FAMILY OFFICE BLUEPRINT

November 2019

IDEAS | PEOPLE | TRUST

BDO

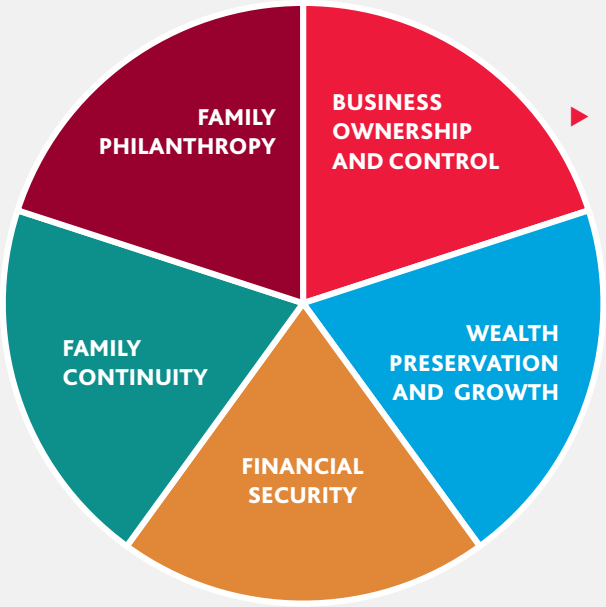
RISK MANAGEMENT IN THE FAMILY OFFICE

Establishing a family office is a significant step towards preserving and growing wealth for future generations. In this report we examine the rationale behind a family office, people and governance, risk and reputation management.

Throughout the report, we define a single family office as a private wealth advisory operation established by the family to oversee the management and administration of the family's assets and investments, with the objective of preserving and growing wealth for the next generations. Family offices also typically advise on tax, legal, financial reporting, real estate, philanthropy and banking issues.

COMMON GOALS OF FAMILY OFFICES

Most families of wealth who want to preserve their assets for future generations work together to accomplish one or more of five common goals.



- Create Impact and Rewards from Shared Giving
- Maintain Family Control of Enterprises
- Identify, Embrace and Convey Family Values and Aspirations
- Sustain Purchasing Power across Generations
- Secure Family Lifestyles during Generational Wealth Transfers

In our experience, the nexus of a family office is often the private office within a successful family business, typically where the family wish to clearly segregate their business interests from their family wealth. Some are established when there has been a liquidity event such as the sale of the core family business, and some have their origins in a fund management business which has closed its doors to outside investors.

Many commentators refer to a minimum value of assets under management to justify establishing a family office, however in practice the decision to proceed is usually driven by much more than economics:

- Building an enduring legacy
- Managing family succession
- Privacy and data security
- Reputation risk
- Family governance
- Managing direct private equity
- Co-investment opportunities
- Family philanthropy
- Regulatory pressures
- Cyber security
- Risk management
- Economies of scale.

PEOPLE

The family office business model will determine its staffing requirements, but a fully insourced model for a complex investment office could involve:

Oversight

Family, Trustees, Non-Executives

Executive

CEO, CFO, CIO, CRO, CTO

Front office

CIO, Trading team

Middle office

Banking and settlements team, investment analysts, PE and Hedge Funds team

Back office

CFO, Finance team

IT

CTO, IT team

Risk and compliance

CRO, risk management, legal, tax and regulatory team

Philanthropy

Philanthropy team

GOVERNANCE

Governance is fundamentally important to financial performance and security in the family office, since it will set the tone for a culture of risk management throughout the organisation. Key considerations include:

Oversight	A family office oversight board typically includes family members, their trustees, non-executives and close professional advisers. The primary roles (some of which are often delegated to an investment advisory board) include approval of asset allocation and major direct investments, appointment of senior management, remuneration, distributions and oversight of key risk management controls
Legal structure	A family office will typically be incorporated as a private company or a limited liability partnership, and the constitution will determine the powers and duties of the partners, directors and investors. The family office will usually have an advisory or management agreement with investment asset owning entities (companies or limited partnerships) which hold the family wealth. In some cases the family office will act as general partner of asset owning partnerships.
Management	The management board typically comprises the CEO and the functional leaders (CIO, CFO, CRO, CTO, etc) and the board will take primary responsibility for strategic planning, asset allocation, budgeting, operations and the design and operation of risk management controls.
People	Good governance requires clear responsibilities and reporting lines. The management board will establish vetting procedures, compliance and whistleblowing procedures designed to embed a culture of risk compliance.
Regulation	Many family offices are supervised to some degree by their national financial services regulator, and compliance with financial regulation is a key reputation risk objective. In today's globally regulated business environment, registration can reduce anti-money laundering compliance fatigue, and provide privileged access to premium investment products.
Investment management	Our analysis of risk management below explores the design and operation of key controls to mitigate principal risks including breach of mandate, unauthorised trading, failed trades, uncollected income, incorrect financial reporting, subscription and distribution errors, counterparty failure, beneficial ownership risks, cyber risks and business continuity.
Privacy and cyber security	Family offices are natural targets for cyber criminals since they typically manage high value, transferrable assets but they don't always have the security infrastructure typically seen in a bank. Our analysis of risk management below discusses the design and operation of cyber controls, including security protocols surrounding authorisation of instructions to the custodian, sensible and proportionate restrictions over data storage on public cloud services, and penetration testing.
Business resilience	Many family office business continuity and disaster recovery plans rely heavily on the recovery of data from the custodian. What is often missing is a plan for the effective recovery of a secure communications channel between the family office and the custodian.
Outsourcing	Investment management functions are often outsourced to third party managers, custodians and fund administrators. In these circumstances, the family office will exercise its oversight functions through monitoring compliance with the investment mandates and the custody agreements.
Assurance	Most investment managers, custodians and fund administrators will engage independent auditors to report on the description, design and operating effectiveness of controls which they operate (SOC Type 2 Report) and such reports will assist family offices in their oversight of managers, custodians and administrators.

