Operational Risk White Paper

Assessing and Mitigating Operational Risk in a Changing Environment

---

by

NICSA Compliance and Risk Management Committee

April 2009

NICSA

NICSA Compliance and Risk Committee Members

Donna Barrette
Bill Cady
Robert Casey
Joan Dowd
Richard Garner
Martinez George
Donald Gignac
Joanna Haigney
Timothy Johnson
Robertson Mansi
William Monaghan
Daniel New
Kevin O'Connell
Michael O'Reilly
Mike Opal
Jay Regan
Debbie Seidel
Eileen Storz-Salino
Bruce Treff
Mark Trenchard

Note

Although the techniques, tools, observations, thoughts, and conclusions contained in this white paper represent the best thoughts of the individuals comprising the NICSA Compliance and Risk Management Committee, they do not necessarily reflect the views of the National Investment Company Service Association or any of its member organizations. Similarly, although the matters addressed in this white paper relate to operational risk management within organizations, nothing herein is intended to be or should be construed as legal advice. You should contact your own counsel in order to obtain legal advice regarding these or any other matters.

Assessing and Mitigating Operational Risk in a Changing Environment

FIRST IN A SERIES OF WHITE PAPERS BY NICSA'S COMPLIANCE AND RISK MANAGEMENT COMMITTEE

Abstract: The business, legal, technological, and regulatory environment in which the mutual fund industry operates is increasingly dynamic. The identification and mitigation of operational risks in such an environment presents challenges for investment management firms in the industry and their service providers. NICSA's Compliance and Risk Management Committee attempts to assist by categorizing, analyzing, and recommending the best practices in addressing these risks.

Introduction: Scope and Purpose of This Paper

The business, technological, and legal and regulatory environment in which the mutual fund industry operates is increasingly dynamic. The industry continues to face challenges integrating business, operational, and compliance processes into a broad risk management framework. For mutual fund organizations, the importance of implementing comprehensive and effective risk management has increased significantly in recent years. In part, this is the result of the interests of various constituencies (clients, boards of directors, regulators, chief compliance officers, chief risk officers, and independent audit firms) influencing each organization's approach to risk management. As a result, mutual fund companies continue to evaluate the structure and make-up of their risk management functions.

Part of the process of evaluating risk management is to identify and define the categories and subcategories of risk a firm faces. Clear articulation of the risks is necessary for the consistent application of risk management techniques across business lines. As a helpful review and to establish consistent terminology at the outset of this work, definitions of the risks are listed in Exhibit A in the Appendix.

The NICSA Compliance and Risk Management Committee (the "Committee") determined to add its voice, through this white paper, to the body of work geared to the identification and mitigation of operational risk. For this purpose, we have defined operational risk as the risk of direct or indirect loss resulting from inadequate or failed internal processes, controls, and systems, or from external events. It is important to remember that operational risk is embedded in almost all other types of risk as well.

This paper reflects the Committee's opinion that risk is "owned" by all employees of mutual fund investment management firms, particularly by the individual business lines, which are in the best position to identify, analyze, monitor, mitigate, and respond to the risks their businesses face. An

effective risk management program does not require the elimination or even the exhaustive mitigation of operational risk. Rather, calculated risk taking often opens doors for competitive advantage and leads to new ideas and concepts. The Committee's goal is to foster an environment and a process for the knowledgeable and comprehensive assessment and acceptance of risks posed by the internal processes, people, and systems of any enterprise in the mutual fund industry. To that end, it is critical that operational teams be comfortable identifying, assessing, and accepting risks within the framework, where appropriate, and similarly comfortable communicating macro risks to senior management for vetting and further action. We support a model that requires important risk decisions to be made and communicated at the proper level. This integral part of the decision-making process serves two purposes: (1) senior leaders are able to retain accountability for operational risk decisions, and (2) frontline operational managers are comfortable that risk decisions are affirmatively and properly communicated and understood. Finally, it is extremely important for operational teams and management to continually evaluate risk commensurate with their operations.

