recovery plan	can command move from response to recovery?

2.3 One source of operational truth

The crisis team should maintain one controlled situation report. It records known facts, open questions, assumptions used for temporary decisions, service status, obligations due, staff welfare, provider incidents, security actions and the next review. Each entry identifies its source and time. Rumour, media reporting and unverified messages can be logged as signals, but they do not become operating facts until corroborated.

3. ACTIVATION TRIGGERS AND CRISIS LEVELS

3.1 Activation is a control decision

A crisis plan should activate before the office is visibly failing. Useful triggers are defined around service interruption and control impairment. Examples include loss of access to a payment or custody platform; unavailability of both a principal and an authorised alternate; a cyber event affecting identity, email or document systems; inability to contact a material portion of staff; closure or inaccessibility of a principal workplace; a provider notice that affects transaction, settlement or data availability; and a credible threat to people or premises.

The trigger register should distinguish observation, escalation and activation. An observation is recorded and monitored. An escalation assigns an owner and review time. Activation starts the crisis governance structure and its temporary controls. This distinction prevents every service issue from becoming a full crisis while still allowing early containment.

3.2 A four-level ladder

The following ladder is illustrative. Each office should set thresholds that reflect its structure, jurisdictions, provider contracts and obligations.

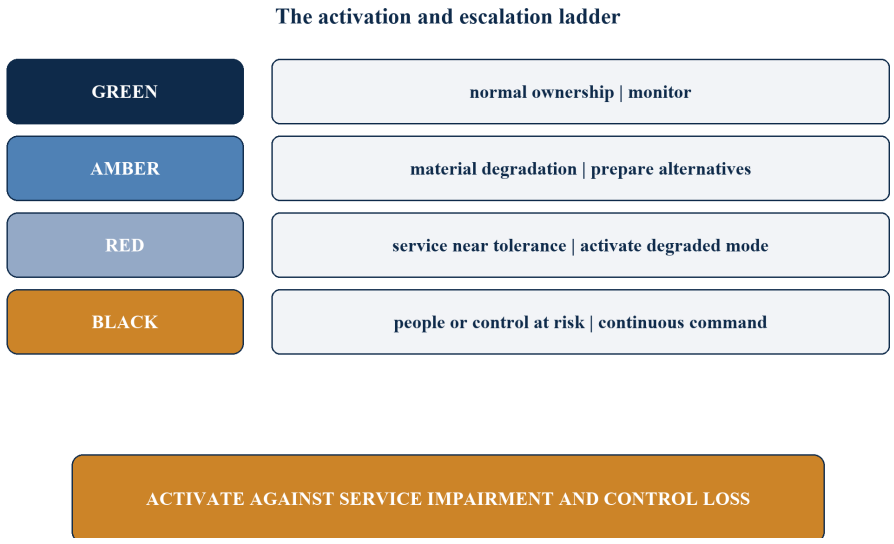
Level	Operating condition	Authority	Cadence	Example response
Green	normal operations with isolated issue	business owner	daily	service desk and normal approvals
Amber	material degradation or credible threat	incident lead	every four hours	protect access, prepare alternatives
Red	critical service outside or near tolerance	crisis lead and deputies	every one to two hours	activate degraded mode and executive reporting
Black	people safety event or loss of control over assets, identity or instructions	designated family authority with legal and security support	continuous command	preserve life, contain access, notify relevant parties

The office should define objective indicators where possible: number of unavailable signatories; value of payments due within a stated period; percentage of staff confirmed safe; age of last verified backup; number of compromised privileged accounts; number of critical providers unavailable; and time remaining before a contractual or legal deadline.

3.3 Deactivation requires evidence

The crisis lead should not deactivate merely because a platform appears to work. Deactivation should require confirmed people safety, stable access, reconciled balances and transactions, restored logging, reviewed privileged access, cleared payment exceptions, provider confirmation where relevant and named remediation owners. A lower crisis level can remain in place while long-term recovery continues.

Figure 2. The activation and escalation ladder.



4. DELEGATED AUTHORITY AND SUCCESSION

4.1 Authority must be both legal and operational

A job title does not automatically create the power to bind a company, trust, foundation, partnership or account. The office must map authority to the relevant legal person, governing document, resolution, bank mandate, investment-management agreement, power of attorney and provider instruction. A crisis matrix summarises those sources; it does not replace them.

The matrix should separate decision authority from execution authority. One person may approve a payment while another inputs it. A custodian may recognise a specific signatory set that differs from the company's internal delegation. A trustee or foundation council may have duties that cannot be transferred through an informal family instruction. Counsel should validate the legal architecture before an event.

4.2 Succession by function

Authority succession should be defined for each critical function rather than as one broad transfer of control. Treasury, payroll, custody, investment decisions, cyber containment, staff safety, external statements, legal notices and regulatory notifications may require different deputies and evidence.

Function	Primary decision-maker	Deputy	Executor	Independent check	Crisis limit
staff safety	operations lead	HR or office manager	local coordinators	crisis lead	welfare actions only
payroll and essential bills	treasury lead	finance director	payment operator	second approver	approved payee list and cap
custody access	investment COO	authorised deputy	operations analyst	external administrator or second officer	access and reconciliation only
investment protection	CIO	deputy CIO	approved dealer	risk officer	pre-approved hedges or exposure reduction
cyber containment	technology lead	external incident responder	system administrators	legal and privacy adviser	isolate, preserve, recover
public communication	crisis lead	designated family representative	communications adviser	legal review	approved factual statements

4.3 Dual control remains active

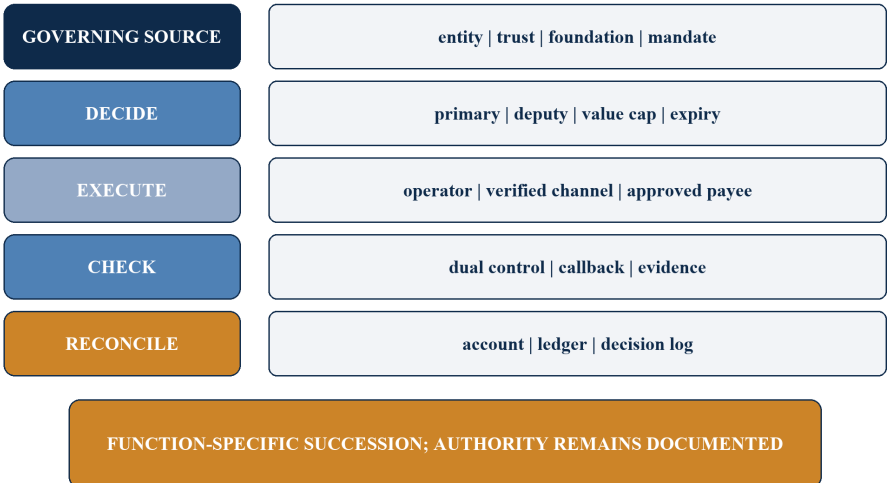
Crisis speed does not justify abandoning segregation of duties. CBUAE operational-risk standards identify clear authorities, segregation, dual control, safeguards over assets and records, and transaction reconciliation as core controls [3,4]. A family office should retain a second-person check for beneficiary creation, payment release, custody transfer, privileged-access reset and external statements. Where an emergency mandate permits one-person action, the action should be capped, logged and subject to rapid retrospective review.

