# The 90% Strait

*A family-office operational resilience framework for custody, cash, insurance, travel and investment operations during severe disruption to the Strait of Hormuz*

**Authored by Chennakeshav Adya**
Independent Researcher
August 2026

## ABSTRACT

**Background.** A globally diversified family office can still depend on one corridor of people, authority, banks, custodians, communications and travel. Severe disruption around the Strait of Hormuz can transmit through energy markets, transport, insurance, payments, sanctions controls and staff availability.

**Objective.** This paper develops a family-office operational-resilience framework for custody, cash, insurance, travel and investment operations.

**Approach.** The analysis combines current official energy, financial-infrastructure, operational-resilience, travel, sanctions and cyber sources with service mapping, impact tolerances, liquidity ladders, custody controls and severe-but-plausible scenarios.

**Findings.** Balance-sheet diversification does not establish operational diversification. A family office can remain exposed when several critical services depend on the same person, location, identity platform, bank, custodian or provider. Resilience follows tested alternate authority, accessible liquidity, independent records, current policy terms, secure communications and disciplined crisis governance.

**Implications.** The office should identify important services, set time and non-time tolerances, map common-mode dependencies, test alternatives and obtain board approval for residual risks through a 90-day implementation programme.

**Practical priorities**

1. Define important family-office services and measurable impact tolerances.
2. Build independent authority, custody access, liquidity, communications and travel routes.
3. Test severe-but-plausible scenarios and fund remediation before disruption.

**JEL Classification:** G23, G32, G28, F65, H56, L91

**Keywords:** family office, operational resilience, Strait of Hormuz, custody, liquidity, insurance, travel, sanctions, cyber resilience, impact tolerance, crisis governance

*Research paper only. This document provides general information and is not legal, regulatory, tax, investment, insurance, aviation, maritime, security, medical, sanctions, cyber or travel advice. Every worked scenario is hypothetical and simplified. Current fact-specific professional advice and official guidance are essential.*

# 1. INTRODUCTION

A family office can hold assets across many countries while running its daily authority through a narrow operational corridor. The same people may approve payments, access custodians, instruct advisers, manage travel, speak with insurers and coordinate family decisions from one city. A regional disruption can therefore reach a globally diversified balance sheet through concentrated control, communications and service providers.

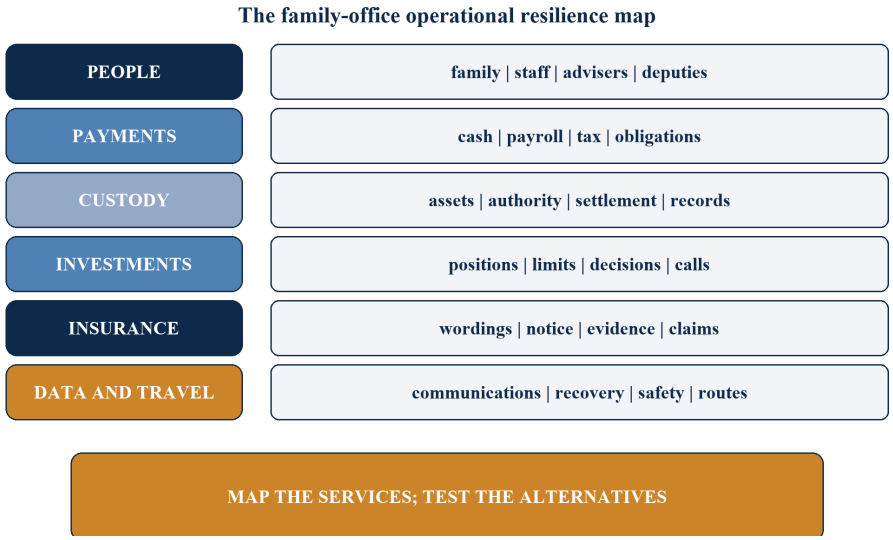
The Strait of Hormuz is a useful stress point because its significance extends beyond vessels. The US Energy Information Administration reported that oil flows through the Strait averaged about 20 million barrels per day in 2024; this represented more than one-quarter of global seaborne oil trade and about one-fifth of global petroleum-liquids consumption. Around one-fifth of global liquefied natural gas trade also passed through the Strait in 2024 [1,2]. A severe interruption could affect energy prices, freight, insurance, air travel, market volatility, sanctions screening, bank operations and the availability of senior decision makers at the same time.

The title uses 90 per cent as a hypothetical concentration warning, not as a statement about the Strait, global trade or any particular family office. A family office may discover that 90 per cent of its payment authority, custody access, institutional memory or crisis decision capacity depends on one location or a small group of people. The correct percentage must be measured from the office's own dependency map.

This paper converts operational-resilience principles into a family-office framework. It identifies important services, sets impact tolerances, maps dependencies, builds liquidity and custody alternatives, reviews insurance and travel controls, integrates sanctions and cyber response, and establishes a 90-day implementation programme. The framework assumes that disruption will occur, consistent with Basel Committee guidance, and asks whether critical operations can remain within documented tolerances [3,4].

The objective is continuity of lawful authority and access. Every recommendation remains subject to the family's legal structures, fiduciary duties, regulatory perimeter, bank and custodian contracts, insurance wording, residence position, data-protection obligations and current government advice. A plan should preserve safety and compliance while maintaining the minimum services required to protect people, meet obligations and govern capital.

**Figure 1. The family-office operational resilience map.**



# 2. WHY THE STRAIT MATTERS TO A FAMILY OFFICE

## 2.1 A physical chokepoint with financial transmission channels

The Strait is one of the world's most important energy chokepoints by volume [1]. EIA analysis states that most oil volumes transiting it have no practical alternative route, although Saudi Arabia and the UAE possess pipelines that can bypass part of the flow. EIA estimated that about 2.6 million barrels per day of unused Saudi and UAE pipeline capacity could have been available in a disruption scenario in 2025 [2]. These figures establish materiality; they do not forecast closure, duration or price effects.

A family office should model transmission channels rather than make a geopolitical forecast. The first channel is market risk through oil, gas, freight, currencies, rates and listed securities. The second is operating risk through airspace, ports, travel, physical security and employee availability. The third is financial infrastructure through payment approvals, sanctions screening, correspondent banks, custodians and settlement. The fourth is insurance through exclusions, notification duties, aggregation limits and claims handling. The fifth is information through cyber events, misinformation and degraded communications.

## 2.2 Correlated disruption

Traditional continuity plans often test one failed supplier or one unavailable office. A Strait scenario can create several linked failures. Travel may be disrupted while principals are abroad. Markets may move while investment staff cannot reach normal systems. Banks may apply enhanced reviews while time-critical payments increase. Insurers may require immediate notice while policy documents are inaccessible. A cloud platform may remain available while local identity, electricity or telecommunications access becomes unreliable.

The important question is whether several controls share the same underlying dependency. Two bank accounts provide limited diversification when both require the same signatory, device, telephone number, relationship manager or correspondent route. Two offices provide limited resilience when both rely on one identity provider and one administrator. The dependency map must reach the person, process, technology, facility, information and third-party level [3,9-11].

## 2.3 A scenario-planning boundary

The paper does not predict military action, closure of the Strait, bank failure, payment-system failure or evacuation. It uses severe but plausible operational scenarios to test governance. Current government, regulator, bank, custodian, insurer and local-authority information should replace planning assumptions whenever an event occurs.