Overview of an Enterprise Risk Management Theory

Although many approaches and resources are available that articulate techniques for enterprise risk management, a compelling framework is that outlined in 2004 by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO"). The concepts and theories set forth by COSO are applicable to the assessment and mitigation of operational risks. For readers not acquainted it, COSO's "Enterprise Risk Management – Integrated Framework" ("Framework") is a seminal work in the field. NICSA's Compliance and Risk Management Committee encourages readers to review this Framework in detail.

To foster a common nomenclature for understanding the present paper and to enhance discussion of techniques for the assessment and mitigation of operational risks, the essential points of the COSO Framework, a 125-page document supplemented by a 105-page resource of application techniques are summarized here. The COSO document's executive summary may be accessed via this link:

http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

The COSO Framework defines enterprise risk management as follows:

> "[A] process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its appetite, to provide reasonable assurance regarding the achievement of entity objectives."[1]

The COSO definition is broad but comprehensive. The end goal of enterprise risk management is to "provide reasonable assurance regarding the achievement of entity objectives," while the process for achieving that goal clearly must involve all levels of the organization. The process requires establishing strategies across the organization to identify potential risk events and to manage risk in accordance with the risk appetite of the organization.

COSO identifies four broad categories of objectives:

1. Strategic – high-level goals
2. Operations – use of resources
3. Reporting – reliability
4. Compliance – with applicable laws and regulations

COSO identifies eight components of enterprise risk management:

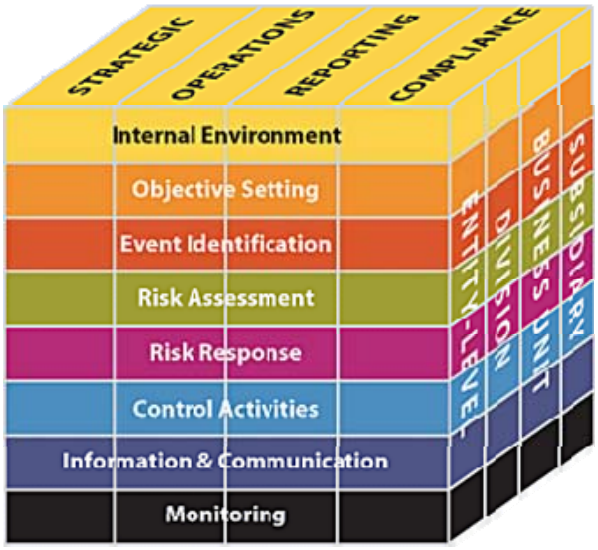
1. Internal Environment – the tone of the organization; the basis for the way risk is viewed within an organization and, ultimately, the risk appetite of the organization
2. Objective Setting – a process for establishing objectives that are in accordance with an organization's mission and articulated risk appetite
3. Event Identification – identification of internal and external events that impact the attainment of an organization's objectives
4. Risk Assessment – analysis of the likelihood and impact of identified risks
5. Risk Response – development of an action plan to bring identified risks within the organization's risk appetite
6. Control Activities – procedures to ensure that the risk responses are implemented

[1] COSO. "Enterprise Risk Management – Integrated Framework," 2004. <http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf>

7. Information and Communication – identification, recording, and communication of information so as to facilitate the discharge of responsibilities

8. Monitoring – ongoing management, independent evaluations, or both, with the goal of monitoring the process and adjusting it as necessary

COSO developed a three-dimensional matrix, known as the COSO Cube, to illustrate the direct relationship between a company's objectives (what the organization is attempting to achieve), the enterprise risk management components (the actions required to achieve the objectives), and the levels of the organization (the people responsible for achieving them).