RISK MANAGEMENT IN THE FAMILY OFFICE

The central purpose of a family office is to manage family wealth for current and future generations, and wealth protection through effective risk management is right at the heart of that agenda.

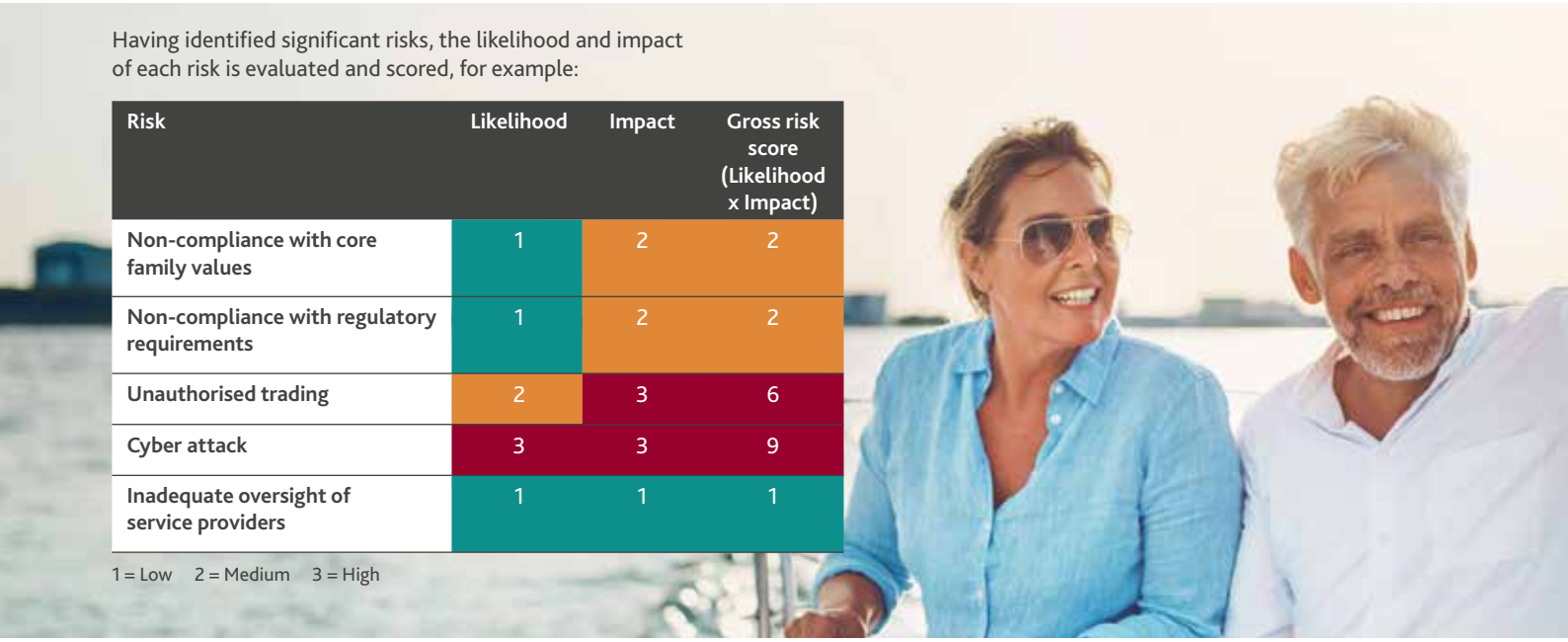
Effective risk management in the family office starts with identifying significant risks, for example:

Segment	Risk categories	Examples of principal risks
People	Values Performance Remuneration	Non-compliance with core family values such as integrity, quality, social responsibility and diversity
Governance	Regulatory Tax Oversight Privacy	Non-compliance with regulatory requirements, causing reputational damage and financial penalties
Trading operations	Rogue trader Beneficial ownership Performance	Unauthorised trading, leading to financial loss
Financial reporting	Valuation Completeness Disclosure	Fraud and error in financial reporting, leading to financial loss
Technology	Cyber security GDPR Business continuity	Cyber-attack leading to financial loss
Outsourcing	Custodians Administrators Brokers	Inadequate oversight of service providers, leading to financial loss

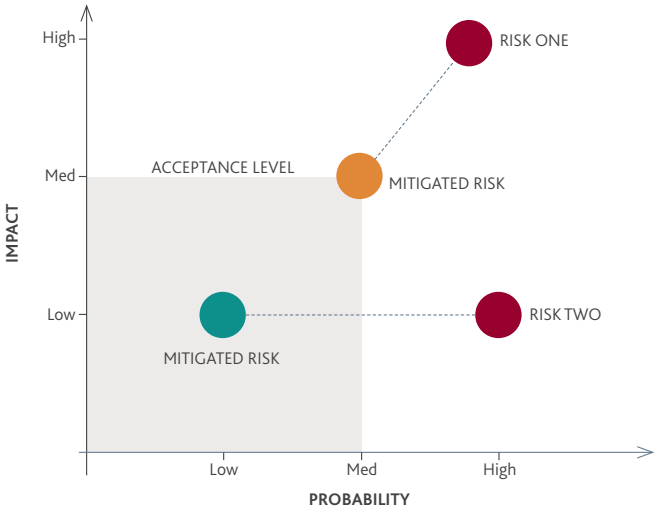
Having identified significant risks, the likelihood and impact of each risk is evaluated and scored, for example:

Risk	Likelihood	Impact	Gross risk score (Likelihood x Impact)
Non-compliance with core family values	1	2	2
Non-compliance with regulatory requirements	1	2	2
Unauthorised trading	2	3	6
Cyber attack	3	3	9
Inadequate oversight of service providers	1	1	1

1 = Low 2 = Medium 3 = High



The family office will design mitigating controls to reduce the likelihood and impact of identified risks:



Mitigating controls are then mapped against the risks in a matrix of risks and controls, to identify the net risk score, for example:

Risk	L	I	Gross risk	Mitigating controls	L	I	Net risk
Non-compliance with core family values	1	2	2	Due diligence on new employees	1	2	2
Non-compliance with regulatory requirements	1	2	2	Independent regulatory assessment	1	2	2
Unauthorised trading	2	3	6	Authorisation protocols, trading limits, automated alerts, settlement on a delivery versus payment basis	1	3	3
Cyber attack	3	3	9	Cyber consultants review, penetration testing, Cloud restrictions	2	3	6
Inadequate oversight of service providers	1	1	1	Review of SOC 2 reports	1	1	1

L=Likelihood I=Impact
1 = Low 2 = Medium 3 = High

The matrix of risks and controls enables the family office to focus attention on high risk areas and key mitigating controls. Ideally, the design and implementation of key controls will be assessed by management and tested by independent auditors.