Plans should avoid automatic market trades, unapproved asset transfers or unsafe travel responses. Pre-agreed authority, legal review and verified information remain part of every control. The family office should know what it can do, who may approve it, which evidence is required and when a decision must be escalated.

# 3. THE SEVERE-BUT-PLAUSIBLE SCENARIO LADDER

## 3.1 Scenario one: 24 to 72 hours

The first scenario assumes sudden regional escalation, rapid market volatility, flight cancellations, intense media coverage and higher client-service volumes. Banks, custodians and core payment systems remain available, but call centres and compliance teams experience pressure. One senior signatory is travelling and a second cannot use the usual authentication device. No physical damage to the family office is assumed.

The test is whether the office can confirm people, preserve decision authority, access verified information, make urgent payments, pause non-essential activity and communicate with banks, custodians, insurers and advisers. The outcome should be measured in hours, failed instructions, unreconciled positions and people not contacted.

## 3.2 Scenario two: 7 to 30 days

The second scenario assumes intermittent airspace restrictions, longer shipping routes, increased insurance scrutiny, persistent market volatility and slower cross-border payment reviews. One office is inaccessible for part of the period. A key administrator or technology provider experiences a service interruption. Family members are distributed across three jurisdictions.

The test expands to payroll, household funding, medical access, investment settlement, collateral, private-market capital calls, tax deadlines, entity governance and policy notifications. The office should operate through alternate people, locations, devices and service providers without losing its control record.

## 3.3 Scenario three: 30 to 90 days

The third scenario assumes prolonged regional disruption with variable transport capacity, elevated compliance reviews, staff relocation and material changes in portfolio liquidity. It does not assume that every financial market or institution is unavailable. The stress comes from duration, correlation and decision fatigue.

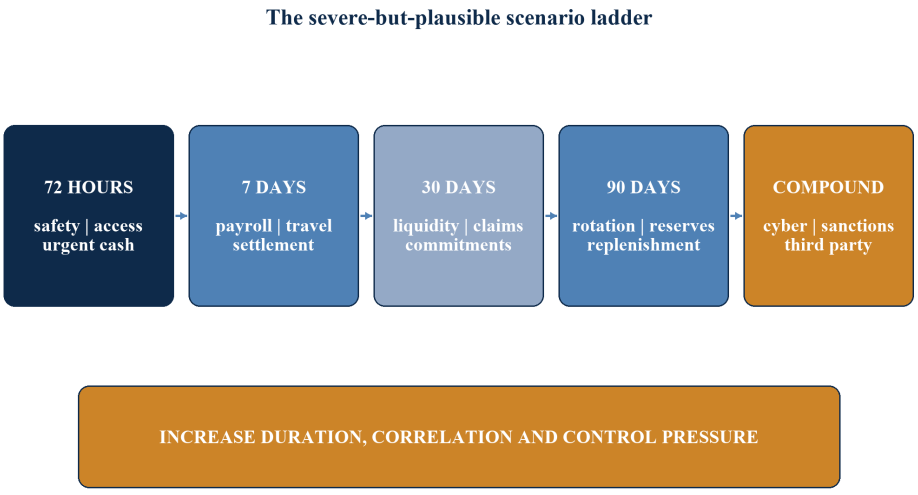
The test asks whether reserves, delegations, data, contracts, physical arrangements and third-party capacity remain adequate. The family office should be able to rotate personnel, replenish cash, maintain board and trust decisions, continue essential reporting and review portfolio risks without improvising authority.

## 3.4 Scenario four: a compound cyber and sanctions event

The fourth scenario combines geopolitical disruption with a targeted phishing campaign, one compromised administrator account and a payment delayed for enhanced sanctions review. No assumption is made that any family member or counterparty is sanctioned. The purpose is to test whether urgency weakens verification and segregation of duties.

The office should preserve strong authentication, callback verification, dual approval, sanctions screening, evidence and incident response. A crisis does not reduce legal obligations. UK Iran sanctions guidance, FATF standards and the rules of every relevant jurisdiction remain applicable to payments, funds, financial services and counterparties [20-22].

**Figure 2. The severe-but-plausible scenario ladder.**



# 4. IMPORTANT SERVICES AND IMPACT TOLERANCES

## 4.1 Start with outcomes

Operational resilience begins with the services whose interruption could create unacceptable harm. The FCA framework uses important business services and impact tolerances; Basel guidance uses critical operations and tolerance for disruption [3,9,10]. A family office can adapt these concepts even when it is outside a specific regulatory rule.

An important service should be described as an outcome. "Pay essential family and entity obligations" is more useful than "access online banking." The outcome can be delivered through several processes and technologies. This distinction creates alternatives when one resource fails.

## 4.2 Family-office service inventory

| Important service | Potential harm from disruption | Example tolerance dimensions |
|---|---|---|
| Emergency family support | Safety, health or inability to travel | minutes or hours; people reached; funds available |
| Essential payments | Missed payroll, medical, household, tax or debt obligations | time; amount; number of failed payments |
| Custody and settlement | Failed trades, missed corporate actions or inaccessible assets | settlement deadline; value; market exposure |
| Investment oversight | Uncontrolled exposures or missed portfolio decisions | data age; exposure limit; approval delay |
| Insurance response | Lost notification rights or delayed protection | notification time; policy access; claim status |
| Entity governance | Invalid or delayed board, trust or partnership decisions | authorised decision makers; quorum; record completeness |
| Regulatory and tax reporting | Breach, penalty or incomplete disclosure | filing deadline; jurisdictions; evidence quality |
| Secure communications | Misdirection, fraud or loss of command | verified channels; contact coverage; recovery time |

## 4.3 Time and non-time tolerances

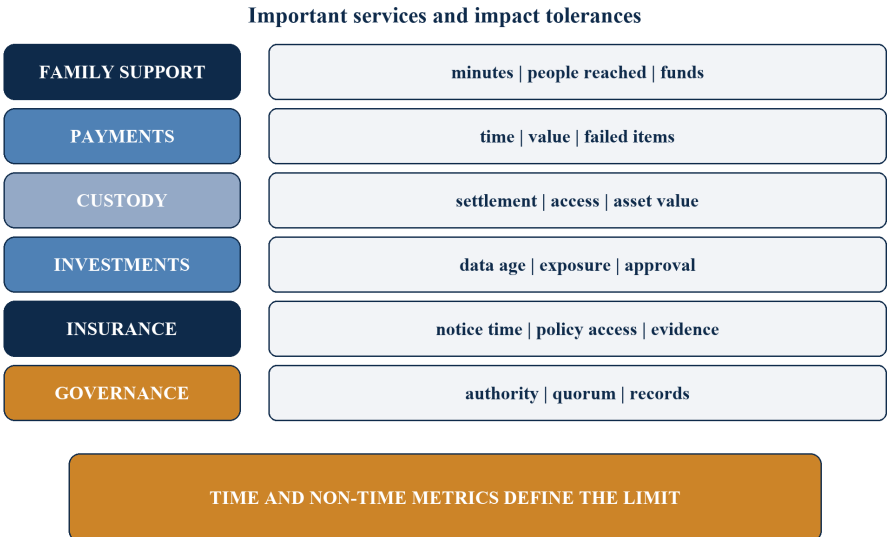
Time alone is insufficient. FCA observations encourage firms to complement time-based tolerances with metrics such as transaction value, volume, criticality and estimated loss [10]. A family office should add safety, fiduciary, confidentiality and family-governance measures.