COSO's Framework concludes that the effectiveness of an entity's risk management techniques ultimately depends on whether the eight components are present and functioning properly within the organization. Making that judgment assumes that all four objectives (strategic, operational, reporting, and compliance) are present and functioning at all levels of the organization (subsidiary, business unit, division, and entity level) and that the entity's risks are within the articulated risk profile of the organization.

Designing an Operational Risk Framework

To facilitate efforts to manage operational risk, a fund firm should design a risk framework that formalizes the identification, measurement, and reporting of operational risks and provides an easy-to-use system of recording and reporting risk events and trends. A tool that some fund firms use is the 'risk scorecard.' Such a scorecard outlines not only categorical risks plotted by probability and impact but also key actions to be taken to mitigate risk exposure. A firm should develop its risk ratings and then evaluate and adjust them on a regular basis, taking into consideration industry trends, regulatory changes, number of recent exceptions, and department staffing changes. Another

tool designed to assist leaders in the identification of risks within their teams is key risk indicators. A key risk indicator (KRI) is a metric that alerts managers to potential risk exposures.

A solid risk management framework is needed to proactively identify and manage potential risks and to make consideration of risks an integral part of decision making and business planning. A firm needs to identify and evaluate the risks it faces so it can operate efficiently and reduce its exposure to losses rather than commit time and resources to addressing issues that arise because of the firm's failure to manage its risk.

Please refer to Exhibit B, Example Tools and Techniques of Risk Assessment (page 14), for details on how to implement and maintain an operational risk framework. Exhibit B supplements the Committee's recommendations on how to identify, assess, and analyze operational risks, which are discussed in the following text.

Proactively Identifying Emerging Risks

Proactively identifying potential risk events can not only increase a firm's operational efficiency and reduce operational losses but also enhance the firm's ability to achieve objectives and identify areas in need of improvement. If the process is managed effectively, the results contribute to the overall strategic decision-making process and can be better integrated with the business planning process.

One key difference between routine monitoring and more robust risk assessment is the time horizon and ability to be proactive in identifying potential risk events. Monitoring typically focuses on current or past activities. Risk assessments tend to be more forward looking with the aim of identifying potential problems before they arise and adversely impact the firm. In the evaluation of risk values, consider the impact of recent control or operational failures so as to guard against repetition of either.

Below are some techniques to consider for identifying patterns of issues and trends.

Key Risk Indicators (KRIs) are risk measures designed to help leaders and managers identify potential risk exposure within each risk category. As indicated above, a KRI is a metric that alerts managers to potential risk exposures within a risk category. For processes that lend themselves to quantitative measurement, consider establishing a series of metrics that can be captured regularly, whether weekly, monthly, or quarterly. KRIs must be measurable and well documented. Firms should leverage existing metrics if they are applicable.

Review the results of the metrics along with commentary from the business process owners regarding any exceptions. For critical measures, consider setting thresholds to trigger an immediate escalation process when results exceed established limits. Monitor the results over time to review trends or evaluate the thresholds.

Environmental Scan Develop a continuous process to monitor changes in legislation, regulations, and industry practices. Take a proactive approach to evaluating the impact of issues at other firms to confirm controls and mitigating factors in place in your fund complex.

Issue/Incident/Event Tracking Consider developing consistent practices across the organization to capture and track incidents and events. Learn from weaknesses or issues that have already occurred in other areas to help prevent similar issues in other functional areas.

Periodic Review of Risk Assessments Periodically review the risk assessment results to reflect changes in the organization, business process, and business environment.

Periodic Interviews of Management Include senior management in the periodic discussions to determine significant risks and issues that they may be concerned about.

Interaction with the Funds' Board Incorporate periodic updates to the Board regarding results from the risk assessment process and involve board members in discussions about risk from multiple perspectives, such as updates from Internal Audit, the Chief Compliance Officer relating to compliance risks, and the Chief Risk Officer relating to enterprise risks.

