Operational resilience

How leadership teams are turning enterprise risk management into a growth advantage

WIPFLI

Introduction

Is risk blocking your business from growth?

You probably understand the concept of enterprise risks: Organizational-level challenges that can create financial, operational, regulatory and reputational dangers for your business. But what you may not know is that risk is also a threat to growth.

If you don't have a clear awareness of your enterprise-level risks, you may find that your growth strategy keeps running headfirst into walls you didn't know were there. Worse, your efforts to grow could actually increase your risk exposure, as you add new people, processes, partners and potential failure points to your organization.

That's why more growth-minded leaders are embracing enterprise risk management (ERM) to build operationally resilient organizations. A more resilient business is more aware of risks, better able to mitigate them and more prepared to withstand even unexpected challenges whenever they arise.

Greater resilience can even lead to new growth opportunities. Understanding your enterprise risks delivers a clearer awareness of how your whole organization functions, which drives smarter decisions that help you outdo your competition or uncover new growth areas.

In this guide, you'll learn a practical approach to enterprise risk management that helps organizations become more resilient, adaptable and prepared for growth.

Section 1: A proactive risk strategy is now essential

Your top business risks are complex and interconnected

Most businesses have traditionally approached risk management as a compliance exercise.

Companies in regulated industries have focused on meeting regulatory compliance standards, while those in less-regulated sectors have often viewed risk as primarily an item on a due diligence checklist during a transaction.

Yesterday, that strategy may have been good enough. But today, the risk environment is more complex than ever.

- Regardless of industry, your business exists in the midst of a wave of technological change that's fundamentally shifting how businesses operate while creating new exposures that didn't exist even a decade ago.
- While AI is at the forefront of this wave, leaders must also navigate the challenges that arise from moving core systems to cloud-based platforms that offer operational advantages but create third-party vendor risks. Cybersecurity threats continue to grow as well.
- All this technological change is also happening during a time of notable geopolitical and economic uncertainty — which means business leaders should be prepared for anything.

Embracing a proactive approach to managing enterprise risk is essential. A cohesive ERM strategy creates a more operationally resilient business that can navigate these challenges to achieve growth even in stormy seas.

Section 2: Major risks that threaten operations and growth

Consider four crucial risk areas

An effective enterprise risk management strategy should address your risks in crucial risk areas or domains that affect your business as a whole.

This book focuses on four: operational risks, AI risks, broader technology risks and cybersecurity risks.

Operational risks

Operational risks are risks that can harm the day-to-day operations of your business. These include technology-related risks that are explored in greater detail below. However, operational risk is an expansive category that also covers fraud, succession or personnel problems, poor information and internal control failures, as well as growth-related risks like those that can occur when an organization grows quickly through a merger or acquisition.

Managing your operational risks and becoming more resilient reduces the likelihood that your business will suffer serious operational disruptions due to a triggering event.

AI risks

Your business, like most, is probably actively experimenting with how to integrate AI into your processes and workflows. But in doing so, you're opening the door to a wave of new risks: shadow AI, hallucinations, bias, inaccurate information flowing up to leaders, poor ROI on AI investments, internal data shared with public AI models and ineffective AI use that does more harm than good.

Ignoring AI completely will likely put your business at a competitive disadvantage — but so will jumping in without taking steps to manage your AI risks.

Technology risks

AI isn't the only area where businesses are experiencing significant technological change. More businesses than ever operate in the cloud, using SaaS platforms like an ERP and CRM to manage their core operations.

This shift has happened because these platforms often offer major operational advantages over legacy systems. But they come with risks too. Most carry significant implementation costs in both time and money, which means a poor implementation can set your business back considerably.

Adopting cloud-based systems also means that more of your data gets shared with the third-party vendors who run those systems. From a security perspective, this means that a data breach or hack involving a vendor can put you at risk even if your own systems remain secure.

Cybersecurity risks

Finally, you should consider cybersecurity risk as its own standalone category. This is because the volume of cyberattacks has never been greater. It's essentially inevitable that your business will be attacked — so the question is less about when and more about whether you're prepared to deal with it.