4.4 Principal unavailability

The principal-unavailability protocol should define evidence of attempted contact, the elapsed time before succession, which decisions can proceed, which decisions must wait, and when counsel or a fiduciary body is involved. It should avoid medical speculation and preserve confidentiality. The protocol also needs a route for restoring ordinary authority when the principal returns.

Figure 3. The delegated-authority architecture.

The delegated-authority architecture



5. IMPORTANT SERVICES AND IMPACT TOLERANCES

5.1 Start with outcomes

An asset register describes what the family owns. A service register describes what the office must continue to do. Important services can include confirming people safety, maintaining access to cash, paying staff and critical suppliers, safeguarding assets, meeting collateral or capital calls, receiving bank and custodian information, managing cyber incidents, preserving legal deadlines and communicating with the family.

FCA guidance distinguishes impact tolerance from recovery time. An impact tolerance defines the maximum tolerable disruption to a service; a recovery-time objective defines the target time to restore the supporting system. Recovery may need to occur well before the tolerance is reached because backlogs and reconciliations remain after the system returns [8-10].

5.2 Time and non-time limits

Every important service should have a time limit and at least one non-time limit. For payroll, the time measure may be the latest safe release time, while non-time measures include number of unpaid employees and maximum unresolved value. For custody reporting, the time measure may be the age of the last verified position file, while non-time measures include percentage of assets reconciled and number of unresolved corporate actions.

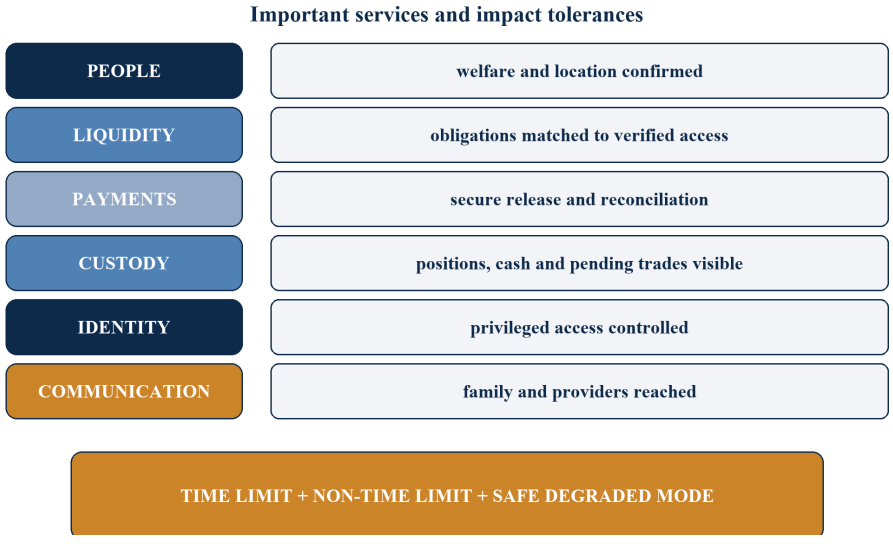
Important service	Illustrative time tolerance	Non-time measure	Safe degraded mode
staff welfare confirmation	2 hours	100% of staff assigned a status or search owner	phone tree through local coordinators
critical cash visibility	4 hours	all operating accounts and next 72-hour obligations covered	last verified statements plus callback confirmation
payroll and essential payments	12 hours	zero critical beneficiary changes outside dual control	pre-approved offline payment pack
custody position visibility	12 hours	at least 95% of liquid assets value reconciled	prior-day file plus custodian confirmation
privileged-access control	1 hour	all suspected accounts disabled or monitored	isolated clean admin account
family decision communication	4 hours	all designated decision-makers reached or formally deputised	encrypted secondary channel

These values are illustrative. The office should calibrate them to obligations, time zones, staffing and provider capabilities, then obtain approval from the appropriate governing body.

5.3 Dependency mapping

Each service should map people, premises, technology, data, providers, legal entities and financial rails. The map should identify common dependencies. Two banks may depend on the same mobile network. Two custodians may use the same authentication device or email domain. A cloud backup within the same identity tenant may fail with the primary environment. The plan should test independence rather than relying on the number of logos in the provider list.

Figure 4. Important services and impact tolerances.



6. CRISIS COMMAND AND COMMUNICATIONS

6.1 The command cell

The command cell should be small enough to decide and broad enough to see the system. Core roles are crisis lead, deputy, operations recorder, staff-safety lead, treasury lead, technology and cyber lead, investment and custody lead, and legal or compliance adviser. Specialist providers join only for their workstream. The recorder maintains the action log, decision log and next-update time.

A disciplined meeting can last fifteen minutes. It asks: what changed; which people are unsafe or unconfirmed; which service is nearest its tolerance; what decision is required; what evidence supports it; who owns the action; and when will it be checked. The output is a versioned situation report, not a loose chat transcript.

6.2 Communication hierarchy

The office should pre-approve a communication hierarchy. Primary corporate email and collaboration tools are convenient during normal operations. Secondary encrypted channels, verified phone numbers and an offline contact list are needed when identity or network systems may be compromised. Instructions involving funds or credentials should never rely on a newly introduced channel or number without independent verification.

The contact register should include family decision-makers, staff, trustees or foundation officers, banks, custodians, brokers, administrators, technology responders, cyber insurers, legal counsel, tax advisers, security providers, critical vendors and emergency contacts. Each record requires an owner, last verification date and an out-of-band verification method.

6.3 External statements

External communication should be factual, limited and approved. The holding statement can confirm that the office is managing an operational incident, protecting stakeholders and working with relevant providers. It should avoid attributing cause, naming affected parties, estimating loss or announcing restoration before evidence is available. Legal, privacy, employment and regulatory advice may be required before notification.

7. STAFF SAFETY AND WELFARE

7.1 A verified roll call

Staff safety begins with a controlled roll call, not with general broadcast messages. Every employee and essential contractor receives one of five statuses: safe and working; safe and unavailable; assistance required; unconfirmed with an assigned contact owner; or travelling with a separate itinerary status. The register should avoid unnecessary medical detail and restrict access to those coordinating the response.

NCEMA guidance treats human resources, work environment, transport, information, technology, financial resources and suppliers as business-continuity dependencies. Its guidance also emphasises leadership, remote work, staff distribution and flexible procedures during disruption [1,2,32-34]. These principles support a staff plan that addresses physical safety before productivity.

