MITRATECH

Where to Start With Your ERM

Designing Your Risk Framework

Managing your organization's risk landscape can be daunting, and often stakeholders are unsure where to start. There is not a consensus across industries and communities on how a company's enterprise risk management (ERM) program should be built. There is not even consensus on what it should be called: ERM, GRC and IRM are just a few of the acronyms thrown around.

But everyone agrees that you must start somewhere to acknowledge and manage the risks and pressures facing modern business in the digital age. Ideally, a risk-aware culture should develop multiple approaches to risk at once. At the same time, one silo of risk management will likely not be fully developed all at once.

How to Read This eBook

There are many options for successful ERM implementation, and this guide is designed to help you plot the path that is the most appropriate for your organization. Review it like a "Choose Your Own Adventure" book, letting your answers to questions and circumstances guide you through your implementation planning.

The key for a robust ERM program is to progress in a way that is reasonable for your organization. The right choices will ensure consistent, accurate and useful insight into what risks your organization is exposed to and how well you are mitigating those risks.

All the elements discussed in this book will not necessarily be used in all risk programs. To find the right fit, explore the many pathways for ERM below.

Click Here to Begin

To navigate to a specific section, click one of the links below:

- Board and Executive Support
- Risk Culture
- Responsibility Alignment
- Risk Framework
- Risk Appetite
- Risk Register
- Control Library
- Risk Ownership
- Control Ownership
- Risk Assessments
- Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs)

BACK TO INTRO

01

Choose any Combination of These Approaches:

BOARD AND EXECUTIVE SUPPORT

RISK CULTURE

RESPONSIBILITY ALIGNMENT

RISK FRAMEWORK

RISK APPETITE

RISK REGISTER

CONTROL LIBRARY

BACK TO INTRO

Board and Executive Support

The most common starting place for risk management is to create buy-in with your Board and/or Executive team, but this is not the first step for everyone. Review the reasons you may or may not and then continue reading.

Is this the right fit for my organization?

What is it?

- Buy-in from leadership at the C-suite and board level that are required by stakeholders or even regulations to champion risk management, compliance and governance.

Why should I start here?

- Gaining the board's support can demonstrate to the rest of an organization that rolling out comprehensive risk management and removing silos is a priority.
- The board has the power to approve allocation of necessary resources.
- The board can make the final decision when silos are unable to agree on certain elements of integration.

How do I set it up?

- Meet with leadership to discuss the value of risk management and get their perspectives.
- Strategize with them on how to roll out risk management.
- Ensure that leadership is aware that they are ultimately responsible for any risk management failure at the organization. Convince them that you want to help protect the company and the board.

CONTINUE TO NEXT PAGE

Who should start here?

- This is an advisable starting point for any business — small, mid-sized or large.

Is there a better approach?

Why not start here?

- There aren't any negatives to this approach. Leadership support is crucial to successful risk management under any circumstances.
- But if your leadership is focused on other strategic priorities, the project may not progress quickly if you're waiting on their buy-in. In some cases, you may want to inform leadership you're working on the project, and then build a more complete framework to circle back to them at a later stage.

Challenges to implementation

- Finding and convincing champions who understand efficient risk management will provide strategic advantage — and won't be a cost or hindrance to business.
- Time constraints for your leadership team — they may slow your project or not be able to contribute as much time as is needed.

CHOOSE TO START WITH ANOTHER ELEMENT

Risk Culture

Is this the right fit for my organization?

What is it?

- A Risk Culture is how employees throughout the organization feel, think about and approach risk and risk management.

Why should I start here?

- Effective risk management requires enterprise-wide engagement — especially by those who understand the processes that drive the company.

How do I set it up?

- The entire organization will need to be trained and educated about risk.
- Leadership needs to set a tone from the top that risk management is a priority.

Who should start here?