AI has made cybersecurity more difficult, in part because it's lowered the barrier to entry for would-be cyber attackers. What used to take technical knowledge can now be done with vibe-coding, while AI also makes it simpler to pump out phishing emails that hackers use to gain access to your systems.

Growth amplifies each of these risks

Consider that each of these four risk areas involves some element of change. If you have a relatively stable organization, you may be less exposed to some or all of them than if you are growing, because growth itself also introduces more change into your business.

That change can strain your existing controls or create new gaps you didn't need to worry about before. Often, you may not even be aware that your risk has increased — unless you have a proactive enterprise risk strategy in place.

Section 3: Real-world examples of enterprise risks

Look for similar patterns across industries

To get a better sense of how specific risks can affect your business, consider the following examples:

- **Shadow AI**: A financial services company encourages its team members to use AI in their daily work, but doesn't establish governance or AI use policies. While preparing for a board meeting, an executive asks an AI chatbot to analyze a huge dataset of customer information, feeding details on tens of thousands of customers to a public AI model that could expose that data to any other user, including those outside the company.
- **Fraud:** A construction business acquires a rival company in an M&A. The rival uses a newer purchasing system, so the acquiring firm decides to transition onto that system. However, its team doesn't fully understand the new system's controls and gives unrestricted access to multiple team members without oversight or proper segregation of duties, allowing a disgruntled team member to issue fraudulent purchase orders.
- **Vendor risk:** A food and beverage manufacturer implements a new ERP to improve its inventory management and product development capabilities. But then the tech company that makes the ERP falls victim to a data breach. As a result, propriety recipe information the manufacturer has stored in its new ERP gets sold on the dark web.
- **Business email compromise**: An operations manager at a hospital clicks on a link in an email and enters his login details without verifying that the link is safe. It's a phishing scam, and the hackers are able to spend months poking around inside the hospital's operational and patient management systems undetected, setting the stage for a ransomware attack.

None of these examples are limited to a particular industry or type of business. And each of them carries not just potential financial consequences, but also ripple effects like reputational harm, regulatory challenges, increased competition or serious operational disruptions.

All of these consequences can make it harder to grow by limiting opportunities, reducing your appeal to investors, customers or partners or simply chipping away at the financial resources you need to drive growth.

So then, how do you take action to better manage your enterprise risk and make your business more operationally resilient?

Section 4: Assessing your risks and enterprise risk maturity

Here's how to get started understanding your risks

If you want to manage your enterprise risks, become more resilient and set your business up for growth, you need to know where you are now. That's why a good first step for enterprise risk management is to perform a risk and maturity assessment.

From a high level, a risk and maturity assessment should:

1. Define the risk areas and scope being evaluated.
   Consider the four risk areas covered in this book — operational, AI, technology and cybersecurity risk — along with any others that make sense for your business.

2. Gather evidence about your organization's current capabilities through interviews, documentation, data and process reviews.
   This includes identifying any risks you're already trying to manage, current controls and overall organizational risk awareness.

3. Evaluate risk areas against consistent risk rating and risk maturity criteria.*
   Use a set of risk rating criteria to classify risk areas and specific risks as low, moderate or high. A set of maturity criteria can likewise help you evaluate your organizational preparedness to manage enterprise risks, typically on a 5-point scale.

4. Distinguish the significance of each risk from your organization's maturity in managing it.
   As your resources are limited, it's more important to demonstrate high maturity in managing high-risk areas.

5. Identify specific capability and control gaps.
   Find out where you're weak and where you need to be strong.

6. Produce a report to show leaders where risk is high and maturity is low, moderate or high.
   This will help focus your enterprise risk management efforts as you work to become a more mature organization.

*The **enterprise risk maturity self-assessment tool** included in the next section of this e-book can help you do all this.

