BASG Insights

OPERATIONAL RISK MANAGEMENT .... SCOPE, CHALLENGES, SOLUTIONS AND BENEFITS

March 2024

THE SCOPE OF OPERATIONAL RISK MANAGEMENT (ORM)

In the beginning "Risk" was a single initiative, driven by one team, and focused on all the possible risks facing an organization. Over time, "Risk Management" has grown into a multi-faceted effort within most organizations, a package of varied initiatives linked under the umbrella of Enterprise Risk Management (ERM).

In this article the focus is 100% on Operational Risk Management (ORM) which is a subset of ERM but excludes strategic, reputational, financial and market risk.

Operational risk is an organization's risk of loss because of **ineffective or failed internal processes, people, systems, or external events which can disrupt the flow of business operations.** While this risk can result in monetary loss or the diminution of a company's good name or goodwill, ORM is not the same as, or restricted to, either Reputational Risk or Financial Risk.

When considering ORM, the #1 goal is to **prioritize potential risks to the organization** based on their **impact on the organization.** Though most organizations have specific job categories that are exclusively focused on avoiding and mitigating risk, a successful Operational Risk Management program belongs to everyone within the organization, every person who is charged with leadership, every employee who touches a process, engages with a client, or performs any task within the organization.

It cannot be stressed enough that ORM is a top to bottom effort and an organization's mantle of protection is only as strong as the weakest link within the company. History has shown that major risk issues can be caused by the action, or lack of action, of someone buried deep in the organizational chart.

> IF EVERYONE IS POTENTIALLY PART OF THE PROBLEM, IT FOLLOWS THAT EVERYONE MUST BE PART OF THE SOLUTION.

Examples of operational risk include:

- Employee conduct whether intentional or un-intentional
- Employee error, frequently related to a lack of training or a lack of communication
- Cybersecurity attacks
- Technology risks
- Business processes and/or controls that are ineffective, outdated, not enforced, or non-existent
- Physical events, such as natural disasters
- Internal and external fraud
- Workplace safety
- System failures

The Standardization of Operational Risk

As Risk Management passed through its maturation phases, several factors led to a standardization of ORM. At the top of that list are (1) An overall demand for higher levels of insight. (2) The heightened competitive, regulatory and reputational pressure to know that a company can survive a risk disaster and efficiently mitigate the risk.

Though originally geared towards financial services, today risk management has spread throughout the business world. The original release of COSO's Internal Control-Integrated Framework, and the subsequent release of the Sarbanes-Oxley Compliance Act, plus an array of other governance directives, inevitably led to increased pressure on organizations to have an effective ORM discipline in place.

IDENTIFICATION, ASSESSMENT, MITIGATION, MONITORING

Operational Risk Management attempts to reduce risks through a multi-step process of **Identification, Assessment, Measurement and Mitigation, Monitoring and Reporting.**

There are four steps to consider at the onset when creating an ORM program:

1. Decide what overall level of risk to accept across the organization.
2. Identify those risks where the benefits that come from accepting the risk outweigh the potential cost.
3. Develop, document and assign accountability around a plan to anticipate and manage risk.
4. Ensure that risk decisions are managed at the appropriate level within the organization and that all the essential contributors are identified and involved.

Primary Objectives of Operational Risk Management

While other risk disciplines, such as Enterprise Risk Management (ERM), emphasize optimizing risk appetites to balance risk-taking and potential rewards, ORM processes primarily focus on controls and minimizing or eliminating risk. The ORM framework starts with risks and decides on a mitigation strategy.

The Risk Management Association defines operational risk as:

"The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events, but is better viewed as the risk arising from the execution of an institution's business functions."

If an organization adopts this definition, then the scope of operational risk management will include cybersecurity, fraud, and all internal control activities.

Applying a control framework, whether a formal framework or a home-grown model, will help when designing the internal control processes. Arranging the sources of risk into definable categories is a good starting point.

People

In the context of ORM, "people" includes both employees and non-employees such as customers, vendors, contractors, and other stakeholders.

