PERKINS COIE

COUNSEL TO GREAT COMPANIES

Mutual Fund Directors Forum

Board Oversight of Third Party Vendors: Building a Practical Oversight Process

May 31, 2017

Molly Moynihan

Perkins Coie LLP

Introduction: The Whats and Whys

What is Vendor Risk Management?

- A systematic approach for identifying and decreasing potential business uncertainties and legal liabilities arising from third-party vendors.

Why does it matter?

- Mutual funds rely on a myriad of third-parties to perform vital services from pricing to trading to IT hosting.
- These third-party vendors can create vulnerabilities and service issues.

Understanding Vendor Risk Management

Vendor Risk Management (VRM) and Contracting is a profession, with its own sets of professionals and standards, much like internal audit.

Depending on its size, a complex may have a sophisticated program for VRM or it may have no program at all.

Nonetheless, big or small, the risks are the same and the components for managing are the same.

Risks

Third-Party Vendors, like all service providers, can introduce a variety of risks into the operations of a mutual fund.

- Market Risk—e.g., Trading systems
- Operations Risk—e.g., Business continuity
- Regulatory Risk—e.g., Pricing services
- Cyber and Data Privacy—e.g. IT providers
- Reputational—All of the Above

Recent Examples

All-Night Push After Glitch Hit BNY Mellon

September 2015

At the height of the market volatility on Aug. 24, executives at Bank of New York Mellon Corp. BK 0.06%▲ got the news they wanted to hear: A glitch affecting the system that keeps more than a thousand mutual funds running was likely to be fixed soon. BNY Mellon relayed the news to some clients.

But the problem was far from over.

By nightfall, BNY Mellon vendor SunGard Systems Inc. hadn't been able to repair problems with its system, which allows money managers to give investors the values of their holdings. Thus began a weeklong crisis in one of the most basic but crucial sections of Wall Street's infrastructure.

From Wall Street Journal

Recent Examples

Bloomberg Terminals Go Down Globally

April 2015

Bloomberg LP was hit by a massive computer-network outage Friday, forcing its terminals out of action for hours and leading to major disruptions for traders around the world who rely heavily on the machines.

From Wall Street Journal

Recent Examples

NSA officials worried about the day its potent hacking tool would get loose. Then it did.

May 2017

When the National Security Agency began using a new hacking tool called EternalBlue, those entrusted with deploying it marveled at …the widespread havoc it could wreak if it ever got loose…… for more than five years, the NSA kept using it — through a time period that has seen several serious security breaches — and now the officials' worst fears have been realized. The malicious code at the heart of the WannaCry virus that hit computer systems globally late last week was apparently stolen from the NSA….

Washington Post

Role of the Mutual Fund Board

Mutual Fund Directors Forum

Role of the Mutual Fund Director in the Oversight of the Risk Management Function

…. [T]he goal of effective risk management is not to eliminate risk. Instead, investment advisers and other key service providers develop systems and processes designed to identify risks and manage those risks appropriately in light of the information available.

While boards of directors of mutual funds ("boards" or "fund boards") are not directly responsible for risk management of the funds they oversee, **directors should be aware of their fund's adviser's and key service providers' risk frameworks, policies, procedures, and systems in place for identifying, analyzing, and managing risks**.

Role of the Mutual Fund Board

It is appropriate for a Board to seek reporting from Management with respect to Vendor Risk Management systems in place for key third party service providers. This is in addition to the Board's oversight of risk management at its primary service providers, i.e. Adviser, Transfer Agent, Distributor, Administrator and Custodian.

The funds generally do not contract directly with third-party service providers.

Focus should be on understanding:

- **Risk Ranking**
- **Contracting and Onboarding**
- **Vendor Risk Assessment and Oversight Program**
- **Significant Events**

Risk Ranking

VRM programs should begin with risk ranking—various terminology is used, but typically vendors are ranked by Tiers. Important to ensure that business units are risk-ranking all vendors.

Risk	Tier 1	Tier 2	Tier 3
Market	High	Medium	Low
Operations	High	Medium	Low
Regulatory	High	Medium	Low
Cyber and Data	High	Medium	Low
Reputational	High	Medium	Low

Risk Ranking

A failure at a Tier 1 Vendor presents an immediate risk of material harm to fund operations. Board accordingly, should focus on Tier 1 vendors and oversight processes in place with respect to onboarding, contracting and oversight.

Examples of Tier 1 Vendors

Core Services	Trading Related
Bloomberg DST/BFDS Sunguard – InvestOne Sunguard – Availability IBM services	Fiserv Swift

Onboarding and Contracting

Board should seek to understand Onboarding and Contracting process.

Many larger complexes have dedicated staff who can provide an informational presentation to Board on contracting process and standards.

Onboarding and Contracting

The Liability Hole

Almost all contracts with vendors include negligence or gross negligence liability standards and may limit damages to fees paid; many vendors are dominant industry players (SunGard, Bloomberg, IBM), giving funds little leverage for negotiation; and may or may not be well-capitalized.

In a “liability stack”, may have unlimited liability on the bottom—fund losses—but capped liability at the top—vendor liability. This was true in the SunGard incident, following which SunGard is reported to have further limited its liability.

Contractual Risks

Best practices

- Identify risks and related contractual terms.
- Mitigate by endeavoring to negotiate better contractual provisions, including SLAs.
- Manage risk by building redundancies and processes to protect against potential harm (example, processes around patches) or seek to lay off through insurance, if feasible.
- Accept.

Vendor Risk Assessment & Oversight

Process for Risk Assessment & Oversight can include:

- Questionnaires—covering topics such as vendor's policies, procedures and processes, IT and data security profile; business continuity.
- Collection of evidence or documentation covering areas of concern, which could include: professional certifications or licenses; SSAE 16, SOC 2, and SOC 3 reports; policies and procedures; financial reports; and external or internal audit reports.
- Onsite visits.

Record-keeping

VRM Program should include robust process for cataloguing all vendors, including profile system showing contract renewal schedule, risk ranking, oversight schedule, relevant business units, etc.

Tip--Surprising how often firms do not have a centralized system; individual business units may enter into vendor contracts with little or no legal review over contracting.

Event and Board Reporting

- VRM Process should include process for receiving and documenting reports concerning material incidents, including response and mitigation.
- Board should have a process for prompt reporting of material incidents to CCO, Audit Committee or Board Chair, as appropriate given reporting structures of particular Board.
- Board may wish to receive annual dashboard reporting on VRM process, with emphasis on Tier 1 Vendors