Additional factors to consider during an assessment

Here are some questions, actions or additional areas of evaluation you may include in your risk and maturity assessment:

- **Look at your organizational talent, knowledge and experience.** Do you have an in-house understanding of the operational risks you face? Is your leadership risk-aware?
- **Consider the type of industry you're in.** What are the industry-specific challenges you face? Are you in a regulated industry? Are you a startup in a fast-evolving space?
- **Assess your capital challenges.** Can you afford to spend money to be operationally mature? Where should you target your investments to deliver the most impact?
- **Evaluate your systems.** Are you investing in good ones? Better systems typically mean higher operational maturity, better financial reporting capabilities and more support for your organization as a whole. Crucially, vendors who make those systems typically have stronger controls of their own in place to protect your shared data.
- **Remember succession planning**. Are you prepared for a leadership transition? What about an exit in a key mid-level role your team relies on as a source of institutional knowledge?
- **Plan for growth.** How do you plan to grow? Consider your growth strategy from an operational risk standpoint to identify failure points. But also look at how managing those risks could create new opportunities. For example, if you mitigate your AI risks better than your competitors do, could this help you gain market share?).

Section 5: Enterprise risk and maturity self-assessment tool

Use this worksheet to complete a risk and maturity self-assessment

This enterprise risk and maturity self-assessment tool offers a practical starting point for identifying priority risks and evaluating how prepared your organization is to manage them. Use it to get a clearer understanding of your current levels.*

How to complete this assessment

Complete the worksheet with a small cross-functional group rather than relying on one person's perspective. Base ratings on observable evidence rather than intent. When evidence is mixed or a practice exists only in isolated areas, choose the lower rating.

- Identify and rate a small set of enterprise risks.
- Evaluate seven capabilities needed to manage risk consistently.
- Connect high-rated risks with the weakest relevant capabilities.
- Choose a first action, owner and target date for each priority.

Keep risk and maturity separate

A risk rating estimates the significance of a specific risk. A maturity rating evaluates the organization's capability to identify, manage, monitor and respond to risk. A high risk does not automatically mean low maturity — and a mature ERM program does not eliminate risk.

Question	What it measures	Output
How significant is this risk?	Likelihood and potential impact	Low, moderate or high risk
How capable are we of managing risk?	Governance, process, ownership, controls, information and adaptation	A 1–5 maturity profile by capability
What should we address first?	Risk significance considered alongside relevant capability gaps	Prioritized action

*This is a directional self-assessment, not a formal risk maturity model assessment, certification or substitute for a facilitated enterprise risk assessment. Use it to surface priorities and guide deeper discussion.

Step 1 Identify and rate priority risks

Start with the objectives, operations or growth plans that matter most. Write each risk as a cause–event–impact statement: **Because [cause], [event] may occur, leading to [impact on the organization or objective].**

Risk statement	Objective affected	Owner	Existing controls	L	I	Rating

Likelihood and impact criteria

Score	Likelihood	Impact
1	**Unlikely:** Not expected under normal conditions; limited history or warning signs.	**Limited:** Manageable within normal operations with minor effect on objectives.
2	**Possible:** Could occur; some history, indicators or plausible conditions exist.	**Significant:** Meaningful operational, financial, compliance or strategic disruption requiring management attention.
3	**Likely:** Expected, recurring or supported by strong indicators.	**Severe:** Threatens critical operations, financial stability, regulatory standing, reputation or a major strategic objective.

Risk-rating matrix

Likelihood ↓ / Impact →	1 — Limited	2 — Significant	3 — Severe
1 — Unlikely	Low	Low	Moderate
2 — Possible	Low	Moderate	High
3 — Likely	Moderate	High	High

Optional refinement: Rate the risk once before considering controls (inherent risk), then again after considering the design and effectiveness of existing controls (residual risk).

Step 2 Evaluate risk-management maturity

Score each indicator from 1 to 5. Consider three questions:

1. How consistently does the practice work?
2. Is it proactive or mostly reactive?
3. How broadly is it applied across functions and levels?

Record the evidence supporting each rating.

Score	Stage	What the stage looks like
1	Reactive	No consistent practice. Risk is generally addressed after a problem occurs and depends on individual effort.
2	Developing	Basic practices exist in some areas, but ownership, execution and documentation are inconsistent or siloed.
3	Defined	Core practices are documented, repeatable and used in important areas, although coverage or follow-through may vary.
4	Integrated	Practices are consistently applied across the organization and embedded in operations and decision-making.
5	Adaptive	Practices are measured, forward-looking and continually improved as objectives, conditions and risks change.

Scoring rule: For each capability, use the lower of its two indicator ratings as the capability score. Do not average all seven capabilities into one number; a single score can conceal a critical weakness..