7.2 Local coordinators and safe work

The office should nominate local coordinators for each material location. Their role is to confirm welfare, relay verified instructions and escalate assistance needs. They do not interpret security intelligence or direct staff into uncertain conditions. Travel, evacuation, shelter and office-access decisions should use current official advice and qualified security support.

Remote work should be activated deliberately. Staff need a clean device, approved identity method, secure communications, access limited to their role and instructions for handling confidential family data outside the normal workplace. A crisis may justify narrower access rather than wider access.

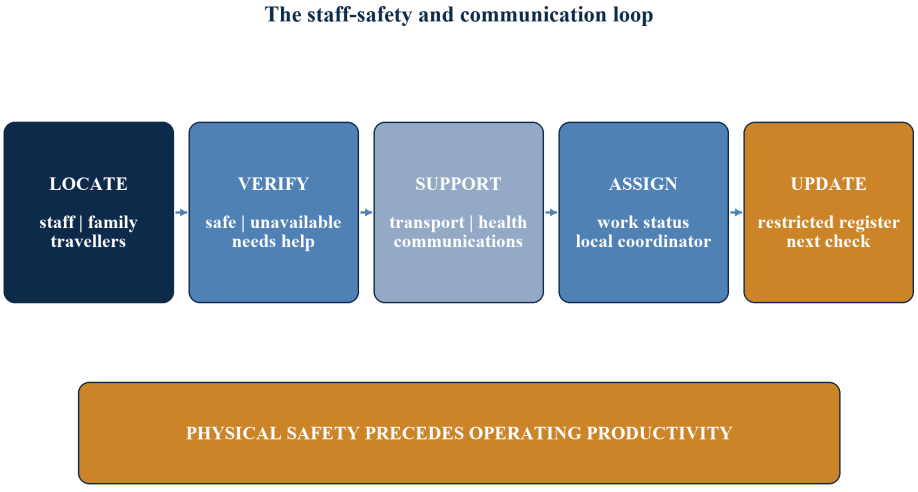
7.3 Payroll, expenses and practical support

The crisis plan should identify the payroll cutoff, bank route, approved backup operator and exception process. Emergency expenses may be necessary for transport, accommodation, communications, healthcare or replacement equipment. The plan should define caps, evidence requirements and a reimbursement route that can operate even when the main expense platform is unavailable.

7.4 Family and staff separation

Family welfare and employee welfare are linked but different workstreams. The family may have private security, medical, education and travel arrangements that should not be exposed to the broader office. The staff-safety lead should receive only the information needed to coordinate work and welfare. The family representative retains control of private family information.

Figure 5. The staff-safety and communication loop.



8. LIQUIDITY ACCESS AND THE 72-HOUR LADDER

8.1 Liquidity is access plus authority

A cash balance is not operational liquidity when the office cannot authenticate, approve, transfer or reconcile it. The liquidity register should therefore record legal owner, bank, currency, balance source, value date, available amount, lien or restriction, payment rail, cut-off, signatory set, authentication method, daily limit, beneficiary controls and escalation contact.

The 72-hour ladder begins with obligations. The office lists payroll, healthcare, security, accommodation, utilities, insurance, debt service, collateral, tax, legal deadlines and contractually critical suppliers. Each obligation is assigned a latest safe payment time, amount, currency, legal payer, approved payee details and consequence of delay.

8.2 Four liquidity tiers

Tier	Horizon	Purpose	Evidence
one	same day	staff safety, healthcare, security, communications	verified immediately available balance and working rail
two	24 hours	payroll, essential suppliers, margin or collateral	confirmed account access, mandate and cutoff
three	72 hours	operating runway and foreseeable investment obligations	reconciled near-cash and tested transfer route
four	beyond 72 hours	recovery funding and portfolio actions	approved liquidation, borrowing or capital plan

The office should distinguish committed liquidity from potential liquidity. An untested overdraft, expected asset sale, unsettled redemption or informal family contribution is not the same as a confirmed balance or committed facility. Potential sources can appear in the recovery plan with prerequisites and decision rights.

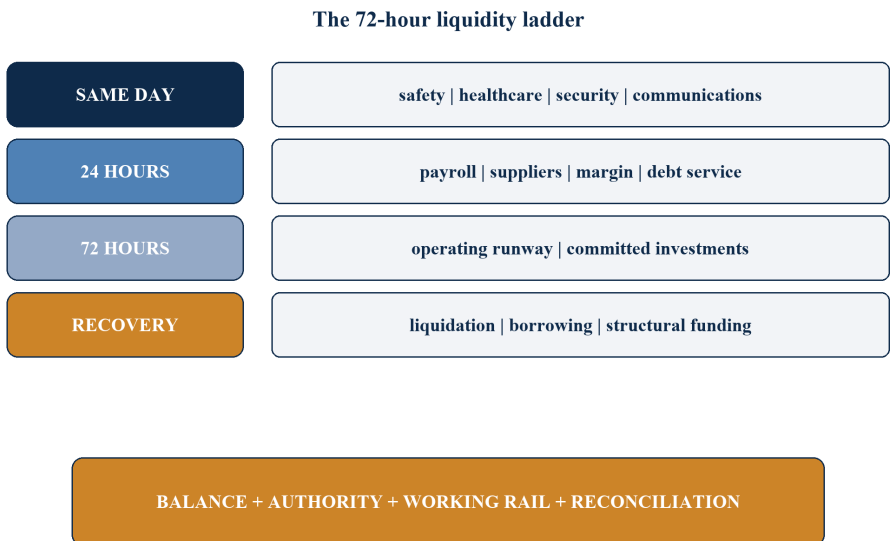
8.3 Currency and rail diversity

Multiple currencies and accounts can improve flexibility while increasing control complexity. The ladder should identify which obligations require AED, GBP, USD or another currency, which account can legally pay them, expected conversion steps, time-zone cutoffs and settlement risk. A backup account should have current mandates, verified beneficiaries and routine controlled use before a crisis. Dormant or untested arrangements create false comfort.

8.4 Daily treasury packet

During activation, treasury produces a packet at each command cycle: opening balances from verified sources; confirmed available liquidity; obligations due within 6, 24 and 72 hours; payments released; payments pending approval; rejected or uncertain transactions; provider incidents; and the next cutoffs. A second person reconciles the packet to bank or custodian evidence.

Figure 6. The 72-hour liquidity ladder.



9. PAYMENT SECURITY AND RECONCILIATION

9.1 Freeze change before moving money

Social engineering exploits urgency, authority and channel change. The crisis plan should freeze new beneficiaries, changes to settlement instructions, signatory changes and payment-limit changes unless the crisis lead and an independent verifier approve a documented exception. Callback verification uses a previously validated number, not contact information supplied in the request.

