Operational Risk

Tailoring the right model for asset management firms

Broadridge®

sifma

Introduction

The past decade has flooded asset managers with challenges and complications—from escalating cyber-attacks, service provider and exchange outages, and devastating natural disasters to insider trading allegations against certain hedge fund companies, unprecedented regulatory changes with complex operational impacts, information security threats and controls required to protect that data, and the need for more complex investment solutions to satisfy client needs. All of which are challenging to not only understand but manage effectively.

Asset managers continue to look for solutions that enables them to excel in the face of unexpected challenges. Many asset managers find that Operational Risk Management (ORM) could be the path to manage challenges and complications.

Operational risk is defined as the 'risk of loss resulting from inadequate or failed processes, people and systems or from external events (BASEL II)'. Effective ORM should be considered a critical component of any financial firm's Enterprise Risk Management (ERM) program, as it mitigates a variety of risks across multiple disciplines that may materially impact the achievement of the firm's corporate and strategic objectives. Regardless of the pressure, firms should be able to proactively meet, contain and control these challenges via an ERM framework that includes Operational risk as a critical component.

The recent financial crisis has elevated the importance of how financial firms manage credit and market risks. And while there is a heightened awareness of risk management in general, how to implement the best operational risk program can be elusive. A 2013 risk management survey conducted by Deloitte & Touche to gauge the state of risk management noted that while most financial firms rated themselves as effective in managing liquidity risk (85%), credit risk (83%) and regulatory and compliance risk (74%), only 45% of the 86 respondents gave themselves a high rating for ORM.1 Approximately one-half of the 86 financial firms surveyed were stand-alone investment management firms or investment managers of larger integrated financial institutions.

While banks and insurance companies have fairly prescriptive guidance from regulators for an effective ORM program, the requirements and expectations for stand-alone asset managers may be less prescriptive. Some additional challenges faced in particular by smaller asset management firms may include:

- Small number of support staff relative to assets under management where there are limited internal resources to cover operational risks;
- Potential for inadequately established independent lines of defense due to commonly flat organizational structure of the industry

There is no single universal approach to developing an effective operational risk program. Each firm's operational risk strategy will vary depending on a number of factors including:

- Complexity of the company's operations;
- Uniqueness of its investment offerings;
- Requirements from local regulatory bodies;
- Breadth of services, scale and global reach.

This paper will explore efficient and effective ways boutique and mid-sized asset management firms can, with limited risk resources, develop the most critical aspects of an operational risk framework including:

- Business model complexity assessment
- Methods for risk and control
- Vendor oversight and management

While the size of the firm does not necessarily dictate what elements of the ORM framework are the highest priority to implement, as the complexity of the operations increase, so does the sophistication of the tools necessary to mitigate operational risk. We hope that you find this paper insightful in customizing the right program for your respective firm.

Finding the Value

Operational risk is inherent in nearly every business activity; it touches every department, system and process. Large losses from operational risk events are well publicized. One need look no further than UBS/SOC Gen rogue trading, Knight Capital and Insider Trading cases. Small losses from operational risk events tend not to be reported publicly, however, they can erode a business's ability to fully meet its strategic objectives and introduce adverse reputational and regulatory consequences. Pervasive lack of controls could also lead to regulatory fines and sanctions. For this reason, asset management firms should view a strong ORM program as an important means to reduce risk and avoid loss. Additionally, clients and fund boards are demanding that firms demonstrate a sound ORM program and are increasingly inquiring about a firm's ORM procedures and practices to ensure strong fiduciary oversight and responsibility practices. But although understood as an important business continuity effort, employing the appropriate operational risk tools, people, and processes may be challenging to implement, regardless of where a firm is in the complexity spectrum.

Determining Complexity

A primary consideration for a firm to ascertain in building an effective ORM program is its business model complexity. Larger, global firms may have increased pressures from various regulatory bodies due to the products and markets in which they trade, but may have more staff and resources to execute risk management effectively. They may have less agility in instituting new procedures or systems, but more capital to hire external resources. Smaller firms may have less product complexity, but fewer resources with which to manage operational risk. Process changes may be easier to absorb, implement consistently and implement in smaller or mid-size firms, but the build-out may have to be phased due to the need to prioritize resources.

