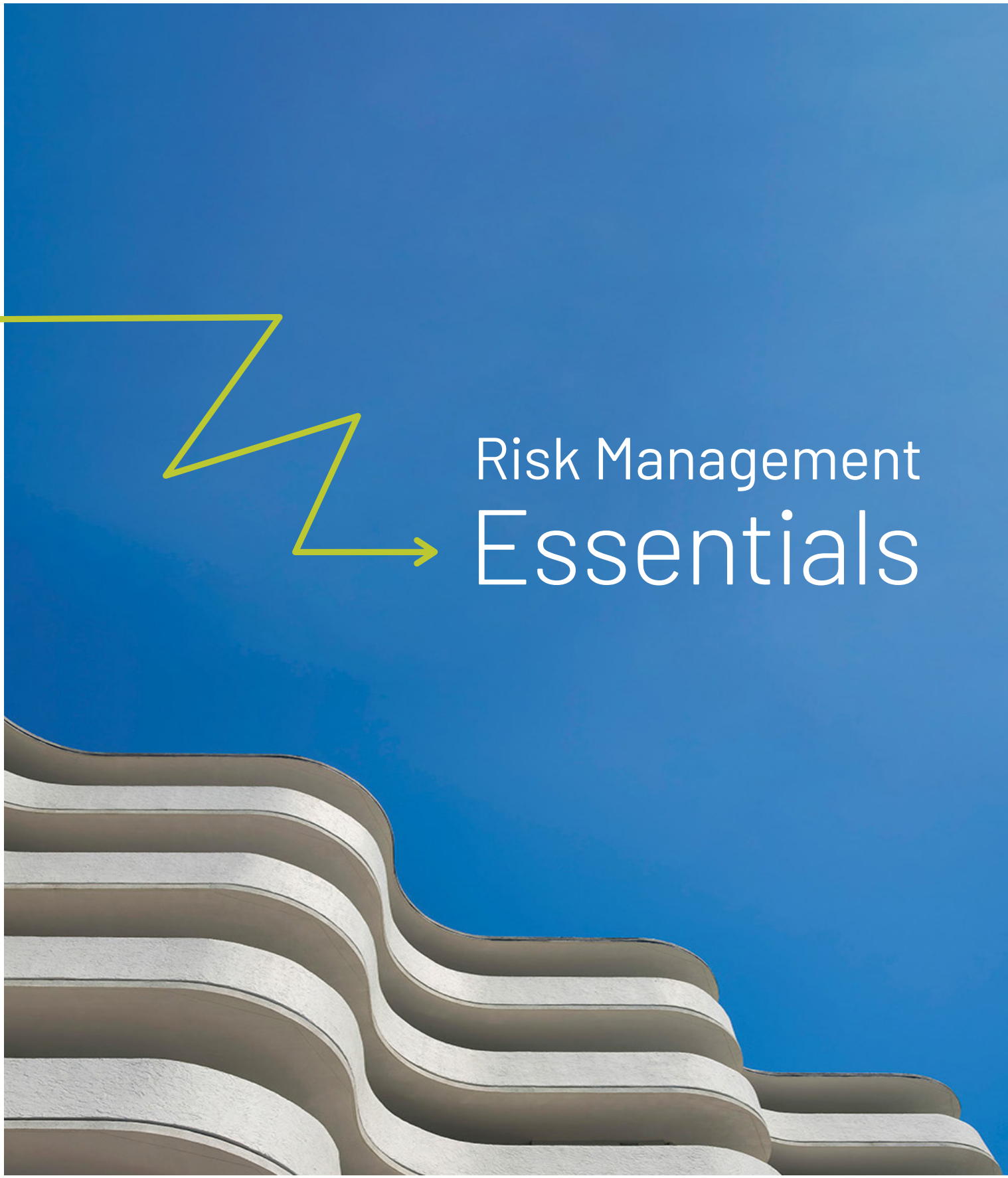


Risk Management Essentials

NAVEX®

Contents

Introduction

The most important part of risk management is understanding that no risk management strategy, approach or mindset is foolproof.

Risk is unavoidable. It's an unwavering, unwanted companion accompanying every decision, strategy, activity and daily operation. It's an inevitable part of life and doing business – and much like having a lifejacket on a boat, you can only be prepared for whatever challenges come your way to limit the damage it can do.