9.2 Payment queue discipline

Every payment receives an identifier, legal payer, beneficiary, purpose, source invoice or obligation, amount, currency, deadline, approval state, input operator, release approver, callback evidence and reconciliation state. The queue separates prepared, approved, released, confirmed, rejected and reversed items. Screenshots can support evidence but do not replace bank statements or formal transaction records.

9.3 Manual and alternative routes

An offline payment pack can contain verified bank contacts, mandates, account identifiers, approved payees and specimen instruction formats. Its use depends on provider acceptance and current authority. The office should test the process with the provider during normal operations and store the pack securely with controlled access and version dates.

9.4 Reconciliation closes the control loop

Restored access can reveal duplicated, delayed or partially executed instructions. Treasury should reconcile every crisis-period payment to the bank record, accounting ledger, obligation and approval log. Unmatched items are escalated before normal processing resumes.

10. ALTERNATIVE CUSTODY AND ASSET ACCESS

10.1 Separate the layers

Custody continuity has at least six layers: legal ownership; account title and segregation; safekeeping; information access; trading authority; and cash or securities settlement. A portal outage may affect information and instruction while legal ownership and safekeeping remain unchanged. A settlement disruption may delay cash without changing the investment decision. The office should diagnose the affected layer before acting.

IOSCO custody standards and securities regulation emphasise segregation, books and records, reconciliation and qualified custodians as investor-protection mechanisms [18,19,25-27]. The family office should obtain legal and regulatory advice for its own structure, especially where assets are held through funds, nominees, trusts, foundations, special-purpose vehicles or digital-asset arrangements.

10.2 The custody continuity register

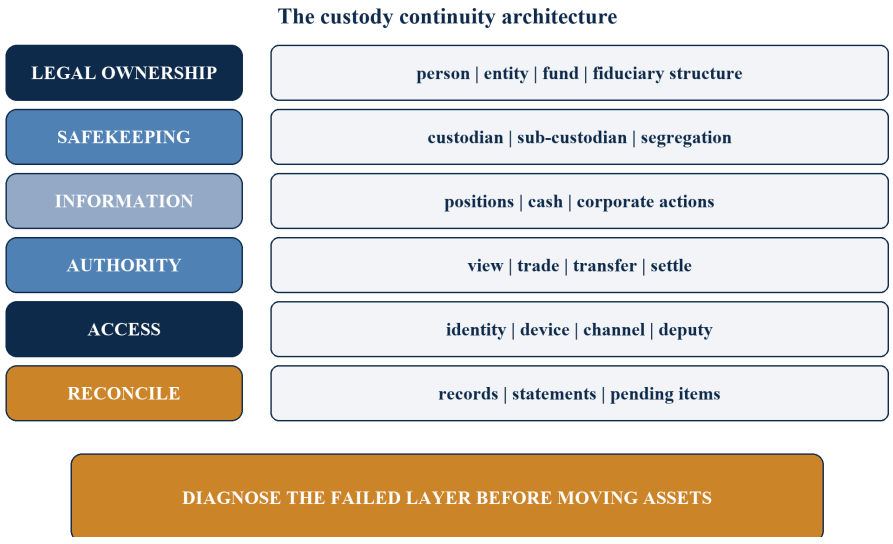
Field	Control question
legal owner	which person or entity owns the asset or account?
custodian and sub-custodian	who holds the asset and through which chain?
account title	how is segregation or client designation recorded?
authorised actors	who may view, trade, transfer and settle?
authentication	which devices, tokens and channels are required?
alternative access	what verified offline or secondary route exists?
settlement cash	where do proceeds and obligations move?
last reconciliation	when were positions, cash and transactions independently checked?

10.3 Diversification requires tested independence

Using more than one custodian can reduce some concentrations and create others. The office should assess legal entity, geography, sub-custody chain, settlement bank, authentication, market infrastructure, administrator, data vendor, telecoms and internal operator. Two accounts dependent on one employee's phone and one email domain do not provide independent access.

The minimum data set should reconstruct prior-day positions, cash, pending trades, collateral, corporate actions, private-market commitments, contacts and account authorities without the primary portal. It should be encrypted, controlled and refreshed on a defined schedule. Asset transfer remains a governed recovery option requiring legal review, authority, a verified destination and complete reconciliation.

Figure 7. The custody continuity architecture.



11. DATA, CYBER AND IDENTITY CONTINUITY

11.1 Critical information assets

The office should identify the information needed to operate for 72 hours: contact registers; governing documents and mandates; bank and custody account schedules; payment and obligation queues; current positions; private-market commitments; insurance and security contacts; identity and travel documents where lawfully retained; provider contracts; incident plans; and clean system-recovery instructions.

NIST, CISA, CBUAE and DFSA sources emphasise preparation, incident response, recovery, tested backups, identity controls, communications and third-party dependencies [5,11,20-24,28-31]. A family office should apply those practices proportionately and obtain specialist incident-response advice when an intrusion is suspected.

11.2 Contain identity risk

If email, identity or a privileged account may be compromised, the technology lead should preserve evidence and follow the approved incident plan. Potential actions include isolating affected devices, disabling or monitoring accounts, revoking sessions, protecting authentication factors, restricting privileged roles and establishing a clean administrative route. Technical actions should be directed by qualified responders so that evidence and recovery options are not damaged.

The crisis plan should identify break-glass accounts, their storage, permitted use, independent oversight and post-use review. A break-glass account should not depend on the same compromised identity chain as the primary account.

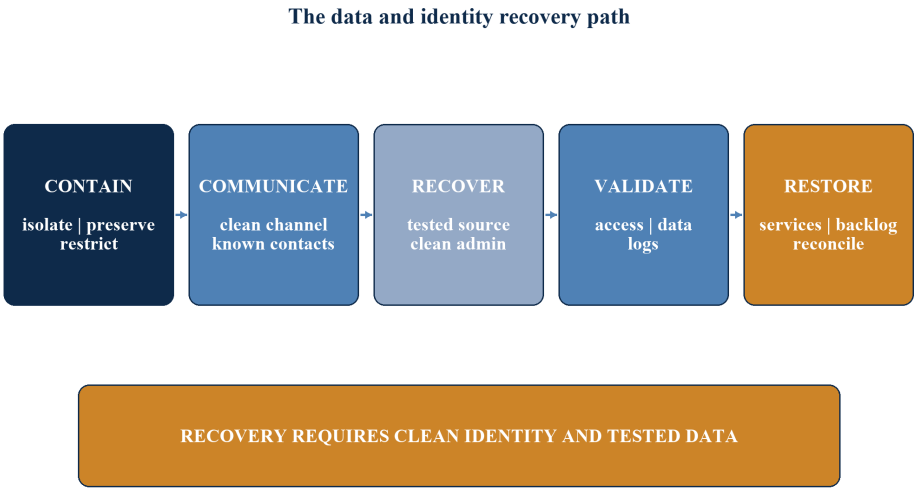
11.3 Backups and recovery

Critical data needs tested recovery, not merely a backup label. CISA recommends offline encrypted backups and regular restoration testing for critical data. NIST contingency guidance covers alternate equipment, manual processes, alternate locations and recovery priorities [20-23]. The office should document recovery-point and recovery-time objectives, backup immutability, encryption, administrator separation, test results and the clean environment used for restoration.