An emergency-support tolerance could require contact with every dependent within two hours, confirmation of safe location within four hours and access to a defined amount of local currency within six hours. A custody tolerance could require confirmation of positions by a stated time, zero unapproved asset transfers and settlement of specified critical trades. These are examples; management and advisers should set values from actual obligations and capacity.

## 4.4 Degraded service

The office may operate a controlled degraded service during disruption. Non-essential investment activity may pause. Reporting may use a verified snapshot. Payment batches may be smaller and more frequent. Manual instructions may require additional callbacks. Degradation should have an approved scope, expiry time and reconciliation process.

**Figure 3. The important-services and impact-tolerance map.**


Important services and impact tolerances
FAMILY SUPPORT
minutes | people reached | funds
PAYMENTS
time | value | failed items
CUSTODY
settlement | access | asset value
INVESTMENTS
data age | exposure | approval
INSURANCE
notice time | policy access | evidence
GOVERNANCE
authority | quorum | records
TIME AND NON-TIME METRICS DEFINE THE LIMIT

# 5. MAPPING THE DEPENDENCY CORRIDOR

## 5.1 Six dependency classes

For every important service, map people, processes, technology, facilities, information and third parties [3,10]. Each dependency should have an owner, location, recovery objective, evidence source, concentration rating and tested alternative.

People mapping should include principals, trustees, directors, protectors, investment committee members, signatories, relationship managers, administrators and specialist advisers. Process mapping should follow an instruction from initiation through approval, screening, execution, confirmation, booking and reconciliation. Technology mapping should include devices, identity providers, telephone numbers, password vaults, virtual private networks, market data and document systems.

Facilities mapping should cover offices, homes, data rooms, safe-deposit access and physical records. Information mapping should identify legal documents, account details, policies, powers, contact lists, asset registers and source records. Third-party mapping should extend beyond the contracted provider to material subcontractors and market infrastructures where known.

## 5.2 Common-mode failure

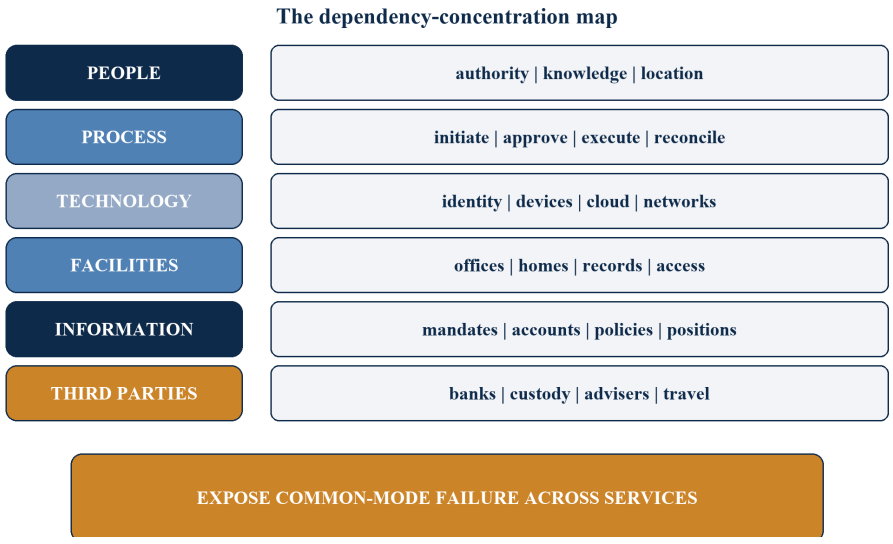
The map should expose alternatives that fail together. A secondary custodian may use the same sub-custodian in a key market. A separate bank may share the same correspondent. Two software applications may use one identity provider. Two authorised signatories may travel together. A backup office may use the same power, telecom and access-control provider.

The objective is independent recovery, not a larger vendor list. Independence should be demonstrated through legal entity, jurisdiction, technology, authority and operating-route evidence. The Financial Stability Board toolkit recommends lifecycle management of critical third-party services, including due diligence, contracting, monitoring, incident response and exit planning [8].

## 5.3 The dependency register

The register should show each dependency's normal route, alternate route, maximum tolerable outage, activation trigger, owner, contract, data location and last test. A red status means no tested alternative exists within tolerance. An amber status means an alternative exists but depends on an untested person, provider or manual step. A green status requires evidence from a recent test.

**Figure 4. The dependency-concentration map.**



# 6. CUSTODY RESILIENCE

## 6.1 Legal and operational layers

Custody resilience begins with the legal entity that owes the service, the location and legal status of client assets, the sub-custody chain, the settlement infrastructure and the office's ability to issue valid instructions. A brand name alone does not reveal these layers.

The office should document account owner, custodian entity, governing law, asset segregation, cash treatment, omnibus or segregated arrangements, sub-custodians, liens, set-off, securities lending, cash sweeps, settlement venues, complaint and escalation rights. Current legal advice is required for insolvency and asset-recovery conclusions.

## 6.2 Access and authority

Assets can remain safe while operational access is disrupted. The control set should include at least two authorised people, independent devices, offline contact details, tested callback procedures and a documented manual-instruction route. Powers of attorney, board mandates and trust authorities should be reviewed before a crisis.

The office should test read-only position access, trading access, cash transfer, corporate-action election and document retrieval. A successful login is not a complete custody test. The test should trace an instruction through confirmation and reconciliation.

## 6.3 Diversification decisions

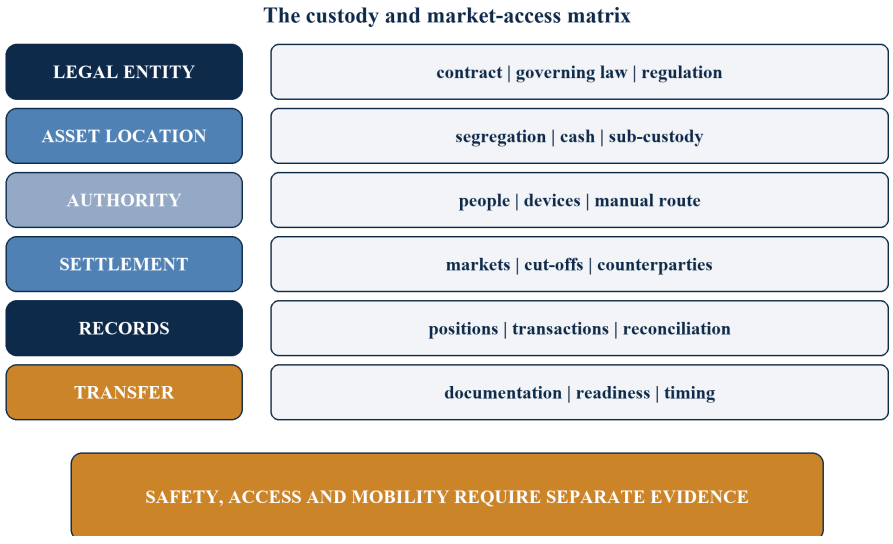
A second custodian can reduce concentration and add complexity. Splitting assets may increase reconciliation, tax reporting, collateral fragmentation and corporate-action risk. The decision should compare service independence, asset mobility, market coverage, cost, information quality and crisis capacity.

