



Cracking Complexity: Smarter Due Diligence for Modern Investing

Institutional investing has become more complex, but the fiduciary obligation has not changed: make prudent, informed, documented decisions on behalf of beneficiaries and stakeholders. That simple mandate is now being tested by a market environment defined by product innovation, public-market dispersion, private-market influence, artificial intelligence, cyber risk, geopolitical shocks, fee opacity, liquidity fragility, and heightened stakeholder scrutiny.

At Institutional Connect’s Innovation and Resilience Forum, our panel - “Cracking Complexity: Smarter Due Diligence for Modern Investing” - addressed a timely question: how do institutional investors strengthen due diligence without creating bureaucracy that slows decision-making or obscures accountability? The answer begins with reframing due diligence from ‘manager-search checklist’ to multifaceted governance system.

Due Diligence Must Move Beyond Performance

Traditional manager diligence often began with performance: three-year, five-year, and ten-year returns; alpha; information ratio; drawdowns; benchmark comparison; and peer ranking. Those metrics still matter. But performance is an output, not a process. The better question is whether the institution understands how the performance was produced — and whether the process remains repeatable.

CFA Institute’s investment-manager selection framework distinguishes between investment due diligence and operational due diligence. Investment due diligence examines the manager’s investment process, personnel, and portfolio construction. Operational due diligence examines the manager’s infrastructure, vehicle structure, terms, operations, and personnel.¹ That distinction is critical. A manager can have attractive returns and weak controls. A compelling investment thesis can be undermined by poor valuation practices, cybersecurity

deficiencies, operational fragility, fee misalignment, or governance weaknesses. Modern allocators should require due diligence memos that document not only the reasons to invest, but the risks considered and rejected. The discipline should be explicit: What could go wrong? What would change our view? What evidence would disconfirm the thesis? What monitoring triggers apply after approval?

A Canadian lens sharpens the point. CAPSA'sⁱⁱ risk-management guidance explicitly brings together investment governance, third-party service providers, ESG, leverage, and cybersecurity — the same issues now embedded in modern manager due diligence. OSFI has similarly emphasized that pension administrators need robust processes to manage complex investment risks, independent oversight of risk-taking activities, valuation discipline, and due diligence over outsourced operational management and risk oversight functions. That is the new standard: due diligence must look through the manager's investment thesis into the operating model, control environment, service-provider network, valuation process, liquidity terms, cyber posture, and governance culture.ⁱⁱⁱ

A key element of 'beyond performance' is organizational culture. Cultures which embrace and enhance curiosity (investigation), courage (taking risks), collaboration (proactive teamwork), communication and creativity result in higher productivity, efficiency, effectiveness and, an unusual term in business, joy. Cultures which strive for repeatability - policies documented, risk appropriately measured and managed, compliance required, accountability and ownership established – in conjunction with these elements of culture will thrive. And, lastly, organizations which seek to build partnerships with clients based on real 'fit' (mission, values, actual needs) will find long-term relationships both robust and enriching.^{iv}

Governance Determines Whether Due Diligence Works

Due diligence is only as strong as the governance structure that uses it. Boards, investment committees, CIOs, consultants, counsel, accountants, and operational due diligence specialists all play different roles. Problems arise when those roles blur. Trustees may assume staff or consultants "own" the diligence conclusion. Staff may assume the board understands the risk trade-offs. Consultants may present recommendations that are technically sound but insufficiently connected to the institution's risk appetite, liquidity profile, or stakeholder obligations. Institutions can rely on expert analysis, but they cannot outsource accountability.

A strong governance framework defines who recommends, who challenges, who approves, who documents, who monitors, and who decides when a manager moves to watch list or termination. The best investment committees do not try to become experts in every strategy. They become experts in disciplined challenge.

Canada's large pension organizations also illustrate how due diligence is becoming an integrated governance discipline. PSP Investments describes board-level responsibility for risk appetite and risk philosophy, ESG integration into risk analysis, and initial and annual reviews by its risk teams.^v OMERS' annual reporting describes quarterly board and committee oversight across investments, actuarial assumptions, risk management, governance, liquidity, portfolio construction, foreign currency strategy, and economic trends.^{vi} These examples reinforce a core lesson for institutional investors: manager diligence should not be siloed from actuarial assumptions, liquidity planning, risk appetite, governance structure, or stakeholder accountability.

Operational Resilience Is Investment Risk

Operational due diligence has moved from back office to boardroom. Cybersecurity, business continuity, data governance, vendor oversight, trade operations, valuation controls, compliance history, succession planning, and key-person risk now belong at the center of diligence. NIST's Cybersecurity Framework 2.0 provides guidance for organizations to manage cybersecurity risks across industry and government, and it is increasingly relevant for institutional-investment ecosystems involving managers, custodians, consultants, administrators, and data providers.^{vii} Best-in-class investment managers and allocators do diligence to the nth degree – not simply third-party providers, but also the providers' own vendors – and assess these nth providers': 1) controls (COSO, SSAEs); 2) AI models and systems; 3) cyber security systems, pentests, scenarios and insurance; 4) quantum readiness – inventory, processes and controls, policies and overall post-quantum security; and 5) succession planning of key roles.