Many risks are predictable but insidious. Countless organizations suffer from the impact of information silos, disconnected systems and disjoined communication between "risk owners". All of these seem minor and common until they get in the way of you handling more immediate, spreading damage from other risks that arise. Most damaging of all is the lacking the ability anticipate risk until it's already at the door.

A proactive strategy involving thorough screening and due diligence can help avoid many risk-related dilemmas. Continuity plans should be ironclad, regardless of where your primary risks lie – and there should always be an understanding that risk is always alive and evolving.

Your organization's broader goals and ethos rely on risks being identified, not thriving unchecked. Effective risk management involves exploring diverse solutions, from risk transfer to mitigation, and periodically reviewing what you have found, what went wrong, and the results of your efforts to continuously improve.

When devising a risk management strategy from the bottom up, there are many places to start. But whether risk assessments take up half your servers or if your last audit resides in a dusty filing cabinet in the corner, understanding where your risks lie must be a vital part of your organization's strategy for survival.

This eBook is your guide to crafting a risk management strategy that not only safeguards your operations, but also positions you to find new successes and opportunities to lead and face risk head-on.

Risk is unavoidable. It's an unwavering, unwanted companion accompanying every decision, strategy, activity and daily operation.

NAVEX

Risk Management Essentials
Turning "Oh No" Into Opportunity

From small mom-and-pop shops on the corner to global conglomerates, risk is an ever-present companion in the workplace and in life. It's in the decisions you make, the strategies you adopt, and the daily operations you oversee.

Most importantly, risk is unavoidable. But think of it this way: just like having a lifejacket aboard a boat, the precautions in place to foresee and navigate risks are just as crucial as knowing what to do if you fall overboard.

In other words, the true measure of an organization's effectiveness isn't in its ability to avoid risk completely, but in its determination to quickly face it, get back up, learn, and adapt.

David vs. Goliath: which is the risk?

Take a look at powerhouse names like Apple and Netflix. These global juggernaut brands didn't just sidestep risk – they barreled into it and used it to their advantage.

Apple ventured into uncharted waters with the first iPhone, entering a market dominated by established manufacturers and brands. While some might say the market for success was slim, it pushed forward with a unique approach to marketing its products and redefined smartphones and desktop technology. Netflix, taking the emerging concept of digital content consumption into stride as a pioneer, evolved from LoveFilm DVD rentals into streaming right into our living rooms.

In the wider B2B sphere, there's BlackBerry. Once the go-to for business communications handheld devices, they saw a decline in interest as touch-screen smartphones evolved. When its once-dominant market share slipped away, BlackBerry pivoted with the challenge. They ventured into cybersecurity – a move that transformed their trajectory. They are now a familiar name in the cybersecurity software space.

Key benefits of effective risk management

So, what can effective risk management mean, generally speaking?

- **An enhanced field of vision** – More perspective opens up more doors – Netflix, Apple and BlackBerry are good examples. By not just focusing on immediate achievements, instead anticipating hurdles and building up the resources you need to respond to them, your organization is equipped to gauge challenges and seek out solutions.
- **Resilient operations** – Picture your organization as a smoothly running machine. Effective risk management ensures you face fewer disruptions, making operations seamless and efficient.
- **Stakeholder dependability** – Trust is earned over time. Everyone recognizes that risks are a fact of life. By acknowledging your unique risks and planning for them, you assure stakeholders of your organization's resilience and long-term viability. Proactively discussing these risks fosters trust far better than an unexpected crisis announcement and rushed damage control.
- **Active sustainability efforts** – Whether making small strides or massive leaps towards a green future, it's undeniable that regulations are getting stricter, and customers globally are becoming more eco-conscious. Recognizing and addressing the environmental and regulatory risks positions you ahead in reducing your corporate footprint.

Third-party risk: the linchpin of risk management

Risk management isn't just about theory or preparation. It involves having a full view of your unique business risks and how they interact. Third parties are a major element of any approach around risk, as all risks will have threads across your operation – but third-party risks are largely invisible on a day-to-day basis.

Though the inner workings of your third-party suppliers aren't accessible to you in the same way as your internal operations, your suppliers share your spotlight. Their actions reflect on your organization as a result. Regarding third-party risk, there are two major points to keep in mind:

Supply chain vigilance

Regularly reviewing and auditing suppliers for compliance with current legislation and ethical practices is a must for third-party risk management.