Internal and External Risk Control Assessments

Depending on its organizational structure and the services it engages in, a fund complex may rely on a combination of internal, affiliated service providers and external, unaffiliated service providers to support its day-to-day operations. The service providers fulfill critical investment, administrative, and operational roles, including investment adviser, fund administration, custodian, principal underwriter or distributor, transfer agent, accounting, auditing, and other functions, such as securities lending.

Some key considerations in the use of service providers include service agreements, qualifications, and capabilities of the firm, fees, potential conflicts of interest, board involvement in the selection or approval of service providers, and quality or service levels. Funds typically rely on assessments from both internal and external sources. It is critical to understand the level of assessment and testing being performed by the service provider for consistency with standards that a fund might apply to internal service providers.

Internal Risk Control Assessments

Internal assessments may come from a variety of perspectives to cover particular functional areas. For example, Internal Audit may conduct a risk or control assessment regarding the nature, maturity, and effectiveness of the overall control environment. Other assessments may be conducted that relate to certain focus areas such as business risks, IT risks, and contingency planning. Additional sources of information for assessment of risks and controls include:

- Periodic certifications from service providers
- Results of due diligence meetings or due diligence questionnaires

- Periodic meetings with management and compliance and operational personnel of service providers regarding escalation of significant compliance and operational matters
- Results of trend reporting regarding critical operational and compliance areas

External Risk Control Assessments

Some service providers may provide an independent third-party review such as a Statement on Auditing Standard Number 70 (SAS-70),[2] developed by the American Institute of Certified Public Accountants (AICPA) for auditing of service organizations. SAS-70 reports are designed to provide an accounting firm's assessment of a service organization's internal controls.

SAS-70 Type I certification essentially asserts the opinion that the service organization's controls are consistent with its own description of the controls and that controls placed in operation are suitably designed to achieve the specified objectives. Type I certification typically covers a specific point in time and may not include testing of the controls.

SAS-70 Type II certification includes information contained in a Type I report but also asserts that that the controls were tested and demonstrated sufficient effectiveness in operating over a specific period (typically six months.) The certification provides reasonable assurance that the controls achieved the specified objectives.

Other Key Components of an Operational Risk Program

Policies and Procedures

Well-documented policies and procedures are at the core of managing operational risk. Policies specify the requirements and obligations to be addressed. They typically set limits, boundaries, and restrictions. Procedures specify how the requirements are to be fulfilled. Significant benefits result from associating key policies with the risks that are affected by the policy. Changing a policy may require changes to controls to prevent falsely identifying risks. Associating policies with certain risks can keep these elements in alignment over time. In some cases, multiple levels of policies or procedures focused on different audiences may exist in an organization. For example, policies approved by the board at a summary level specify requirements to be executed by various

[2] "SAS No. 70 provides guidance on the factors an independent auditor should consider when auditing the financial statements of an entity that uses a service organization to process certain transactions. It also provides guidance for independent auditors who issue reports on the processing of transactions by a service organization for use by other auditors." Source: AICPA

functional levels. High-level policies and procedures that describe key attributes are needed. At a more detailed level are operational or "desktop" policies for the functional business unit to follow. It is critical that the policies be reviewed periodically (at least annually) and aligned to manage risk.

Training and Communication

An additional consideration for a successful risk assessment program is training and communication. It is critical that employees and others involved in the process be consistent in the use of a standard framework, risk ratings, and common terms to avoid confusion. The Committee suggests firms develop their own formal training programs to give instruction on the way the risk assessment process should operate in the firm at different levels of management and across different entities. Another key success factor is communication. The process should include a communication plan for periodic reviews with compliance and risk management personnel and senior management regarding results identified and mitigation plans for key risk items.

Periodic Review

The scope and effort of the periodic review will be minimized if a comprehensive approach is used initially. The periodic review should be conducted at least annually. However, semiannual or quarterly reviews are a best practice depending on the rate of environmental change for the service provider, operational group, or compliance program.

