Converting critical enterprise risks into a usable risk matrix

Received (in revised form): 23rd February, 2022

Janice Powell
Senior Compliance Consultant, Core Compliance, USA

Janice Powell

***Janice Powell**, MBA, IAACP, is a senior compliance consultant at Core Compliance & Legal Services, Inc. Ms Powell has dedicated her career to continuous collaboration with firms throughout the industry in an effort to enhance their risk-based compliance programmes and understanding their fiduciary responsibilities to their clients. Her dynamic approach and experience working with C-Suite executives to mitigate conflicts of interest and regulatory scrutiny, while developing solutions to help firms expand and grow their business in a compliant way, has made her a rising star in the compliance arena. Throughout her career, Ms Powell has focused on perfecting custom methods for how to build and develop a culture of compliance. Ms Powell provides compliance consultation to multiple business models from hybrid advisers, multi-family offices, dual registrants, bank-owned advisers and broker-dealers, advisers to mutual funds, trust companies and independent advisers. Her consultation practice areas include investment adviser, investment company, broker-dealer and private fund compliance programmes, marketing reviews, Code of Ethics and compliance programme development and training, policy and procedure, surveillance and internal control development, risk assessment and annual reviews.*

Core Compliance,
1350 Columbia Street,
Suite 300,
San Diego, CA 92101,
USA
Tel: +1 619-269-6155;
E-mail: janice.powell@corecls.com

Journal of Financial Compliance
Vol. 5, No. 4 2022, pp. 370–377

2398-8053

Abstract

Successful compliance is built upon a solid foundation of risk management. Effective compliance programmes begin with a thorough assessment to identify areas of risk within the organisation. Developing a risk management framework is crucial to an organisation's ability to develop appropriate protocols to identify, monitor, and if needed, mitigate the risks. Aside from the practical benefits a risk assessment can provide, it can also demonstrate to a regulator that a compliance programme is 'reasonably designed' to prevent violations of federal securities laws.[1] The purpose of this paper is to discuss practical ways to develop and implement a risk management programme as well as conveying identified risks to senior management for use in practical business decisions.

Keywords: Risk management, compliance programme, risk assessment, controls

INTRODUCTION

Risk is a part of everyday life and is often mitigated or addressed through a variety of methods. For example, you can address the risk of a serious illness by purchasing health insurance or the risk of a motor vehicle accident by purchasing car insurance. In these examples, the risk of a catastrophic event occurring, and the subsequent financial outlay is mitigated by capping the out-of-pocket loss you may end up paying upon the unexpected circumstance. Similarly, other risks could include the inability to provide for your expenses in retirement, so you mitigate by putting money in savings or deferring compensation into a retirement account. Every day, individuals make decisions related to risk and frequently trade one risk for another. As you navigate daily risk and make decisions about how much risk you are willing to accept (eg how high is the deductible going to be), businesses must do the same. Businesses must evaluate how much risk they are willing to withstand and how to mitigate the risk to

ensure not only compliance with regulations but also long-term success.

With the evolution of technology, the state of the COVID-19 pandemic at the time of writing, and the ever-changing political and regulatory environment, financial service firms face increasing scrutiny on their business practices and compliance programmes. If you ask a financial adviser what risk means to them, the likely response they will give considers portfolio risk, a client's tolerance for risk, or several factors that make up risk in managing the assets, such as interest rate risk, business risk, inflation risk, liquidity risk, political risk and so on.[2] An enterprise risk management system breaks down risk into similar categories, must evaluate controls and review and revise as necessary. Investopedia defines enterprise risk management (ERM) as

> a methodology that looks at risk management strategically from the perspective of the entire firm or organisation. It is a top-down strategy that aims to identify, assess, and prepare for potential losses, dangers, hazards, and other potentials for harm that may interfere with an organisation's operations and objectives and/or lead to losses. ERM takes a holistic approach and calls for management-level decision-making that may not necessarily make sense for an individual business unit or segment. Thus, instead of each business unit being responsible for its own risk management, firm-wide surveillance is given precedence.[3]

Think of it as a collection of departments across a firm or a hierarchy of entities owned by a holding company. Risk is found at every level.

At a CCOutreach National Seminar on 8th February, 2011, Carlo Di Florio, former Director, Office of Compliance Inspections and Examinations at the Securities and Exchange Commission (SEC), discussed ERM and stipulated that examinations of investment advisers and broker dealers would focus on three areas.