For instance, imagine discovering that a key supplier was recently fined for non-compliance with new legislation. If they are willing to improve and take immediate steps to rectify the issue and take steps to limit the damage, an option to limit disruption might be to collaborate with them to ensure compliance with that legislation to the standards you (and the law) expect.

However, when ethical issues compound legal breaches and the risk of further reputational or financial damage, you need to look at the bigger picture. Is this the first time they have had such issues? Has their communication with you been immediate and clear on what they will do next? Has your data privacy been affected?

Depending on the severity of the issue and the context of what it means to their, and your, organization, cutting ties might be the best way forward to maintain your integrity and reduce extended risks.

Ironclad continuity plans should be built into your risk management strategy regardless, whether your main risks lie with third-party suppliers or outside the business completely – as the world recently experienced with COVID-19.

Of course, a more proactive strategy that involves thorough screening and due diligence as part of a third-party risk management strategy will help you to avoid these dilemmas.

Diversification

In a volatile market, heavily relying on a single revenue stream, vendor or key figure to drive growth can make or break an organization, from one department to the entire operation. Proactively identifying and venturing into new, complementary markets, identifying silos and taking steps to limit the impact of realized risk can serve as a buffer. For example, diversification can stabilize revenue flow, ensuring business continuity even when one segment faces challenges.

The same concept applies to supply chains, as well as subject matter experts and vendors of assets, software or resources your organization needs to survive. Putting all your eggs in one basket means being absolutely certain that the basket is 100% bulletproof 100% of the time. Who can guarantee that? If you can't, if one line of revenue is disrupted, what plans are in place to keep the business afloat?

Regularly reviewing and auditing suppliers for compliance with current legislation and ethical practices is a must for third-party risk management.

Prioritizing risks: what matters most?

Understanding and prioritizing risks is half the battle. The next step is taking action. Here's how to navigate this:

1. Strategic alignment: Before deciding on a risk action, ensure it aligns with the organization's broader goals and ethos. Every action taken, even in risk management, reflects on your company's identity, reputation and brand.

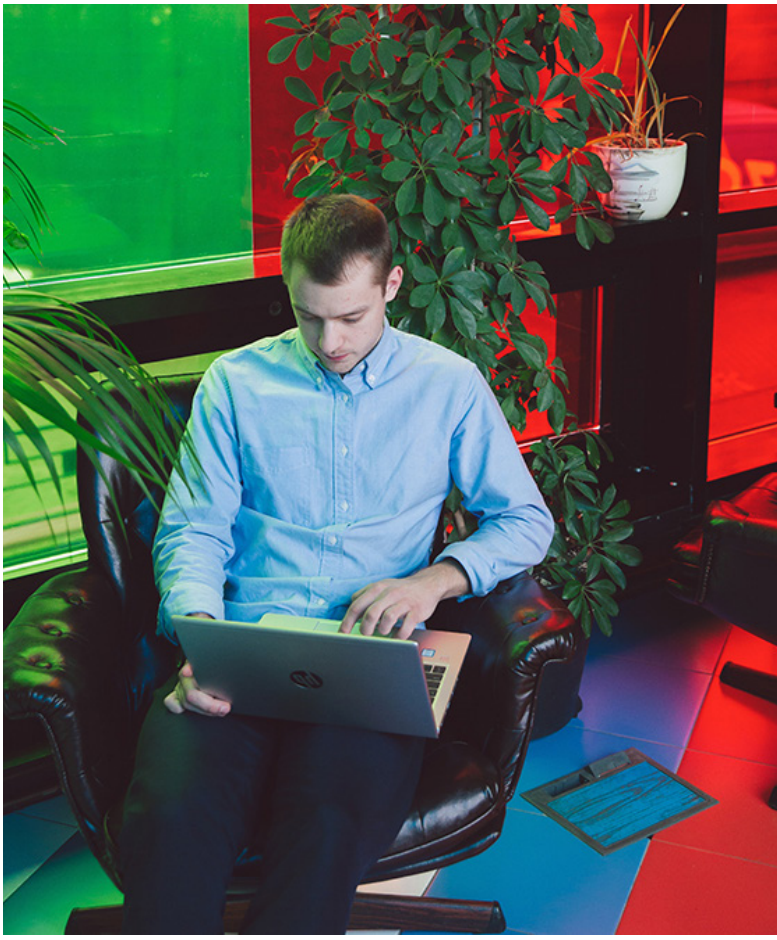
2. Diverse solutions: Sometimes, risks can be avoided; other times, they need to be accepted. There are various strategies at play – from transferring the risk (like insurances) to mitigating it (like backup plans). Understand the pros and cons of each, including what other factors might impact them.