| Custody question | Evidence | Stress test |
|---|---|---|
| Which legal entity holds the account? | agreement and regulatory register | contact and escalation drill |
| Where are assets and cash held? | custody schedule and statements | market and currency access review |
| Who can instruct? | mandate and specimen authority | alternate-signatory transaction |
| Which third parties support delivery? | sub-custody and service map | critical-provider outage scenario |
| Can positions be reconstructed? | independent books and statements | offline reconciliation |
| Can assets be transferred? | transfer terms and account readiness | documentation and timing exercise |

## 6.4 Market closure and settlement

The plan should distinguish inability to trade, inability to settle, inability to instruct and inability to access information. Each requires a different response. The Principles for Financial Market Infrastructures emphasise custody, investment, liquidity and operational risks, including timely recovery after major disruption [7]. A family office should rely on its custodian and market documentation for specific obligations.

**Figure 5. The custody and market-access matrix.**



# 7. THE CASH AND LIQUIDITY LADDER

## 7.1 Liquidity follows obligations

Liquidity planning should begin with uses of cash by time, currency, entity, jurisdiction and approval route. A single cash balance can be misleading when funds are held in the wrong entity, require unavailable signatories, sit outside deposit protection, are pledged, or cannot reach the required beneficiary.

The ladder should cover emergency family support, medical costs, payroll, household operations, debt service, taxes, insurance premiums, adviser retainers, portfolio margin, private-market capital calls and operating-company support. Each obligation needs a due date, amount range, legal payer, currency, normal rail and alternate rail.

## 7.2 Four liquidity horizons

The first horizon covers zero to 72 hours. It should fund immediate safety, medical, travel and essential-payment needs through accessible accounts and authorised people. The second covers days four to fourteen; it adds payroll, recurring household and entity obligations, collateral and urgent professional costs. The third covers days fifteen to thirty; it includes debt, tax, premiums and investment commitments. The fourth covers days thirty-one to ninety; it supports prolonged operations and replenishes the earlier layers.

The amounts should be approved as management estimates and tested against real payment limits. The ladder should record gross cash, encumbrance, access time, transfer limits, concentration, currency mismatch and replenishment source.

## 7.3 Banks, currencies and rails

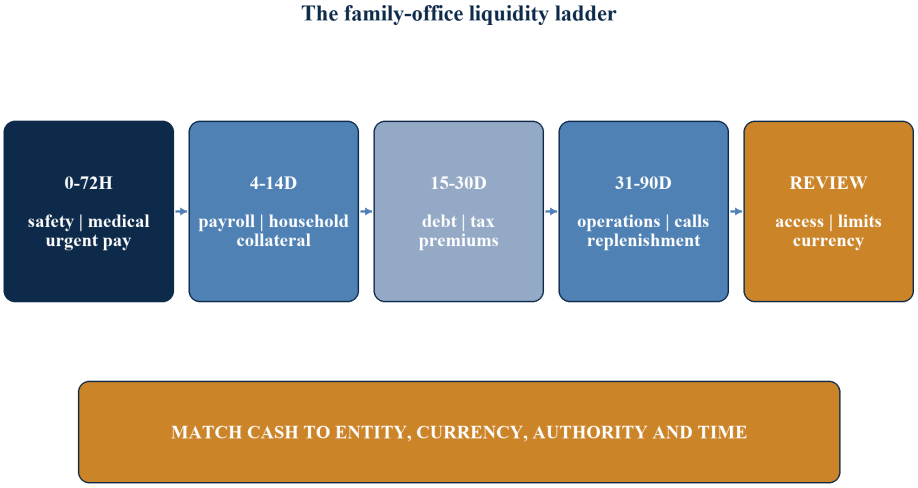
The UAE Central Bank owns and manages UAEFTS, the country's real-time gross settlement system, and oversees several retail systems [12-15]. Aani provides instant account-to-account payments through participating institutions [16]. These infrastructures support domestic payments; the office still depends on its bank, account status, authentication, limits, beneficiary controls and cross-border routes.

A resilient design may use more than one institution and more than one payment route, subject to compliance, cost and account-operating requirements. The office should test domestic and cross-border payments, beneficiary creation, bulk payroll, callback procedures and after-hours escalation. It should not route funds through informal or unapproved channels.

## 7.4 Intraday control

Basel liquidity guidance states that institutions using correspondents or custodians should assure themselves that arrangements allow timely obligations under varied circumstances [6]. A family office can apply the same discipline. It should monitor payment status, cut-offs, collateral, rejected instructions and late counterparties during stress. One dashboard should show available cash, pending payments, failed payments and the owner of each exception.

**Figure 6. The family-office liquidity ladder.**



# 8. PAYMENT AND SETTLEMENT CONTINUITY

## 8.1 Payment-critical data

The office should maintain a controlled register of approved beneficiaries, bank coordinates, purpose, sanctions status, expected frequency, payment limits and verification evidence. The register should be available through a secure alternate channel and should never include authentication secrets in plain text.

Emergency payments should preserve segregation of duties. One person initiates; another approves; a third or automated control reconciles where practical. Callback numbers should come from verified records rather than an urgent email or message. Any change to beneficiary details should trigger enhanced verification.

## 8.2 Manual alternatives

Manual instructions can restore access and introduce risk. The office should pre-agree the format, authorised signatures, delivery channel, callback, cut-off and record retention with each bank and custodian. A manual route should be tested with a low-value transaction before it is needed.

The plan should include a queue for delayed payments. Each item receives a harm rating, legal deadline, value, available alternative and escalation owner. Safety, payroll, medical, tax and secured obligations may receive priority; the final hierarchy requires adviser and board approval.

## 8.3 Reconciliation after recovery

Every degraded or manual process must end with reconciliation. The office should match instruction, approval, bank confirmation, general ledger, portfolio system and beneficiary receipt. Duplicate-payment detection is essential when a delayed instruction and an alternate instruction may both complete.

# 9. INSURANCE AS AN OPERATING CONTROL

## 9.1 Coverage must be read from the contract

Insurance response depends on policy wording, endorsements, exclusions, insured entities, geography, cause, notification, deductibles, limits, aggregation and claims cooperation. Terms such as war, terrorism, political violence, cyber, marine, aviation, business interruption, travel and medical have policy-specific meanings. The family office should not assume coverage from the policy title.

The register should include insurer, policy number, insured parties, period, limits, deductibles, broker, claims contact, notice deadline, governing law, key exclusions and location of the current wording. Legal and broker advice should address any uncertainty.

## 9.2 Coverage map

The office should map property and business interruption, cyber, crime, directors and officers, professional indemnity where relevant, political violence, terrorism, marine or aviation interests, travel, medical and household coverage. Trusts, holding companies, operating businesses, aircraft, vessels, homes and employees may sit under separate programmes.

A single event can reach several policies. The incident team should coordinate facts and notifications while avoiding inconsistent descriptions. Notice should follow policy and adviser instructions; premature conclusions about cause or liability should be avoided.