The matrix on the following page explores firm complexity and basic questions to initiate realistic discussions regarding ORM gaps.

Asset Manager Attribute	Level of Complexity: BASE LEVEL	INCREASING COMPLEXITY	COMPLEX	CONSIDERATION AS COMPLEXITY INCREASES
Scope of Regulations	• One country • Asset Manager is a private, stand alone entity	• Subject to oversight by more than one country • Asset manager is a publicly listed company	• Arm of a sell size organization • Global operations, investments and customers means wide applicable regulatory framework	• Do you have the appropriate expertise as you are covered by expanding regulations? • Do you have a way to stay ahead of changing regulations from multiple regulators?
Investments	• Exchange traded securities • Single currency	• Public and private securities • Use of derivatives	• Bespoke, illiquid securities • Use of leverage and/or derivatives central to investment strategies	• Do you have the systems and agreements in place to monitor/limit new risks? • Where do/don't these new investments fit into existing processes and systems? • Do you have the right people for these new investments?
Clients	• Few or one client • Institutional only (non-pension) • Well defined strategy/limits/ goals/reporting needs	• Retail & institutional • In more than one country • Customers have different strategies/ goals/reporting requirements	• Large number of and institutional clients globally • Heavy and/or varied reporting/ due diligence requirements (i.e. pension funds)	• Do you need to adapt your on-boarding processes? • Are new clients needs fully risk assessed before business commitments are made?
Business Model	• Registered investment advisor • Centralized management with one or few offices performing key processes in house	• Multiple offices • Multiple regions/ time zones • Multiple and/or changing business strategies • Need for integration of multiple systems/ vendors	• Has publicly traded funds • Securitizations, VIEs central to strategies • De-centralized management • Many and changing strategies • Integration of a large number of systems and vendors critical to business	• How will you monitor people and processes who are in different locations/time zones? • What adaptations does your vendor oversight process need? • Where are your critical dependencies? • Have changing strategies been appropriately risk assessed?

Strategy

Once a firm's complexity is assessed, an overreaching ORM strategy may be discussed before tactical efforts are set in motion. There are some basic steps, elaborated later in this paper, in establishing a high-level, intuitive risk framework strategy:

1. **Culture:** Firms should have a solid and realistic understanding of their culture and what protocols and practices will work within said culture.

2. **Risk tolerance analysis:** Firms should know their risk tolerance. What is a firm willing to undertake in terms of risk, and what resources do they have to manage it? Under the oversight of the firm's board, management teams should work in forum toward agreement on what risks are, how, where and when to measure them, and every process and function should be assessed to determine how it affects a firm's risk tolerance.

3. **Risk priorities:** Firms may determine their risk priority or risk map—what are the most material risks, which landmines need to be uncovered and diffused first—categorizing high, medium and low priorities. Determining key processes and how these processes may impact a firm if shut down is essential to this task. Process mapping exercises will also point out key systems, people, as well as both up- and downstream dependencies.

4. **Lines of defense:** Firms should consider how to engage different levels of defense (traditionally three) to monitor and remediate risk, and may need to initiate business cultural change to achieve this.

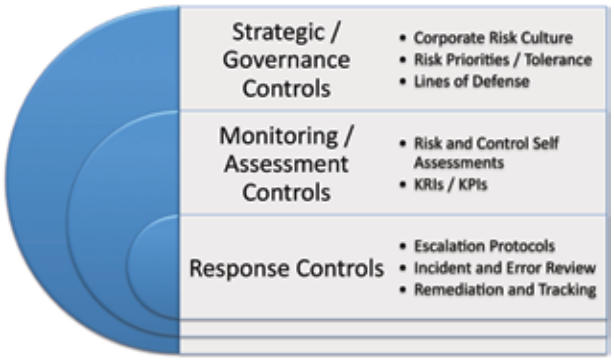
5. **Risk and control self assessments:** Understanding key processes and risks applicable to the firm is a critical component for proactive management and remediation of risks. Firms should be able to develop a framework for measurement and prioritization of its risks (risk priorities/risk map), remediation actions to be taken to enhance controls and develop a measurement approach through both lagging and leading indicators to evaluate changes to risk levels. Even if an industry event occurred from which the firm was fortunately isolated, firms may ask if their operational risk controls are strong enough to have stopped the event from happening to them. (ID, assess, response and monitor)

