Risk Management Framework (RMF)

By
THE INVESTOPEDIA TEAM
Updated December 30, 2022

Reviewed by
KHADIJA KHARTIT
Fact checked by
RYAN EICHLER

What Is Risk Management Framework (RMF)?

All companies face risk; without risk, rewards are less likely. The flip side of this is that too much risk can lead to business failure. Risk management allows a balance to be struck between taking risks and reducing them.

Effective risk management can add value to any organization. In particular, companies operating in the investment industry rely heavily on risk management as the foundation that allows them to withstand market crashes.

An effective risk management framework seeks to protect an organization's capital base and earnings without hindering growth. Furthermore, investors are more willing to invest in companies with good risk management practices. This generally results in lower borrowing costs, easier access to capital for the firm, and improved long-term performance.

KEY TAKEAWAYS

- Risk is a reality for business owners and managers regardless of the industry sector or size of the company.
- Well-run companies will have a comprehensive risk management framework in place to identify existing and potential risks and assess how to deal with them if they arise.
- Risk identification, measurement, mitigation, reporting and monitoring, and governance are the six key pieces of an effective framework.

Understanding Risk Management Framework (RMF)

Effective risk management plays a crucial role in any company's pursuit of financial stability and superior performance. The adoption of a risk

management framework that embeds best practices into the firm's risk culture can be the cornerstone of an organization's financial future.

The 5 Components of RMF

There are at least five crucial components that must be considered when creating a risk management framework. They include risk identification; risk measurement and assessment; risk mitigation; risk reporting and monitoring; and risk governance.

Risk Identification

The first step in identifying the risks a company faces is to define the risk universe. The risk universe is simply a list of all possible risks. Examples include IT risk, operational risk, regulatory risk, legal risk, political risk, strategic risk, and credit risk.

After listing all possible risks, the company can then select the risks to which it is exposed and categorize them into core and non-core risks. Core risks are those that the company must take in order to drive performance and long-term growth. Non-core risks are often not essential and can be minimized or eliminated completely.

Risk Measurement

Risk measurement provides information on the quantum of either a specific risk exposure or an aggregate risk exposure and the probability of a loss occurring due to those exposures. When measuring specific risk exposure it is important to consider the effect of that risk on the overall risk profile of the organization.

Some risks may provide diversification benefits while others may not. Another important consideration is the ability to measure an exposure. Some risks may be easier to measure than others. For example, market risk can be measured using observed market prices, but measuring operational risk is considered both an art and a science.

Specific risk measures often give the profit and loss ("P/L") impact that can be expected if there is a small change in that risk. They may also provide information on how volatile the P/L can be. For example, the equity risk of a stock investment can be measured as the P/L impact of the stock as a result

of a 1 unit change in, say, the S&P500 index or as the standard deviation of the particular stock.

Common aggregate risk measures include value-at-risk (VaR), earnings-at-risk (EaR), and economic capital. Techniques such as scenario analysis and stress testing can be used to supplement these measures.

ISO 31000 is a set of international standards associated with risk management and mitigation.

Risk Mitigation

Having categorized and measured its risks, a company can then decide on which risks to eliminate or minimize, and how many of its core risks to retain. Risk mitigation can be achieved through an outright sale of assets or liabilities, buying insurance, hedging with derivatives, or diversification.

Risk Reporting and Monitoring

It is important to report regularly on specific and aggregate risk measures in order to ensure that risk levels remain at an optimal level. Financial institutions that trade daily will produce daily risk reports. Other institutions may require less frequent reporting. Risk reports must be sent to risk personnel who have the authority to adjust (or instruct others to adjust) risk exposures.

Risk Governance

Risk governance is the process that ensures all company employees perform their duties in accordance with the risk management framework. Risk governance involves defining the roles of all employees, segregating duties, and assigning authority to individuals, committees, and the board for approval of core risks, risk limits, exceptions to limits, and risk reports, and also for general oversight.

What Is the NIST Risk Management Framework?

The NIST Risk Management Framework is a federal guideline for organizations to assess and manage risks to their computers and information systems. This framework was established by the National Institute of Science and Technology to ensure the security of defense and intelligence networks.

https://www.investopedia.com/articles/professionals/021915/risk-management-framework-rmf-overview.asp

Federal agencies are required to comply with the risk management framework, but private companies and other organizations may also benefit from following its guidelines.1

What Is the COBIT Risk Management Framework?

COBIT, or the Control Objectives for Information and Related Technology, is a framework for the management and governance of enterprise IT. It was developed by the Information Systems Audit and Control Association (ISACA) to set reliable auditing standards as computer networks became more important in financial systems.2

What Is the COSO Enterprise Risk Management Framework?

The Enterprise Risk Management–Integrated Framework is a set of guiding principles established by the Committee of Sponsoring Organizations to help companies manage their business risks. It was originally published in 2004, although COSO has issued several updates to the framework as risk management practices have evolved.3

The Bottom Line

Risk management is an essential part of running a business. As the market landscape changes, companies must constantly evaluate and re-assess their own risk profiles. Having a strong risk management framework can help organizations identify and prepare for the different threats and dangers that they might face.

https://www.investopedia.com/articles/professionals/021915/risk-management-framework-rmf-overview.asp