MITRATECH

ERM
Mitratech
White Paper

Enterprise Risk Management

A single platform for the entire risk management lifecycle.

INTRODUCTION

Proper Enterprise Risk Management is not a tick-the-box exercise, but rather a business value exercise.

In today's ever changing business world, the risk landscape of all organizations, no matter the size, is constantly evolving. Lower depth in value chains, fastly rising risks, and demands for greater resiliency, to mention a few, are being forced upon businesses with a fierce velocity.

Capturing these impacts and evaluating them within the context of a mature enterprise risk management lifecycle is essentially demanding a full transformation of the discipline.

New risk management dimensions in Environmental, Social and Governance (ESG), Third-Party Risk Management (TPRM), operational and cyber resilience are emerging and expanding in importance, as threats to the organization become more dynamic and frequent than ever, drastically compressing the optimal reaction time of enterprises. For this reason, risk managers might find it exceedingly challenging to navigate the broad range of interrelated risk scenarios.

Risk managers are being called to meet higher standards, adhere to rising regulations and demonstrate greater transparency in their risk management processes. Business is complex and volatile by nature, meaning that organizations need to utilize the correct information in order to prioritize and effectively manage changes. The stringent requirements for company-wide risk management, is challenging business leaders in a variety of ways by introducing concepts like risk-bearing capacity or risk aggregation – posing questions around the methodology of the risk management system and also to what extent, and at which process, quantitative approaches are useful and/or necessary. For many risk managers, these requirements mean a significant adjustment of the previous risk management processes within the company, which they have to deal with in addition to everyday tasks.

Not too long ago, risk management was nothing more than an afterthought for business executives, isolating the task within the company's risk team, if there even was one. Nowadays, executive boards, decision makers and regulators alike, are highly focused on the risk management landscape, as they are very much aware that critical risks must be identified, managed and mitigated efficiently to avoid them from derailing the entire company, resulting in massive losses.

Many organizations are still using a spreadsheet approach to managing their risks, which more often than not results in questions such as, "What are my actual risks?" Along with subjective values placed on non-financial risks, rather than objective ones. On the other hand, many teams still view risk management as a tick-in-the-box exercise that becomes a tedious task for quarterly reporting to board and senior management.

Proper risk management can provide your organization with tremendous value, enabling you to not only meet compliance requirements easily, but help you truly gain value from the process to ultimately serve the wider business. When conducted well, you gain clarity on your risk posture and understand your business better, meaning that risk management should no longer be an obstacle, but rather a critical process that enables the business to succeed.

Simply designing mitigation strategies is no longer an option. Business leaders need sophisticated analytics and expert insights to accurately navigate the diversity of risks organizations face. They need a holistic enterprise risk management solution capable of covering all bases, from risk identification to calculating value at risk. Using highly integrated, AI-enabled and data-driven tools can help design risk strategies with the mission of protecting the company.

In this document, we will be taking you from a conventional spreadsheet risk management approach, to identifying actual Value at Risk – which is not a simple topic to address, particularly when dealing with cyber risk and non-financial risks. Learn how you can implement a full end-to-end risk management process within your organization.

RESHAPING THE RISK LANDSCAPE & CYBER RISK MANAGEMENT

Reshaping the Landscape

The current business landscape requires proactive, integrated solutions encompassing people, data and infrastructure. Organizations should establish well-defined direction from the top level so that there is clarity on how to act when challenges emerge.

Organizations need to move at a rapid pace to deal with risks as they evolve, and this can't be accomplished if risk management is not a priority. New technologies enable organizations with cutting-edge capabilities that encompass data, analytics and modeling. Furthermore, collaboration is key to achieve smarter processes that will ultimately save valuable time, effort and money.

When developing a fully holistic ERM strategy we must consider key use cases like Cyber Risk Management, Environmental, Social and Governance (ESG) Risk Management and Third-Party Risk Management. These topics are already top of mind for many risk professionals and will only increase in importance as the years go by.

Cyber Risk Management

Cyber risks are changing the game in ways that we never thought possible and have become more frequent and precise than ever before.

Strengthening your organization's cyber risk management capabilities is key to building a comprehensive ERM strategy that ensures defense against information security attacks. Leveraging both mandatory and voluntary standards is a crucial step in successful cyber risk management practices.