6. **KRIs/KPIs:** A Key Risk Indicator, also known as a KRI, is a measure used to indicate how risky an activity is, and the possibility of future adverse impact. KRIs give an early warning to identify a potential event that may harm continuity of the activity/project. This differs from a Key Performance Indicator (KPI) in that the latter is meant as a measure of how well something is being done. Firms typically have a combination of both KRIs and KPIs that are incorporated into dashboards.

7. **Escalation protocols:** Escalation protocols should be clearly delineated and effective to quickly move issues through the organization; issues can be transparently handled and remediated once exposed. Firms may question if the right escalation protocols and procedures are in place to aid the speed

8. **Incident and error review:** It may be impossible to prevent mistakes from happening even when there is a well-designed control environment. However, firms can use incidents and errors as learning opportunities to understand if there are any systemic root causes that should be addressed to prevent similar issues from reoccurring.

9. **Remediation and tracking:** Once it is determined that corrective actions are needed, it is important to assign ownership and timelines (which could be short-term containments as well as longer term permanent fixes), and track these actions through completion.



It should be noted that employing risk scenarios, which are not included in the above chart, in addition to supporting capital calculation, is an effective tool for identifying risks and controls that are important to a firm.

Firms must understand what is realistically achievable in regards to their respective ORM staffing, budget and technology limitations. Again, risk priorities or risk map will help determine material and high priority risk and, via utilization of the below efforts, will help set firms on a path to proactive rather than reactive ORM.

Culture Change

Operational risk is not encapsulated in one department but touches nearly every department within a firm. Therefore, ORM should be both a company-wide mindset and imperative for the program to be successful. The proper socialization message from the top down is vital to its acceptance; senior management sponsorship of a risk-aware culture is where it begins.

But change management is not an easy task even with executive buy-in. Senior management as well as the operational risk manager must have a realistic understanding of the idiosyncrasies of the firm's business culture and practices, legacy or rigid mindsets that may persist, and what is truly achievable given the cultural framework within which they must work. In general, three primary approaches have evolved in building an ORM. A centralized option has a dedicated team overseeing and implementing risk management practices and protocols, as well as monitoring and data analysis. Decentralized teams are embedded within various business functions with dotted reporting lines to a chief reporting officer or similar positions. A hybrid approach consists of a smaller, dedicated risk management team with counterparts in each of the vital business functions reporting to this team. Some pros and cons of each approach are:

	PROS	CONS
Centralized	• Consistent practices, methodology, tools, language, technology • Clear authority via reporting structure to internal forum or CRO • Clear delineation of roles	• By definition, the group is in a silo and must work to ingrain themselves with business teams • May be viewed as risk police, impacting open communication • May be seen as a material cost center • Rest of firm may be less likely to see themselves as part of the risk management process, reducing their perceived accountability
Decentralized	• Model that is closest to business function/ risk • All employees seen as risk managers • Fortifies a risk-aware culture • Breaks cultural silos • Less intimidating • May reduce ORM costs by utilizing existing employees	• Less independence and authority • Risk reporting may seem more complicated from a hierarchy or protocol perspective • Adds additional duties to existing positions that may not have the appropriate bandwidth to assume them, thereby reducing the intended level of attention on risk • May be more challenging to instill consistency in reporting and implementation, as employees may be more focused on "their area"
Hybrid	• Small centralized team offers core ORM • Risk managers embedded in various business functions • Departmental risk managers get to know business inside and out • Less intimidating to employees • "Best of both worlds"	• Dotted line reporting may cause priority confusion • Smaller core team may not have as much pull or influence as centralized team • Small core team may have to wear numerous "risk" hats; causing them to be spread too thin

These are simply broad models; each firm should understand the psychology of their business culture to determine the most efficacious or least disruptive model for greatest business productivity and continuity. Additionally, regardless of the ORM approach taken, a strong risk leader who is not only well-versed in monitoring and managing risk but also possesses strong leadership qualities is increasingly beneficial in the risk management space.