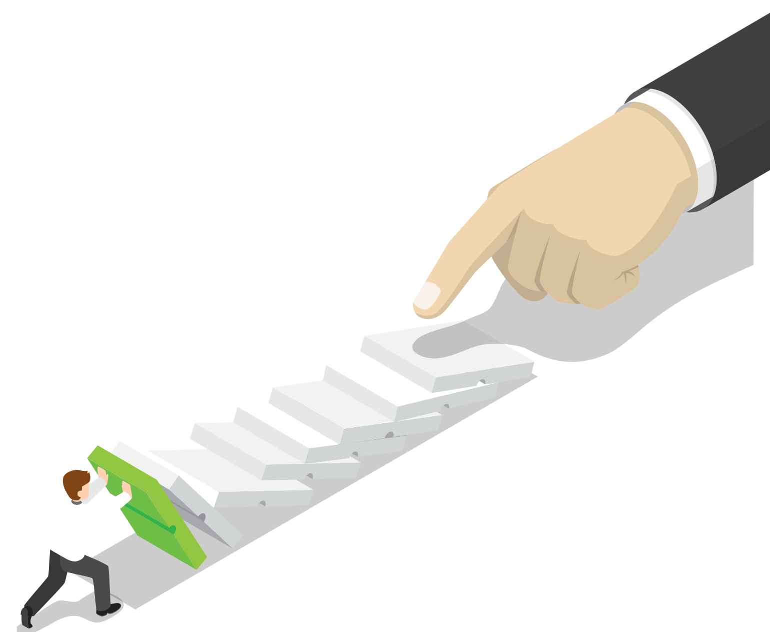
- With leadership support and risk knowledge, you can sell the value of risk management to the rest of the organization.

CONTINUE TO NEXT PAGE

Is there a better approach?

Why not start here?

- Gaining buy-in throughout the organization can be difficult without leadership support and/or clearly defined goals.
- Risk management without fleshed-out processes and procedures can be abstract, conceptual and difficult to grasp for some team members who think in more concrete terms.



Challenges to implementation

- Risk management is sometimes viewed as a restriction to business processes and innovation.
- Risk management is also often viewed as superfluous, less-important work compared to primary responsibilities.

CHOOSE TO START WITH THE RISK CULTURE AND COMPLEMENT IT WITH RESPONSIBILITY ALIGNMENT

CHOOSE TO START WITH ANOTHER ELEMENT

Responsibility Alignment

Is this the right fit for my organization?

What is it?

- The determination of who is responsible for which parts of your organization's risk management.

Why should I start here?

- The board is ultimately accountable for risk, but the responsibility for day-to-day management can be distributed throughout the organization.
- Some areas of risk management may slip through the cracks or be performed by two redundant stakeholders if roles are not defined and assigned to the best-suited individuals.

How do I set it up?

- The Three Lines of Defense (3LoD) model provides a powerful outline for parsing out responsibility:
- The model essentially designates the frontline staff and/or managers as the First Line of Defense (FLoD), responsible for implementing controls and answering risk assessments. The FLoD ideally has dedicated risk management staff who may report up to a Chief Risk Officer (CRO) who answers to the board.
- The Second Line of Defense (SLoD) is responsible for designing controls and overseeing and assisting the first line in assessing and identifying risk. The SLoD often includes compliance, risk management, and sometimes people from IT and/or information security (InfoSec).
- The Third Line of Defense (TLoD) is a team that performs internal audits of the first and second lines of defense.

CONTINUE TO NEXT PAGE

Who should start here?

- The 3LoD model is becoming more common and has gained regulatory support and recognition. Some argue it has shortcomings, but there are no current comparable alternatives.
- Organizations can assign responsibility using a 3LoD model if they:
    - Have the budget and leadership support for a CRO.
    - Have a strong compliance department that wants to implement ERM and is confident in their ability to keep audit functions independent of the risk functions that report to them.

Is there a better approach?

Why not start here?

- You may have an effective way to divide responsibilities already.
- You may want to keep risk management simple if you aren't ready to mature and don't need to have a risk management program that is robust in this way.

Challenges to implementation

- Defining the SLoD's responsibilities can be challenging. The SLoD is unique from the FLoD but not independent like audit. Partnering with the FLoD is critical.
- Your organization may not have a CRO. The board may not want the CRO as a direct report.
- The FLoD may feel that compliance is overbearing when they deal with the compliance-focused and risk-focused staff from the same department.
- It is important that audits stay independent, even when they oversee risk management.

