SQUIRE PATTON BOGGS

Family Office Insights

Managing Family Office AI Risk

July 2026

Introduction

Artificial intelligence (AI) is rapidly becoming embedded in family office technology infrastructure and increasingly shaping how family offices operate. Across the sector, principals are seeking greater efficiency, improved decision quality and more effective systems to navigate an increasingly dynamic and complex investment and operational environment.

When appropriately deployed, AI can streamline processes, enhance the synthesis of complex information and improve responsiveness across lean teams. More fundamentally, AI has the potential to strengthen decision-making, particularly in environments where information is fragmented, workflows are distributed and institutional knowledge is not always formally captured.

However, family offices operate in a highly sensitive environment, where confidentiality, discretion and trust are paramount. At the same time, AI introduces a range of new and evolving risks. Threat actors, too, are also beginning to make increasingly sophisticated use of AI to target vulnerable high-value targets. As AI adoption accelerates, the central challenge is therefore no longer whether AI can deliver productivity gains, but how those gains can be realized within a controlled and risk-aligned framework. In short, the use of AI without appropriate governance and guardrails has the potential to become a significant area of strategic risk for family offices.

Key AI-related risks for family offices

The risks presented by AI in the family office context are not uniform; they will be use-case dependent and may arise across multiple layers, such as technology, data and information security, human resources, third-party relationships and organizational behavior, among others. Fundamental risks that we are increasingly observing include:

- **Model level and operational risks**
  Systemic risks may be baked into AI models themselves and, given the lack of transparency in how AI models behave, the risks may be difficult to detect during routine operations. For example, where AI models are trained on historical data, biases can be embedded that produce systematically skewed outputs.

  Models can also experience drift, whereby performance degrades as underlying data patterns, model behaviors, market dynamics and regulations evolve. Additionally, staff usage may lead to inadvertent prompt injections. Inputs used from third-party materials, such as emails, could be malicious and lead to misleading outputs or even disclosure of sensitive data.

- **Hallucinations and automation bias**
  AI models are known to confidently produce inaccurate information that is not obviously wrong, but convincingly wrong. The quality and clarity of such hallucinations can create a tendency to place undue reliance on them; a phenomenon often described as "automation bias".[1] This can reduce critical scrutiny, particularly where outputs align with pre-existing assumptions, or are produced efficiently relative to traditional methods. In decision-making contexts, such as investment, this creates a risk that AI shifts from being a decision-support tool to an implicit decision driver, without appropriate oversight or challenge.

- **Data exposure and confidentiality risks**
  The use of AI tools, particularly externally hosted or publicly available systems, creates a risk that personal and sensitive information about families, often spanning generations, may be disclosed, stored or processed outside the organization's control, potentially resulting in breaches of confidentiality, loss of proprietary information or noncompliance with data protection requirements. Unlike traditional cybersecurity incidents, this form of exposure may arise through ordinary use without a clear breach event, making it more difficult to detect and manage.

1 However, automation bias can occur for reasons other than hallucinations as well.

- **Cybersecurity risks**
  Family offices face growing exposure to cybersecurity threats as they manage significant concentration of wealth, sensitive personal data and complex transactions across multiple entities, which makes them high-value targets. Vulnerabilities can also be introduced by third parties who have privileged data about families who expand the attack surface. A single successful breach could result in material financial loss, reputation damage and compromise of highly sensitive data.

- **AI-enabled fraud and social engineering**
  AI is increasingly being used to enhance the sophistication of fraud and social engineering attacks. This includes the generation of highly convincing written communications, as well as the use of voice cloning and deep fakes to impersonate trusted individuals. Family offices can be key targets given the nature of the data they deal with, the lean structures of the team, reliance on informal communication channels and the premium placed on speed and discretion in decision-making. The risk is not limited to technical compromise, but extends to manipulation of human behavior through increasingly credible forms of impersonation.

- **Vendor opacity**
  The use of third party AI tools introduces dependencies on external systems which often have underlying models, data practices and operational controls that are not fully transparent. Limited visibility over the full AI supply chain and underlying contractual arrangements can create legal, operational and jurisdictional risks that may not be apparent at the point of adoption, particularly where sensitive information is involved, or outputs are relied upon for decision-making.

- **Regulatory exposure**
  Although AI-specific regulation, such as the EU AI Act, continues to evolve, the use of AI is already subject to a wide range of existing legal and regulatory frameworks in most jurisdictions, such as data privacy and other regimes governing automated decision-making, laws prohibiting discriminatory practices and laws relating to product safety. Sector-specific regulators, such as the Information Commissioner's Office and the Financial Conduct Authority in the UK, have also published specific guidance on how existing rules can be aligned with the UK government's AI regulatory and policy objectives, and the same trend can be observed in many other jurisdictions. Inadequate controls over AI usage may therefore trigger exposure under these adjacent regimes, even where no AI-specific rules have been expressly breached.