Scoring sheet

Capability	Indicator	1–5	Evidence or gap
1. Leadership and governance	Leaders demonstrate active understanding of enterprise risk and reinforce its importance.		
	Roles, decision rights, oversight forums and escalation paths are clear.		
2. Risk identification and assessment	A consistent process captures enterprise, emerging and interconnected risks.		
	Likelihood, impact and control effectiveness are evaluated using defined criteria and evidence.		
3. Ownership, appetite and escalation	Named risk owners are accountable for monitoring risks and completing agreed actions.		
	Risk appetite, tolerance and escalation thresholds guide decisions and responses.		
4. Controls and response	Key controls are documented and periodically evaluated for both design and operating effectiveness.		
	Mitigation plans are prioritized, resourced, assigned and tracked through completion.		
5. Information, metrics and reporting	Metrics provide timely, meaningful and increasingly forward-looking insight into risk and control performance.		
	Reporting is tailored to management and board needs and explains significance, trends, residual risk and required decisions.		
6. Integration and decision use	Risk information informs strategy, budgeting, operations, projects, technology and third-party decisions.		
	ERM outputs inform audit, compliance, continuity planning and other assurance activities.		
7. Monitoring and resilience	Risks, controls and action plans are reassessed on a defined cadence and when material changes occur.		
	Scenario planning, disruption response and lessons learned strengthen readiness and continuous improvement.		

Your maturity profile

Capability	Score	Strongest evidence	Most important gap
Leadership and governance			
Risk identification and assessment			
Ownership, appetite and escalation			
Controls and response			
Information, metrics and reporting			
Integration and decision use			
Monitoring and resilience			

Interpretation: Scores of 1–2 signal foundational gaps. A score of 3 indicates a defined practice that may need broader or more consistent execution. Scores of 4–5 indicate stronger capability, but they should still be tested against evidence and changing conditions.

Step 3 Turn the results into priorities

Review each high- or moderate-rated risk and identify the capabilities most relevant to managing it. The goal is not to fix every gap at once. Focus first on high-risk, low-maturity areas.

Priority	Use when	Typical response
Act now	High risk + one or more relevant capability scores of 1–2.	Establish ownership, stabilize critical controls and define immediate mitigation.
Build the roadmap	High risk + relevant capability score of 3, or moderate risk + score of 1–2.	Set a target state, sequence improvements and assign resources and milestones.
Monitor	Low risk or moderate risk supported by relevant capability scores of 4–5 and within tolerance.	Track indicators, test controls and reassess when conditions change.

Section 6: How to build a more operationally resilient business

Learn key action steps to manage your enterprise risk and become more resilient

Once you understand your enterprise risks, how do you take action to reduce them and build a more resilient business?

You can't boil the ocean, so the key is to prioritize risks and set about solving those that will deliver the greatest impact.

Here are key action steps to help strengthen your operational resilience:

1. Establish risk management goals

Set clear organizational goals for managing your enterprise risk. Based on your priorities list created in the previous section, determine where you should invest your time and resources, which will typically be areas that are high risk but rank low on the maturity spectrum.

Just as important, be sure to understand why you want to manage certain risks. For example, could reducing your risks around technology or AI make it easier to grow? Could stronger controls give you more accurate organizational data you can use to make smarter business decisions?

Understanding the value will help you stick with risk management as a long-term effort.

2. Create a risk and resilience roadmap

Next, use your goals and risk priorities to create a roadmap to address them. Your roadmap should lay out your risk priorities in order, starting with those high-risk, lower-maturity areas you've already identified and then moving down to moderate-risk, moderate-maturity issues.

If you haven't already done so, you'll also want to conduct additional gap assessments to understand your current controls in the areas you plan to improve on. You can use what you learn from those gap assessments to inform your roadmap.

3. Empower risk champions

Most organizational efforts fail without effective, empowered leadership. To make sure your enterprise risk roadmap actually gets implemented, you need to empower risk champions within your business to lead your risk management and resilience efforts.

This should include someone within your C-suite, as you'll need executive leadership to help ensure risk remains a priority.

4. Monitor and reassess

Risk management and building resilience take ongoing effort. Think of this work as a process that should be integrated into your regular operations, not a single event like an annual cybersecurity training.