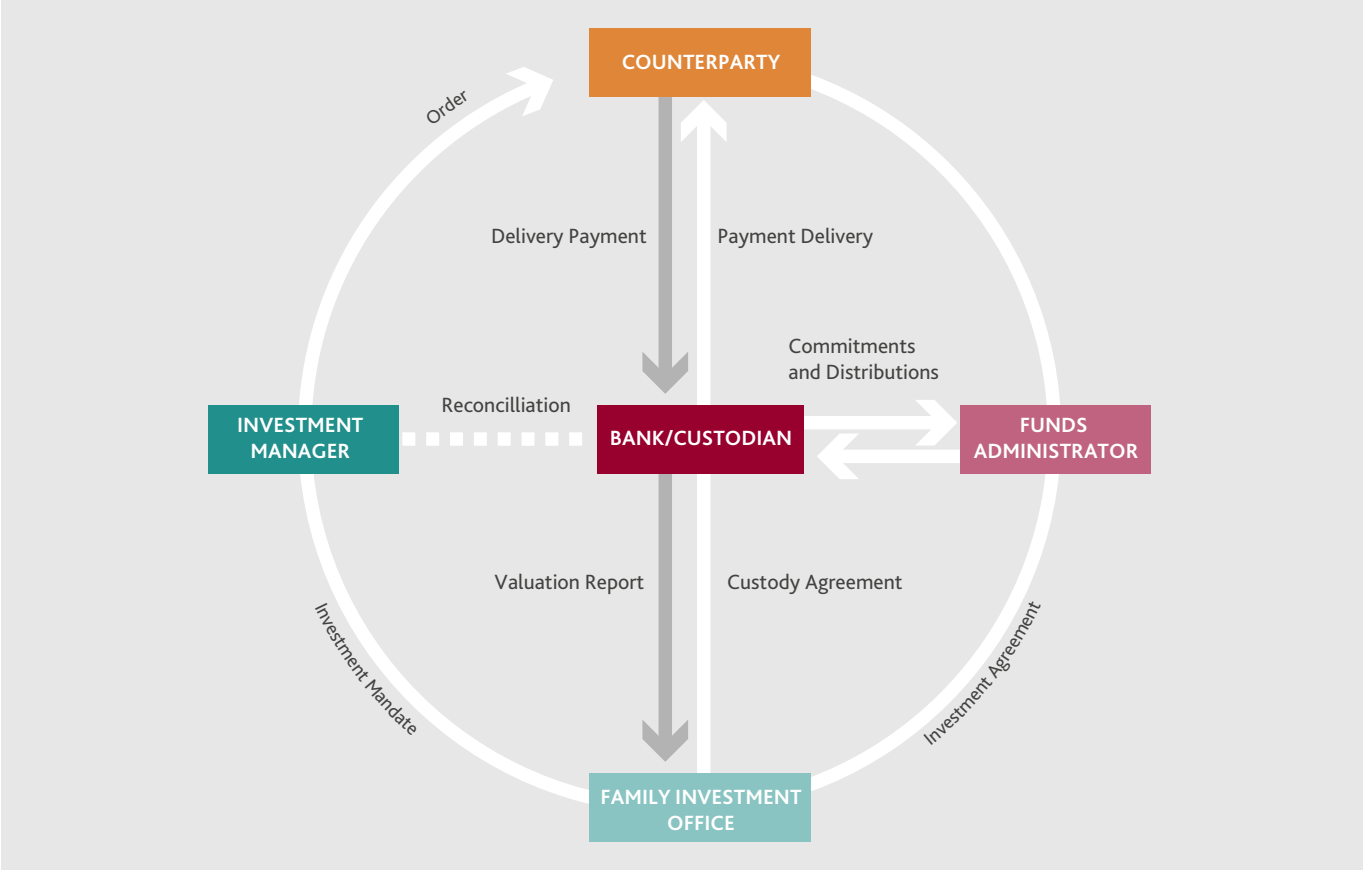
High level controls around governance and oversight risks will always be critical. It is likely that the matrix of risks and controls will highlight investment trading risks as high risk areas because of their financial impact. Our analysis of our clients' investment risk management priorities highlights the following top three risk management priorities for family investment offices:

- Operational design
- Operational due diligence
- Cyber security.

OPERATIONAL DESIGN

Family investment office business models range from fully outsourced models, where investment management, treasury, funds administration and custody functions are outsourced to third parties, to in-house models where the family office has its own trading function, treasury and settlements team.

A typical outsourced model is summarised:



In this model, the family office acts solely as a limited partner, effectively outsourcing most risk management functions to external investment managers, custodians and administrators. Typically, the investment manager will implement its own controls designed to mitigate key risks such as breach of mandate, unauthorised or failed trades. The custodian will implement key controls such as:

- SWIFT settlement on a delivery versus payment (dvp) basis
- Matching trade orders to confirmations
- Reconciliation between depository, custodian and manager
- Building anticipated income models and analysing variances between actual and predicted income
- Automated pricing feeds
- Credit ratings
- Cyber security controls
- Business continuity and disaster recovery.

Fund administrators will operate key controls such as:

- Pricing models
- Fund level financial reporting and performance measurement
- Monitoring capital commitments, subscriptions and distributions.

The family office will typically exercise an oversight role, including high level risk management controls such as:

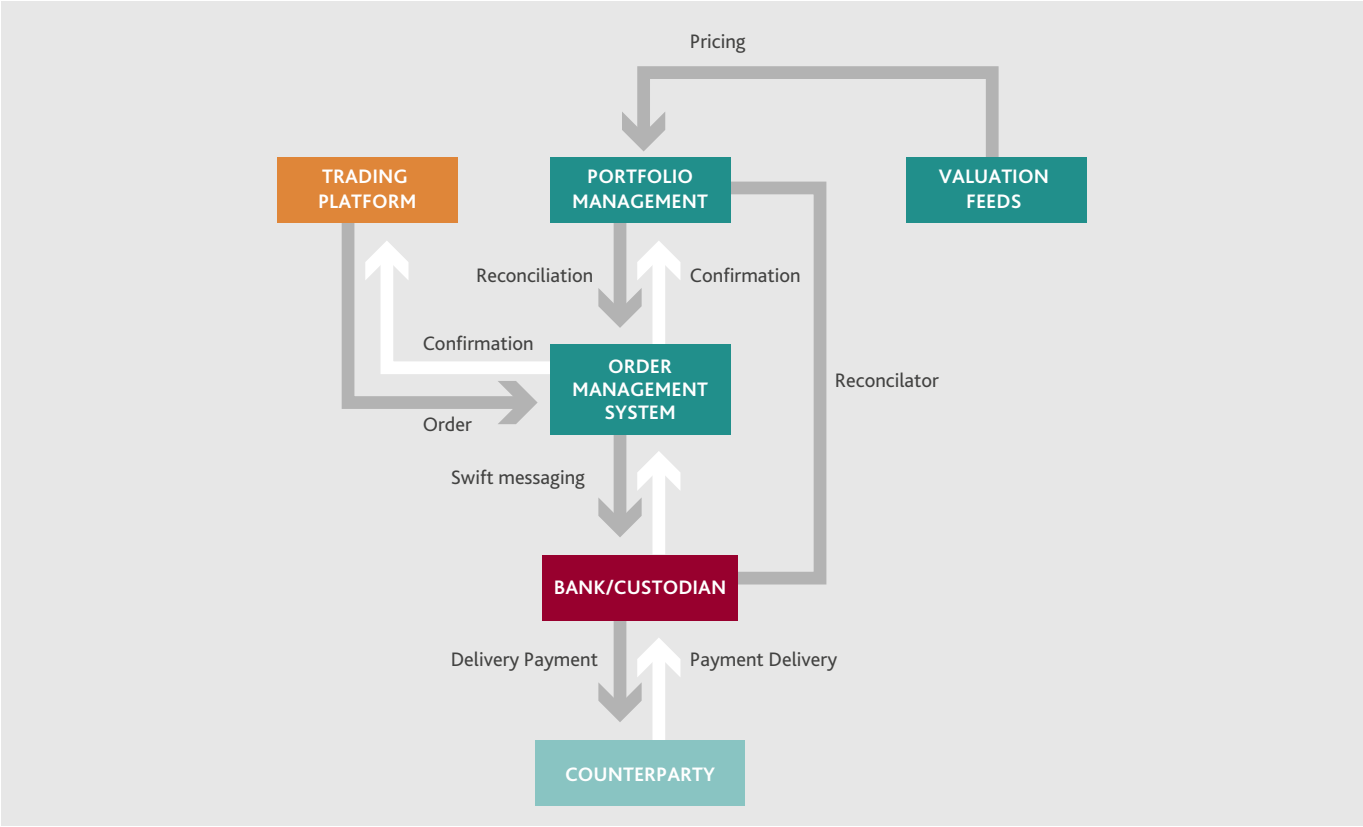
- Asset allocation
- Operational due diligence
- Portfolio-level financial reporting and performance management
- Investment mandate, custody agreements
- Compliance monitoring.

Most investment managers, custodians and fund administrators will engage independent auditors to report on the description, design and operating effectiveness of controls which they operate (SOC Type 2 Report) and such reports will assist family offices in their oversight of managers, custodians and administrators.

To summarise the principal risk management controls under the fully outsourced model:

Risk	Family office	Investment manager	Custodian	Fund administrator
Investment manager breaches mandate	Operational due diligence Investment mandate Compliance monitoring	Hard-wired order management system Compliance monitoring	Compliance monitoring	Compliance monitoring at fund level
Unauthorised trade	-	Hard-wired order management system Compliance monitoring	SWIFT settlement controls Matching order to confirmation	Compliance monitoring at fund level
Failed trade	-	Reconciliation	Reconciliation Matching order to confirmation	Compliance monitoring at fund level
Uncollected income	-	-	Anticipated income models Variance analysis	Compliance monitoring at fund level
Valuation error	Compliance monitoring	-	Pricing feeds Variance analysis	Valuation modelling
Incorrect financial reporting	Portfolio level financial reporting and performance measurement	-	-	Fund level financial reporting and performance measurement
Subscription and distribution error	Compliance monitoring	-	-	Monitoring capital commitments, subscriptions and distributions
Counterparty failure	Compliance monitoring	-	Rating feeds Risk limits	Compliance monitoring at fund level
Beneficial ownership	Custody agreement Custodian confirmation	-	Depository confirmation Reconciliation	Compliance monitoring at fund level
Cyber risks	Penetration testing Automated alerts	Penetration testing Automated alerts	Penetration testing Automated alerts	Penetration testing Automated alerts
Business continuity	Disaster recovery and business continuity programme	Disaster recovery and business continuity programme	Disaster recovery and business continuity programme	Disaster recovery and business continuity programme

A typical insourced model is summarised:



In this model, risk management controls are built into the front office and back office. Typically, the front office trading platform will include controls such as:

- access restrictions
- authorisation protocols
- trading limits (value, volume, rating, etc)
- alerts for unusual trading patterns
- validation checks to eliminate "fat finger" input errors.

An order management system tracks buy and sell orders placed in the front office, and matches orders to trade confirmations received directly from counterparties. Validation routines such as authorisation protocols and alerts for compliance breaches are designed to detect trading errors and unauthorised trading. Settlement instructions are then generated for validated transactions, typically using the SWIFT messaging platform, on a dvp basis. Failed trades will be highlighted and resolved.