3. Review periodically: After action is taken, always circle back to see the results. Was the risk managed effectively? What could have been done better? Regular reviews ensure that the organization is always learning and improving.

A risk by any other name

Whether it's the tech titans like Apple or security pioneers like BlackBerry, there's a consistent narrative: embrace risk to chart new realms of innovation and growth and work out which risks are pitfalls vs. which are propellers.

Managing risk is really about building a comprehensive understanding of your surroundings, having the tools to monitor, measure, and manage, and then making informed choices that drive your business forward.



NAVEX

Risk Management Essentials
Navigating the Tightrope of Third-Party Risks

Let's talk tightropes

Picture this: a daring tightrope walker maneuvers gracefully across a thin wire. Suspended high above a bustling circus, each step is deliberate, each movement a calculated risk.

In many ways, managing third-party risks mirrors this high-stakes performance. Every decision carries weight – and one misstep could result in a dangerous fall.

So, how do you maintain this precarious equilibrium? Is your organization the tightrope walker or the tightrope?

What is third-party risk management?

Before we dive too deep, let's set the stage by defining third-party risk management.

Far from simply being a subcategory of general risk management, it's a unique, multifaceted discipline. Imagine a chess match, but instead of only trying to checkmate your opponent, you're also working together first to defeat a common enemy.

Here, vigilance isn't optional. It's a necessity.

Third-party collaboration can offer specialized skills, open doors to new products and markets, and boost growth. Every organization, from a small organic grocery chain to a multinational tech conglomerate, knows this. However, in the same way a glass of expensive wine can leave a sour taste in your mouth, third-party associations without the proper screening and audits in place can become a vulnerability faster than you can say "data breach".

Third-party risks are as prevalent and varied as any internal risk – and even more unpredictable since they're wrapped up in another entity's actions and the veil of all the other operations and processes you don't have insight into. Sweeping these risks under the rug? Big mistake.

Subcategories of third-party risk

Navigating third-party risk isn't a one-size-fits-all endeavor, so there isn't one single field to watch out for pitfalls underfoot.

Let's break the major risk areas down:

Cybersecurity – With the increasing number of cyberattacks every week, there's no glossing over how big a risk cyberthreats are to anyone, anywhere. The best crisis management processes in the world can't prevent a risk brought through the front door by a partner you thought you could trust.

Evaluate and press the buttons of security measures like you would your own, keeping in mind you may not have access on a daily basis – and the cyberthreat landscape is always one step ahead. Some of these factors are easy to check, while others are more subtle. For example, are your partners using outdated software? Do they regularly train their staff in cybersecurity best practices?

Compliance – Regulatory pitfalls are everywhere. Your third-party partners need to meet the same local, regional and international standards that you do. Why? Because if they slip up, you're implicated too. Use compliance management systems to continuously monitor their activities, identify where risk areas lie and assess risk on an ongoing basis.

Financial – The financial stability of your third-party partners can directly impact your operations. If suppliers or vendors suddenly go bankrupt or face cashflow problems, you're left holding the empty bag. Ensure you regularly review your third parties' financial health through credit reports, audits and other financial assessments to confirm cash flow is healthy from A to Z.

A playbook for third-party risk management

Data is a global currency, and some countries want to keep their citizens' data squarely under their control. Russia's data privacy law, passed in 2022, provides new rules for personal data processing and cross-border data transfer. It establishes mandatory requirements for data controllers and processors, including a new requirement on data breach notification.

Your next move is to create a clear-cut plan that lays out how you'll identify, assess, monitor and respond to third-party risks. Think of this as your treasure map: it outlines the terrain, warns you of pitfalls and guides you to your destination – which is nothing less than robust risk management!

The following points are your directions to get you through the maze of complexities that come with dealing with third parties:

1. Identify and classify – This is your first filter. Separate the wheat from the chaff by understanding the nature and degree of risk each third-party brings:

- **High-risk** – These entities require extensive audits and frequent check-ins
- **Medium-risk** – Adequate due diligence is enough
- **Low-risk** – Minimal oversight is required – just don't get complacent

2. Conduct due diligence – You're the detective; your third parties are the subjects. Use tools like background checks, credit reports and compliance certificates to verify credentials and screen partners for concerns.