If everyone within a firm's culture is trained as a risk manager and empowered to speak up about potential vulnerabilities as well risk events, the more robustly and completely risk may be managed and mitigated.

Risk Universe/Taxonomy:

Depending upon their complexity and resources, many firms engage a team to help determine internal and external risks, creating a taxonomy or universe of potential risks. Firms frequently use BASEL Risk Categories as a starting point to define the risk taxonomy. Risk level standards are also used to standardize measurement using impact and the frequency of occurrence. Types of risk—economic, regulatory, vendor, fraud—are also key. Knowing this risk taxonomy or universe can then better allow risk management teams to think about how processes or systems need to be monitored and controlled to reduce occurrence of inventoried risks. Smaller firms may just be looking at 30 items; a larger firm may look at thousands, with varying degrees of granularity. Regardless, determining where the risk hot spots are allows firms to zero in on the business controls, processes and activities that touch and feed into those high-priority risks, and can then move to set up measurements around these.

Risk and Control Self-Assessments are about challenging assumptions and uncovering blind spots.

Three Lines of Defense:

The most common and perhaps effective way to deal with risk occurrence and remediation is to empower three lines of defense, which should work collaboratively and transparently for a robust ORM:

First line: The front line of the business, the business unit or function that is performing the processing. The first line of defense is critical. These are the most informed individuals of the process or procedure, the subject matter experts. Authorizing this first line of defense to alert the appropriate supervisors when problems arise essentially creates an entire enterprise of risk managers; by empowering process owners and smart problem solvers to identify challenges immediately, a firm not only builds a strong ORM but a stronger culture. It is vital, however, that strong escalation protocols are in place and understood so that the first line of defense does not try to fix the problem individually—they must be aware of the escalation chain and what the next step should be. Open communication and policies to support the front lines are also vital.

Second line: Compliance and risk management teams. These teams monitor and assess, identify and address risks as well as provide subject matter expertise on tangible risks. The second line examines policies and protocols in regard to risk, measures aggregate risk, looks at KRIs and KPIs, and works with senior management personnel to administer Top Down Risk Assessments (TDRAs). Compliance and risk management teams should work as an independent yet complementary line of defense.

Third line: Audit. The overseer, the internal and/or external audit teams perform testing to ensure that the first two lines are delivering on expectations and provides risk management guidance. Internal audit reports to management and the Board of Directors on the effectiveness of the firm's risk controls.

Risk and Control Self-Assessments:
Risk and Control Self-Assessment (or self-assessment) is the practice of employing a systematic practice of looking at the most important risk processes from an internal organization perspective and measuring those based on specific risk variable standards, and the frequency and impact of those standards. It is at its core a tool to determine and prevent both higher impact, low frequency incidents as well as lower impact, higher frequency errors before a firm's reputation and business continuity are damaged.

Self-Assessments also measure the robustness of an ORM practice within a firm, and may give glimpses into the engagement of senior management and the risk culture of the overall firm.

Two primary approaches to determining risk are evolving within firms: Top Down Risk Assessments (TDRAs) and Bottom Up Risk Assessments (BURAs). TDRAs start at the top level of a firm—senior management, audit, Chief Information Officer, Chief Compliance Officer—which assess and outline higher priority, broader risks and impacts. TDRAs focus on current external and internal concerns, help build the risk strategy and road map of a firm, and provide an aggregate view of conflicts.

BURAs are more process-oriented—the connective tissue of the organization—and look at the entire chain of events and process flow order from the first step of a risk-attached business process. Where TDRAs are more universal and higher level, BURAs are more data-driven and granular. This approach is important because it ensures disciplined processes to negate risk from the first line of defense upward. BURAs are oftentimes driven by changes or errors, they typically pinpoint bottleneck or potential system disconnects, and are the impetus for improvements in controls and mechanisms to mitigate risks.