## 9.3 Claims readiness

Claims readiness requires current wordings, asset schedules, valuations, photographs, invoices, maintenance records, access logs, cyber logs, travel records and contact details. Copies should be stored securely in more than one location. The office should test whether an authorised person can notify a claim when the normal risk manager is unavailable.

## 9.4 Insurance and travel advice

FCDO travel advice states that no travel can be guaranteed safe and recommends appropriate insurance for the itinerary and planned activities [17]. Current advice can change quickly. The family office should check whether a route, destination, activity or government warning affects coverage before travel.

# 10. TRAVEL, PEOPLE AND FAMILY SAFETY

## 10.1 Current information and decision rights

As of 24 July 2026, FCDO advice for the UAE referred to unpredictable regional conditions, possible flight cancellations, periodic airspace closures and travel disruption [17]. This is time-sensitive information. The office should monitor current official advice, local authorities, airports and airlines at the time of action.

The travel protocol should define who can recommend, approve and fund a change of plan. It should distinguish shelter, delay, relocation and departure decisions. A generic evacuation trigger can create unsafe movement. The decision should consider location, official advice, medical needs, available routes, destination entry rights, insurance and confirmed transport.

## 10.2 Family and staff register

The controlled register should cover family members, staff, guests and key advisers; location; citizenship and residence; passport and visa expiry; medical needs; emergency contacts; dependants; current itinerary; transport; accommodation and communication channels. Access must respect privacy and data-protection obligations.

The register should record confirmation status rather than continuous unnecessary surveillance. A crisis check-in sequence should use primary and alternate channels. One coordinator owns unresolved contacts and records the time and source of each confirmation.

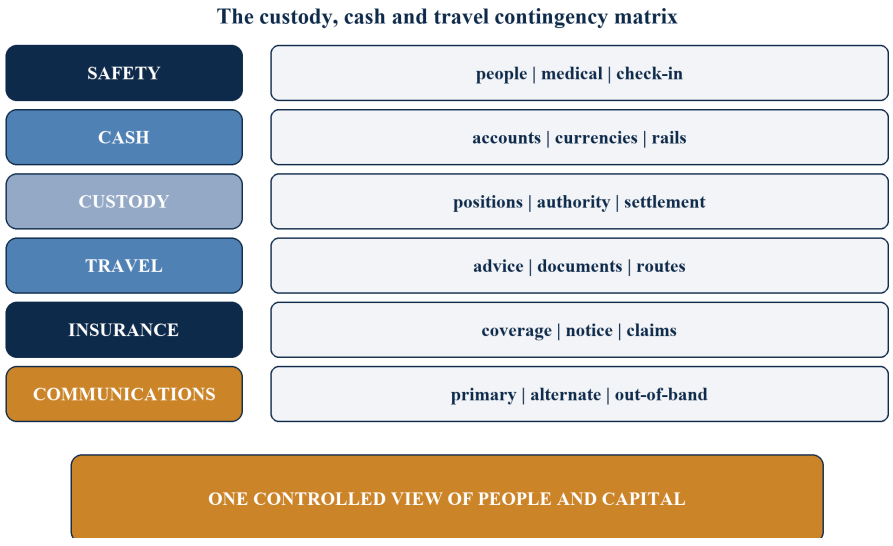
## 10.3 Documents and funding

Current passports, visas, residence documents, medical information, consent letters for minors where required, prescriptions and insurance contacts should be accessible through secure physical and encrypted digital copies. Emergency funds should be held in appropriate currencies and legal entities. Payment cards, cash and bank transfers have different failure modes; the plan should use a lawful mix suited to the family.

## 10.4 Marine and air routes

FCDO guidance advises careful enquiries before entering sensitive Gulf waters and notes increased maritime-attack risk in several regional waters [18]. The office should use qualified aviation, marine, security, legal and insurance advisers for any private transport. Availability, permits, crew duty, airspace, port status, fuel, insurance and destination acceptance must be verified for the specific movement.

**Figure 7. The custody, cash and travel contingency matrix.**



# 11. INVESTMENT OPERATIONS THROUGH DISRUPTION

## 11.1 Portfolio facts before market views

The investment team should begin with verified positions, cash, collateral, leverage, derivatives, settlement obligations, redemptions, capital calls and concentration. A market narrative cannot substitute for position data. Each asset should be linked to custodian, legal owner, liquidity terms, valuation source, hedge, counterparty and decision authority.

The first objective is control. The office should confirm that no exposure is unmanaged because a person, system or price feed is unavailable. The second objective is liquidity. The third is deliberate portfolio action within an approved mandate.

## 11.2 Decision tiers

Tier one decisions protect obligations and risk limits: margin, settlement, collateral and known cash needs. Tier two decisions reduce exposures that exceed approved limits. Tier three decisions rebalance or deploy capital. Tier four decisions pursue new opportunities. Lower tiers should not consume capacity required for higher-priority controls.

The investment policy should state which actions may proceed under delegated authority during disruption. It should include size limits, permitted instruments, price checks, counterparty requirements, communication methods and post-trade review. Emergency authority should expire automatically.

## 11.3 Private markets and operating assets

Private funds may issue capital calls while secondary liquidity is limited. Operating businesses may request working capital. Real assets may face insurance, tenant, logistics or maintenance issues. The family office should maintain a 90-day schedule of expected and contingent cash demands across these assets.

Commitments should be classified as contractual, discretionary or support-related. Any decision to delay, default, fund or sell requires legal and investment analysis. Relationship considerations do not change contractual obligations.

## 11.4 Market volatility

The paper makes no forecast for oil, equities, rates, currencies, freight or insurance. Stress tests should use transparent hypothetical shocks and several durations. The investment committee should record scenario assumptions, model limitations and the decision that each result informs.

# 12. SANCTIONS, FINANCIAL CRIME AND PAYMENT FRICTION

## 12.1 Compliance remains integral

Regional escalation can increase payment scrutiny and sanctions change risk. UK Iran sanctions guidance describes prohibitions involving designated persons, funds, financial services and specified goods or technology [20]. FATF identifies Iran as a high-risk jurisdiction subject to a call for action and urges enhanced due diligence and, in the most serious cases, countermeasures [21]. The applicable rules depend on persons, entities, jurisdictions, products and conduct.

The office should maintain current screening across family entities, counterparties, banks, vessels, aircraft, investments, directors, beneficial owners and payment beneficiaries where relevant. Screening results require competent review. A name match is not a legal conclusion, and urgency is not a reason to bypass controls.

## 12.2 Pre-clearance and evidence

Expected payments should have documented purpose, source of funds, source of wealth where requested, underlying contract, beneficiary ownership and sanctions review. This can reduce avoidable delay; it cannot guarantee bank approval or processing time.

The office should identify payments with regional shipping, energy, aviation, insurance, dual-use, Iranian nexus or complex intermediaries for specialist review. OFSI licences and exceptions are legal mechanisms with defined conditions; advisers should determine whether they apply.

## 12.3 Escalation

A delayed payment should move through a documented escalation path: bank operations, relationship manager, compliance, legal adviser and board owner as appropriate. The office should record requests, responses, evidence supplied and timing. It should avoid repeated resubmission through different channels without coordination.