CHOOSE RESPONSIBILITY ALIGNMENT AND THEN COMPLEMENT IT WITH RISK CULTURE

CHOOSE TO START WITH ANOTHER ELEMENT

Choosing a Risk Framework/ Methodology

Is this the right fit for my organization?

What is it?

- A methodology that can be used to systematize, implement and practice risk management throughout the organization.

Why should I start here?

- Risk management generates massive amounts of data. A framework simplifies organization, application and understanding of that data.
- Defining the approach makes it easier to define elements of risk management. A framework can also provide a common language.
- Depending on the framework, the work of defining your organization's risk management may already be started.
- Established frameworks utilized by other organizations have peer groups, forums, and/or conferences where expertise and experience are shared.

How do I set it up?

Adopt a framework outlined by your regulator:

- Some regulators give very specific directions for risk management. Those directions can be an obvious choice for heavily regulated companies because it will make the regular exams easier. It should be stated, however, that your regulator's guidance doesn't need to be followed exactly as outlined.
- Many organizations in heavily regulated industries use frameworks from recognized global organizations. They may also use in-house developed frameworks, which ties back to the guidance with great success.

CONTINUE TO NEXT PAGE

- Most regulatory frameworks are simpler than those of risk organizations/societies.

Adopt a framework from a risk management organization or society:

- Regulators readily accept properly implemented risk frameworks from reputable organizations and societies. Some even suggest them or elements of them.
- There will be communities and consultants who can support you in the implementation of these frameworks. They will have readily-available information on the frameworks.

Utilize a framework from a consultant:

- A consultant will bring their expertise and experience and help you adapt a proven approach from a risk organization or society or one that they have developed.
- They will provide objective, informed perspective and help direct the project.

Utilize a framework from a software provider:

- Some software providers provide one approach or multiple approaches in their software as templates.
- These approaches may be based on regulatory guidance or risk organization/societies' frameworks. The software may also include proprietary frameworks.
- The advantages of each approach will vary depending on the basis for the framework. All of these options will have the synergy of a framework designed for the software.

Develop a framework internally:

- Organize and evaluate risk and controls according to your:

  - Organizational structure
  - Strategic goals
  - Primary risk concerns
  - Regulatory considerations and company culture
  - Risk management best practices

CONTINUE TO NEXT PAGE

- Even highly regulated companies dealing with strong guidance can be very successful with in-house risk frameworks. The frameworks, however, must be thoughtfully conceived and easy to explain.

Who should start here?

- Heavily regulated companies without an ERM program who place regulatory compliance as a top priority.
- A company that wants to meet fixed standards or wants extensive guidance and is not concerned about its ability to manage complexity.
- Companies that have a relationship with a consultant that is training or willing to train and educate internal risk managers.
- Companies who have not started an ERM program yet but have hired risk managers who understand how to build a risk program.
- Companies that have effective risk management in various silos but are looking for an easy way to integrate enterprise-wide risk management practices.
- Companies who have some awareness of their risks and how they relate to strategic or operational goals. These companies most likely have some in-house risk management expertise already.

Is there a better approach?

Why not start here?

- You may not be aware of gaps in your program if you have not yet defined the full scope of your company's risk management program/ needs or if your primary regulatory body has not provided guidance.
- Your organization may not need or be ready for the level of complexity and maturity that goes along with a framework from a risk management organization or society. Not being prepared may result in lengthy implementation and/or the implementation of practices/ processes that are not necessary.

CONTINUE TO NEXT PAGE

- It can be difficult to develop a framework that effectively encompasses all the risks and controls your organization faces without a full understanding of those risks.

Challenges to implementation

Each kind of framework presents its own obstacles and potential drawbacks. Each organization should determine the style of framework they feel most comfortable with.

Framework based on regulatory guidance

- Regulatory risk frameworks often do not include specific guidance on how to implement the approach in all areas of an organization and those frameworks may not even address certain areas of risk.
- It can be difficult to avoid a “check-the-box” mentality to risk management when the foundation is regulatory guidance.

Framework based on a society’s approach

- Implementing an organization/society’s framework is often complex, difficult and expensive.
- There are often materials to purchase and audits to certify that your program satisfies the framework. Many companies end up using consultants.