Depending on a firm's complexity and resources, blending both TDRAs and BURAs is advantageous to ensure risk monitoring and controls occur throughout the enterprise. It is important to note that in combining both risk assessment approaches, lack of consistent taxonomy and protocol will reduce the synergies gained from this combination.

Key risk and performance indicators: Once risk tolerance and prioritized risks are established, disciplined self-assessment checks enable firms to assess how well processes and controls are preventing those risks. Assessments should not be just an annual exercise nor should it be exclusive; auditing and self-testing must be an ongoing, and it must be a firm-wide collaborative effort supported by the senior management.

ORM is more than loss avoidance; it is a valuable component to business continuity and growth and one that promotes holistic perspective and process understanding.

Once key risks are identified from TDRAs and/or BURAs, firms will understand the risks that should be monitored and may engage key risk indicators (KRIs) and Key Performance Indicators (KPIs) related to those areas. KRIs and KPIs are often-employed tools in monitoring and controlling risk that use business impact analysis to figure out key processes and the effect of malfunction. Again, which KRIs and KPIs a firm employs is determinate on the firm's identified vulnerabilities and the resources it has to monitor and control those.

A Key Risk Indicator, (also known as a KRI), is a measure used in management to indicate how risky an activity is. It differs from a Key Performance Indicator (KPI) in that the latter is meant as a measure of how well something is being done while the former is an indicator of the possibility of future adverse impact. KRIs give an early warning to identify potential event that may harm continuity of the activity/project. A KPI can also provide an early warning signal via changes in the performance of the measured activity.

Many firms administer thousands of metrics and analyses to obtain information. But the amount of information isn't what is important—the power of the information lies in its usability. Metrics, incident management review, loss review, risk assessments via internal audit, are all vital, but if measurements are burdensome and paralyzing, they aren't providing value. Key means key—the primary goal is to only use the KRIs, KPIs and some balance of leading and lagging indicators to proactively evaluate in a repeatable, consistent and productive way.

Additionally, self-assessments may be particularly administered when process, policy or procedure changes happen within in a firm. Risk management and self-assessments may also be performed at the implementation stage of new processes or technology to avoid undiagnosed vulnerabilities.

Incident and error reviews: Regardless of how sound an ORM a firm builds, no matter what proactive monitoring, preventive and detective controls are in place, incidents and errors will happen. It is the speed to detection, remediation and ultimate "containment" that exemplifies a robust ORM. Effective incident and error review begins with a disciplined taxonomy of operational risk incidents, which may range from trading errors to system instability and information security breaches. Categorizing potential operational risk incidents allows a firm to prioritize and attach appropriate escalation procedures to match the incident, and create an appropriate process for incidents, particularly material ones, to be escalated to the right stakeholders in a timely manner. Effective ORMs also institute a strong practice of collecting, tracking and analyzing errors including conducting post-mortems, determining and fixing root causes, and therefore reducing future vulnerabilities. The level of transparency that surrounds errors, incidents and near misses is also relevant.

Proper escalation protocol should involve some rendition of the following steps:

1. **Identify:** The speed of error detection and correction is the most important aspect of effective incident and error remediation. The first line of defense typically will be the first to spot issues. If this line is not trained in properly escalating the error, the incident could easily amplify. Again, the first line should not act in isolation, rather, they should be the warning signal to the next level of risk responders.

2. **Communicate and assess:** If an error or incident occurs, a firm must be able to quickly ascertain the next steps in remediating the issue. How material is this error or incident? What impacts does it have on the firm and what are the broader ramifications? Does this root cause effect other processes or accounts? What key stakeholders need to be involved? Do clients or counterparties need to be notified?

3. **Action toward resolution:** Again, timely action is critical once an error or incident is exposed. A firm should be able to control the resolution, employ mitigation actions, and if necessary, reimbursement enacted. Typically higher impact errors will take longer to resolve and cautious transparency must be used.