> In a time of resource constraints, we hope to realise three benefits from this approach: (i) this will keep us focused on the most significant risks; (ii) by focusing on a somewhat smaller but high-priority range of issues in each exam we will be able to extend our resources further; and (iii) engaging firms at a higher level of management will have a more effective impact on a firm's culture.[4]

Di Florio continued his remarks, highlighting that examiners would seek to understand the oversight of the risk management process, appropriate setting of risk tolerances, monitoring, addressing and reporting of exceptions. Furthermore, examiners would focus on training and communication within the firm as well as whether or not an appropriate compliance culture or the 'tone at the top' is established to ensure risk is addressed.

WHAT IS RISK MANAGEMENT?

Each firm that considers implementing a tailored compliance programme faces the challenge of designing a governance structure that is specific to the business model and strategy of the entity. In order to understand where to start, firms must answer one basic question, 'What is risk?' Merriam-Webster dictionary defines it as, 'possibility of loss or injury; someone or something that creates or suggests a hazard'.[5] *Harvard Business Review* in 2012 recounted an interesting example of a CEO attempting to manage risky behaviour.

> When Tony Hayward became CEO of BP, in 2007, he vowed to make safety his top priority. Among the new rules he instituted were the requirements that all employees use lids on coffee cups while walking

> and refrain from texting while driving. Three years later, on Hayward's watch, the Deepwater Horizon oil rig exploded in the Gulf of Mexico, causing one of the worst man-made disasters in history. A US investigation commission attributed the disaster to management failures that crippled 'the ability of individuals involved to identify the risks they faced and to properly evaluate, communicate, and address them.' Hayward's story reflects a common problem. Despite all the rhetoric and money invested in it, risk management is too often treated as a compliance issue that can be solved by drawing up lots of rules and making sure that all employees follow them. Many such rules, of course, are sensible and do reduce some risks that could severely damage a company. But rules-based risk management will not diminish either the likelihood or the impact of a disaster such as Deepwater Horizon, just as it did not prevent the failure of many financial institutions during the 2007–2008 credit crisis.[6]

While it may seem ridiculous when contemplating this type of behaviour in retrospect, Mr Hayward probably thought that he was managing risk by creating rules that were designed to prevent risk. Does your firm have a 'rules-based' risk management programme, or one that effectively evaluates internal controls when assessing risk and then continues to modify the programme based on new risks? Risks can be found at every level in the enterprise from a job function to the entity level. Identifying these risks and gauging controls formulates an enterprise risk management process.

A formal risk assessment, or matrix, is generally not required by securities laws;[7] however, regulators like the SEC and the Financial Industry Regulatory Authority (FINRA) continue to have expectations that firms employ some form of risk management process. Through risk alerts, publishing exam priorities, the use of notices to members and public comments, it is very clear that regulators expect firms to have robust and effective risk management practices. Therefore, it is crucial for firms to develop a practical process to identify risks within their organisation that may make them vulnerable to violations. The firm must assess those risks as to their importance so resources can be allocated to areas posing the most significant risk.

There is a perception that implementing a risk framework is overly complex, expensive and requires years of education devoted to risk management. This perception is common, but unsupported. These misconceptions should not prevent a firm from implementing a robust risk management framework. Regulators are not looking for perfection, but for effort.

A risk management programme should be a living, breathing process designed to keep up with changing risk environments. Identifying risks is a task best accomplished by collaborating with management, representatives from each business unit, compliance and any other stakeholder responsible for the business. If possible, implement a risk committee that can brainstorm, assist with evaluating the risks to the firm and weigh in on controls. It can also provide buy-in across the firm. Support from senior management is imperative to establishing the right culture and desired internal environment. Obtaining top level support also ensures the appropriate amount of importance is given to the ERM process, including allocating resources needed to foster the success of the programme.

Uncovering risks, including hidden risks, requires sufficient knowledge of the firm and the business model in which it engages. Risk can be found in rules and regulations, technology, environment (think COVID-19 pandemic), employees, vendors, contracts, firm relationships and compensation, among many other areas. Once risks are identified, define the risks (eg compliance or operational). The firm should then establish an appetite for the risk. Determine how much

risk it is willing to accept while pursuing its objectives before any actions are necessary in order to mitigate the risk. Consider the resources the firm has and the potential likelihood of the event happening.