Straight Through Processing enables the portfolio management system to be updated for buy and sell transactions directly from the order management system on a trade date basis. The portfolio can be priced in real-time using pricing feeds from market data providers such as Bloomberg or Refinitiv.

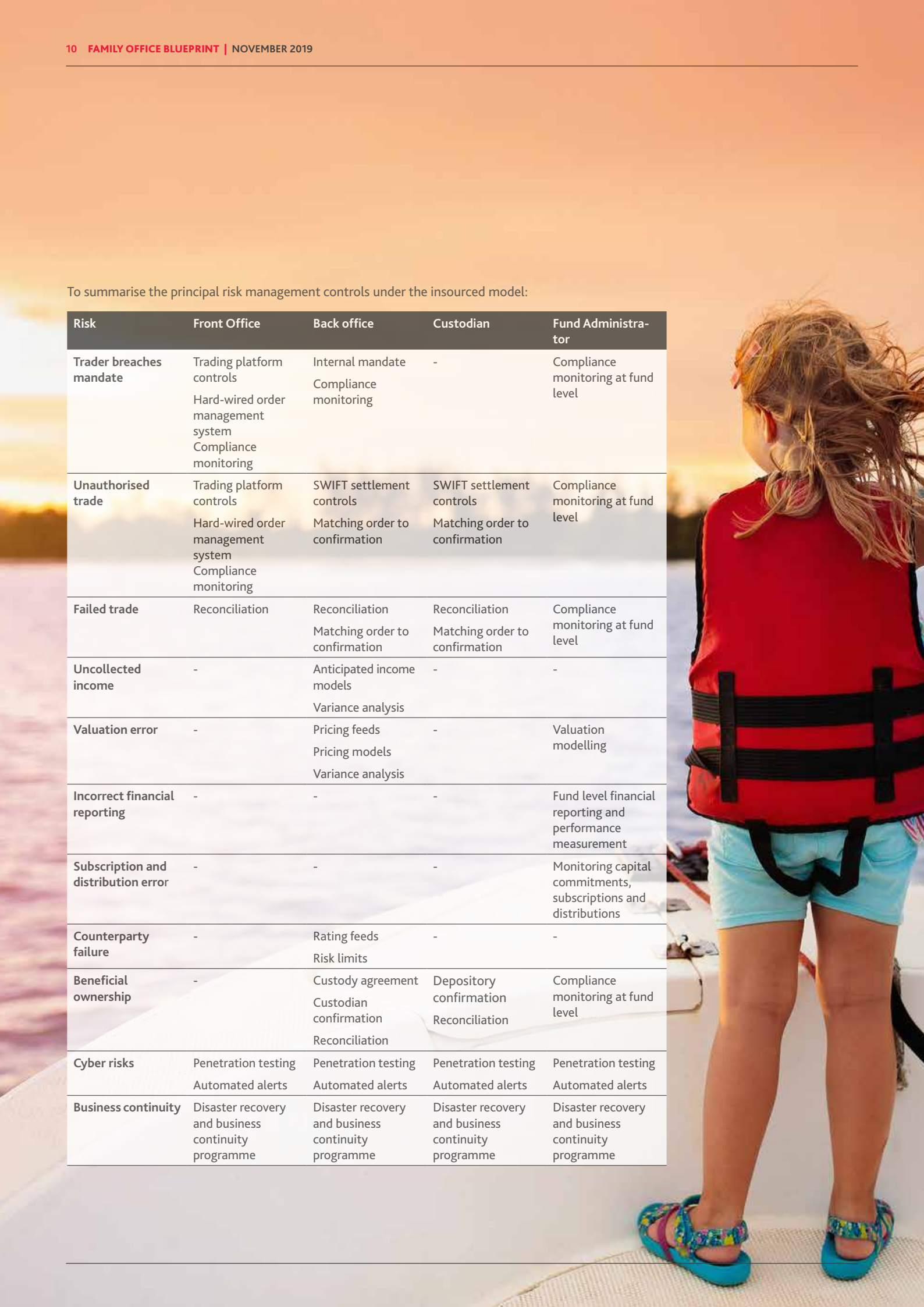
Custodians and fund administrators will still take responsibility for those parts of the control environment delegated to them under the terms of the custody agreement, for example:

- SWIFT settlement controls (custodian interface)
- Matching trade orders to confirmations
- Trade reconciliations
- Reconciliation between custodian records, the family office and depositories
- Fund valuation modelling
- Monitoring capital commitments and fund distributions.

The family office can monitor compliance and performance through regular review meetings with the custodians and fund administrators, and review of documentation such as SOC Type 2 reports.