Framework provided by a consultant

- It is difficult to know if you are selecting a consultant whose approach will be universally accepted.
- You must determine if the consultant’s experience and expertise is great enough to identify and address your specific organizational concerns, culture and practices.
- Your organization must be able to take over the program completely from your consultant, and if that is not possible you must continue to engage the consultant on an ongoing basis.
- You could place your risk management on an island if you rely too much on a consultant’s framework, and it may be challenging to find support outside of that consultant.

CONTINUE TO NEXT PAGE

BACK TO INTRO

Framework built by a software provider

- You risk creating a dependency on the framework's specific approach, and you require ongoing management or further development in that framework as your organization grows and/or changes.
- Without defining the scope and approach, you may be limiting your future risk management to the capabilities of the software you choose today.
- Be sure to review the flexibility of the platform you're considering to determine if you must use an existing framework or if multiple templates and customization options are available.

Framework built in-house

- Frameworks require high-level conceptual thought about the organization and its risks and need to capture all the complexity and scope of data necessary to handle the company's full risk management program.
- The framework must remain simple enough that it can be easily explained to the board, frontline managers, auditors and regulators.

CHOOSE TO COMPLEMENT WITH RISK APPETITES

CHOOSE TO COMPLEMENT WITH RISK REGISTER

CHOOSE TO COMPLEMENT WITH CONTROL LIBRARY

CHOOSE TO START WITH ANOTHER ELEMENT

Risk Appetites

Is this the right fit for my organization?

What is it?

- Statement of how much risk your organization is willing to accept.

Why should I start here?

- This helps define risk management goals. A risk appetite also provides context and purpose to assessments and/or KRIs.

How do I set it up?

- Risk appetites usually start as a general statement at the board level.
- Risk appetites can be set up in a top-down way. Each more granular part of the organization will then reflect its portion of risk in the company's overall statement.
- Sometimes, you have well-established risk management in various silos, but the organization does not have risk management at the enterprise level. It might make more sense to begin by defining risk appetites within each silo. Each of your silos will have a practical and working knowledge of how much risk is appropriate throughout their respective areas. These siloed risk appetites can provide a foundation for the company's overall risk statement.

Who should start here?

- Risk managers that need a strong top-down risk management approach.
- Companies with silos of effective risk management that want to establish an organization-wide risk appetite.

CONTINUE TO NEXT PAGE

BACK TO INTRO

Is there a better approach?

Why not start here?

- It takes time to get a risk appetite approved and even longer to apply it.
- It is easy to change targets, and targets don't have any practical use without a way to effectively measure risk.
- The risk appetite should be determined by the board.
  - The bottom-up approach means that the board gives risk managers the responsibility to determine the company's appetite for risk.
  - The bottom-up approach could also result in back-and-forth revisions to clarify and correct several appetite statements before an enterprise statement is formulated.

Challenges to implementation

- The board needs to create and approve a risk appetite statement.
- Breaking down the appetite into practical risk measures to use throughout the organization is a challenge.
  - The enterprise statement is usually broad and generic.
  - Not all departments and operational areas share the same risk appetite. Some areas should be more conservative, while others should account for more of the overall risk.
- Experienced people are needed to manage risk with well-developed processes in many parts of the organization.
- Gaps between the different approaches to risk management in the different silos must be bridged.

CHOOSE TO COMPLEMENT WITH CHOOSING A FRAMEWORK/ METHODOLOGY

CHOOSE TO COMPLEMENT WITH RISK REGISTER

CHOOSE TO COMPLEMENT WITH CONTROL LIBRARY

CHOOSE TO START WITH ANOTHER ELEMENT

BACK TO INTRO

Risk Register

Is this the right fit for my organization?

What is it?

- Library of all the organization's risks with key data for each risk, as well as categorization as a key enterprise risk, when appropriate

Why should I start here?

- Having a defined list of all the risks provides focus. These can serve as a foundation for risk assessments, KRIs, assigning risks and identifying where controls are needed.
- Identifying key risks to the organization highlights disruptions to the company's strategy and provides high visibility to these potential issues.