Periodic Audit Reviews

Incorporate an independent review of critical areas identified by management and the audit team. The scope may vary in depth and topics covered through formal engagement definitions. Document and report findings and perform follow-up review to confirm that risk remediation has been completed.

Testing

Tailor the testing program based on risk assessment results to make the most effective use of business and compliance resources. The testing plan should leverage techniques that can address the most significant exposure areas. For example:

- Evaluate key measures over time to identify potential trends.
- Sample transactions over a period rather than rely on results from one point in time.
- Observe the process or workflow to identify potential weaknesses and compare it to documented policies and procedures.
- Interview key stakeholders and management to determine if they have any concerns and if there may be underlying weaknesses or potential improvements.
- Review recent exception items to determine how they were resolved, how quickly, and whether they were completely resolved.

Look for changes in process 'drivers' such as the related regulations, supporting systems, or support personnel. Any changes to the key drivers are likely to be detectable in the form of changes to the process and documentation.

Where applicable, use financial analysis to determine how specific financial measures compare with those of industry peers to identify potential issues or trends.

Also where applicable, use forensic accounting techniques to review process flows and specific transaction activity in order to identify potential problems.

APPENDIX

Exhibit A
Risk Categories and Definitions

Risk Category	Definition
Strategic	Risks that are an inherent part of the business environment and affect business objectives and performance
Organizational	Risks that are part of a business unit's environment relating to the unit's management and staff, organizational structure, culture and values that can impact overall organization effectiveness. For example: Succession planning Turnover Supervision Staffing Key person dependency Ethics
Financial	Exposure to loss relating to financial performance, uncertainty in the market, counterparty credit, or access to capital. Potential subcategories: Liquidity Capital and funding Credit Market Financial reporting Corporate financial controls (e.g., payment of expenses)

Risk Category	Definition
Tax	The risk that failure to accumulate and consider relevant tax information may result in noncompliance with tax regulations or adverse tax consequences that could have been avoided
Currency/ Treasury	The risk that volatility in foreign exchange rates exposes the organization to economic and accounting losses
Pricing	The risk that prices of key resources and services are higher than their expected levels, resulting in increased costs or lower margins
Legal and Regulatory Compliance	Risks relating to enforceability of contracts, interpretation of laws, and compliance and noncompliance with laws and regulations
Technology and Security	The risk that information technologies are compromising the integrity and reliability of data and information or threatening the organization's ability to sustain the operation of critical processes. Potential subcategories: Availability Security Capability Efficiency Integrity Privacy
Operational	The risk of loss resulting from failed processes; external, natural, or societal events; fraud or other infractions. Potential subcategories: People Process Events
Reputational	Risks that the firm's brand will be diminished in some way. Reputational risk is often the result of events in other risk categories.

Risk Category	Definition
Business Interruption	The risk related to timely resumption of critical operations in the event of an emergency: Terrorism Weather System failure/disaster recovery Business continuity
Fraud	The risk of loss resulting from fraud committed by employees, clients, or others involved with the organization, as well as outsiders or external entities.
Competitive	The risk that actions of competitors or new entrants to the market could hurt an organization's competitive position and its capacity to conduct business efficiently. Potential subcategories: New product development Clients Mergers and acquisitions

Exhibit B

Example Tools and Techniques for Risk Assessment

The risk assessment process should be designed to be comprehensive in scope but tailored to the specific risks of the business entity being evaluated. Depending on the business entities involved, overlap may occur between the risk assessment requirements and other regulatory requirements or compliance frameworks, such as Sarbanes-Oxley, FINRA 3012/3013, Investment Company Act Rule 38a-1, and Investment Advisers Act Rule 206(4)-7. Where possible, a firm should apply an integrated approach because some programs have similar objectives (refer to Exhibit D as to what can occur if the processes are not integrated.) The approach described here reflects the goals of establishing a risk-based program with continuous monitoring supported by metrics that can be strengthened and maintained over time.