To summarise the principal risk management controls under the insourced model:

Risk	Front Office	Back office	Custodian	Fund Administrator
Trader breaches mandate	Trading platform controls Hard-wired order management system Compliance monitoring	Internal mandate Compliance monitoring	-	Compliance monitoring at fund level
Unauthorised trade	Trading platform controls Hard-wired order management system Compliance monitoring	SWIFT settlement controls Matching order to confirmation	SWIFT settlement controls Matching order to confirmation	Compliance monitoring at fund level
Failed trade	Reconciliation	Reconciliation Matching order to confirmation	Reconciliation Matching order to confirmation	Compliance monitoring at fund level
Uncollected income	-	Anticipated income models Variance analysis	-	-
Valuation error	-	Pricing feeds Pricing models Variance analysis	-	Valuation modelling
Incorrect financial reporting	-	-	-	Fund level financial reporting and performance measurement
Subscription and distribution error	-	-	-	Monitoring capital commitments, subscriptions and distributions
Counterparty failure	-	Rating feeds Risk limits	-	-
Beneficial ownership	-	Custody agreement Custodian confirmation Reconciliation	Depository confirmation Reconciliation	Compliance monitoring at fund level
Cyber risks	Penetration testing Automated alerts	Penetration testing Automated alerts	Penetration testing Automated alerts	Penetration testing Automated alerts
Business continuity	Disaster recovery and business continuity programme	Disaster recovery and business continuity programme	Disaster recovery and business continuity programme	Disaster recovery and business continuity programme



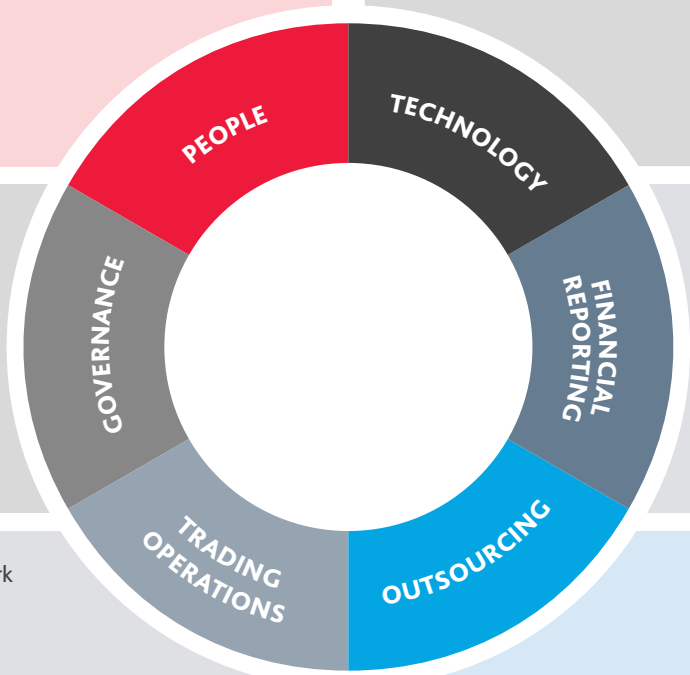
OPERATIONAL DUE DILIGENCE

Any analysis of investment failures over the past decade has consistently highlighted operational issues over and above investment strategy as the root cause of failure. First and foremost are people issues, with regulators around the world taking every opportunity to remind us that the right people, values and culture are the first line of defence against failure.

Most family office investment funds now take pre-investment due diligence on potential fund investments and direct private equity opportunities seriously, often using standardised checklists such as the due diligence questionnaire issued by the Institutional Limited Partners Association (www.ilpa.org) and we look to support our clients on operational due diligence, including:

- analysis of key personnel
- organisational chart
- remuneration structure

- cyber security
- GDPR
- business continuity and disaster recovery



- fund structure
- management structure
- regulatory oversight
- advisory board oversight
- tax and automatic exchange of information
- financial stability

- valuation modelling
- NAV reporting
- internal control over financial reporting
- accounting framework
- policies and procedures
- performance reporting
- benchmarks

- risk management framework
- strategy compliance
- asset allocation

- fund administrators
- custodians
- bankers
- brokers

CYBER SECURITY

Family offices are natural targets for cyber criminals since they typically manage high value, transferrable assets but they don't always have the security infrastructure typically seen in a bank.