How do I set it up?

- Work with frontline managers and staff to identify what could go wrong and what would interrupt their respective processes:

CONTINUE TO NEXT PAGE

    - Look for common industry risks.
    - Organize risks by areas or departments and identify which risks can impact multiple parts of the business.
    - Add to the list as new risks are identified, while being careful not to duplicate risks under different names.
- Meet with leadership to discuss top strategic priorities. What could get in the way of these strategies?
- Lists of risks with more than 25 entries must be prioritized with leadership to narrow the focus. The list must then be shared throughout the organization.

Who should start here?

- Companies that plan to monitor and/or assess risks at the frontline and roll scoring up. Those companies also need to have the data analytics abilities to prioritize and analyze risk effectively.
- Companies who need to be able to focus on key risks.

Is there a better approach?

Why not start here?

- Focusing entirely on building out a robust risk register doesn't mitigate or manage risk.
- An organization's risk profile will evolve, and risk managers could, theoretically, just focus on creating and updating the risk register. A risk profile can be especially volatile in a changing industry or growing company.
- Focusing on a limited view of risk may give the organization a false sense of security which can lead to overlooking risks outside of this library.
- Vigilance for other risks at lower levels may be discouraged when risks are dictated from the top.

CONTINUE TO NEXT PAGE

Challenges to implementation

- If you collect risks from the frontline:
    - It can be difficult to collect and organize a large number of risks from throughout the organization without generating duplicates. A single type of risk can also impact different parts of the organization.
    - The sheer amount of data can get in the way of effective risk management.
    - Risk managers will need to work with frontline staff and managers to clearly identify how risks relate to their specific areas of the organization.
- If you have a more limited risk register defined by leadership, it may be difficult to determine how effective your mitigation strategies are when risks are so broadly defined.

CHOOSE TO COMPLEMENT WITH CHOOSING A FRAMEWORK/ METHODOLOGY

CHOOSE TO COMPLEMENT WITH RISK APPETITES

CHOOSE TO COMPLEMENT WITH CONTROL LIBRARY

CHOOSE TO START WITH ANOTHER ELEMENT

BACK TO INTRO

Control Library

Is this the right fit for my organization?

What is it?

- Library of the organization's controls with key data for each risk.

Why should I start here?

- A control library provides documentation of what controls the organization already has in place. That awareness can be used as a starting point for evaluating effectiveness of those controls.

How do I set it up?

- Review policies, procedures and conduct interviews with frontline staff and managers to identify controls.

Who should start here?

- Companies that prioritize assessment or testing of controls for risk management and have a basic idea of what controls they need in place.
- Companies with regulatory requirements to have certain controls in place.

Is there a better approach?

Why not start here?

- Identifying controls only clarifies how well you are practicing those controls. It does not provide much insight into overall risk management or make clear where new controls are needed.
- It is likely that you'll end up focusing on the areas with the strongest risk management already in place. Those areas will have well- documented controls.

CONTINUE TO NEXT PAGE

BACK TO INTRO

Challenges to implementation

- Finding existing controls can be very difficult if they have not been documented. Often controls are simply embedded in procedures over time and can become difficult to isolate.
- Policies and procedures are sometimes not managed well. The controls may be missed, or outdated versions may be documented.
- You must determine where there are unique controls and where a single control is impacting multiple processes, departments, etc.

CHOOSE TO COMPLEMENT WITH CHOOSING A FRAMEWORK/ METHODOLOGY

CHOOSE TO COMPLEMENT WITH RISK APPETITES

CHOOSE TO COMPLEMENT WITH RISK REGISTER

CHOOSE TO START WITH ANOTHER ELEMENT

BACK TO INTRO

02

Most choose only one of these approaches:

- RISK OWNERSHIP
- CONTROL OWNERSHIP

Risk Ownership

Is this the right fit for my organization?

What is it?

- Risk ownership is who is assigned responsibility for managing each defined risk.

Why should I start here?