Aim for the following in your cyber risk management lifecycle:

1. Obtain full visibility of your assets.

   Because cyber risks are often linked to assets that are capable of being attacked (this includes applications, servers and end user computers), it is imperative to have an overview of all potentially compromised assets.

2. Define which protection measures must be ensured.
3. Determine which of your assets must have specific protection measures.
4. Link standards, laws and regulatory policies to protection measures.
5. Check compliance with protection measures and identify information risks.

Learn all about Mitratech's Cyber Risk Management capabilities here.

ESG RISK MANAGEMENT

ERM and ESG risks have a significant intersection. It is important that your organization understands its ESG performance, risks, and impacts.

In recent years, corporate sustainability has become a widely used global benchmark for non-financial performance. 'Sustainability', a term used to encompass a broad spectrum of topics, is today a concept that is not just about environmental factors but involves building resiliency into infrastructures. With the recent press release from the US Securities and Exchange Commission (SEC), the Climate and ESG Task Force will be coordinating and developing initiatives to identify ESG-related misconduct, in response to the increasing investors' focus and reliance on ESG-related performance and disclosure.

Consistent with the non-profit organizations that are championing ESG causes, regulators are also imposing stricter ESG regulations and demanding greater transparency and accountability through ESG disclosures. In the past decade, we have witnessed the growing investor requirement for ESG data in response to increased awareness of the financial materiality of ESG risks, amongst other factors. In doing so, these socially conscious investors will use ESG ratings in several ways, including assessing and managing their exposure to ESG-related risks and engaging with investee companies. As a result, most firms recognized the commercial need to take action; such that they do not miss out on valuable investment opportunities.

The increased scrutiny and pressure on ESG topics can be felt, even as business leaders continue to wait for a clear mandate for their sustainability reporting. While there are varying requirements for corporates and sovereign bodies, and no single framework has yet emerged as an industry standard, there are different relevant classifications and approaches that organizations can take. Mitratech has selected three key standards to map the Mitratech ESG Risk Framework, to simultaneously support corporate reporting.

Learn all about Mitratech's ESG Framework here.

THIRD-PARTY RISK MANAGEMENT (TPRM)

Being able to have a 360 degree risk view of your organization's vendors is key to achieve a fully holistic ERM lifecycle.

Aim for the following in your cyber risk management lifecycle:

1. Configure your Vendor Management Workflow

Start with all required vendor governance workflows that follow your organizational processes. Categorize your vendors by risk exposure and other criteria to fully refine your analysis.

2. Gather Data

Gain data and information on your vendors through security performance indicator platforms like SecurityScorecard. Filter and sort your vendor portfolio based on security criteria in real-time.

3. Launch Assessments

At scale assessments provide a detailed analysis of your vendors. Make sure you are asking the right questions and getting meaningful answers in compliance with relevant standards, laws and regulations.

4. Analyze Maturity Details

Advanced analytics enable you to pinpoint uncertainty in performance and potential sources of risk in assessment responses, as well as automate risk identification and qualification.

5. Benchmark and Aggregate Vendor Portfolio

Analyze similar data points and compare or aggregate results. Benchmark vendor cohorts in the context of standards, laws and regulations.

6. Continuously Manage Vendor Risk

Integrate vendor insights into your Enterprise Risk Management (ERM), by executing the full risk lifecycle of your vendors, from status and review workflows, on an asset or portfolio basis.

Learn all about Mitratech's TPRM capabilities here.

SIX STEPS FOR END-TO-END ENTERPRISE RISK MANAGEMENT

1. Define Context

- Define risk bearing capacity and risk appetite.
- Determine hierarchies and organizational levels.
- Harmonize risk taxonomy and align control framework.

2. Identify Risks

- Leverage predefined risk scenarios paired with an easy RCSA process.
- Apply maturity gap analysis (RCSA) in a structured questionnaire.
- Facilitate scenario analysis where appropriate and meaningful.
- Follow risk documentation requirements.

3. Qualify Risks

- Understand the root cause of identified risks.
- Classify risks by organizational structure and risk categories.
- Calculate impact and probability based on defined risk scenarios and deviations in maturity.