# 13. CYBER, DATA AND COMMUNICATIONS

## 13.1 Crisis pressure increases control risk

Urgent travel changes, bank requests, policy notices and executive messages can create opportunities for impersonation. The family office should assume that attackers may exploit public disruption. Verification controls should strengthen during crisis.

The control set includes phishing-resistant authentication where available, privileged-access review, device management, encryption, secure backups, tested restoration, alternate communications, fraud callbacks and incident reporting. NIST's Cybersecurity Framework 2.0 organises cyber risk through Govern, Identify, Protect, Detect, Respond and Recover functions [25].

## 13.2 Critical information assets

Basel guidance recommends identifying critical information assets and maintaining integrity through resilient ICT and secure backup, including offline or immutable media for critical operations [4]. A family office should classify trust deeds, mandates, account data, legal records, policies, contact lists, asset registers, tax records, passwords and cryptographic keys by criticality.

Backups should be encrypted, access-controlled, geographically appropriate and tested. A backup that has never been restored is an unverified control. The office should know the last clean recovery point and the maximum tolerable data loss for each important service.

## 13.3 Communications hierarchy

The office should maintain primary, secondary and out-of-band channels. The crisis team needs an offline contact list and pre-agreed identity challenge. Messages should distinguish verified facts, decisions, actions, owners and next update times.

Public or family communications should be approved. Investment positions, travel details and security arrangements should remain confidential. Misinformation should be corrected through a single verified source, not amplified through broad forwarding.

# 14. THIRD-PARTY AND CONCENTRATION RISK

## 14.1 The extended service chain

Critical services may depend on banks, custodians, administrators, trustees, law firms, accountants, tax advisers, cloud providers, identity platforms, telecom operators, insurers, brokers, market-data vendors, property managers, travel providers and security firms. Each provider may depend on further parties.

The map should focus on services whose disruption could breach an impact tolerance. The FSB toolkit provides a proportionate lifecycle approach: identify critical services, perform due diligence, set contractual expectations, monitor, manage incidents and plan exit [8].

## 14.2 Contract and service evidence

For each critical provider, the office should know the contracting entity, service scope, data location, support hours, incident-notification terms, subcontracting, audit information, recovery commitments, termination rights, data return and tested alternative. Contractual rights do not establish operational capacity; testing is required.

## 14.3 Concentration dashboard

The dashboard should show services by provider, location, technology and authorised person. It should highlight a provider supporting several services, a cloud region supporting several applications, a bank supporting several entities or a principal whose approval is required across the estate.

The 90 per cent warning should be calculated for each dependency category. Examples include the share of urgent payments requiring one person, the share of liquid assets at one custodian, the share of critical applications using one identity provider or the share of family members relying on one travel route. These are management calculations, not external benchmarks.

# 15. CRISIS GOVERNANCE AND COMMAND

## 15.1 Roles before events

The crisis structure should include an accountable principal or board sponsor, incident commander, family-safety lead, treasury lead, investment lead, operations and technology lead, legal and compliance lead, insurance lead and communications lead. One person may hold several roles in a small office; deputies and conflicts must be documented.

The incident commander coordinates. Specialist owners retain accountability for decisions within their authority. The plan should state who may declare an incident, activate alternate authority, pause trading, approve emergency spending, communicate externally and close the incident.

## 15.2 Decision log

Every material decision should record time, verified facts, assumptions, options, advice, authority, decision, owner and next review. A concise log supports continuity across shifts and creates evidence for boards, trustees, insurers, banks and regulators.

Information should carry a source and timestamp. Government advice, bank notices, custodian confirmations and insurer instructions should be distinguished from media reports and management scenarios. Where a fact cannot be verified, the team should record the uncertainty and the decision's sensitivity to it.

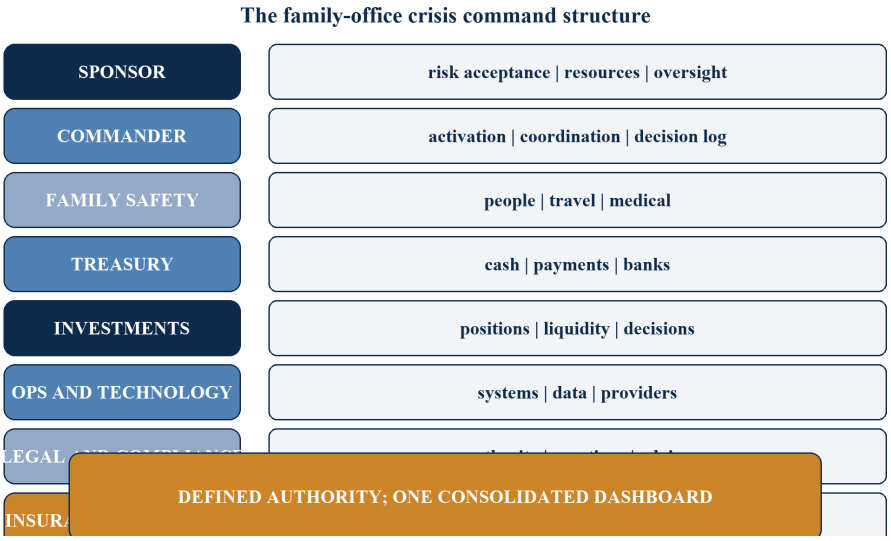
## 15.3 Meeting rhythm

The first hours may require frequent short calls. A prolonged event needs a sustainable rhythm. The command team should separate safety, operations, investments and communications while maintaining one consolidated dashboard. Each meeting should end with actions, owners, deadlines and the next checkpoint.

## 15.4 Authority succession

Succession should cover directors, trustees, protectors, signatories, investment committee members and technology administrators. It should respect governing documents and law. Emergency convenience cannot create authority that the structure does not grant.

**Figure 8. The family-office crisis command structure.**



# 16. A HYPOTHETICAL FAMILY-OFFICE STRESS TEST

## 16.1 Model facts

This case is hypothetical and simplified. It illustrates method and does not describe any client, family, return expectation or current event. The office oversees 100 units of capital: 45 units of listed securities, 25 of private funds, 10 of operating businesses, 10 of real assets and 10 of cash and short-duration instruments. Two family branches live in the UAE; family members and advisers also operate from the United Kingdom and continental Europe.

Ninety per cent of urgent payment authority depends on three UAE-based individuals. Eighty units of assets sit with one global custodian, although several markets use different sub-custodians. Six of eight critical applications use one identity provider. Travel management, insurance broking and physical security are each concentrated with one provider. These percentages are hypothetical concentration inputs.

Thirty-day obligations total 5.5 units: 1.0 for family and medical reserves, 0.8 for payroll and operations, 1.2 for tax and debt, 1.5 for committed investments and 1.0 for contingent margin or operating-company support. Only 3.0 units are immediately accessible through independently authorised routes at the start of the test.

## 16.2 Scenario results

| Scenario | Initial vulnerability | Control introduced | Residual limitation |
|---|---|---|---|
| 72-hour escalation | travelling signatory; urgent family payments | alternate mandate, verified callback and local reserve | bank limits and beneficiary controls remain |
| 30-day disruption | 2.5-unit liquidity gap | four-horizon ladder and documented replenishment | asset-sale timing and market value remain uncertain |
| Custodian-access outage | one portal and one administrator | alternate device, manual instruction and independent position file | sub-custody and market closure remain external |
| Compound cyber event | shared identity provider | isolated break-glass accounts and offline recovery material | secure use requires training and monitoring |
| Travel interruption | one provider and incomplete family data | controlled register, secondary provider and approval matrix | routes and official advice remain dynamic |

## 16.3 Risk-adjusted interpretation

The model should not assume every alternative works at the same time. The office assigns a management-estimated probability of availability to each route and tests failure of the primary and one alternative together. It also applies time to access, legal restrictions, transaction limits and human capacity.