3. Monitor and review – Ever heard of the saying "trust but verify"? In other words, to scan while you sustain, implement automated governance, risk and compliance solutions to track performance metrics and flag risks and anomalies. Known risks mean you're aware of what to watch out for; no risks on your radar means there's something (or several things) you aren't seeing.

4. React and revise – If you discover a risk, don't just put a band-aid on it. Dig deep, find the root cause and revise your approach to either prevent it from reoccurring or manage it to avoid damage, escalations or losses to your organization.

Data is a global currency, and some countries want to keep their citizens' data squarely under their control.

Tools and technologies

Technological advancements have changed the world – including how organizations can manage third-party risks. From automated oversight to real-time auditing, today's tools are light-years ahead of clunky manual processes that struggle to sort a mountain from a molehill.

Whether you're a seasoned pro or new to the field, there's a suite of digital solutions designed to make your life easier and your strategies more effective:

- **AI-based analytics platforms** – Your secret weapon for sniffing out third-party vulnerabilities, these platforms use advanced algorithms to detect potential external risk areas before they escalate.
- **Contract management systems** – Keep track of every term and condition with your external vendors. These systems make sure compliance is upheld and financial agreements are clear, agreed in advance and subject to airtight non-disclosure agreements and data security. If you've ever been burned by the fine print, you know how vital contract management is. These systems help you monitor and manage every agreement with third-party vendors, ensuring compliance is maintained, and any financial implications are clear from the get-go.
- **Collaboration portals** – Secure spaces to share sensitive information and collaborate on risk assessments with your third parties.

- **Risk management software** – When risks can change in days rather than weeks, the adaptability of an integrated risk management can't be underestimated. Automated alerts for periodic assessments and can help you keep you on top of the risk admin work that keeps current data feeding into the system.
- **Audit solutions** – Get real-time snapshots of third-party compliance. These tools alert you to potential issues before they blow up, helping you keep your eyes on any potential problems on the horizon.

The view from the tightrope

Managing third-party risk is more than a one-time task. It's an ongoing act of agility, awareness and adjustment on both your part and the part of your partners and suppliers.

As you contemplate the path ahead, remember that it's always better to be proactive than reactive. There are both internal and third-party risks in your organization's future – that's a fact. It's how you manage them that keeps your organization safe.

Risk Management Essentials
The Human Touch

Everyone plays a role in managing risk

Risk management isn't one team's concern, so keep those communication lines open. A collective understanding of potential risks sets a strong foundation. Conduct surveys, engage in brainstorming sessions and encourage a culture where everyone feels empowered to voice their concerns and share their insights.

Elements to consider for effective risk management collaboration across different teams:

1. Operations and supply chain: It's all about maintaining a smooth flow. By staying in close communication with suppliers and anticipating potential delivery issues, teams can ensure there are no unexpected interruptions. It's beneficial to always have a backup plan, so when hiccups do arise, you're already steps ahead.

Beyond the operational and strategic benefits, understanding the emotional and psychological implications of risk can pave the way for deeper, more impactful decisions focused on how risk affects people inside and outside your business.

2. IT and cybersecurity: A proactive approach goes a long way. By staying informed about the latest cyber threats and conducting regular system checks, IT teams can keep the company's data and infrastructure safe. This isn't just routine – it's the most important risk factor of running a business in the digital age, so the whole organization has to be aware of and invested in managing this area of risk.

3. Human resources: The wellbeing of the team affects the whole organization. Regular check-ins, surveys and addressing any concerns promptly can help avoid larger issues and people-related risk down the road. Recognizing and acting on these insights keeps morale high, talent retained and operations smooth sailing.

4. Sales and marketing: Feedback from the field is gold. By actively listening to customers and keeping an eye on competitors, these teams offer early warnings about market shifts and any problems in important client relationships that might crop up. This real-time information can be crucial for adjusting strategies quickly when needed.

5. R&D and product development: Innovation doesn't exist in a vacuum. Regular brainstorming sessions can help the team anticipate industry challenges, ensuring the next big thing is truly groundbreaking and not just a fleeting idea. It also gives you a starting point to check your sales and marketing is in alignment with the reality of your product.