4. Quantify Risks

- Calculate value at risk with guided risk loss estimator calculator.

5. Manage Risks

- Risk exposure vs risk appetite.
- Easily implement mitigation measures.
- In-app collaboration and communication.

6. Aggregate Portfolio

- Run Monte Carlo simulations across the risk portfolio to calculate value at risk.
- Provide guidance on interpretation of value at risk.
- Accomplish board-ready reporting.

1. Define Context

Conventional Approach	The Challenge	Mitratech's Approach
Typically start with threats, then move to vulnerabilities and risks to arrive at their controls.	Redundancy. Achieving completeness.	Define risk bearing capacity and risk appetite. Determine hierarchies and organizational levels. Use harmonized risk taxonomy and align control framework.

Many use a risk-first approach to arrive at their controls, starting with the threats and vulnerabilities that already exist – resulting in gaps and a great lack of completeness within their control framework. Mitratech's GRC platform offers a harmonized control framework based on, and mapped to, relevant standards, laws and regulations that are applicable to your organization, helping you achieve completeness in your control framework. Each control is also designed to be specific, atomic and most importantly, understandable.

Another common procedural approach to addressing risk and compliance is across the second line, where each function is mandated with identifying all relevant risks and formulating controls to mitigate these risks. If stakeholders in the second line are doing a good job, this will lead to a large overlap of redundant controls that create maintenance costs. When a regulator or auditor changes the regulatory landscape, this excessively large control framework must be analyzed for compliance resulting in higher cost.

When risks are initially recorded, the question of how the organization deals with these risks still remains. An essential basis for considering whether risks are to be accepted, reduced or transferred is a clear definition of organizational tolerances. Informed decisions about the treatment of individual risks is only possible if sensible 'guard rails' in the form of both, risk-bearing capacity and risk appetite, are defined.

An overall position above the defined risk appetite should be addressed using suitable mitigating measures. From a business perspective, the gap between the defined risk appetite and the actual overall position can be used for strategic initiatives. These decision-making options can only be achieved through transparency and a methodically accurate survey of the risk appetite.

In order to define the context for your risk management lifecycle, you need to first define the specifics regarding which levels of the organization should raise and manage risk and, lastly, create hierarchies. For example, this could be segmented by region, business units, business entities or headquarters.

Success Factors

Involving the Right Stakeholders is Critical

In order to define your Risk bearing capacity, you need to understand the overall financial situation of your organization and only after, determine your risk appetite – the loss potential that the company is willing to accept. The relevant procedures for determining these are never easy and unfortunately there is not a one-size-fits-all solution, however, involving the right stakeholders is critical to understanding roles, tolerances and deciding on the level in which the risk appetite is defined (organizational level, technical dimensions, board departments, etc.). Defining the context of your risk appetite is driven by the company's reality, as you can't decide based on equity or liquidity that does not exist.

Continuous Review

Risks are continuously developing, sometimes suddenly, and their changes are of course not adapted to any quarterly survey frequency. Therefore, the collection, evaluation and management should also be a continuous process, ensuring that the sum of all values does not exceed the risk appetite.

2. Identify Risks

Conventional Approach	The Challenge	Mitratech's Approach
Ask different business units to contribute with their risks.	Articulating risks without factual and centralized data leads are often subjective and prone to error.	Leverage predefined risk scenarios paired with an easy RCSA process. Apply maturity gap analysis (RCSA) in a structured questionnaire. Facilitate scenario analysis where appropriate and meaningful. Follow risk documentation requirements.

With a control framework in place, you need to move on to the actual process of identifying the risks you need to manage. A typically bad, and far too common, approach is having different business units contribute their risks on a quarterly basis, based on risks that they can think of, leading to the process of risk identification being subjective and people-driven, as opposed to data-driven. To counter this, Mitratech has defined more than a thousand risk scenarios, as well as suggestions of which risks apply based on actual deviations and deficiencies within controls.

The risk identification capabilities in Mitratech's GRC platform 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 a successful risk management lifecycle further down the line.

Success Factors

Completeness

The structure of risk recording should aim to be complete. Regarding risk recording as a pure re-release of already recorded risks, or to complete it prematurely due to a lack of creative techniques, is certainly not a sufficient approach. Standards and considerations along the process chain or questionnaires offer a good starting point.