- The board is ultimately legally liable for risk management failures. However, they can't effectively manage each risk and control individually.
- Risk managers are risk experts, but they will not have the same knowledge of business processes as business managers and/or frontline staff.
- Business managers and frontline staff have the most expertise in, awareness of and time to manage their respective areas. The FLoD, however, may view risk management as a less important task added onto their primary responsibilities.

How do I set it up?

- Gain support from the board and executive level.
- Create a risk culture.
- Assign specific risks to specific owners.

Who should start here?

- Companies who have already identified risks and will have the frontline actively engaged in risk management.

CONTINUE TO NEXT PAGE

Is there a better approach?

Why not start here?

- A risk register is needed in order to assign owners to risks.
- This approach could damage a risk culture if you assign responsibility for risk to people without first defining their responsibilities. They also need to know how they will receive help from the risk and/or compliance team.

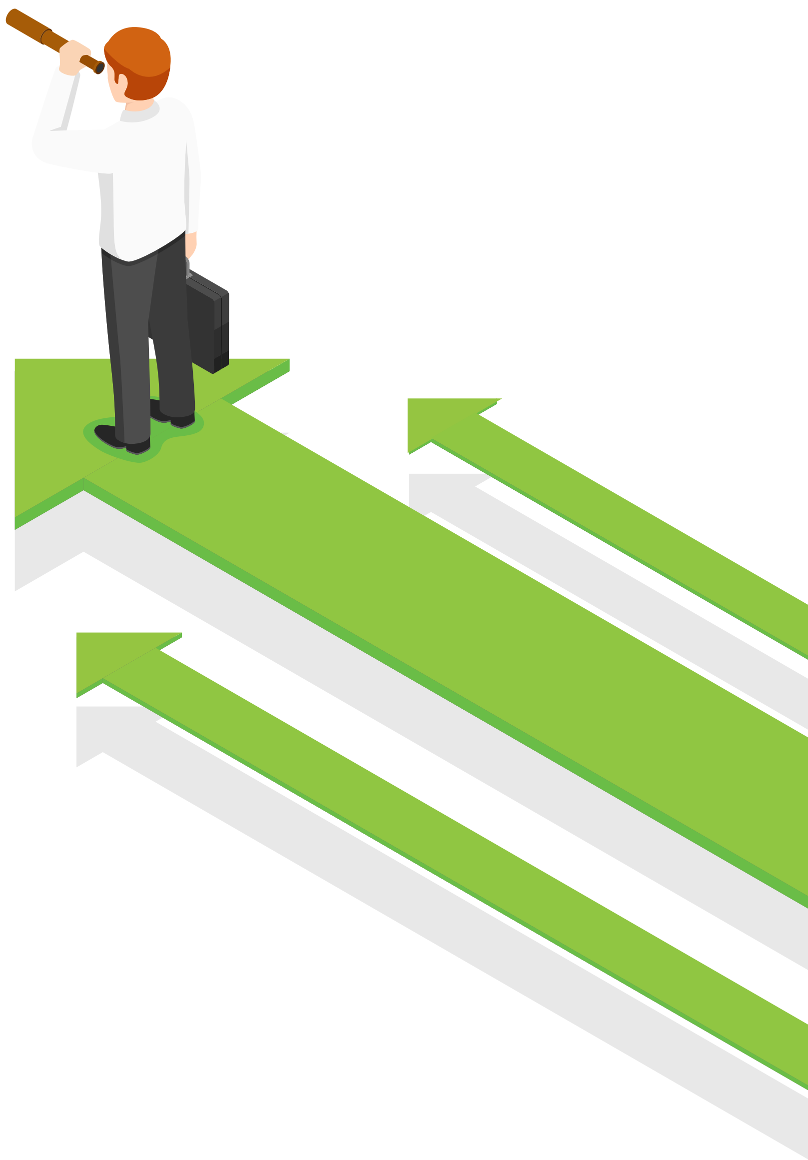
Challenges to implementation

- No one wants to own a risk and take responsibility for it.
- Assigning ownership to a risk is just a starting point. Owners still need support and oversight in managing the risk.

CHOOSE CONTROL OWNERSHIP INSTEAD OF RISK OWNERSHIP

CHOOSE TO START WITH ANOTHER ELEMENT

Control Ownership



Is this the right fit for my organization?