IMPLEMENT AND MANAGE

There are many ways to document and complete a risk matrix. Microsoft Excel or Word can be used for a limited risk assessment or there are elaborate automated systems available for more complicated risk structures. Find one that works for the size and complexity of the business being assessed. The risk matrix is intended to be an ever-evolving framework that should be adjusted routinely as the business changes, controls are deployed, and new risks are identified. The following steps should be considered when implementing the programme.

Develop a risk inventory

As previously stated, creating an inventory of risks associated with the firm can help it evaluate whether necessary policies and procedures with related controls exist or need to be developed. It will also help to determine the frequency of testing of the compliance programme.

Starting this inventory can be a daunting task. Firms should begin by preparing a comprehensive list of risks posed by the business. Begin with a top-down focus. Consider the most important risk exposures from across the organisation. Include risks inherent to the firm's business model, contractual obligations and types of products and services offered. Consider conflicts of interest posed by compensation, employee and vendor relationships. Utilise previous regulatory exam deficiencies or regulatory document request lists and determine which item in the document request may be an issue during your next examination, as well as publicly available risk assessments.[8] Regulators often issue guidance and exam priorities outlining focus areas based on previously inspected firms. These documents outline priorities and items of importance with a roadmap to expectations regarding risks. Assess the ramifications of regulatory violations occurring and the need for mitigation.

Gather ideas from colleagues and counterparts at other similarly situated firms. Industry networking groups and local compliance roundtables are a good resource if conducting an initial assessment. Conduct interviews, surveys, questionnaires and focus groups with facilitated discussion.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), a leading expert and thought leader on risk management, governance and fraud deterrence, developed a list of questions that can help identify the most significant strategic or emerging risks within an organisation. When interviewing senior management regarding risks, consider these questions:

- What are the primary business objectives or strategies?
- What are the key components of enabling the business strategy or objectives?
- What internal factors or events could impede or derail each of these key components?
- What events external to the organisation could impede or derail each of the key components?
- What are the three most significant risk events that concern you regarding the organisation's ability to achieve business objectives?
- Where should the organisation enhance its risk management processes to have maximum benefit and effect on its ability to achieve business objectives?
- What types of catastrophic risks does the organisation face? How prepared is the organisation to handle them, if they occur?

- Can you identify any significant risks or exposures to third parties (vendors, service providers, alliance partners etc) that concern you?
- What financial market risks do you believe are or will be significant?
- What current or developing legal/regulatory/governmental events or risks might be significant to the success of the business?
- Are you concerned about any emerging risks or events? If so, what are they?
- What risks are competitors identifying in their regulatory reports that we have not been addressing in our risk analysis?[9]

The answers to these questions and the methods described above may also provide insight into risks not previously considered.

Next, step outside the realm of the securities industry and consider non-securities laws, regulations, and relationships that may be applicable to the firm. Examples include tax, insurance, banking and other financial organisations and affiliates, Department of Labor (DOL) and Employee Retirement Income Security Act (ERISA) regulations and client relationships. Finally, consider the firm's corporate culture. Evaluate corporate initiatives, financial strength and reporting, potential reputational risks as well as the firm's competitors. These areas are often overlooked when contemplating the totality of risks associated with a firm.

Assign a risk rating

Upon completion of the inventory, assess each inventoried risk. Determine the significance and assign a rating. Make a judgment with each risk of what is the likelihood the risk would materialise and the negative effect that event would have on the firm and its clients if the risk were to occur. Analysing each item allows the firm to prioritise initiatives so that appropriate resources can be allocated towards those activities that present the highest risk.

Use a risk rating that makes sense considering the breadth and scope of the risks identified. Larger financial institutions will use complex rating systems calculating risk based on a number of factors, including inherent and residual risk among other associated risks. Using a more simplified version of a risk scale, such as colour-coding red (dangerous), yellow (proceed with caution), and green (presents little or no risk) or a high, moderate, low-ranking system works just as effectively. With any scale, ensure that it aligns appropriately to the item being evaluated and is easily discernible from the other risks. For example, if a ten-point scale is used without any other values to clarify the assigned rating, recognising that ten (10) might be high, five (5) might be medium and one (1) would be considered low, how does a ranking of 4 or 6 identify the risk? Firms can be assured that a regulator will focus on these details.

As a part of this step, consider documenting the reason the firm made the decision to place risks into one category versus another, as recollecting these conversations at a later date may be difficult. This is where a culmination of the firm's risk appetite, the regulatory landscape, and the controls in place will shape whether the rating is elevated or not. Determine what the consequences could be if the risk materialises and assess the importance. What risks are significant enough to warrant formal, written procedures versus the risks that are less serious that can be managed through other means?