Senior Management Commitment
A critical consideration in the risk assessment process is the commitment by senior management to support and participate in the process by communicating the importance of the effort and supporting the results, action plans, and gap remediation efforts.

Business Unit Commitment
Another critical consideration in the process is commitment and involvement of business control owners. The risk assessment process can stall without the buy-in of business partners. The risks, control activities, and control ownership can be verified with business partners and captured in the risk assessment documentation through a series of process "walk-through" meetings. It is imperative for the success of the program that control owners be fully engaged in the design and description of the controls. The firm should make clear that the control owners are accountable and ensure that they have a clear sense of responsibility for performance against the controls on an ongoing basis.

1. Identify the Risks
A systematic approach to managing the process can be very beneficial. A crucial first step is to create an inventory of all key risks. Several items for the inventory may be derived from contractual obligations, disclosures, potential conflicts, and regulatory requirements. These obligations should be associated to the primary responsible service provider or business entity and to existing policies and procedures.

Inherent Risks
Identify the key risks to the organization by using a comprehensive list of potential events or risks that may apply to the respective business entity or process. The related events or risks may be defined based on the organization's specialized activities and obligations. These risks are viewed from an inherent risk perspective and can act as the risk profile for the entity or organization.

Business Process Flow Analysis
For specific business objectives or obligations, a best practice is to outline the process flow at a high level. The process flow should represent the end-to-end process and reflect key controls. This analysis may identify potential areas in which new or enhanced controls need are required.

Loss Events
Review loss events both internal and external that relate to the organization's business activities. Events that have resulted in losses at other firms can provide valuable insights to potential risks within your processes or organizations. Firms should consider establishing an ongoing consistent process to capture loss event data related to the industry and the activities of the organization.

Potential Service Providers
To further develop the list, identify all internal, affiliated, and unaffiliated service providers and operational and support areas that could present risk exposure. Examples of potential service providers to consider include the following:

- Transfer agent
- Distributor
- Fund accountant
- Investment adviser
- Custodian
- Administrator
- Fund counsel
- Intermediaries
- Distribution platforms
- Auditors/accountants
- Other service providers

Risk Inventory
With this approach, the initial documentation can serve as a 'risk inventory' that can be leveraged, reviewed periodically, and updated to reflect changes in the operational environment. It also

provides the framework for identifying gaps where policies and procedures either do not exist or are inadequate, either of which may increase the organization's risk exposure.

2. Categorize the Risks

Categorize the risks according to agreed risk types developed by the firm. Refer to Exhibit A for a list of risk types and definitions.

3. Rate the Risks

Once the critical functions for each provider or operational area of the firm are identified, they should be documented. (See Exhibit C for an example Risk Assessment template.)

Risk ratings should be developed, evaluated, and adjusted on a regular basis, taking into consideration industry trends, regulatory changes, recent exceptions, and department staffing changes. The Committee suggests the following approach.

In many cases, the risk management, audit, or compliance team may take the first steps to develop risk rating; they will draft the assessment template, identify key risk areas, and assign initial ratings. The approach will depend to a large extent on the organizational structure of the risk management, compliance, and audit groups and the degree of centralization of risk management functions. The initial ratings should be discussed, reviewed, and validated with management and key stakeholders.

Rate Risks Inherent in Core Functions

For each core function, review and rate the inherent risk. The inherent risk is the risk of the activity without consideration of the effectiveness of the controls or mitigating factors that are in place. Rate the level of *probability* (likelihood) and level of *impact* (significance) for each risk item.

Describe Control Activities

Next, identify and briefly describe the control activities performed to mitigate the risk identified. (For details, see item 4 below.)

Rate Residual Risks

Review and rate the residual risk. The residual risk represents the level of risk that is not eliminated by the control activities or mitigation factors that have been put into place. Rate the level of *probability* (likelihood) and level of *impact* (significance) for each risk item.