11.4 Data minimisation during crisis

Crisis teams often over-share information in order to move quickly. The command cell should limit each participant to the data required for the action, use approved secure channels, avoid public links, and keep a distribution record for sensitive packs. Privacy and confidentiality obligations continue during disruption.

Figure 8. The data and identity recovery path.



12. THIRD-PARTY AND CONCENTRATION RISK

12.1 The extended operating model

A family office may rely on banks, custodians, brokers, fund administrators, trustees, company-service providers, accountants, payroll vendors, cloud platforms, managed technology, security, travel support and external advisers. The office remains responsible for its decisions even when an important activity is outsourced.

The provider register should record service, legal entity, jurisdiction, contract owner, service level, incident channel, escalation contacts, data handled, subcontractors where disclosed, exit assistance, alternative provider, last test and evidence of assurance. FSB and Basel third-party guidance emphasise criticality, dependency mapping, concentration, contractual arrangements, monitoring and exit planning [6,7].

12.2 Provider triage

During the first six hours, providers are placed into four groups: unaffected and verified; affected with a known workaround; affected without a tested workaround; and status unknown. The command cell focuses attention on providers supporting services nearest their impact tolerance.

Provider status should come from formal service notices, known contacts or verified technical evidence. A social-media post can prompt a check; it should not automatically drive a payment, transfer or access change.

12.3 Exit and substitution

An alternative provider requires more than a name. The office should understand onboarding time, data portability, legal authority, account setup, compatible assets, payment routes, privacy restrictions, fees and reconciliation. Some substitutions can occur within hours, such as a secondary communication channel. Others may take weeks or months, such as changing a custodian or administrator. The 72-hour plan should identify the realistic degraded mode for each horizon.

13. COMPLIANCE, SANCTIONS AND FRAUD CONTROL

13.1 Controls remain part of continuity

A crisis can change counterparties, routes, jurisdictions and transaction purposes. Banks and other institutions continue to apply customer due diligence, sanctions, fraud and transaction-monitoring controls. The office should preserve beneficial-ownership, source-of-wealth, source-of-funds and transaction-purpose evidence so that urgent activity can be explained accurately [14-17,29,30].

13.2 Exception does not mean exemption

The crisis lead may approve an operational exception within the office's authority. The exception does not override law, provider requirements, fiduciary duties or account mandates. Every exception should identify the rule being varied, reason, scope, value cap, expiry, approver, independent check and remediation.

13.3 Fraud indicators under pressure

Escalation indicators include a new beneficiary; changed bank details; an instruction to bypass the normal channel; a request for secrecy; unusual urgency; a new device or number; refusal of callback; inconsistent invoice or contract data; pressure from a senior person's purported account; or an unexpected jurisdiction. The response is verification through known channels and documented approval, not informal debate in the same potentially compromised thread.

13.4 Notifications

Legal, regulatory, privacy, insurance, employment and contractual notifications depend on facts and jurisdiction. The plan should maintain a decision register with responsible adviser, trigger, deadline, recipient, approved content and evidence of submission. It should avoid generic promises about notification timing.

14. FAMILY GOVERNANCE AND CONFIDENTIALITY

14.1 The family decision perimeter

The office should identify which family body or authorised individual receives crisis reports and which decisions require family approval. Investment, liquidity, public communication, staff support and structural transfer decisions may sit in different governance channels. The plan should respect governing documents and avoid exposing private family information beyond need.

14.2 A family crisis briefing

The briefing should be short: current people-safety status; critical services outside or near tolerance; confirmed cash and custody access; decisions required; prohibited actions; next update; and unresolved facts. Technical detail belongs in workstream logs. The family body should be able to decide without reading every operational message.

14.3 Confidentiality rings

Information can be organised into three rings. Ring one covers sensitive family, identity, health and security information. Ring two covers financial, transaction and provider information used by the command cell. Ring three covers operational instructions needed by staff. Each ring has named recipients, secure channel, retention and onward-sharing rules.

14.4 Records and privilege

Legal advice and incident-response materials may require careful handling. Counsel should advise on privilege, preservation, regulatory access and cross-border data transfer. The office should not label ordinary operational records as privileged without legal basis, and it should not delete records in response to an incident.

15. THE SIX CONTROL WINDOWS

15.1 Hours zero to two: protect and contain

The crisis lead activates the plan, opens the decision log and confirms deputies. The staff-safety lead starts the roll call. Technology protects identities and critical evidence. Treasury freezes beneficiary and mandate changes. The investment and custody lead preserves the latest verified position and cash files. The command cell identifies the next hard deadline and publishes the first verified update.

15.2 Hours two to six: establish the fact base

The team classifies important services, provider status and staff welfare. Treasury produces the first obligations and liquidity ladder. Technology identifies affected systems and clean communication routes. Legal and compliance identify immediate notification or evidence-preservation questions. The family receives a concise briefing and approves any temporary authority required within governing documents.

15.3 Hours six to twelve: secure obligations

The office confirms cash access, payment rails, payroll, healthcare, security and critical suppliers. It reconciles custody positions and pending transactions using the best verified source available. Provider escalations are active. Alternative channels are tested with low-risk actions where appropriate. High-risk structural changes remain subject to legal and independent review.

15.4 Hours twelve to twenty-four: prove the degraded mode

The command cell tests whether important services can operate within tolerance for the next day. It validates the offline contact list, clean administrator access, alternative communication, payment instruction process and minimum custody data set. It confirms staff coverage across time zones and assigns rest periods so that fatigue does not become a control failure.

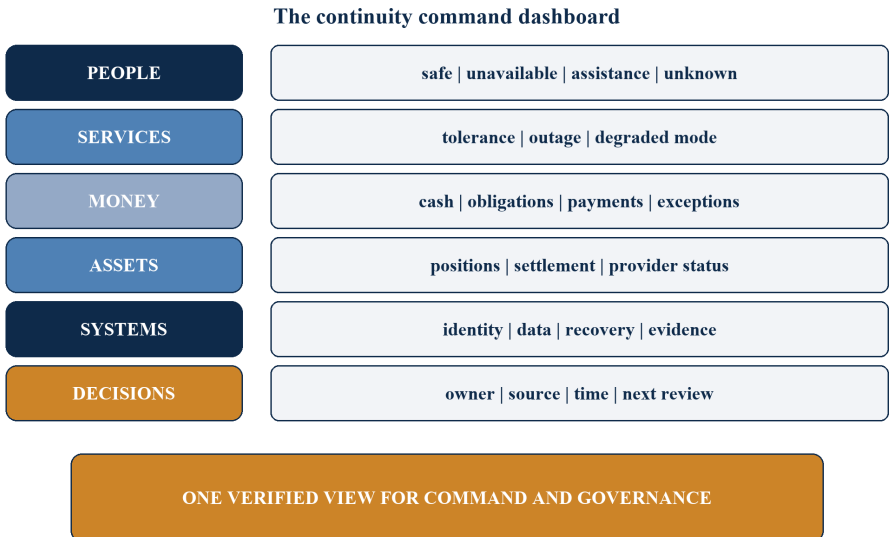
15.5 Hours twenty-four to forty-eight: stabilise

Day two focuses on reconciliation. Treasury reconciles balances and payments. Technology reviews access, logs and recovery evidence. Custody operations reconcile positions, cash, pending transactions and corporate actions. Staff plans address sustained remote work or alternate premises. Providers supply written incident and recovery information where available.