4. **Documentation and prevention:** As part of self-assessments, incidents and errors should also be tracked, root causes identified, as well as classification of the timeliness to process organizationally. From the root cause analysis, incident management reporting, and post-mortem audit, additional checks or process changes should be implemented control improvements. Additionally, escalation protocols may be tweaked to improve efficiency, communication and timeliness. Finally, communication with any employees up- or downstream of any procedures and protocols that may have been altered as a result of this error or incident is necessary for effective implementation of improved controls.

Even at a basic level, firms should ensure that they: 1. Capture, document, remediate and report incidents for the most important processes; 2. Minimize opportunity for failure; 3. Place governance around processes.

Vendor Management

All asset managers rely on vendors for at least some aspect of their business. Also, as an asset manager increases its level of outsourcing, their operational risks changes and they may not always have the ability to monitor key processes directly. Effective vendor vetting, onboarding and ongoing management is critical to an effective ORM.

Existing vendors: Contracting vendors does not relinquish firms from responsibility; therefore, vendors should be highly vetted before and during engagement. Similar to a risk roadmap, many firms have found it beneficial to rank vendors according to material risk and the firm's dependencies on that vendor. If a firm does not have an internal vendor management team, an inventory of what services a vendor supplies should be compiled by a task force, and a risk rating must be assigned to determine material or immaterial vendor relationships. Material vendor relationships—those that hold a key component of a firm's business operations—should have strong due diligence vetting. Additionally, a firm must ascertain the impact if that vendor became non-operational and how difficult would it be to replace that vendor. The harder a vendor is to replace, the more critical that vendor is on the risk profile.

New vendors: Before engaging new vendors, a vetting process must occur, including answering such questions as:

- Does the vendor have good security and information security practices?
- What is the credit risk and financial stability of the vendor?
- Have we run a background check and are they responsive to questions?
- Do we have a reasonable service level agreement (SLA) and if there are incidents, are they resolving issues according to the SLA?

- Does the vendor supply a scorecard, dashboards or other KPIs?
- Are we running internal checks, validation and measurements on vendors to monitor for delivery of services that are timely, accurate and complete?
- Does the vendor have a robust Business Continuity Plan?

Also, firms may ensure that appropriate due diligence groups and invested parties are in place at vendor on-boarding, that all contracts have been reviewed by legal, and that any affected business owners or departments have signed off on the relationship or service.

Dashboards can easily go from a performance indicator to a risk indicator.

Managing vendors: Among the considerations in regards to managing vendor risk is to understand the risk profile of the vendor, key monitoring, escalation plays, and forming an exit strategy from the vendor relationship. A strong first line of defense—the business owners who have contact with the vendors—is a substantial control check. Assignment of and subsequent discussions with internal relationship owners on how vendor practices match their policy may also provide insight and additional level of risk assessment. If a Service Organization Control (SOC) 1® or SOC 2® report is used—which provides "Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy "2—firms should identify if user entity controls are administered and if any exceptions are occurring in the report. KPIs can also be placed on vendors as well as information security and credit reviews.

Challenges

Instituting an effective ORM, although a logical, proactive and preventative tool, is not without its challenges and roadblocks:

Internal Challenges

Buy-in: Without senior management backing and cross-departmental buy-in, instituting an effective ORM is difficult. Senior management should be in tune with the enterprise-wide benefits of ORM for it to be successful. Legacy mindsets are an additional hurdle. Departments who inherently understand risk and the importance of analysis—such as IT, business analysts, project managers—more intuitively accept the concept of ORM; however, other departments may not understand the value or the need for process change as readily, and may present obstacles to culture-wide adoption of internal best practices.

Vying for resources: Competition for internal resources to support ORM is challenging. Although proactive, effective risk management may reduce overall costs in the long-term, sometimes that is not a strong enough immediate argument. Conversely, because an effective ORM keeps risk events at bay, this efficaciousness may, in turn, disguise the need for additional ORM resources; senior management may assume that because nothing material is impacting a firm, there may be no inherent value in funding additional risk exercises.

Quantifying value: As with many internal departments, proving the value of ORM—particularly one that has not experienced a major risk event—is difficult to quantify. Proof of sound controls and preventative policies can point to potential loss avoidance (particularly when compared to other firms or industries who have suffered a risk event), but that can be considered anecdotal and not substantially quantifiable. Additionally, because extensive ORM is not always prescribed by regulatory demands, a robust ORM can be seen as somewhat subjective.