Your risk champions should monitor your progress as your roadmap gets put into effect. You should also regularly reassess your risk environment to understand how changes could affect your business and your growth potential.

Section 7: Why businesses struggle to tackle enterprise risk internally

Could a fresh perspective make you more resilient?

Businesses (even those that operate in regulated industries) rarely have a large internal risk management team.

Even if you do have team members actively working on risk, their focus is likely on day-to-day compliance.

This can make it harder for you to fully assess, understand and mitigate your risks on an enterprise level. If your team lacks strategic risk capabilities, you may not even know what to look for, let alone how to solve it.

Internal teams also suffer from being too close to a problem to see it clearly. Your team members know your processes so well that they may overlook gaps without even realizing it. Or you may miss the big picture because you're too siloed to gain the necessary perspective.

All of this means that the most effective enterprise risk management efforts usually involve getting guidance from a third party advisor.

This doesn't just mean an audit of your existing controls (although that can be useful), but leaning on an advisor to facilitate your enterprise risk management maturity assessment and help you take action to become more resilient.

An advisor's strategic-level perspective can also help you link risk management efforts to growth. An advisor can help you translate information on your control environment into clearer organizational insights, find gaps in your processes and even identify areas where mitigating risk could directly translate into growth opportunities.

What an external enterprise risk assessment should (and shouldn't) do

What it should do

- ✓ Help leaders see how risk moves across ystems, teams and decisions.
- ✓ Highlight old assumptions that haven't been revisited as conditions have changed.
- ✓ Identify where ownership drops once data leaves its original system.
- ✓ Focus on driving smarter decisions, not just controls or compliance.
- ✓ Prioritize where attention matters most, not everything that could be reviewed.

What it shouldn't do

- ✗ Turn into a control inventory or audit exercise.
- ✗ Overwhelm teams with technical details or jargon.
- ✗ Assign blame for workarounds or shortcuts.
- ✗ Produce a report that sits on a shelf.
- ✗ Slow the business down in the name of rigor.

What you should expect to see

1. Clear patterns rather than exhaustive documentation
2. Plain-language insights
3. A focused list of risk priorities
4. Guidance on where visibility gaps create the most risk exposure
5. A clearer understanding of what to do next

Section 8: What does a more operationally resilient business look like?

More resilience means a stronger organization that's ready to grow

You don't manage enterprise risk to get an assessment report that sits on a shelf. You do it to make your business more resilient and prepared for growth.

That's what you should expect to see after implementing an enterprise risk management strategy like the one outlined in this book. The benefits won't just be avoiding risks that could have happened, but will include quantifiable, meaningful benefits, such as:

- **More confident decisions:** A more resilient organization delivers more accurate information to leaders. You'll be able to make decisions with greater confidence, knowing you're doing so based on sound data.
- **Streamlined processes:** As you assess your processes to look for risk, you'll inevitably uncover opportunities to streamline and make your work more efficient.
- **Integrated silos:** Implementing stronger controls gives you a much clearer understanding of how your organization functions, which helps you integrate siloed departments and find efficiencies or areas for improvement.
- **Visibility on redundancies:** If you've got redundancies within your business, a risk assessment and controls review will usually uncover them.
- **Simplified financial audits:** If your business needs regular financial statement audits, you'll find this process simpler and faster because your financial statement auditor will have greater confidence in your controls.
- **Ready for growth:** Get your operations better aligned with your growth needs by identifying gaps in your current systems and processes.
- **Faster crisis recovery:** If your business does experience a risk incident, you'll be better prepared to move through it more quickly, demonstrate greater operational resiliency and get back to business as usual faster.

A more resilient business is better prepared to thrive even amid big challenges. Honing that starts with managing enterprise risk.

How Wipfli can help

We advise businesses on managing enterprise risk and building resiliency. If you're a mid-market organization that's growing (or preparing to), we can help you become more agile, flexible and adaptable as you navigate your growth journey.

Ask us to help you identify resilience gaps, assess enterprise maturity across critical risk domains and develop a practical roadmap that aligns risk management with your core growth goals.

Let's talk risk and growth

ADVISORY & ACCOUNTING

WIPFLI