Identify Meaningful Risks

The risk identification process is often neglected and fragmented across the central risk departments, as well as left to the decentralized departments who conduct these processes without guidance nor oversight. Generating value and transparency in risk management requires reliable risk assessment routines – a single source of truth which is easily accessible. Spend time identifying non-trivial risks and look much further than just the obvious, generic ones. Simply copying and pasting risks from the last cycle won't suffice here as risks are constantly changing.

Making sure that you identify meaningful and actionable risks will set you in good stead for mitigation and management. Having a single integrated platform that contains consolidated qualitative and quantitative data, allows risk managers to easily and efficiently identify problems in order to make informed decisions. This method encourages business leaders to take a preventive approach rather than a reactive one.

Involve the Right People

Risk identification needs to be a bottom-up approach. Involve people who deeply understand the different areas of risks and not only the one person who was delegated the task.

Involve People in an Active Risk Culture

Favor collaboration and communication over bureaucracy, have people collaborate actively throughout the risk process – especially for identification. Qualify risks rather than just simply capturing them.

3. Qualify Risks

Conventional Approach	The Challenge	Mitratech's Approach
Set generic criteria for setting the scale of impact and probability.	Interpretation of the specific risk on how it relates to the generic criteria.	Understand the root cause of identified risks. Classify risks by organizational structure and risk categories. Calculate impact and probability based on defined risk scenarios and deviations in maturity.

Now that you have identified your risks and scenarios, you need to understand the deviations in maturity levels and be able to calculate the probability of those risks.

Through Mitratech's radar diagrams and controls linked to maturity levels, methodology and risk trees; teams are able to visually articulate the maturity level to stakeholders and qualify their risk automatically. This not only takes an enormous amount of mental load off your business, but also creates objectivity in the way that teams actually qualify risk, allowing them to categorize risks in relation to organizational hierarchies and risk categories, too.

Success Factors

Objectivity

Try to create a meaningful scale to apply for those people raising risks. The scales need to be understandable, or better yet – the qualification of risks should be partially or fully automated.

Simplicity

Start simple and don't over complicate the process initially. It makes sense to get a first draft together fairly quickly and then iterate and improve it, rather than creating a far too complex process initially that people would rather avoid. Guiding your community even at early stages is a key aspect to ensure consistent application of the process.

4. Quantify Risks

Conventional Approach	The Challenge	Mitratech's Approach
Don't quantify. Ask for an expert assessment.	Providing guidance to individual risk assessors is difficult and tough to scale. Expertise may vary.	Calculate value at risk with guided risk loss estimator calculator.

In addition to qualitatively assessing risks, organizations should strive for quantitative risk assessments in order to enable a meaningful aggregation of risks. Risk quantification involves analyzing and evaluating risks and their environment (e.g. process, level of automation) to specify the potential magnitude of risk events. Every organization has different tolerance for risks, meaning that portfolio managers do not have a one-size-fits-all approach for all risks. Quantification is concerned with determining and justifying the costs for mitigation as well as driving the urgency and implementation timelines for the risk mitigation. The quantification process also considers the following factors:

- Opportunities and threats which can interact in unexpected ways.
- Single risk events that can cause multiple knock-on effects.
- Opportunities for one stakeholder which may be seen as threats to another.
- Mathematical techniques that can create a false sense of precision.

It is not uncommon for financial institutions to use a range of risk models to analyze their risk profiles, in particular in the area of financial risk. However, the challenge with risk models is that they are often generalized and overlook the complexity of the individual organization. Digitalisation and technologies have enabled business leaders with the capabilities to easily conduct assessments to quickly identify risks that can potentially cause damages to the organization. These technologies allow organizations to assign a monetary value to each individual risk and ultimately quantify their investments.

An excellent and effective risk quantifying process is one that offers scalable guidance to the risk assessor, and speaks the language of the business through context-driven risk loss estimation. Ideally, it should be paired with a risk control framework that is tailored to the company's profile and environment.

Success Factors

Automation That Supports The Outcome

The more qualification and quantification steps that are automated – or at least supported with constructive suggestions – the more reliable the risk data becomes. This is incredibly useful as many risk contributors would find it difficult to assess risks qualitatively and quantitatively on their own.