The exercise reveals that balance-sheet liquidity and operational liquidity are different. Ten units of cash exist, but only three units are accessible through independent authority. The solution may involve authority, account structure, reserve location and testing rather than holding more cash.

## 16.4 Board decisions

The board approves a minimum 30-day accessible reserve, a second independent approval route, an offline custody file, alternate identity access, a policy-notification protocol, a controlled family register and quarterly scenario tests. It records the remaining concentrations and funds remediation.

# 17. TESTING THE SYSTEM

## 17.1 Test types

The programme should progress from document review to tabletop exercise, communication drill, payment test, system failover, data restoration, custodian instruction, claims notification and multi-provider simulation. FCA observations encourage testing that increases severity and incorporates third parties [10].

Tests should use real people, current contact details and controlled low-value transactions where possible. They should record start time, completion time, failed steps, workarounds, control breaches, decisions and evidence. A test is incomplete until remediation has an owner and deadline.

## 17.2 Core exercises

The emergency-contact drill verifies every principal, dependent and critical staff member through primary and alternate channels. The payment drill sends a low-value instruction through the alternate bank or manual route and reconciles it. The custody drill retrieves positions, issues an authorised instruction and confirms settlement. The cyber drill restores selected critical records into an isolated environment. The insurance drill prepares a compliant notice from offline records without submitting a fictitious claim.

The travel drill tests itinerary changes against current official advice, entry documents, medical needs, insurer requirements and verified provider capacity. No person should undertake unsafe travel merely to complete an exercise.

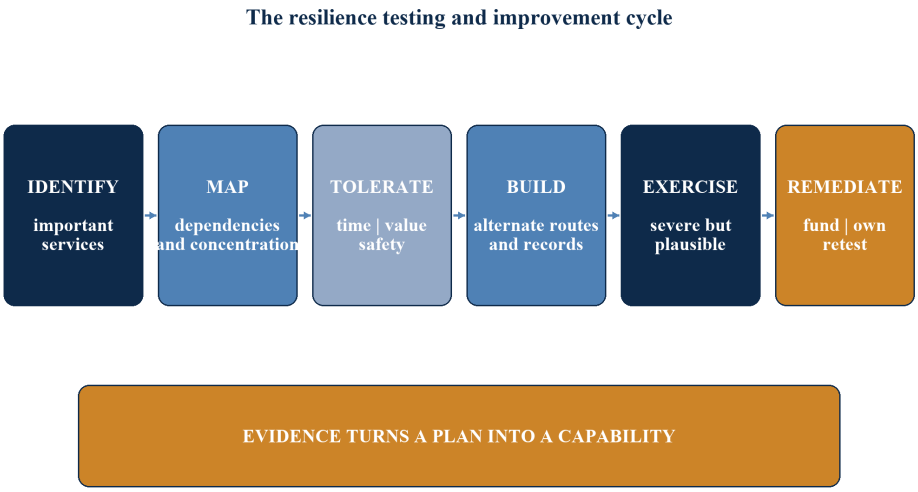
## 17.3 Metrics

Metrics should include impact-tolerance compliance, people confirmed, payments completed, data age, failed authentications, unresolved exceptions, policy-notification time, decision-log completeness and third-party response time. The dashboard should show trend and evidence date.

## 17.4 Lessons and investment

Post-exercise review should identify common-mode failures and fragile manual workarounds. The board should prioritise remediation by potential harm and proximity to tolerance. Technology expenditure should follow the service and dependency map.

**Figure 9. The resilience testing and improvement cycle.**



# 18. A 90-DAY IMPLEMENTATION PROGRAMME

## 18.1 Days 1 to 15: establish the mandate

Appoint the board sponsor and programme owner. Define the scope of family, entities, offices and important services. Approve information classification and privacy rules. Record current regional, travel, sanctions and operational sources that will be monitored.

## 18.2 Days 16 to 30: map services and dependencies

Describe service outcomes and harms. Map people, processes, technology, facilities, information and third parties. Identify common providers, locations, identity systems, signatories and records. Build the concentration dashboard and record missing evidence.

## 18.3 Days 31 to 45: set tolerances and scenarios

Approve time, value, volume, safety and control tolerances. Design 72-hour, 30-day, 90-day and compound cyber scenarios. Record each hypothetical assumption and the decisions it will test.

## 18.4 Days 46 to 60: build alternatives

Complete the liquidity ladder, custody access plan, payment queue, insurance register, family and staff register, communications hierarchy, crisis roles and authority-succession review. Negotiate missing provider information and test low-value alternate transactions.

## 18.5 Days 61 to 75: exercise

Run contact, payment, custody, cyber restoration, insurance and travel exercises. Include critical third parties where practical. Record failures, evidence and residual limitations.

## 18.6 Days 76 to 90: remediate and approve

Fund priority remediation. Update mandates, contracts, reserves, access, data and training. The board approves the service inventory, tolerances, scenarios, crisis structure, residual risks and next test schedule.

# 19. LIMITATIONS AND CONCLUSION

This paper provides an operational-resilience framework based on official sources available at the publication date. It is not legal, regulatory, tax, investment, insurance, aviation, maritime, security, medical, sanctions, cyber or travel advice. Government guidance, sanctions, routes, insurance terms, payment conditions and institutional capacity can change without notice.

The EIA data demonstrate the Strait's material role in energy trade [1,2]. They do not establish the probability, duration or operational effect of a future disruption. The stress scenarios and case values are hypothetical and simplified. Every family office should calibrate them to actual people, assets, entities, jurisdictions, obligations and providers.

Operational resilience is a governance capability. A diversified portfolio can still depend on one corridor of authority, access and information. The service map makes that corridor visible. Impact tolerances define the point of unacceptable harm. The custody plan, liquidity ladder, insurance register, travel matrix, cyber controls and third-party alternatives create recovery routes.

The practical standard is evidence. The office should be able to show who can act, which service must continue, how long disruption is tolerable, which dependencies support the service, which alternative was tested, what limitation remains and when the board will review it. This discipline protects people and capital while preserving lawful, controlled decision making.

# APPENDIX A. IMPORTANT-SERVICE REGISTER

For each service, record the outcome, users, harm, owner, regulatory or fiduciary obligations, time tolerance, value tolerance, volume tolerance, safety threshold, data-loss threshold, normal route, degraded route and recovery route. Link every dependency and test result.

The register should distinguish an important service from the resources that support it. Review at least annually and after a material change, incident, provider change, family event or restructuring.

# APPENDIX B. LIQUIDITY-LADDER TEMPLATE

Record obligation, entity, beneficiary, purpose, due date, currency, amount range, priority, legal deadline, normal account, alternate account, normal rail, alternate rail, signatories, evidence, payment limit, expected processing time, replenishment source and owner.