Getting a seat at the table: A truly effective ORM means risk management teams are the main players in strategic decision-making and are able to offer subject matter expertise to guide a productive and operable change within the firm. Although this is becoming more common, it is not a consistent practice across the industry, and oftentimes ORM teams find themselves downstream of strategic initiatives.

Competent resources: It's not enough to just hire resources to design, implement and run an ORM program, but firms must find competent employees that possess the correct skill set—whether that be analytic and/or leadership – to fit a firm's needs.

Continual resources: ORM evolves, it is not a program that is simply stood up and left alone. Continual monitoring, reevaluation and assessment must be done to ensure controls are holding up and that new external or internal events aren't jeopardizing the firm, but again, dedicated funding and enthusiastic buy-in may wane and force constant re-selling of the program. ORM strategies themselves should not be static but should evolve and change with the firm's objectives, restructuring efforts, etc. Again, by securing a "seat at the table", ORM programs and protocols may more easily adapt to and guide changes in an enterprise.

Legacy systems: Dealing with outdated technology or systems continues to present obstacles for ORM teams, particularly in dealing with different systems across departments, business units or locations. Trying to re-engineer systems to the right operating support model has been cumbersome as well.

External Challenges

Regulatory challenges: Regulatory challenges continue to operationally tax firms. Ensuring staff are competent and prepared to adjust to new regulatory standards is difficult, and staying lock-step with regulatory changes is demanding yet vital to business continuity.

Information security: Information security is rapidly becoming not just a technology issue but an enterprise issue. Internal and external threats are proliferating and are seemingly random in attack. Instituting a sound information security system has become a necessary component of any asset manager's ORM.

Data: The exponentially increasing volume, complexity and speed of data are of great concern. Monitoring that information correctly, systematically, and effectively is necessary for business compliance and growth.

Vendor management: As mentioned above, vendor vetting and management is a growing issue as more firms outsource and engage third- and fourth-party vendors for vital processes and services. Ensuring vendors are sound operationally and from an information security standpoint is key, as well as understanding how dependent you are on that vendor if a need to replace them arises.

Evolution of markets: Markets continue to evolve new instruments and services to meet client needs. ORM practices need to keep pace with new product and/or service capabilities and attendant risks.

Geopolitical and market events: The increasingly connected global investing environment more acutely feels the reverberations of geopolitical tensions and global market events. ORM programs should be agile enough to respond to any necessary changes in processes or practices.

Emergency preparedness: Natural events such as Hurricane Sandy quickly identified weaknesses in many firms' emergency preparedness. Ensuring back-up and business continuity in the face of such disasters is another aspect of ORM that many firms may not grant priority until after the fact.

Non-events: Counter-intuitively, the lack of major risk events within the industry may back-burner ORM in some firms that don't have senior management buy-in, or those that are averse to cultural change.

Differentiating, Not Just Peripheral

Even with these challenges, ORM is finding a seat at the table of enterprise strategy. ORM not only reduces risk incidents, provides process analysis and transparency, aids with client due diligence, but also provides distinct differentiation among peers with unsubstantial ORM programs.

Collaborative and aligned culture:
As stated above, working collaboratively to prevent, discover, and remediate errors and risk engages the entire firm, building a cohesive, connected, aligned framework upon which other processes, protocols and relationship will move more fluidly. Empowerment across the firm also increases motivation and morale. Additionally, strong, collaborative ORM also fosters intellectual diversity as individuals are prompted to challenge assumptions and view things in a different, progressive way.

Holistic view:
A robust ORM buoys other areas and processes; by allowing perspective into the entire enterprise from a risk and process orientation, it facilitates the sharing of best practices while allowing senior management a more holistic view of how departments work together and how processes and actions have an affect both up—and downstream.

Good fiduciary/reputational support:
Increasingly clients want to know if and how a firm periodically administers risk self-assessments to determine the level of governance, transparency, and best practices within a firm, particularly in comparison to its peers. Sound ORM and remediation practices not only retain current clients but attract potential clients as well.