This matters because investment outcomes depend on operational integrity. A manager that cannot protect confidential information, reconcile positions, maintain trading controls, recover from a cyber incident, or manage vendors is not merely operationally weak. It is investment-risky. Minimum diligence should include the organization's SOC-1 and SOC-2 review where relevant, cyber incident history and ongoing controls, disaster recovery / business continuity plans and testing, valuation policies, trading controls, segregation of duties, compliance independence, personal trading policies, vendor-risk mapping, and succession planning for key investment and operations personnel. The question is no longer: "Does the manager have controls?" The better questions are around a range of controls and whether they have been tested under stress

AI Is Now a Diligence Issue

Artificial intelligence is changing both how managers invest and how allocators evaluate them. AI may improve research synthesis, risk monitoring, anomaly detection, portfolio surveillance, trading analysis, and operational controls. But AI also introduces risks: data leakage, hallucinated analysis, opaque models, unvalidated outputs, embedded bias, overreliance on automation, and cybersecurity vulnerabilities. AI is not only a technology tool. It shapes which facts surface, how risks are framed, and which arguments appear persuasive. That makes AI a governance issue before it is an investment issue.

The NIST AI Risk Management Framework gives institutions a useful language: govern, map, measure, and manage.^{viii} AI does not reduce fiduciary responsibility. It increases the need for explainability - allocators should move beyond asking managers, "Do you use AI?" and instead ask:

- How has AI changed the investment process we originally underwrote?
- What data is used, and who verifies it?
- What model validation occurs?
- Where is human override required?
- What outputs are prohibited from entering investment decisions?
- How are errors escalated and documented?
- Can the manager explain an AI-assisted decision in plain fiduciary language?

Transparency Must Include Fees, Structure, Liquidity and Clear Definitions of Sustainability

Complex structures can hide misalignment. Institutional allocators should evaluate not only headline management fees, but all-in economics: performance fees, trading costs, embedded fund expenses, platform charges, securities-lending splits, soft-dollar arrangements, FX costs, transition costs, and termination expenses. Performance reporting also requires discipline. CFA Institute's GIPS standards are voluntary ethical standards for calculating and presenting investment performance based on fair representation and full disclosure.^{ix}

For institutions, this means performance diligence should examine composite construction, benchmark appropriateness, portability of track records, dispersion, valuation methodology, and verification. A manager's return history should be understood as evidence, not accepted as marketing. Liquidity deserves equal scrutiny. Prior public-fund risk work emphasized that liquidity is not simply a cash-management report; it is a governance mechanism.

Institutions should understand redemption terms, settlement cycles, derivatives exposure, counterparty obligations, securities lending, margin requirements, gates, notice periods, and the first 24 hours of a market stress event. A "liquid" public-markets strategy can become operationally illiquid if it depends on crowded trades, derivatives collateral, fragile counterparties, or thin market depth.

And if sustainability is to be incorporated by the investor or manager, there must be clarity of terms, foci, metrics, communication and collaboration. Specifically, is the client choosing a screening in or out method, requiring managers to integrate non-financial metrics or follow certain themes? Is the client using MSCI, FTSE Russell, Dow Jones, Morningstar/Sustainalytics, LSEG/Refinitiv or some other index provider to measure results – and has the client required the manager to use the same? Has the investor required its staff to be trained in these metrics – CFA Institute Sustainability, TCFD, ISSB, PRI or other – so their personnel can assess responses and activities? And has the investor designed reports that meet stakeholders' needs for information and progress towards goals?

Macro and Geopolitical Risk Belong in Diligence

Manager diligence cannot ignore the operating regime.

Geopolitical shocks, sanctions, tariffs, supply-chain realignment, energy volatility, FX disruptions, and cyber threats increasingly affect portfolios and managers. Prior Opal geopolitical materials emphasized that trustees should incorporate geopolitical scenario analysis into manager selection, monitoring, and risk budgeting, rather than treating it as a quarterly macro commentary. While every manager does not need to be a macro strategist, but managers must understand the risks embedded in their strategies.^x

For example, a global equity manager should understand revenue dependence on China, semiconductor supply chains, FX translation, sanctions exposure, and tariff sensitivity. A credit manager should understand refinancing risk, covenant protection, private-market valuation spillover, and issuer exposure to policy shocks. A quantitative manager should explain model behavior during regime shifts.

Regulatory risk also remains dynamic. The SEC's private-fund adviser rulemaking and the subsequent Fifth Circuit vacatur underscore that regulatory expectations can shift materially, even when rules are contested or delayed. Due diligence should therefore include regulatory adaptability: compliance culture, legal resources, reporting infrastructure, disclosure practices, and escalation processes.