Either category can pose a risk to the organization in a wide variety of ways. The most common are human error or intentional wrongdoing such as fraud or breach of policy. But risk vulnerability can also be the result of insufficient management guidance or poor training, bad decision-making at any level of the organization, or even careless/irresponsible use of social media.

Because dealing with risk is a top to bottom effort, it is imperative that everyone is fully trained and that frequent communication is shared across the organization to update policies, procedures, processes, and plans as needed. Keeping the full team aware of any potential risks and sharing what has gone right or wrong within the organization and its competition can be key to managing risk.

Further, the more each person understands and is conscious of his/her individual role in risk protection, the greater the chance of avoiding a problem. Motivating vigilance comes in large measure from instilling an enterprise wide understanding of the potential consequences from even a minor ORM event.

Technology

Technology risk from an operational standpoint includes hardware, software, privacy, and security spanning the entire organization. Creating and maintaining effective Business Continuity Plans to address risks related to technology failures and other disruptions is essential.

Examples include:

- Hardware limitations can hinder productivity, especially in a remote work environment.
- Software can reduce productivity when applications suffer an outage or employees lack training.
- Software can impact customers as they interact with the organization.
- External threats include hackers who attempt to steal information or hijack networks.

Regulations

The risk of non-compliance with regulation exists in some form in every organization. Some industries are more highly regulated than others, but all regulations come down to operationalizing internal controls.

Understanding the sources of risk will help determine who manages risk. Enterprise Risk Management and Operational Risk Management both address risks in the same areas but from different perspectives. In an effort to consolidate these disciplines, some organizations have implemented Integrated Risk Management or IRM. IRM addresses risk from a holistic point of view. Depending on the objective of the particular risk practice, the organization can implement technology with different parameters for both ERM and ORM.

Steps in the ORM Process

Operational Risk Management is generally applied as a five-step process and all five steps are critical.

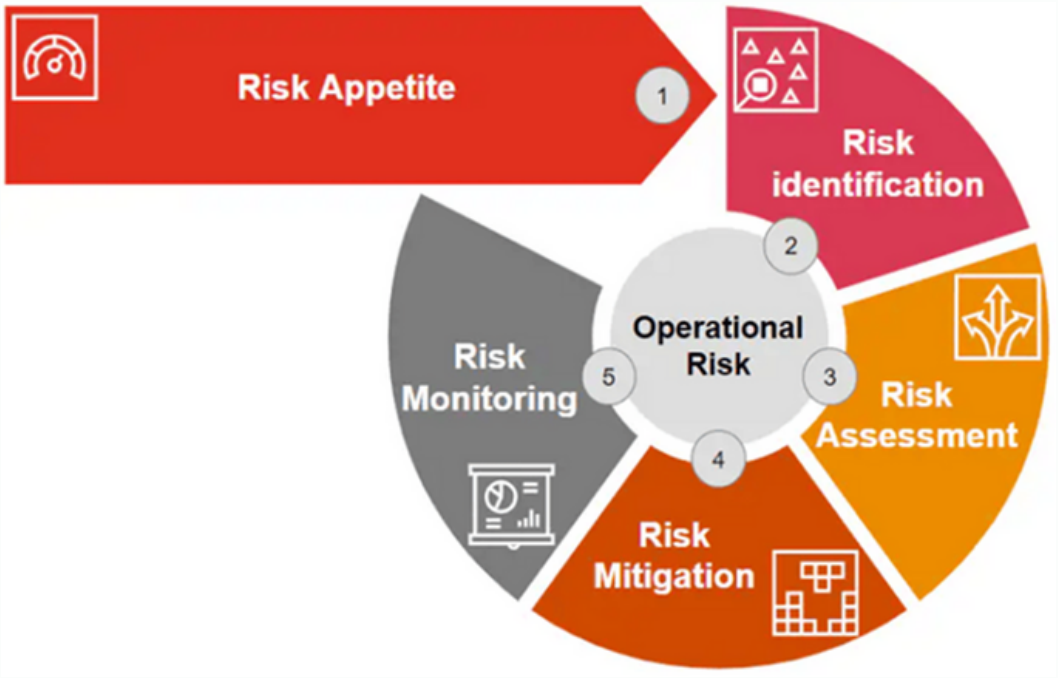

Image source: PWC Operational Risk Management

Step 1: Risk Identification

You cannot control what you have not identified. Risk identification starts with understanding the organization's objectives. Risks are anything that would prevent the organization from achieving those objectives. Asking "What could go wrong?" is a great start when talking about risk identification. No area, no process, no program, no interaction is off the table when it comes to that discussion and the decisions made.

