MITRATECH

Operational Risk Management Framework

Operational risk management consists of implementing 6 individual steps for all risks that occur within the organization. The purpose is to identify, assess, analyze measures, make decisions, mitigate and review. Essentially, these steps would repeat each time a new or major risk event surfaces.

1 Identify the Risk

- Review the task.
- List the risks.
- Understand the scope of the risks.
- Review current and future business strategy against the list of possible risks.
- Create a library of risks and related items which include policies and procedures, regulations, controls, tests and indicators.

2 Perform Regular Cyber Risk Assessments

- Assess the level of exposure.
- Assess the severity of the worst possible event outcome.
- Assess the probability that the event will occur.
- Determine the level of risk.

3 Analyze Risk Control Measures

- Identify control measures for each risk.
- Change the process to eliminate the risk.
- Improve task design.
- Limit exposure.
- Provide additional training.
- Provide appropriate warnings or cautions.
- Effectiveness of control measures can be determined by assessing the residual risk remaining after control measures are in place.

4 React, Recover & Review

- Decisions are made so that actions can follow.
- Make decisions as early as possible, so that you have more time to assess your risk.
- Make control decisions to take advantage of all potential benefits.

5 Implement Risk Controls

- Controls are implemented to limit the exposure of the organization to the risk and the potential damage.

6 Supervise & Review

- The implemented risk controls should be reviewed regularly to ensure that controls are being followed correctly.
- Additional reviews are necessary if the implemented control does not provide the required level of risk control at optimum cost.

Mitratech's Operational Risk Components

Diving deeper into the six-step framework detailed above, an organization's operational risk framework should consist of further key components, which are namely: Risk and Control Self Assessments (RCSA's), Risk Identification, Risk Quantification, Internal and External Loss Events and Scenario Modelling.

It is the responsibility of the organization to ensure that the operational risk framework provides comprehensive coverage across the different operational risk event types, and to perform ongoing assessments of not just the individual components, but the overall success of the framework.

1 RCSA's & Risk Identification

- Incorporates 6-step ORM framework.
- Gathers results from assessments.
- Involves various business units.
- Provides risk transparency.

RCSAs are an integral component of an operational risk framework, they involve the participation of both top management and staff across all levels in order to better assess the organization's overall risk profile. Cross-functional controls and risks are also better understood and discussed which further promotes transparency. However, problems can arise given the variety of views around topics such as who should perform the RCSA and which methods to use. Thus, it is not surprising that many organizations unwittingly fail to perform these tasks adequately.

Challenges can also include:

- Administrative: Reliance on paper processes or a plethora of spreadsheets with a lack of version control or security.
- Cultural: Lack of management support in the process.
- Value to the firm: Inadequate reporting and monitoring across the organization.

Mitratech's GRC Platform offers predefined RCSAs, yet still customisable to your business needs and can be sent across the organization and to external stakeholders within minutes. Assessment answers and risk insights are derived in real-time, providing deep insight and clear identification of risks.

The Risk Control Self Assessment (RCSA) funcionality within Mitratech's Alyne offers a structured variant for identifying and recording risks. Based on a library of over 1000 questions, surveys can be carried out across your organization. Based on the answers received, Alyne can automatically suggest risks which can be transferred directly to a risk register.

The risk identification capabilities within Mitratech's Alyne will help your business units – your primary sources of risk information within the organization – to articulate their risks as accurately as possible. Actively placing greater emphasis on the risk identification stage will make for successful risk management further down the line.

2 Risk Quantification

- Assesses the level of exposure.
- Places a value on the risks the organization faces.

Every financial institution has different tolerance for risks, meaning that portfolio managers do not have a one-size-fits-all approach for all risks. Risk quantification involves analyzing and evaluating risks and their interactions to predict potential risk events. It is not uncommon for financial institutions to use a range of risk models to analyze their risk profiles. However, the problem with risk models is that they are often generalized and overlook the complexity of the individual organization. New advancements in technology, allow business leaders to easily conduct assessments that can help them quickly identify risks that can potentially cause damages and losses to the organization. These sophisticated approaches allow organizations to assign a monetary value to each individual risk and ultimately quantify their investments.

Operational risk management does not stop once risks have been identified and managed. In order to obtain an accurate view of a financial institution's risk profile, actual losses from internal and external events should be captured and recorded.

3 Internal Loss Events

- Inward-looking element.
- Actual event losses that can be quantified and validated.
- Provides opportunity to learn from hindsight.

Quantified and validated data collected from these events helps the organization to better understand their decision-making process and allows for further improvement and adjustments to steps taken for future events.

4 External Loss Events

- Outward-looking element.
- Provides a more holistic outlook towards factors affecting the organization's business objectives.

This prevents organizations from having a myopic view towards potential threat and risks that may otherwise jeopardize business operations. They serve as a constant reminder that risks have to be better managed using peripheral vision.

5 Scenario Analysis

- Forward-looking element.
- Serves as a means to explore potential extreme events.
- Increases preparedness to handle risk events.

Data from external/internal loss events may be utilized for increased accuracy of analysis results. Within the risk identification process, a typically bad and far too common approach here is having different business units contribute their risks for the quarter, based on the risks that they can identify, leading to the process of risk identification being subjective and people-driven, as opposed to data-driven.

Roadmap

- Define RCSA templates and customize for individual business areas and target recipients.
- Define risk categorisation and reporting structure that is sufficiently granular to group the right people without fragmenting to a point where you lose track of the big picture.
- Define risk appetite for each risk category.
- Assess current exposure.
- Establish and operationalise recurring lightweight and smart processes.

Take Action Now

We believe in simplifying, digitizing and automating operational risk management processes.

Mitratech's GRC Platform enables organizations with next-generation technology that optimizes the operational risk management capabilities of any organization.

Learn more about how we can provide you with some powerful advantages to fully enhance your risk management processes.