Securing digital channels is a complex exercise, and one that draws on a range of governance, risk and assurance capabilities as well as in-depth technical and cyber skills. Regardless of the standards adopted, no-one in the family office can ignore this complex and growing threat. At the very least, clients should:

- educate management and employees on security threats and how to respond to them
- architect your risk, policy, technology and standards environments to help you ensure your business operates according to your risk appetite
- assure your process and technology, giving you independent and timely information on your state of information security compliance
- manage your security operation, making sure you blend education, architecture and assurance in a way that is appropriate to your organisation

Clients will typically appoint a global custodian to handle custody of assets, delivery versus payment, income collection, valuation and reconciliation, and hence benefit from the custodian's security infrastructure, however the appointment of a global custodian does not entirely mitigate cyber security risks:

- clients will want to consider the custodian's own cyber security controls, typically through review of SOC type 2 reports
- the custody agreement will require close review, particularly in areas such as liability in the event of cyber attack, use of sub-custodians, custody mandates, and securities lending
- security protocols surrounding the authorisation of instructions to the custodian, and verification of mandate-holders (for example using SWIFT or call-back procedures)
- controls over changes to authorisation instructions (including physical security over SWIFT keys)
- sensible and proportionate restrictions over data storage on public cloud services
- telephone and mobile device security
- connected systems such as pricing feeds, valuation and performance reporting systems
- in-house trading and investment management controls, or external investment managers' own cyber security controls, again through a SOC type 2 report
- clients will want to understand what third parties are holding data relating to their affairs, and be prepared in the event of a data breach which thrusts the family office into the public eye
- viruses and malware, delivered through email links, public wifi or website visits
- employees emailing sensitive data over a public network without it having been encrypted

Most clients have appointed cyber security consultants to consider cyber vulnerabilities, and in particular carry out penetration testing.

FINANCIAL REPUTATION AND THE FAMILY OFFICE

The days when family offices could rely on private financial data remaining private are long gone, thanks to an expanding data footprint, cyber-attacks, leaks and malignant journalism. The public debate on financial reputation has shifted from the established media to fast-moving social media, polarised blogs and online forums, providing the rocket fuel to burn a cherished reputation.

A string of well publicised leaks and scandals, including the Panama papers, has highlighted the need for family offices to protect the family from the stigma of financial scandal. We examine the principal reputation issues surrounding tax transparency, regulation, automatic exchange of information, philanthropy, privacy and data security.

TAX TRANSPARENCY AS THE NEW PARADIGM

Under the new paradigm, high net worth families are expected to carry out their affairs in a fully tax-transparent manner, and many family office clients have restructured their affairs to eliminate opaque structures. For example:

- Unwelcome and often misguided news – or fake news – has led many people to associate trusts with tax evasion, secrecy, greed and grand crimes. For this reason clients are considering alternative enduring asset holding vehicles such as family limited partnerships, which can be designed to provide similar levels of protection, stewardship and governance, whilst being transparent for tax purposes, with considerable flexibility to allocate profits across generations. For example, a family limited partnership can be designed so that parents retain voting control over investment policy and distributions, but the next generation are incentivised to generate family wealth through a variable share of profits.
- Complex offshore structures are regarded as a red flag for bank risk compliance, adding additional layers of due diligence and anti-money laundering fatigue. For this reason we are often instructed to consider onshore structures only, and only those in jurisdictions which participate in Automatic Exchange of Information.
- Ownership of UK residential property through offshore structures is discouraged through a broad range of tax changes including the introduction of the Annual Tax on Enveloped Dwellings, higher rates for stamp duty land tax and bringing the asset within scope for inheritance tax. In many cases clients prefer to own such property in their own name.

REGULATION

Regulatory problems are to be avoided at all costs ! The UK Financial Conduct Authority is not actually that interested in single family offices since they do not act for the public and hence carry little or no public interest. However there could well be a valid reason or obligation to register with the FCA:

- A single family office can easily stray into regulated areas, for example when co-investing with other family offices
- Many family offices have welcomed registration, in the same way as they have welcomed classification as a financial institution under FATCA or the Common Reporting Standard (CRS), since registration has considerably reduced anti-money laundering fatigue, and ultimately provided privileged access to a wider range of investment products.

AUTOMATIC EXCHANGE OF INFORMATION

The introduction of FATCA and the CRS has accelerated the march towards transparency. Whilst tax data exchanges are restricted to the tax authorities, financial institutions, individuals and their advisers, and as such are not available to the public, the regulations have discouraged banks from dealing with opaque structures in order to avoid damage to their own reputation, exposure to regulatory issues, fines and penalties. Many banks have simply stopped dealing with corporate customers registered in non-participating countries, and have closed whole swathes of customer accounts based on risk-profiling.

PHILANTHROPY

In order to protect donors from reputation risks, many family offices carry out extensive due diligence on potential beneficiaries, and on-going assurance programmes directed towards giving some assurance on the effective use of philanthropic funds. Key issues to consider are:

- Identity of beneficiaries
- Management and governance
- Undisclosed related parties
- Solvency
- Impact and effective use of funds.

CRISIS MANAGEMENT

Crisis response is often a defining moment in a family's reputation and for this reason many clients engage crisis consultants to analyse:

- crisis preparedness
- crisis management planning, training and testing
- live crisis PR support
- post crisis review and recovery.

FOR MORE INFORMATION:

Mark McMullen
+44 (0)20 3860 6036
mark.mcmullen@bdo.co.uk

www.bdo.co.uk

42003153