> "WHAT COULD GO WRONG?"

Step 2: Risk Assessment

Risks are assessed using an impact and likelihood scale called a Risk Assessment Matrix. At this stage, risks are categorized by type of risk and level of risk.

It may not be possible or prudent for an organization to address every identified risk. Effective and realistic prioritization is critical for the management of operational risk and allows teams to pinpoint the most significant risks.

Developing an operational risk program begins with a meeting of the minds. A collaborative effort requiring that risk management teams and business process owners work in harmony to identify risks and controls in the organization.

While every organization will approach measuring operational risk differently, one of the first steps to understanding the nature of operational risks is through a **Risk and Control Self-Assessment (RCSA)**. The RCSA is a framework providing an enterprise view of operational risk and can be used to perform operational risk assessments, analyze an operational risk profile, and create an effective plan for managing risk. The RCSA is at the core of an organization's overall operational risk framework.

An RCSA requires:

- Documentation of all the risks.
- Identifying the risk levels for each by pragmatically estimating the frequency and the impact of the risk.
- Codifying the controls and processes related to those risks.

The RCSA should be developed to serve as a reference for an organization's risk initiatives. Below are several widely adopted best practices for developing a Risk and Control Self-Assessment:

- Integrate Risk and Control Self-Assessment programs into operational risk initiatives.
- Establish standard risk terminology and consistent methodologies to measure and assess risk.
- Develop a complete view of risks and controls.
- Incorporate a trend analysis methodology into the RCSA to identify risk patterns and potential control failures.
- Create a method for identifying non-financial risks that may impact the bottom-line.
- Use an RCSA as the guideline for budgeting operational risk management initiatives.

Step 3: Risk Mitigation

In the Operational Risk Management process, there are four options for addressing potential risk events: **transfer, avoid, accept, and mitigate.**

Transfer:
Transferring simply shifts the risk to another organization. This is commonly accomplished by outsourcing or insuring. When outsourcing, management cannot completely transfer the responsibility for controlling risk. But insuring can transfer some of the financial impacts of the risk to an insurance company.

A simple example of transferring risk happens when a company purchases software. Steps taken to fully vet the vendor and the emphasis placed on regular vendor updates improve the success level of the transfer.

- Check out the integrity and history of the vendor.
- Be sure to include a well-defined data breach insurance plan in the contract to ensure that the vendor can pay for damages in the event of a breach.
- Request and receive regular updates from the vendor's data center showing there are sufficient controls in place to minimize the likelihood of a breach.

TRANSFER, AVOID, ACCEPT, AND MITIGATE

Avoid:
Avoidance prevents the organization from entering a risk-rich situation or environment. For example, when choosing a vendor, hiring an employee, or using a sub-contractor for a service, a full and complete due diligence effort is mandatory with no room for short cuts in the procedure. The posture should be, "What you don't know can hurt you".

"WHAT YOU DON'T KNOW CAN HURT YOU"

Accept:
Based on the comparison of the risk to the cost of control or value from the potentially risky action, management could accept the risk and move forward. As an example, there is the risk an employee could become ill from enjoying the box of luscious donuts in the breakroom. However, the goodwill gained by providing these treats outweighs the risk.

Mitigate:
Mitigating risks involves implementing action plans and controls that reduce the likelihood of the risk and/or the impact it would have if the risk were realized. For example, if an organization allows employees to work from home, there is a risk that comes from the use of a public internet. Implementing a VPN, and establishing firm documented policies regarding data and internet usage, can reduce the likelihood of data leakage and mitigate the risk.