Risk management – thinking about human impact

Beyond the operational and strategic benefits, understanding the emotional and psychological implications of risk can pave the way for deeper, more impactful decisions focused on how risk affects people inside and outside your business.

For example:

Embracing vulnerabilities: Going beyond accepting risks at face value and avoiding the action that leads to it in the future. Imagine a leading software company receiving feedback on its latest release. The release saves overhead, is more secure and is easier to update, but feedback from users is overwhelmingly negative. Instead of deflecting or ignoring this feedback and waiting for the customer base to get used to it, the organization could openly admit areas for improvement and open up new means to receive feedback and prioritize which features are causing the most complaints. By actively addressing and refining those issues, they not only enhance their product but also reinforce trust over time with their users.

Changing strategies: Being adaptable doesn't just mean rolling with the punches, and confronting risk sometimes requires taking risks. Think of a small online retail business that starts to see a decline in sales because of changing consumer preferences. Instead of sticking to their tried-and-true inventory, they delve into market research, putting more effort into exploring and updating their product range based on customer desires. Nimbleness turns a potential risk into an opportunity for growth.

Empathy in action: It's not just about managing a brand's image; it's about recognizing and valuing the human experiences intertwined with the business. When an organization faces backlash for a decision, they might initiate community-focused events or forums, not simply as a PR move for damage control, but as a gesture to listen to and understand concerns to avoid a repeat. By actively engaging, they demonstrate a commitment to their values and create an opportunity to strengthen trust.

Analyzing risks: more than just numbers

When diving into risk analysis, remember that risks aren't just abstract concepts – they have real-world implications. Here's how to go about it:

1. The power of data: Data-driven analysis forms the backbone of understanding risks, but it goes further than statistics and percentages. Qualitative data is a powerful form of data that helps you measure the impact of your organization's actions on people. Collecting relevant data of this nature, for example from past incidents, market studies, product reviews and feedback loops, can help you get a full view of potential risks from all relevant data sources.

2. Tools and techniques: Employing tools like SWOT analysis – i.e., looking at your strengths, weaknesses, opportunities and threats – and putting together risk matrices can give you a structured way to visualize and weigh risks. But remember, it's not just about the tools. The interpretation of the results, and perceptions of those results, are just as crucial.

Consultants and experts around risk are a useful avenue for making sure you are getting the most of your data, and that you are aligned with the real risk landscape of your business. However, much of the actions already embedded within your business – such as employee satisfaction surveys, downtime assessments or the nature of complaints concerns reported by employees – are all great risk indicators to include in your risk management processes.

3. Embrace subjectivity: While quantifying risks is important, some risks might be more subjective based on intuition or experience. These insights, especially from seasoned team members and completely fresh eyes, can provide valuable perspectives and suggestions you may not have considered before.

Embracing the full spectrum of risk

Managing risk is as much about understanding people, their strengths and how to keep them safe as it is about process from a purely operational point of view. Though complexities including legal, cybersecurity and financial risks can feel distant from the human impact, organizations don't exist in a vacuum. Every risk impacts a person or people, so reminding yourself of this fact can add depth to your understanding of risk and how best to manage it.

Managing Internal Risks
Why do Internal Risks Matter?

Building risk resilience from the inside

Why bother looking inward when external risks seem so pressing?

The answer is straightforward: you're only as strong as your internal structure. Studying how to manage floods in your neighborhood is only so helpful when your house is on fire.

The role your people play in preventing or enabling risks, for example, cannot be underestimated. Huge scandals in the press don't always start out on the front cover of national newspapers – internal risks can be insidious, starting as small as rumors, a white lie in a meeting, or a statistic or number entered incorrectly.

The culture of your organization makes or breaks your risk management strategy. People raising their concerns when small risks arise, and not staying silent, can be the difference between no issue at all and a much larger risk that spirals out of your control.

Think less "if it happens" and more "how it could happen"

Not seeing risks doesn't mean there are none – it means you're missing something.

When we mentioned earlier that internal risks are insidious, it's really a perfect way to describe them – the changes are so gradual you may not recognize the risk until you're in its headlights. This is where psychological factors like confirmation bias can also play a role. If all your metrics are going green, it's easy to ignore that one red flag waving in the wind.

Secondly, where there are people, there are risks. Humans and human behaviors are messy, and the business of doing business *always* comes with human risks.

Essentially, risks are always present – determining whether risks need to be mitigated, or managed with regular oversight, requires full visibility into the risks facing your organization.