What is it?

- The assignment of responsibility for managing risk and definition for how they will manage that risk.

Why should I start here?

- Frontline staff and managers are more familiar with the operations and controls they manage.
- Frontline staff and managers may be more resistant to owning a risk than owning a control.

How do I set it up?

- Gain support from the board and executive level.
- Create a risk culture.
- Assign specific risks to specific owners.

CONTINUE TO NEXT PAGE

Who should start here?

- Companies who have identified controls and have standards set for their performance.

Is there a better approach?

Why not start here?

- Control ownership is often accompanied by, and serves little purpose without, testing or assessing the control.
- Control ownership could damage a risk culture if you assign responsibility for controls to people without first defining their responsibilities. They also need to know how they will receive help from the risk and/or compliance team.

Challenges to implementation

- Assigning ownership to a control is just a starting point. Owners still need support and oversight in managing the control.

CHOOSE RISK OWNERSHIP INSTEAD OF CONTROL OWNERSHIP

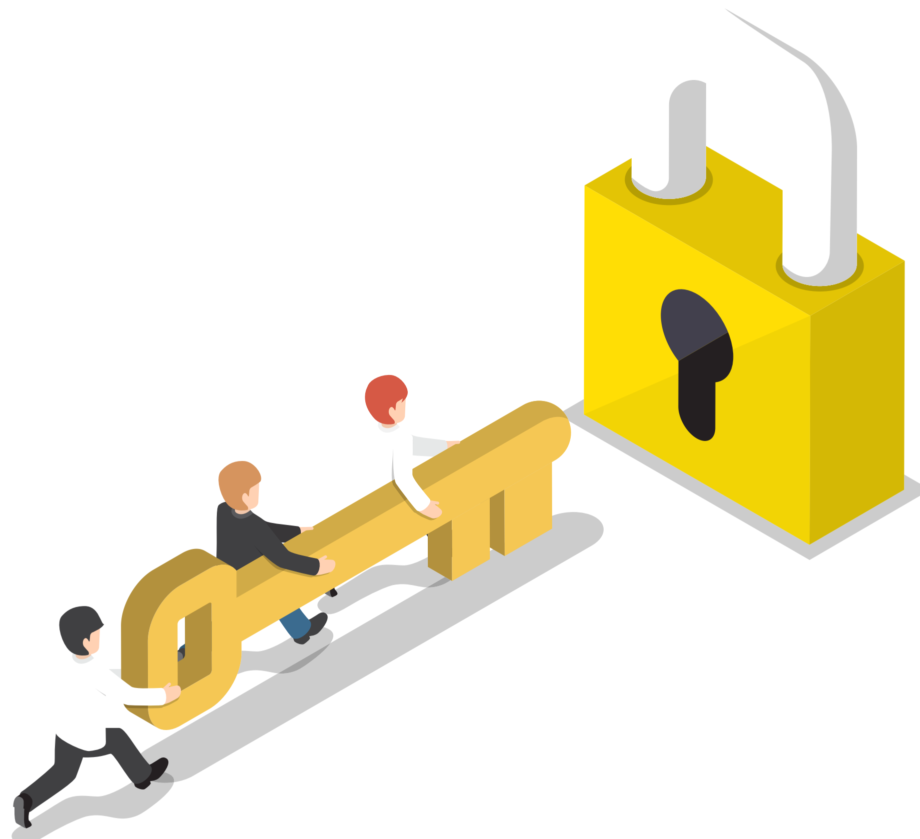
CHOOSE TO START WITH ANOTHER ELEMENT

03

Choose one or do both:

RISK ASSESSMENTS

KRIs/KPIs



Risk Assessments

Is this the right fit for my organization?

What is it?

- A systematic method to gather risk data and calculate risk scores for the purpose of understanding risk throughout the organization.

Why should I start here?

- Risk assessments can provide insight into how much exposure an organization has and where that exposure comes from.
- Risk assessments can expose weakness.
- Risk assessments can be generic or specific — depending on your program's maturity.

How do I set it up?