Map risks to procedures and controls

For each risk identified that warrants a written policy, correlate or 'map' the risk to the appropriate policy and control. For the remaining risks, identify and evaluate any informal processes currently in place that address the risk and map accordingly. If the risk is not applicable, indicate why.

Where there is a gap, or, in other words, a risk with no correlating policy and control

already in place, then the firm should develop one. Developing and adopting a new policy should not be done in a silo. The involvement of the management team as well as key business partners is important to gain perspective from all stakeholders. Receiving input from these areas can also eliminate crafting a policy that cannot be followed in practice.

When drafting a policy, consider a few things. First, examine the root cause of the risk. For example, a root cause of an identified risk might be a single point of failure, or where there is only one employee with knowledge or responsibility for a process but then gets hit by the proverbial bus. Secondly, analyse the objective the policy is intended to achieve. Evaluate the path forward and the probability the objective will be met. Even with the best of intentions, most risks cannot be eliminated entirely. That is why it is important to ensure that good controls are recognised, in place and are routinely validated. Thirdly, contemplate the firm's tolerance for the risk and the strength of controls needed. Delve into the feasibility of the procedures and controls being contemplated to address those risks. Do you mitigate or eliminate the risk? There is a wide array of controls that can be implemented from prohibitions and pre-approvals to audit or independent verification. As in the example of the single point of failure, cross-training on job functions may be an appropriate control. Finally, explore potential technology solutions that can be leveraged which are either already in place or that can be implemented. In almost all facets of compliance, there are quite a few innovative technology platforms that assist with oversight and control environments. These types of resources are increasingly more affordable as advancements in fintech continue to evolve. Weighing the cost of human error, labour and the financial outlay from a fine or sanction makes these automated controls and the technology behind them more cost-efficient.

Within the policy, ensure there is effective oversight, dual controls or functional separation of duties and an appropriate level of detail that ensures clarity regarding the policy. Ambiguous language makes it difficult for employees to comply and opens the door to inadvertent violations.

Risk management programmes can be very valuable tools, but keep in mind that internal controls may still have limitations. Overreliance on the risk framework can be problematic. In 2013, COSO highlighted the fact that,

> Internal controls cannot prevent bad judgment or decisions, or external events that can cause an organization to fail to achieve its operational goals. In other words, even an effective system of internal controls can experience a failure. Limitations may result from the:

- Suitability of objectives established as a precondition to internal control
- Reality that human judgment in decision making can be faulty and subject to bias
- Breakdowns that can occur because of human failures such as simple errors
- Ability of management to override internal control
- Ability of management, other personnel, and/or third parties to circumvent controls through collusion
- External events beyond the organization's control.[10]

Review and revise

An effective risk framework is not a static environment. It should continue to evolve as the risks in the firm are identified. Periodically re-evaluating the firm's risk is a key component to a successful compliance programme. Contemplate circumstances that may trigger revisions in whole or in part to a previously performed risk assessment. Opportunities to adjust the risk matrix may come as a result

of previous or uncovered compliance issues, changes in business initiatives and movement in the regulatory landscape. Consider reviewing the programme at least annually to ensure that risks are identified and mitigated or eliminated.

During this review, also assess whether the likelihood or effect of the risks has changed. Add new risks that have emerged since the previous review and decide whether controls exist or need to be developed. Periodically review and recalculate identified risks.

USING YOUR RISK MATRIX

Once the framework has been established, it should be the cornerstone to manage the compliance programme. It can guide conversations with management regarding new initiatives in the firm, the implementation of policies, procedures and controls, as well as increasing compliance resources. Align the risk assessment towards the key risks identified and use it as a roadmap for testing the compliance programme. Areas that present the highest risk may need to have a more frequent testing schedule than those with a lower risk rating. Use the risk assessment to understand potential conflicts of interest and make appropriate disclosures.

Develop key risk indicators (KRIs) to help safeguard the firm from future risk that may yet to be identified or quantified. What is a KRI? KRIs are metrics that predict potential risks that can negatively affect businesses. They provide a way to quantify and monitor each risk.[11] Their purpose is to predict potential risk and play an essential role in risk management by:

- Identifying any risk exposure relating to current or emerging risk trends.
- Assessing and quantifying each risk and its potential impact.
- Providing perspective through benchmarking.
- Enabling timely and ongoing risk control and monitoring.
- Enabling leaders and key personnel to receive alerts of potential risks in advance.
- Providing time to develop the appropriate and effective risk responses.
- Establishing objectivity within the risk management process.[12]

Ensure that the KRI aligns with the firm's strategic goals to ensure the appropriate priority can be given to key risks.