Reconcile the ladder to bank balances, portfolio cash, debt schedules, tax calendars, capital-call notices, payroll and household budgets. Mark every amount as contractual, forecast or management-estimated.

# APPENDIX C. CUSTODY DUE-DILIGENCE QUESTIONS

1. Which legal entity contracts with the client and under which law? 2. How are securities and cash held, recorded and segregated? 3. Which sub-custodians and market infrastructures support material assets? 4. Which liens, set-off rights, cash sweeps or securities-lending terms apply? 5. Who may instruct and through which primary and manual channels? 6. How are identity, callbacks and beneficiary changes verified? 7. What are incident-notification, recovery and escalation arrangements? 8. Can independent position and transaction records reconstruct the account? 9. What is required to transfer assets or cash to another institution? 10. When was each alternate access route last tested?

# APPENDIX D. INSURANCE REGISTER

For each policy, record insurer, insured parties, policy number, period, territories, subject matter, limits, deductibles, key exclusions, notice conditions, broker, claims contact, legal adviser, premium status, current wording location and last coverage review.

Maintain an event evidence checklist for property, cyber, crime, travel, medical, marine, aviation and liability claims where relevant. Obtain advice before drawing conclusions about cause, coverage or notification.

# APPENDIX E. TRAVEL AND FAMILY CONTINGENCY MATRIX

| Dimension | Current evidence | Primary route | Alternate route | Decision owner |
|---|---|---|---|---|
| Location and contact | timestamped confirmation | approved secure channel | out-of-band contact | family-safety lead |
| Documents | passport, visa, residence and consent records | secure digital copy | controlled physical copy | travel lead |
| Medical | conditions, prescriptions and provider contacts | local care plan | adviser-approved alternative | medical coordinator |
| Transport | confirmed commercial itinerary | verified rebooking | qualified alternative provider | travel lead |
| Funding | cards, account and local reserve | normal bank route | approved alternate route | treasury lead |
| Insurance | current travel and medical wording | broker confirmation | documented self-funding limit | insurance lead |

# APPENDIX F. FIRST-24-HOURS CHECKLIST

1. Verify the event through official and institutional sources. 2. Declare the incident at the approved level and open the decision log. 3. Confirm family, staff and critical adviser locations. 4. Establish primary and alternate communications. 5. Confirm urgent payments, cash, collateral and settlement obligations. 6. Contact banks, custodians, insurers and critical providers through verified details. 7. Preserve sanctions, fraud and dual-approval controls. 8. Review travel and shelter decisions against current official advice. 9. Issue a concise verified update with actions, owners and next review time. 10. Reconcile every manual or degraded transaction.

# APPENDIX G. QUESTIONS FOR ADVISERS AND PROVIDERS

1. Which entities and activities fall within a regulated perimeter? 2. Which fiduciary duties constrain emergency delegation and investment action? 3. Which bank and custodian authorities remain valid when people or offices move? 4. Which payment, sanctions and source-of-funds evidence should be prepared in advance? 5. How are client assets, cash and collateral held through each custody layer? 6. Which policy terms apply to war, terrorism, political violence, cyber, travel and business interruption? 7. What notices must be given, by whom and within which period? 8. Which data may be stored, accessed or transferred across jurisdictions? 9. Which travel and security providers are qualified, insured and currently authorised? 10. Which common third-party and technology dependencies remain unresolved? 11. Which tests can providers join, and what evidence will they supply? 12. Which residual risks require board acceptance or funded remediation?

# REFERENCES


[1] US Energy Information Administration. *World Oil Transit Chokepoints.* Updated 2026. https://www.eia.gov/international/content/analysis/special_topics/World_Oil_Transit_Chokepoints/

[2] US Energy Information Administration. *Amid regional conflict, the Strait of Hormuz remains critical oil chokepoint.* 16 June 2025. https://www.eia.gov/todayinenergy/detail.php?id=65504

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

[4] Bank for International Settlements. *ORR20: Operational resilience.* 2026 consolidated guidance. https://www.bis.org/basel_consolidated_guidelines/chapter/ORR/20.htm

[5] Bank for International Settlements. *ORR30: Third-party risks.* 2026 consolidated guidance. https://www.bis.org/basel_consolidated_guidelines/chapter/ORR/30.htm

[6] Bank for International Settlements. *LQY10: Liquidity risk management and supervision.* 2026 consolidated guidance. https://www.bis.org/basel_consolidated_guidelines/chapter/LQY/10.htm

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

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

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

[10] 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

[11] Financial Conduct Authority. *Outsourcing and operational resilience.* Updated 14 July 2026. https://www.fca.org.uk/firms/outsourcing-and-operational-resilience

[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] Central Bank of the UAE. *Payment System Supervision.* https://www.centralbank.ae/en/our-operations/supervision/payment-systems-supervision/

[15] Central Bank of the UAE Rulebook. *Article 8: Ongoing Requirements of Designated Retail Payment Systems.* https://rulebook.centralbank.ae/en/rulebook/article-8-ongoing-requirements-designated-retail-payment-systems

[16] Central Bank of the UAE. *Aani Delivers a Transformational Leap in the UAE's Digital Payments Landscape.* 10 April 2026. https://www.centralbank.ae/en/news-and-publications/news-and-insights/press-release/aani-delivers-a-transformational-leap-in-the-uae-s-digital-payments-landscape-12-5-million-users-and-instant-transfers-in-3-seconds/

[17] UK Foreign, Commonwealth & Development Office. *United Arab Emirates travel advice.* Updated 24 July 2026. https://www.gov.uk/foreign-travel-advice/united-arab-emirates

[18] UK Foreign, Commonwealth & Development Office. *United Arab Emirates: safety and security.* https://www.gov.uk/foreign-travel-advice/united-arab-emirates/safety-and-security

[19] UK Foreign, Commonwealth & Development Office. *If you are affected by a crisis abroad.* https://www.gov.uk/guidance/how-to-deal-with-a-crisis-overseas

[20] UK Foreign, Commonwealth & Development Office and Office of Financial Sanctions Implementation. *Iran sanctions: statutory guidance.* Updated 1 May 2026. https://www.gov.uk/government/publications/iran-sanctions-guidance/iran-sanctions-guidance

[21] Financial Action Task Force. *High-Risk Jurisdictions subject to a Call for Action.* 24 October 2025. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2025.html

[22] Financial Action Task Force. *Guidance on Countering Proliferation Financing.* https://www.fatf-gafi.org/en/publications/Financingofproliferation/Guidance-counter-proliferation-financing.html

[23] Financial Action Task Force. *Guidance on Proliferation Financing Risk Assessment and Mitigation.* https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

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

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

[26] 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

[27] 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

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

[29] International Civil Aviation Organization. *Middle East Regional Office.* https://www.icao.int/MID

[30] United Nations Security Council. *United Nations Security Council Consolidated List.* https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list

[31] Central Bank of the UAE. *2024 Financial Stability Report.* Published 2026. https://www.centralbank.ae/media/4iznakgl/cbuae-issues-2024-financial-stability-report-en.pdf

# ABOUT THE AUTHOR

Chennakeshav Adya is an independent researcher whose work examines capital, ownership, governance and cross-border decision making. His research converts complex legal, financial and institutional frameworks into practical tools for principals, family offices, investors and management teams.

Authored by Chennakeshav Adya

Independent Researcher