15.6 Hours forty-eight to seventy-two: transition

Day three determines whether the office can return to normal operations, remain in a controlled degraded mode or enter a longer recovery programme. The governing body receives the dashboard, decisions, unresolved exposures, financial effects, legal and compliance status, provider actions and remediation priorities. Temporary authorities expire or are renewed through the correct process.

Figure 9. The continuity command dashboard.



16. HYPOTHETICAL FAMILY-OFFICE PATHS

16.1 Path A: principal unavailable during a payment disruption

Assume the principal is travelling and cannot be contacted for eight hours. A bank authentication service is intermittently unavailable and payroll is due within twelve hours. The governing documents and bank mandate recognise a deputy for payroll and essential operating payments up to a stated cap. The finance operator prepares the approved payroll file, the deputy approves it through the verified alternative process, and a second officer reconciles the bank confirmation. No new beneficiary or payment limit is introduced.

The lesson concerns authority design. A broad informal instruction to keep the office running would be weaker than a function-specific mandate, approved beneficiary set, value cap and independent reconciliation.

16.2 Path B: ransomware affects email and document access

Assume the office detects suspicious encryption and loss of access to corporate email. Technology isolates affected devices, preserves evidence and activates qualified incident responders. The command cell moves to the pre-approved secondary communication channel. Treasury freezes changes and verifies urgent instructions using the offline contact register. The clean recovery store supplies governing documents, mandates, account schedules and prior-day positions.

The office does not assume that every backup is clean or that every account has been compromised. Responders determine scope, restore from tested sources and document decisions. Payment and custody actions resume only through verified identities and reconciled data.

16.3 Path C: staff and provider access fail together

Assume severe transport disruption prevents staff from reaching the main office while a custodian portal is unavailable. Local coordinators confirm staff safety and remote-work capability. The custody lead obtains a provider status through a known contact and uses the last verified position file to identify pending settlements and corporate actions. Treasury covers essential obligations through unaffected accounts. Investment decisions are limited to the authority and data quality available.

The scenario tests common dependencies. An alternative office without access credentials, clean devices or current data does not create continuity. A second custodian without independent authentication or trained operators may not create effective access.

16.4 Path D: a fraudulent instruction enters the crisis queue

Assume an email appearing to come from a family member requests an urgent transfer to a new account for security reasons. The request uses a new mobile number and asks staff to keep the transfer confidential. The payment freeze blocks beneficiary creation. The treasury lead uses the validated contact register and confirms that the instruction is false. The incident is preserved and escalated to the cyber and legal workstreams.

This path demonstrates why urgency should strengthen verification. The office protects the family by maintaining controls that do not depend on the authority asserted inside the request.

17. A HYPOTHETICAL 72-HOUR STRESS TEST

17.1 Model facts

Consider a simplified office supporting four family branches, twelve employees, three banks, two custodians, six private-market funds and operating entities in two jurisdictions. The office has payroll and critical supplier obligations of USD 420,000 equivalent within 72 hours. Verified same-day cash is USD 1.8 million equivalent across two institutions. A third account contains USD 3.0 million but its signatory mandate has not been tested for nine months. All values are hypothetical.

At activation, the principal is unavailable, six staff are remote, corporate email is suspected to be compromised, one custodian portal is unavailable and a capital-call notice is due for verification. The office has a deputy treasury mandate, an offline contact register, a clean recovery store and a secondary communication channel.

17.2 Service results

Service	Initial status	Control action	Status at hour 24	Residual issue
staff safety	six remote, two unconfirmed	local roll call and assigned contact owners	all safe	sustained remote coverage
payroll	primary authentication unstable	verified deputy and alternative bank process	released and reconciled	review authentication failure
custody visibility	one portal unavailable	prior-day file and provider confirmation	97% by value reconciled	one private asset statement pending
cyber identity	email suspected	isolate, revoke sessions, clean channel	clean command access active	forensic scope continuing
capital call	notice received during incident	verify through known fund contact and administrator	due date and account confirmed	governing-body approval pending

17.3 Decisions

The office uses the verified USD 1.8 million rather than assuming access to the untested USD 3.0 million account. It keeps the capital-call payment pending until authority and beneficiary verification are complete. It avoids transferring custody assets solely because the portal is unavailable. It renews the deputy mandate for the defined crisis period through the appropriate governance process and assigns a separate reviewer for every crisis payment.

17.4 Interpretation

The test succeeds because the office preserves outcomes within defined tolerances and keeps irreversible actions controlled. It also reveals weaknesses: an untested cash account, reliance on one email identity domain, incomplete private-asset data and insufficient deputy coverage for investment approvals. Those findings become funded remediation items.

18. IMPLEMENTATION AND TESTING

18.1 Build the minimum viable plan

The first implementation cycle should identify important services, approve crisis roles, validate delegated authorities, establish the contact register, build the 72-hour liquidity ladder, define the minimum custody data set, create the staff-safety process, protect a clean recovery store and write the activation card. Each item has an owner and evidence date.

18.2 Exercise in layers

The office can run four exercise types. A notification test confirms contacts and channels. A tabletop tests decisions against a scenario. A technical recovery test proves that systems and data can be restored. A live operational test executes a low-risk alternative process, such as accessing a backup channel or submitting a controlled payment through the secondary route.

Testing should include unavailability of a principal, failure of the primary bank, loss of the primary custodian portal, compromise of email, denial of the main premises, simultaneous staff absence and a fraudulent instruction. Tests should avoid creating uncontrolled production risk.

18.3 Metrics

Useful metrics include time to activation; percentage of people confirmed safe; time to first verified situation report; percentage of 72-hour obligations covered by confirmed liquidity; percentage of critical providers with verified escalation contacts; age of the last tested backup; percentage of custody value reconstructed; number of crisis payments with complete dual-control evidence; and time to reconcile every crisis transaction.

18.4 Learn and fund

Each exercise or event should produce a short report: what happened; which service approached or exceeded tolerance; which dependency failed; which workaround succeeded; what evidence was missing; which temporary authority was used; which financial effect occurred; and which remediation will be funded. The governing body should approve the priority, owner and due date.