Firms can use the risk matrix to formulate the annual review of the compliance programme and report new or systemic risks to senior management. Align your annual risk assessments towards key risks identified and conduct targeted assessments of key compliance risks with a focus on policies, procedures and controls. For example, how has the COVID-19 pandemic changed your cybersecurity or business continuity planning? How are they addressed in policies and procedures? What are your controls? How are you monitoring and testing? Are there any potential operational losses related to this type of workforce structure? What has changed with oversight of advisers? This is an area where a targeted assessment of potential risk could uncover issues that were not previously considered or addressed.

Furthermore, the risk management programme will be a useful tool when communicating to management the role of compliance, the risks facing the firm and the controls designed to mitigate the risk. As resources are often scarce when it comes to compliance, the matrix can also drive related conversations.

CONCLUSION

There are many ways to conduct this exercise. Whether using the COSO framework, the Institute of Internal Auditors Three Lines of Defence[13] model, the Comptroller's

Handbook on Corporate and Risk Governance,[14] or a combination of methods, there is no wrong way. Firms do not need extensive education and background to develop a programme that identifies risk in order to begin the process. Programmes that are successful may take years to develop through communication, collaboration, oversight and continued revision.

Developing a risk framework as the basis for the compliance programme resonates with regulators. The process of mitigating risk begins with identifying the risks. This is a necessary element in implementing and maintaining a strong compliance programme. Firms can be assured that, at some point, they will be asked by a regulator to produce an analysis of the firm's risks and how they are mitigated.

References

(1) Rule 206(4)-7 under the Investment Advisers Act of 1940, Securities Act of 1933, Securities Exchange Act of 1934, and Investment Company Act of 1940, available at https://www.sec.gov (accessed on 20th January, 2022).

(2) US Securities and Exchange Commission 'What is Risk?', available at https://www.investor.gov/introduction-investing/investing-basics/what-risk (accessed on 23rd February, 2022).

(3) https://www.investopedia.com/terms/e/enterprise-risk-management.asp (accessed on 23rd February, 2022).

(4) di Florio, Carlo V. (8 February, 2011) 'Speech by SEC Staff: Remarks at the CCOutreach National Seminar', available at https://www.sec.gov/news/speech/2011/spch020811cvd.htm (accessed on 23rd February, 2022).

(5) Merriam-Webster Dicitonary (n.d.) 'Risk', in Merriam-Webster.com dictionary, available at https://www.merriam-webster.com/dictionary/risk (accessed on 24th January, 2022).

(6) Kaplan, R. S. and Mikes, A. (June 2012) 'Managing Risks: A New Framework', *Harvard Business Review*, available at https://hbr.org/2012/06/managing-risks-a-new-framework (accessed on 23rd February, 2022).

(7) Rule 206(4)-7 under the Investment Advisers Act of 1940, Securities Act of 1933, Securities Exchange Act of 1934, and Investment Company Act of 1940.

(8) CCOutreach 'Regional Seminars Investment Adviser Case Study Discussion Guide', US Securities and Exchange Commission, available at https://www.sec.gov/info/cco/cco_matrixguide.pdf (accessed on 23rd February, 2022).

(9) Frigo, M. L. and Anderson, R. J., Committee of Sponsoring Organizations of the Treadway Commission (January 2011) 'Embracing Enterprise Risk Management: Practical Approaches for Getting Started', available at https://www.coso.org/Documents/Embracing-ERM-Getting-Started.pdf (accessed on 23rd February, 2022).

(10) Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (May 2013), available at https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf (accessed on 23rd February, 2022).

(11) Auditboard (9th March, 2021) 'How to Develop Key Risk Indicators (KRIs) to Fortify Your Business', available at https://www.auditboard.com/blog/how-to-develop-key-risk-indicators-kris-to-fortify-business/ (accessed on 23rd February, 2022).

(12) *Ibid*.

(13) IIA (March 2015) 'Three Lines of Defence', available at https://www.theiia.org/ (accessed on 3rd February, 2022).

(14) Office of the Comptroller of the Currency (July 2019) 'Corporate and Risk Governance', available at https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/index-corporate-and-risk-governance.html (accessed on 23rd February, 2022).