Monitoring Is Due Diligence After Approval

Too many institutions treat due diligence as pre-hire work and monitoring as performance review. That is too narrow. Monitoring is due diligence after approval. A manager should be re-underwritten no less than annually with on-site visits (with all members of the allocator's investment and operations teams participating in person or virtually), meeting with all members of the appropriate investment team, senior leadership, operations, risk, technology (AI, cyber, transformation), trading, compliance, macroeconomics, FX and also teams of services that could be considered in the future. Underwriting is done, on a simpler basis, with every monthly and quarterly reports, and in more depth when facts change: personnel turnover, ownership changes, asset growth, style drift, drawdowns outside expectations, regulatory inquiry, cyber incident, operational exception, valuation concern, change in liquidity terms, or failure to communicate clearly.

GFOA's pension governance and management best practices emphasize due diligence in selecting investment professionals and policies designed to reduce exposure to loss.^{xi} The practical tool is a manager accountability dashboard. It should include performance attribution, risk-budget usage, style drift, organizational stability, fee transparency, operational exceptions, cyber updates, liquidity profile, compliance issues, and watch-list triggers.

The New Due Diligence Standard

Modern due diligence should be rigorous, but not paralyzing. It is also a two-way street – the vendors (investment managers, analytics providers, etc) must get to know the investors / asset allocators as much as vice versa. How? By asking questions, listening, doing on-line diligence, watching team dynamics, and offering thought leadership to engage beyond products and services. The goal is not to create the longest process, but rather, the clearest basis for decision-making. Institutions should be able to answer five questions before approving any manager or strategy:

- What is the investment thesis?
- What are the key risks, and why are they acceptable?
- What operational, cyber, legal, fee, and liquidity issues were identified?
- Who is accountable for monitoring after approval?
- And how else can we work with this entity – thought leadership, complementary services, peer institutions – to build a more robust partnership?

In a Canadian context, this is especially relevant. The country's pension model is admired globally for scale, professionalism, and long-horizon investing, but scale also increases complexity. As portfolios expand across public markets, private markets, infrastructure, credit, real assets, derivatives, and global partnerships, the diligence burden rises. The lesson is not to retreat from complexity. It is to govern it. The strongest institutions

will be those that preserve speed and innovation while maintaining disciplined skepticism, documented process, independent challenge, and the courage to pass on investments when the diligence does not support the risk.

In a complex market, smarter due diligence is not about avoiding all risk. Institutional investors are paid — and fiduciaries are obligated — to take prudent risks. The real objective is to ensure that risks are understood, priced, documented, governed, and monitored. Complexity is not going away. The institutions that succeed will be those that convert due diligence from a checklist into a resilient fiduciary discipline.

LinkedIn Hook

Due diligence is no longer a manager-search checklist: in modern investing, it's a fiduciary operating system that integrates manager selection, operational resilience, AI / cyber / quantum governance, fee transparency, liquidity, legal structure, stakeholder expectations, and post-investment accountability.

At Institutional Connect's Innovation and Resilience Forum, @daniel perricone moderated a panel with me, @Ela Karahasanoglu and @mickael galvani where we discussed how institutional investors crack complexity to make fiduciary, innovative, stakeholder-appropriate and more effective decisions.

With thanks and gratitude to @john he, @siún-ní-mhuimhneacháin, @abbie oabel, @madelaine henriques and @jenny ho for superior selection of content and participants, and management of the event.

#InstitutionalInvesting #DueDiligence #InvestmentGovernance #PensionFunds #CIO #AssetManagement
#OperationalDueDiligence #RiskManagement #AI #Cybersecurity #FiduciaryDuty #ManagerSelection
#Governance #PublicMarkets #InvestmentCommittees

ⁱ <https://www.cfainstitute.org/insights/professional-learning/refreshers-readings/2026/investment-manager-selection>

ⁱⁱ <https://www.capsa-acor.org/RiskManagementGuidelineCommittee> and <https://www.capsa-acor.org/GuidelinesforIndustry>

ⁱⁱⁱ <https://www.osfi-bsif.gc.ca/en/consultations/consultation-summaries/osfi-summarizes-responses-its-pension-investment-risk-management-consultation-paper/pension-investment-risk-management>

^{iv} See Joanne Irving's C2 Leadership model – advisory firm <https://i2aa.com/> and book

^v <https://www.investpsp.com/en/psp/risk-management/>

^{vi} <https://www.omers.com/2025-annual-report/a-letter-from-the-chair>

^{vii} <https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20>

^{viii} <https://www.nist.gov/itl/ai-risk-management-framework>

^{ix} <https://rpc.cfainstitute.org/gips-standards>

^x <https://www.sec.gov/investment/private-fund-advisers>

^{xi} <https://www.gfoa.org/best-practices/pension-policy-governance-and-management>