19. LIMITATIONS AND CONCLUSION

This paper provides an operating framework rather than a universal emergency manual. Family offices differ in legal structure, jurisdiction, staffing, regulated activity, asset mix, family governance, technology, security exposure and provider arrangements. The crisis plan must be aligned with the actual governing documents, mandates, contracts, laws and official guidance that apply to the office.

The framework also avoids predicting the cause or duration of a crisis. A 72-hour plan is designed around loss of service, access, authority or reliable information. It can support responses to cyber events, provider outages, physical disruption, principal unavailability, fraud attempts and compound events without claiming that the same technical response applies to each.

The central conclusion is operational. A resilient family office can name its important services, define how long they can be disrupted, preserve staff safety, succession and dual control, match liquidity to obligations, reconstruct custody and payment facts, recover critical data through a clean route, and transition temporary authority into governed recovery. Those capabilities are built and tested before the event.

The first 72 hours should leave the office with more reliable facts, tighter authority, reconciled money, safer people and a clear recovery decision. Speed comes from preparation, bounded mandates and verified alternatives.

APPENDIX A. ACTIVATION CARD

Field	Required entry
incident identifier	unique reference and activation date
earliest known event	timestamp and source
activation time	timestamp and approving authority
crisis level	Green, Amber, Red or Black under the approved ladder
crisis lead and deputy	names, verified numbers and authority source
next command update	time, channel and participants
people status	safe, unavailable, assistance required or unconfirmed
services at risk	service, tolerance, current outage and owner
temporary prohibitions	beneficiary, mandate, access and communication restrictions
external advisers	known contacts for legal, cyber, security and providers

Immediate actions: protect people; open the decision log; move to verified channels; freeze high-risk changes; preserve evidence; confirm the next hard deadline; and issue a factual update.

APPENDIX B. DELEGATED-AUTHORITY MATRIX

Legal person or account	Decision	Primary	Deputy	Executor	Second check	Source document	Cap	Expiry
family holding company	essential operating payment	complete	complete	complete	complete	board resolution and bank mandate	complete	complete
investment company	protective market action	complete	complete	complete	complete	investment policy and broker mandate	complete	complete
trust or foundation	beneficiary support	complete	complete	complete	complete	governing instrument and council resolution	complete	complete
operating office	payroll	complete	complete	complete	complete	payroll authority and bank mandate	complete	complete
technology environment	privileged containment	complete	complete	complete	complete	incident plan and access policy	least privilege	end of incident

The completed matrix should be validated by counsel, governing bodies and relevant providers. It is an index to authority; the underlying documents remain controlling.

APPENDIX C. CONTINUITY DASHBOARD

Domain	Metric	Green	Amber	Red	Current	Owner	Next check
people	staff assigned a verified status	100%	90% to 99%	below 90%	complete	complete	complete
authority	critical functions with a reachable primary or deputy	100%	one gap with workaround	material function uncovered	complete	complete	complete
liquidity	72-hour obligations covered by confirmed access	above 150%	100% to 150%	below 100%	complete	complete	complete
custody	liquid asset value reconstructed and reconciled	above 99%	95% to 99%	below 95%	complete	complete	complete
data	age of last tested critical-data recovery	within policy	test overdue	recovery unavailable	complete	complete	complete
providers	critical services with verified status and escalation	all	one unknown	multiple unknown	complete	complete	complete

Thresholds are illustrative and should be approved for the office's actual risk and obligations.

APPENDIX D. LIQUIDITY AND PAYMENT REGISTER

For each obligation record: identifier; legal payer; beneficiary; purpose; source document; amount; currency; latest safe payment time; consequence of delay; primary account; alternative account; bank cutoff; signatory set; input operator; approver; callback method; beneficiary status; release status; bank confirmation; accounting entry; and reconciliation reviewer.

For each liquidity source record: legal owner; institution; account; currency; verified balance time; available amount; restriction or lien; payment rail; daily limit; authentication; primary signatory; deputy; alternative contact; last successful test; and evidence source.

The register should avoid embedding passwords, authentication secrets or unnecessary identity data.

APPENDIX E. STAFF-SAFETY AND COMMUNICATION REGISTER

Person	Role	Location or travel status	Welfare status	Preferred contact	Secondary contact	Local coordinator	Assistance need	Last verified
complete	complete	complete	complete	complete	complete	complete	restricted entry	complete

Communication messages should state the incident identifier, verified instruction, action required, deadline, response format, approved channel and time of the next update. Staff should receive a simple method to report safe, unavailable or assistance required. Sensitive detail should be collected through the restricted welfare process.

APPENDIX F. DATA, CYBER AND CUSTODY RECOVERY PACK

The clean recovery pack should contain current governing documents, authority matrices, bank and custody schedules, verified contacts, prior-day cash and position files, payment and obligation queues, private-market commitment schedules, critical provider contracts, incident procedures, data-recovery instructions and insurance contacts.

Controls should include encryption, least-privilege access, administrator separation, offline or otherwise isolated recovery capability, immutable or protected backups where appropriate, version dates, restoration tests, distribution records and a process for revoking access after the event.

The pack should exclude live passwords, private keys and authentication secrets unless a specialist-approved secret-management architecture explicitly governs them.

APPENDIX G. QUESTIONS FOR GOVERNING BODIES AND PROVIDERS

Questions for the family governing body

1. Which services must continue within two, six, twelve, twenty-four and seventy-two hours? 2. Which decisions can deputies take and which require the principal or a fiduciary body? 3. Which temporary limits and prohibitions apply during activation? 4. Which information can be shared with staff, providers and advisers? 5. Which residual risks justify remaining in crisis mode after hour seventy-two?

Questions for banks and custodians

1. Which alternative instruction and authentication routes are formally accepted? 2. Which mandates, cutoffs, limits and callback controls apply? 3. How are service incidents and suspected fraud escalated? 4. What position, cash, settlement and corporate-action data can be provided outside the portal? 5. Which sub-custody, settlement-bank or technology dependencies are material to continuity?

Questions for technology and cyber providers

1. How are privileged identities isolated and recovered? 2. Which backups are offline, immutable or outside the primary identity domain? 3. When was restoration last tested and what evidence exists? 4. Which logs and evidence should be preserved during containment? 5. Which clean communication and administration routes can operate during compromise?

Questions for legal, compliance, security and insurance advisers

1. Which authorities and governing documents control each crisis decision? 2. Which notifications, preservation duties and contractual deadlines may apply? 3. Which travel, workplace and staff-safety decisions require specialist advice? 4. Which policy conditions, exclusions, consent or notice requirements are relevant? 5. How should temporary powers expire and ordinary governance be restored?