Find The Balance Between Expert Knowledge and Quantitative Methods

Multi-faceted context and many other variables make quantitative methods for non-financial risks much more difficult. It is important to find a good balance between expert knowledge within your organization and appropriate mathematical methods.

Communication

Very rarely will a single person in your organization be able to conclusively assess a risk. It is important to record the expertise and opinions of various people in a structured manner and to document them comprehensively. The forum for this communication must be made simple and accessible.

5. Manage Risks

Conventional Approach	The Challenge	Mitratech's Approach
Have a fixed, quarterly process for reviewing and updating risks.	Risk data can be up to three months out of date.	Risk exposure vs risk appetite. Easily implement mitigation measures. In-app collaboration and communication.

The risk landscape of the organization can shift rapidly, proof of this was the global pandemic we all recently experienced. Risks relevant now, might not be the risks that were identified 3 months ago. Therefore, good risk management should not just be a quarterly tick-the-box exercise, but rather a continuous process of active risk culture. More and more, there will be demand from regulated entities, and of course their auditors, for more collaborative risk management, with far more regular and event-driven updates and reporting.

At Mitratech, we thought about fostering social media-like interaction – for instance, being able to respond to something through the use of likes, reactions and comments. This type of interface allows for easier and quicker collaboration.

Continuous risk management is dependent on actually having continuous contributions from people across the organization. This is unlikely to happen with a tool that is difficult to use. All controls, risks and mitigation plans follow an intuitive social media-like interface, allowing direct communication and collaboration within Mitratech's GRC platform - including reactions!

Continuous Updates

Successful risk management requires continuity in processes, reviews and updates. Keep the momentum going, document your progress, gather opinions and data points across teams and involve all relevant people.

Keep an Audit Trail

Make decisions transparently and document changes. Rather iterate and update often and be able to trace changes than have a rigid, non-inclusive and hard-to-follow process.

Success Factors

6. Aggregate Portfolio - Determine Overall Risk Exposure

Conventional Approach	The Challenge	Mitratech’s Approach
Aggregation and simulation is for financial risks. Sum up values across XLS.	With more focus on non-financial risks this approach becomes insufficient. Regulators are demanding more. Statistically incorrect to simply sum up values.	Run Monte Carlo simulations across the risk portfolio to calculate value at risk. Provide guidance on interpretation of value at risk. Accomplish board ready reporting.

The aggregation and quantification of operational risk, especially in the area of cyber risk , was not common. Putting a financial figure on a cyber risk is not a simple task and without quantitative figures, it is almost impossible for risk managers to come up with an appropriate aggregation. That being said, expensive simulation engines are extremely complex to integrate in spreadsheet-based solutions, causing risk management solutions to be scattered. At Mitratech, we believe in simplifying risk management, within a single platform. We aim to monitor value at risk in real-time.

Success Factors

Enable Different Perspectives

It is extremely important that different decision-makers are able to make risk-aware choices for their respective areas of responsibility. To enable this, it must be possible to aggregate the individual risks quickly, easily and at different risk or organizational levels.

Real-Time Aggregation

The aggregation should not only take place every quarter, but should be available on-demand, at any time. This is the only way to effectively monitor the actual overall risk position of the organization and act if necessary.

Flexibility in Structure

Every organization changes. The structure of risk management must allow for these changes. Adjustments to the risk management processes must aim to be as agile as possible, with the ability to make changes promptly and without significant implementation effort.

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, GRC, and HR teams seeking to maximize productivity, decrease costs, and mitigate risks by deepening operational alignment, increasing visibility, and spurring collaboration across their organizations. By partnering with customers to design, develop, deliver and support the best legal, GRC and HR software solutions on the market; Mitratech enables departments to become hubs of efficiency, innovation and excellence for the entire organization.

Mitratech's Platform provides expert product offerings to organizations worldwide, supplying end-to-end solutions that enable them to implement best practices and standardize processes across all lines of business, as well as effectively manage risks and ensure business continuity.

Mitratech serves over 1,800 organizations worldwide, spanning more than 160 countries.

For more information, please visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com