- **Organizational and reputational risks**
  The risks above are multilayered, and their complexity necessitates a coordinated organizational response, rather than *ad hoc* or tool-specific controls. Given the nature of family office operations, where discretion, trust and long-term relationships are central, AI failure arising from AI use may have consequences that extend beyond operational disruption to include financial loss, legal and regulatory exposure and reputational harm. These risks are compounded by the threat posed by external actors who increasingly deploy AI for its cyber-offence capabilities, as noted above.

Governance response

The multilayered nature of AI-related risk requires a structured and proportionate governance response that aligns with the operational realities of the family office. The objective is not to introduce complexity or reinvent the wheel. It is to establish clear parameters within which AI can be used effectively and responsibly, as well as to introduce these within a governance framework that can be effectively and efficiently adopted by the organization.

1. Use-case identification and risk classification

Family offices should develop a clear understanding of how AI is being used across the organization. This can be achieved by developing and regularly refreshing an inventory of use cases, which can then be categorized by risk level, for example, distinguishing between administrative applications and those that inform investment or strategic decisions. This allows governance efforts to be tailored to the use-cases and focused on where risk is greatest.

2. Understand the AI systems you have deployed

Because of the inherent limitations of AI systems, it is important that family offices have a baseline understanding of how these systems operate, the type of models that have been procured (e.g.: narrow, generative or agentic), the capabilities of the underlying model enabling the use-case, the intended uses of the models that have been procured and whether they are being deployed in alignment with the intended uses, and so on. Where available, it is good practice to refer to dataset nutrition labels, system documentation (such as system or model cards), and evaluation results, as they can provide insight into explainability or interpretation, capabilities, expected behavior, limitations and risks, enabling more informed and disciplined use.

3. AI policies, data governance and regulatory compliance

A foundational step is the implementation of clear internal AI governance frameworks, setting out permitted and restricted uses of AI tools and establishing guardrails around the handling of sensitive data. This should be closely aligned with existing data governance practices, ensuring that confidentiality, privacy and data protection considerations are consistently applied in an AI context. Such policies must also be aligned with any AI-specific and existing legislation in parallel domains.

4. Human oversight and accountability

AI should not be a substitute for judgment, requiring clear lines of oversight and accountability, particularly in higher-risk use cases. Family offices should ensure that AI-assisted outputs are subject to appropriate human review, that the role of AI in decision-making processes is understood and, where material, documented and that ultimate responsibility remains clearly attributable to identified individuals or functions.

5. Supply chain mapping

To the extent possible, family offices should implement a proportionate approach to vendor oversight, focused on understanding the risks being transferred. This includes undertaking targeted due diligence on AI providers and reviewing core contractual terms to ensure, for example, that content submitted to AI systems remains the organization's and is not used in outputs provided by the system to other users. In addition, mapping key dependencies within the AI supply chain can provide greater visibility over indirect exposures and support more informed risk-management.

6. AI literacy and awareness

Family office teams should have a practical understanding of how AI systems operate. They must be trained on limitations and the risks of AI, particularly in relation to hallucinations, potential bias, AI-enabled cyber threats and human behavioral manipulation risk, as well as the creation of security vulnerabilities through untrusted or malicious inputs. This does not require technical expertise, but rather sufficient awareness to ensure that inputs are reviewed and outputs treated with appropriate scrutiny, that suspicious or anomalous behavior is recognized and that AI tools are used in a controlled and security-conscious manner as part of day-to-day workflows.

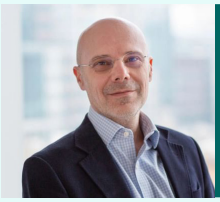
Conclusion

AI presents a clear opportunity for family offices to enhance efficiency, strengthen decision-making and modernize operational processes. However, as its use becomes more embedded within core activities and operational infrastructure, the associated risks, ranging from data exposure and model limitations to external dependencies and AI-enabled threats, become correspondingly more complex and interconnected.

The challenge for family offices is to ensure that AI is integrated in a manner that is consistent with their existing risk profile, governance standards and the high degree of trust and confidentiality that underpins their operations. This requires a shift from viewing AI as a standalone tool to recognizing it as part of the broader operational and decision-making framework of the organization. A proportionate, well-structured governance approach enables family offices to capture the benefits of AI while maintaining discipline and oversight.

For more information, please visit our AI Law & Policy Hub.

Contacts



David Naylor
Partner, London
M +44 792 047 9619
david.naylor@squirepb.com

Uzma Chaudhry
Associate, London
T +44 207 655 1330
uzma.chaudhry@squirepb.com