- Define areas of the company by the type of risk, operational areas or strategic goals.
- Establish some way to measure the risk exposure and/or the control effectiveness. These measures must be performed either for specific areas, generally or a combination of both.
- Measures can be descriptive or quantitative.
- Risk assessments are best answered by the frontline.

Who should start here?

Companies who:

- Have an idea of how they want to organize risk.
- Lack enough risk data to set Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs).
- Want to start quantifying risk exposure to identify and highlight high-risk areas.

CONTINUE TO NEXT PAGE

Is there a better approach?

Why not start here?

- It's hard to determine who should be doing risk assessments, and on what, without at least a rough framework established.
- Risk assessment data may be suspect or difficult to gather without leadership buy-in and/or an established risk culture.
- You will need to identify how the collected data will be used. Risk assessments without an action plan lose their value.

Challenges to implementation

- Measures for specific areas can be difficult and time consuming to define and assess.
- It can be challenging to establish generic measures that are meaningful throughout the organization.
- You'll need a method, like a framework, to organize risk assessments.
- Descriptive measures may introduce too much subjectivity to risk assessment.

CHOOSE KRIS/KPIS INSTEAD OF RISK ASSESSMENTS

CHOOSE BOTH

CHOOSE TO START WITH ANOTHER ELEMENT

KRIs/KPIs

Is this the right fit for my organization?

What is it?

- Measure the frequency or level of exposure for specific risks and the performance levels for specific controls, with stated thresholds.
- Thresholds could be used for a simple “acceptable” or “unacceptable” designation or you can provide tiers to classify risk level — High, Medium or Low.

Why should I start here?

- You will have at least a partial risk register or control library. Someone will be managing these items — at least in some areas.
- KRIs/KPIs are relatively easy for your Audit function to review/validate and to present to the board.
- KRIs/KPIs allow for a quick way to start getting some risk scoring data. You gain access to risk data even if you still need to continue building out the rest of your risk management program.
- Risk exposure/control performance can be converted from various silos into consistent risk ratings.
- Trend information is provided, and high-risk areas are highlighted.

How do I set it up?

- Look at identified risks and set thresholds for risk exposure and/or control performance.
- Discuss each respective KRI/KPI with each risk/ control owner by looking at industry standards, capacity for organization to accept risk and historical data.
- Get leadership approval for the thresholds.

CONTINUE TO NEXT PAGE

Who should start here?

- Companies with risks or controls defined well enough that they can meaningfully measure their exposure and/or performance.

Is there a better approach?

Why not start here?

- KRIs/KPIs can't address emerging risks or assess risk for new products or operations. They rely on live or historical data.
- KRIs/KPIs are not as comprehensive and do not provide the same type of insight as doing risk assessments.
- Leadership may shift focus from rolling out comprehensive risk management and full integration of silos to managing the KRIs/KPIs that you initially identify.
- Frontline risk owners may limit their view of risk management to hitting KRI/KPI targets.

Challenges to implementation

- It can be difficult to ensure that the aggregate of KRI/KPI thresholds expose the organization to an appropriate level of risk if thresholds cannot be tied back to a risk appetite.
- Language must be added to policies so that they define thresholds and link risk and compliance.

CHOOSE RISK ASSESSMENTS INSTEAD OF KRIS/KPIS

CHOOSE BOTH

CHOOSE TO START WITH ANOTHER ELEMENT

In Case You Missed It...

Each of the elements in this ERM implementation guide can be a part of a robust risk management program. Regardless of your starting point, your ERM program is enhanced by a methodical and systematic approach.

- Board and Executive Support
- Risk Culture
- Responsibility Alignment
- Risk Framework
- Risk Appetite
- Risk Register

About **Mitratech**

Mitratech is a proven global technology partner for corporate legal, risk & compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility and spurring collaboration across their organization.

With Mitratech's proven portfolio of end-to-end solutions, organizations worldwide are able to implement best practices and standardize processes across all lines of business to manage risk and ensure business continuity.

For more info, visit: **www.mitratech.com**

MITRATECH

CONTACT US

info@mitratech.com
www.mitratech.com

Mitratech US
+1 (512) 382.7322

Mitratech EMEA
+44 (0) 1628.600.900

Mitratech AUS
+61 (0)3.9521.7077