In some instances, a firm may want to estimate the approximate dollar value of the potential impact of a risk it faces. The ratings serve to identify relative levels of risk, which can help the firm prioritize its risk remediation efforts.

A number of alternative methods and scales may be used for weighting risks. Any of the various options can increase the level of differentiation among the results of the assessments. The resulting values can then be plotted on a grid or "heat map" measuring "Probability" on one axis and "Impact" on the other. High-impact and high-probability items would be initially prioritized for risk mitigation, and over time, moderate- or low-ranked items would follow.

(Refer to Exhibit C for descriptions of ratings.)

When ratings are assigned, the firm can incorporate a numerical value to further differentiate the results. For example, the firm may multiply the values for probability and impact to assign a score for inherent risk or residual risk. Possible ratings and scales include:

- Low / Moderate / High
- Low / Moderate / High / Critical
- Numerical Scales: 1–3, 1–4, 1–10

Probability (Likelihood)
Probability of a risk is the likelihood that the risk will occur within the next 12 months based on prior history and management estimation.

- High – Event is highly likely to occur over the next 12 months.
- Medium – Event is moderately likely to occur over the next 12 months.
- Low – Event has not occurred and is unlikely to occur over the next 12 months.

Impact (Significance)
The impact is the degree to which the risk, if it occurs, would affect the business's ability to achieve its objectives.

- High – Event would have significant impact on the firm and may cause significant reputational harm to brand/image or result in significant financial losses.
- Medium – Event would have moderate impact on the firm and may include reputational harm to brand/image or result in moderate financial losses.
- Low – Event would have limited impact and may include limited reputational harm or minimal financial losses.

A firm should evaluate and adjust its risk ratings on a regular basis, taking into consideration industry trends, regulatory changes, number of recent exceptions, and other factors.

A key benefit of ranking a firm's risks is that it gives the firm the ability to measure the risks for reporting purposes. A tool that some fund firms use is a risk scorecard, which outlines not only categorical risks plotted over probability and impact but also key mitigation steps that specifying the action(s) taken to moderate risk exposure.

Identify Controls that Mitigate Risks
Controls include activities that reduce the impact or probability of a risk event. These may include granting authority to manage impact or events. Controls can be preventive or detective in design. Depending on several factors such as the nature of the controls, criticality, systems environment, it

is prudent to adopt and implement a balance of preventive and detective controls. It is a best practice to distinguish controls as preventive or detective because that may help in the evaluation of the effectiveness of the control environment.

For critical controls of high-risk items, preventive controls are preferable. However, in many cases, detection following process review may be the most feasible option. Controls may be automated or manual and should be identified and tracked as such since automated controls may present additional considerations. Managing risk is achieved in many ways, but the following list captures several likely actions:

Control Methods

- Accept risk (plan for it, self-insure, or offset it)
- Mitigate risk (disperse it, reduce exposure through controls)
- Transfer risk (reinsure, outsource, hedge, insure against, share)
- Avoid risk (eliminate, prohibit, or stop risk events)
- Exploit risk (diversify, expand, reorganize)

Control Types

- Segregation of duties
- System access controls
- Reconciliation
- Authorization/approval
- Management review
- Management oversight/supervision
- Policies and procedures
- Change management approval and testing process
- Exception reporting and monitoring
- Escalation processes
- Restriction limits and parameters
- Disaster recovery and business continuity planning
- Training, awareness, and communication

- Integration with annual business planning
- Testing and audit

Exhibit C

Example Risk Assessment Template

No.	Risk Factors / Conditions	Inherent Risk - Likelihood	Inherent Risk - Significance	Significant Business Risks	Key Management Control Activities	Control Type: Detective or Preventative	Control Method: Automated or Manual	Primary Control Owner(s)	Assessment of Control Effectiveness	Residual Risk - Likelihood	Residual Risk - Significance
	Available Values:	H	H			D	A		Effective	H	H
		M	M			P	M		Partially Effective	M	M
		L	L						Ineffective	L	L
1		L	L								