Step 4: Control Implementation

It is a proven fact that very few risks can be completely eliminated. Understanding the residual risk — the risk remaining after mitigation — is an important part of the risk mitigation phase of ORM.

Once risk mitigation decisions are made, action plans are formed, and residual risk is identified, the next step is implementation. Controls should be designed specifically to address and mitigate **each specific risk.** The control rationale, objective, and actions **must be fully documented** so the controls can be clearly communicated to everyone involved. **Only then is compliance possible and therefore it can be required and expected from each person.**

Controls might take the form of a new process, adding an additional level of review or accountability, or built-in controls that deter malicious activities. Controls should be designed to be preventive, rather than detective or corrective. But there is also a need for some detective and corrective controls. It is often impossible to prevent a risk from occurring, which is where detection and correction come into play. Detecting anomalies and then correcting them may be sufficient to mitigate certain risks.

Once controls are created and in place, **a yearly review (at minimum) is critical** to determine whether additional controls are needed based on changes within the organization that might come from growth or new policies, etc.

Step 5: Monitoring

Since no employee is infallible, and the environment can and will change over time, it is essential that solid control monitoring is in place. This is simply the testing of every control's design and effectiveness. Any issues detected can then be addressed and resolved at the appropriate level.

A YEARLY REVIEW IS CRITICAL

Within the monitoring step in Operational Risk Management, some organizations have adopted continuous monitoring or early warning systems built around **Key Risk Indicators (KRIs)**. KRIs are metrics that provide an early signal of increasing risk exposure and can be designed to monitor any potential risk and send a notification.

KEY RISK INDICATORS ARE ESSENTIAL

CHALLENGES OF MATURING ORM

In today's competitive marketplace, even a well-developed ORM program can get lost or overlooked in the interest of reaching other goals. The challenges of maturing ORM within an organization are many.

- Lack of sufficient resources to invest in operational risk management or ERM.
- Lack of communication and education -- FROM THE C-LEVEL DOWNWARD -- around the importance of operational risk management and the consequences of operational failures on a company's bottom line.
- Lack of consistent methodologies to measure and assess risk reduces the accuracy of a risk profile.
- Carelessly crafted standard risk terminology.
- Processes that are varied, complex or confusing.
- Not giving appropriate attention to ORM.

THE CHALLENGES OF MATURING ORM WITHIN AN ORGANIZATION ARE MANY

SOLUTIONS TO FOCUS ON

In the process of creating an operational risk framework and program, areas the team should focus on include:

- Promoting an organization-wide understanding of the program's value and function.
- Leveraging technology to implement an automated approach to monitoring and collecting risk data.
- Establishing an effective method for evaluating and identifying principal risks in the organization and a way to continuously identify and update those risks and associated measures.
- Working to reduce material risk exposures while conceding activities where the benefits outweigh the risks.
- Partnering ORM with other functions in the organization to better embed best practices into the organization.

BENEFITS OF OPERATIONAL RISK MANAGEMENT

Establishing an effective operational risk management program is critical to achieving an organization's strategic objectives while ensuring business continuity in the event of a disruption.

Having a strong ORM program also demonstrates to clients, investors, and staff that the company is prepared for crisis and results in improved monetary and competitive advantages such as:

- Stronger relationships with customers and stakeholders.
- Greater investor confidence.
- Better performance reporting.
- More sustainable financial forecasting.
- A savings in dollar costs by preventing or correcting loss events.

BASG

About BASG Insights

BASG Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and non-government organizations. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and leaders.

BASG Insights is an imprint of Business Advisory Solutions Group, LLC.

About BASG

Business Advisory Solutions Group supports business profitability and growth by standing at the intersection of People, Process and Technology. BASG has delivered tangible results that improve productivity, mitigate risk, and maximize profits for organizations. Our Clients range from Fortune 500 companies to mid-sized and owner-managed businesses across a broad range of industries.

704.887.3493 WWW.BASGLLC.COM INFO@BASGLLC.COM

15720 BRIXHAM HILL AVENUE, SUITE 300, CHARLOTTE, NC 28277