Interdepartmental support:
Because ORM touches every business function within a firm, the risk management team may support various departments in receiving funding for operationally sound initiatives or system upgrades.

Flexibility and agility:
Although it may seem counter-intuitive that instituting more checks and controls would aid in flexibility and agility, if an ORM is done correctly with clearly communicated protocols and processes, it can assist in freeing a firm's indecisiveness or process- and/or data-heavy paralysis. Being able to quantify impacts and quickly remediate them will also loosen apprehension regarding actions and their consequences.

Fostering growth:
Effective ORM provides identification of and reduction in the number of processes that impede business continuity and growth, and deters internal fraudulent efforts or information security breaches. Alternately, it also fosters key or high-performing employees, departments or processes that aid a firm's success.

Better data and transparency:
By demanding better and cleaner data for ORM purposes, firms have higher quality data for understanding their business as a whole.

Future objectives:
Without an introspective look at a firm's risk appetite, vulnerabilities, and obstacles to growth from an operational standpoint, firms have a weak framework from which to evolve their business.

Conclusion

Risk is, at its foundation, trying to manage the unknown. The goal of any ORM should not be to completely eliminate all risk but rather to understand, monitor, manage, and when necessary, remediate it. To do this effectively, ORM should not be conducted on a stand-alone basis but rather as an enterprise-wide initiative to improve processes and operations, reduce vulnerabilities, while simultaneously creating a collaborative and coalesced business culture. And, as more industry guidance, best practices and key indicators are elucidated and standardized, ORM will continue to evolve and streamline.

There is not one-size-fit-all approach to ORM. Complexity and size of an asset management firm will come into play. A firm's risk appetites and priorities will also be contributors. Resources will vary. But the underlying connective concept, the struggles that asset management firms all face, is the same—for a firm to succeed in today's environment, priority should be given to operational practices that not only reduces risk, vulnerabilities and loss, but also connects processes, systems and people to a common goal of building the firm. While the ramp up may be difficult, we hope that this document helps to guide your ORM improvements by illuminating the key considerations for your firm as well as helping to communicate the sound reasons for making these improvements.

1 Global Risk Management Survey, Eighth Edition, Deloitte & Touche.

2 http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/aicpasoc2report.aspx.

Contact Us

To further discuss the information in this document, please email or email marketing@broadridge.com or call us toll-free at:
Americas: +1 844 988 3429
EMEA: +44 20 3808 0724
APAC: +852 5803 8076

About Broadridge

Broadridge Financial Solutions, Inc. (NYSE:BR) is the leading provider of investor communications and technology-driven solutions for broker-dealers, banks, mutual funds and corporate issuers globally. Broadridge's investor communications, securities processing and business process outsourcing solutions help clients reduce their capital investments in operations infrastructure, allowing them to increase their focus on core business activities. With over 50 years of experience, Broadridge's infrastructure underpins proxy voting services for over 90% of public companies and mutual funds in North America, and processes more than $5 trillion in fixed income and equity trades per day. Broadridge employs approximately 6,700 full-time associates in 14 countries. For more information about Broadridge, please visit **broadridge.com.**

Asset Management Group

SIFMA's Asset Management Group (AMG) is the voice for the buy side within the securities industry, broader financial markets, and beyond. Collectively, members of AMG represent approximately $30 trillion of assets under management. Membership is diverse, ranging from the largest global financial players to independent, small firms across the country. Relying on the experience of its leadership and elite membership, AMG has a demonstrated ability to prescribe solutions for complex issues that regulators and industry participants alike classify as critical. As part of SIFMA, the leading trade association of the financial industry, we are able to leverage extensive trade association resources to update, prioritize and achieve goals on a regular basis.

Asset Managers Forum

Dedicated to facilitating collaboration among the buy-side operations community, the Asset Managers Forum (AMF) brings together subject matter experts to discuss and develop practical solutions to highly topical operational challenges. The AMF's mission is to provide thought leadership and guidance on pertinent industry issues and to create a premier venue for operations professionals to develop and share best practices in order to drive industry change.