REFERENCES

[1] National Emergency Crisis and Disasters Management Authority. *Business Continuity Management.* https://www.ncema.gov.ae/content/documents/BCM%20English%20NCEMA_29_8_2013.pdf

[2] National Emergency Crisis and Disasters Management Authority. *Business Continuity Management programme.* https://www.ncema.gov.ae/en/e-participation/blog/business-continuity-management-program.aspx

[3] Central Bank of the UAE Rulebook. *Operational Risk Standards.* https://rulebook.centralbank.ae/en/rulebook/operational-risk-standards

[4] Central Bank of the UAE Rulebook. *Operational Risk and Operational Resilience.* https://rulebook.centralbank.ae/en/entiresection/6015

[5] Central Bank of the UAE Rulebook. *Business Continuity for Cloud Computing Arrangements.* https://rulebook.centralbank.ae/en/rulebook/business-continuity

[6] Basel Committee on Banking Supervision. *Principles for Operational Resilience.* 31 March 2021. https://www.bis.org/bcbs/publ/d516.htm

[7] Financial Stability Board. *Enhancing Third-Party Risk Management and Oversight: A Toolkit.* 4 December 2023. https://www.fsb.org/2023/12/fsb-publishes-toolkit-for-enhancing-third-party-risk-management-and-oversight/

[8] Financial Conduct Authority. *Operational resilience.* Updated 14 July 2026. https://www.fca.org.uk/firms/operational-resilience

[9] 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

[10] Financial Conduct Authority. *Building operational resilience, PS21/3.* https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience

[11] Dubai Financial Services Authority. *General Module, business continuity and cyber risk management.* https://dfsa-prod.60413.aws.thomsonreuters.com/rulebook/general-module-gen-ver7207-26

[12] Central Bank of the UAE. *Payments and Settlements.* https://www.centralbank.ae/en/our-operations/payments-and-settlements/

[13] Central Bank of the UAE. *UAE Fund Transfer System.* https://centralbank.ae/en/our-operations/payments-and-settlements/uae-fund-transfer-system-uaefts/

[14] Financial Action Task Force. *The FATF Recommendations.* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

[15] Financial Action Task Force. *Guidance on Beneficial Ownership and Transparency of Legal Arrangements.* March 2024. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Guidance-Beneficial-Ownership-Transparency-Legal-Arrangements.pdf

[16] Financial Action Task Force. *Guidance on Politically Exposed Persons.* https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf

[17] Central Bank of the UAE Rulebook. *Best Practices for Technology Risk and Information Security.* https://rulebook.centralbank.ae/en/rulebook/annex-ii-guidance-best-practices-technology-risk-and-information-security

[18] International Organization of Securities Commissions. *Standards for the Custody of Collective Investment Schemes' Assets.* https://www.iosco.org/library/pubdocs/pdf/ioscopd512.pdf

[19] US Securities and Exchange Commission. *How We Protect Retail Investors: Custody of Client Assets.* https://www.sec.gov/newsroom/speeches-statements/speech-driscoll-042919

[20] National Institute of Standards and Technology. *Cybersecurity Framework 2.0.* 26 February 2024. https://www.nist.gov/cyberframework

[21] National Institute of Standards and Technology. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management, SP 800-61 Revision 3.* April 2025. https://csrc.nist.gov/pubs/sp/800/61/r3/final

[22] National Institute of Standards and Technology. *Contingency Planning Guide for Federal Information Systems, SP 800-34 Revision 1.* https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

[23] National Institute of Standards and Technology. *Guide for Cybersecurity Event Recovery, SP 800-184.* https://www.nist.gov/publications/guide-cybersecurity-event-recovery

[24] Cybersecurity and Infrastructure Security Agency. *StopRansomware Guide.* https://www.cisa.gov/stopransomware/ransomware-guide

[25] Committee on Payments and Market Infrastructures and IOSCO. *Principles for Financial Market Infrastructures.* https://www.bis.org/cpmi/publ/d101a.pdf

[26] Committee on Payments and Market Infrastructures and IOSCO. *Guidance on Cyber Resilience for Financial Market Infrastructures.* https://www.bis.org/cpmi/publ/d146.htm

[27] US Securities and Exchange Commission. *Custody of Funds or Securities of Clients by Investment Advisers.* https://www.sec.gov/files/rules/final/ia-2176.htm

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

[29] Central Bank of the UAE. *Guidelines for Financial Institutions Adopting Enabling Technologies.* https://rulebook.centralbank.ae/en/rulebook/guidelines-financial-institutions-adopting-enabling-technologies

[30] Central Bank of the UAE. *Risk Management and Business Continuity.* https://www.centralbank.ae/en/our-operations/risk-management/

[31] Cybersecurity and Infrastructure Security Agency. *Cross-Sector Cybersecurity Performance Goals.* https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[32] National Emergency Crisis and Disasters Management Authority. *National Standard for Occupational Safety and Health Management System.* https://www.ncema.gov.ae/en/e-participation/blog/national-standard-for-occupational-safety-and-health-management-system.aspx

[33] National Emergency Crisis and Disasters Management Authority. *Business Continuity Readiness Guidelines for UAE Organisations.* https://www.ncema.gov.ae/en/media-center/news/14/3/2020/business-continuity-readiness-guidelines-launched-for-uae-organisations-in-event-of-covid-19-outbreak.aspx

[34] National Emergency Crisis and Disasters Management Authority. *National Standard for Business Continuity Management, NCEMA 7000:2021.* https://www.ncema.gov.ae/en/about-ministry/events/7/2023/certified-lead-implementer-for-business-continuity-management-ncema-70002021-course.aspx

[35] Bank for International Settlements. *High-level principles for business continuity.* August 2006. https://www.bis.org/publ/joint17.htm

[36] Bank for International Settlements. *ORR20: Operational resilience.* https://www.bis.org/basel_consolidated_guidelines/chapter/ORR/20.htm

[37] Bank for International Settlements. *ORR30: Third-party risks.* https://www.bis.org/basel_consolidated_guidelines/chapter/ORR/30.htm

[38] Bank for International Settlements. *LQY10: Liquidity risk management and supervision.* https://www.bis.org/basel_consolidated_guidelines/chapter/LQY/10.htm

[39] Financial Conduct Authority. *CrowdStrike outage: lessons for operational resilience.* 31 October 2024. https://www.fca.org.uk/firms/operational-resilience/crowdstrike-outage-lessons-operational-resilience

[40] UK National Cyber Security Centre. *Incident management guidance.* https://www.ncsc.gov.uk/collection/incident-management

ABOUT THE AUTHOR

Chennakeshav Adya is an independent researcher and corporate finance practitioner with more than twenty years of international experience across business strategy, transformation, investment banking, family-office operations, risk, technology and cross-border transactions. His research focuses on practical decision systems for private capital, operating resilience, corporate finance and emerging technology. The views expressed in this paper are his own and do not constitute investment, legal, tax, cyber, security or regulatory advice.