Definitions and Values

Risk Ratings	Values	Evaluation	Considerations
Impact	High (H), Medium (M), Low (L)	Evaluate the relative significance of the impact of the potential risk and likelihood that the risk will occur.	For Inherent risk this evaluation is made assuming the absence of a control environment. For Residual risk this evaluation is made considering the current control environment.
	High (H)	Significant exposure; pervasive impact; threatens corporate strategy or objectives; broadly impacts reputation; potential for significant fines or class actions, i.e. expected impact of $1million or more.	
	Medium (M)	Moderate exposure with financial, operational or compliance impacts, but does not threaten corporate objectives, i.e. expected impact of between $50,000 and $1 million.	
	Low (L)	Minimal exposure with confined business impact of less than $50,000.	
Likelihood	High (H), Medium (M), Low (L)	Evaluate the relative significance of the impact of the potential risk and likelihood that the risk will occur.	For Inherent risk this evaluation is made assuming the absence of a control environment. For Residual risk this evaluation is made considering the current control environment.
	High (H)	Probable that event will occur, may occur more frequently, i.e. annual probability of 100%	
	Medium (M)	Reasonable possibility that event might occur, i.e. annual probability of 10% to 50%	
	Low (L)	Unlikely that event will occur, i.e. annual probability of less than 10%	

Heat Map

Likelihood of Occurrence	*Probable*	**L**	**H**	**H**
		L	**M or H**	**M or H**
	Remote	**L**	**L or M**	**M**
		Inconsequential		*Potentially Material*
		Significance of Impact		

Control Type:	**Control Method:**	**Definition of Assessment of Control Effectiveness:**	**Definition of Effectiveness of Risk Mitigation:**
D-Detective	A-Automated	Effective – Controls are effective in the mitigation of identified risk.	Effective – Controls are effective in the mitigation of identified risk.
P-Preventive	M- Manual	Partially Effective – Controls are not fully effective in the mitigation of identified risk.	Partially Effective – Controls are not fully effective in the mitigation of identified risk.
		Ineffective – Controls are not effective in the mitigation of identified risk.	Ineffective – Controls are not effective in the mitigation of identified risk.
			Open – New or Emerging Risk – controls in the process of being developed.
			Accepts – Management accepts the residual level of risk.

Exhibit D

Risk Convergence

Closely tied to risk management is the concept of *risk convergence*. Risk management, regulatory, and legal compliance requirements are increasing in frequency and complexity and have become a growing operational and financial burden for most financial services firms. Investors are showing less tolerance for the mismanagement of risk and continue to dislike surprises linked to breakdowns in risk management, control, or compliance. Firms often scatter their risk requirements in business and operational silos, which leads to the creation of multiple risk governance processes, methods, and infrastructures. These processes are driven by numerous requirements:

- Regulatory compliance
- Risk management
- Information security
- Business continuity
- Internal audit
- Legal
- Operations
- Sarbanes-Oxley

Lines of business are experiencing "risk management process fatigue," expending significant time and cost to comply with risk requirements, and they can be confused and frustrated by multiple requests that appear duplicative. Some streamlining of risk governance processes may help institutions better coordinate among their various risk functions and optimally manage scarce resources while achieving robust risk management and compliance with regulatory requirements. To eliminate redundancies and reduce associated costs, firms have started to analyze these redundancies to be able to:

- Identify and eliminate redundant risk and control activities
- Reduce the duplication in the business units and lessen "risk fatigue"
- Establish a common methodology for the identification, assessment, monitoring, and measurement of an organization's risk and control environment
- Increase communication and expertise/resource leveraging

- Promote sharing of internal best practices and highlight opportunities to gain further efficiencies
- Explore opportunities to organizationally integrate like processes and rely on common utilities
- Promote more comprehensive and effective enterprise-wide risk reporting to senior management and board committees
- Enhance the internal control structure of the organization