Let's break down the types of internal risks you might be dealing with:

Immediate risks

These risks demand urgent attention and action as they are likely to escalate quickly. They also pose danger for the business, your people, or both. Immediate risks are also the hardest to anticipate, so procedures defining how they should be handled need to be prepared long before they have a chance to happen. Think of these risks as flashing red lights that get the emergency service team on the move ASAP. That emergency service team has to know exactly where to go and what to do.

Essentially, risks are always present – determining whether risks need to be mitigated, or managed with regular oversight, requires full visibility into the risks facing your organization.

Examples

- Incidents involving gross misconduct, violent assault or harassment
- Illegal activity, such as embezzlement or extortion
- The discovery of a dangerous artifact onsite
- A major data breach

Evolving risks

Risks that aren't unheard of – but can also be managed with good processes and regular review. These are things that could happen but aren't necessarily happening today. These risks often start out small and become larger issues over time, like a weed growing in your garden. They often affect teams and productivity over extended periods, risking attrition, poor morale and negatively impacted productivity if they aren't kept under control. A healthy workplace culture where your people can have open conversations about workplace issues before they become longer-term problems will help manage these kinds of risks.

Examples

- Shifting project goalposts over time beginning to risk meeting your SLAs
- Poor budget management and oversight into spending month-on-month
- Inefficient communication and operations – and a struggling pipeline
- Ongoing resourcing issues and stressed, unhappy employees
- Data or knowledge silos causing delays in your production cycle

Situational risks

These are risks you can't prevent and sometimes can't anticipate. These risks may originate externally, but can have huge internal repercussions for your organization and the communities, regions and industries you work in.

Examples

- Regulatory-related risks including legislative updates or new requirements impacting service or processes internally or with third-parties and suppliers
- An economic downturn forcing you to cut budget areas – this might include employee perks, events or even headcount
- Geopolitical conflict requiring an urgent rethink in the countries you work with or hire from, including, but not limited to sanctions
- Natural disasters or health-related crises in a particular area your business operates

Kickstarting your internal risk assessments: where to start

We've examined the types of risk your organization might face that originate or impact your internal operations. Now the key is to start laying groundwork you can build on as part of your management of internal risks. Once you know where to look, you can more easily identify what steps to take.

- **Start with an internal audit** – Before you can manage risk, you need to know where it exists. Enlist your compliance, finance and HR departments to provide an overview of existing procedures and policies so you can see how risks are handled right now.
- **Employee feedback** – Your team knows your internal workings better than anyone else. Make use of anonymous surveys or open forums to get insights into possible areas of concern.
- **Identify critical assets and processes** – What are the non-negotiables your business absolutely can't function without? Make a list and start from there.

- **Assess historical data** – Look into any past incidents that could point to potential risks. Even small issues can serve as indicators for larger, systemic risks.
- **Prioritize** – Not all risks are created equal. Use the data you've collected to categorize risks by their potential impact and focus on the ones that could hit your organization hardest.
- **Measure consistently** – Ensure all areas of the business that are prioritizing and categorizing risk use the same method to measure risk. Doing so ensures you won't need a Rosetta Stone to decipher the difference between a "red", a "thumbs down", or a numerical scale to evaluate risk levels.

Once you've gathered this initial information, you'll have a solid base to start formulating a more comprehensive risk management strategy. Remember, the goal is progress, not perfection. Every productive day starts with a well-organized to-do list.

The heart of the matter

Whether internal risks manifest immediately or evolve over time, they are a part of your organization's fabric. Being proactive in identifying and managing them not only prevents potential damage but also fortifies your operation against external uncertainties.

Remember, situational risks may come from outside, but their impact reverberates internally. As much as external issues may dominate the headlines, it's the internal mechanisms that often dictate how resilient an organization truly is. Being vigilant in identifying, categorizing and acting on internal risks enables you to steer the ship with precision, even when unexpected storms hit.

Ultimately, your internal operations set the stage for how well you can manage external risks – and that's why your internal compass should point just as clearly as your outward radar.

NAVEX

Managing Internal Risks

How to Listen When People Speak Up

What is a 'speak-up' culture, anyway?

If you're hearing the term 'speak-up' culture and picturing your team doing stand-up comedy at company parties, you've missed the point – although a good laugh never hurts morale.

Speak-up culture is all about creating an open environment where employees feel comfortable sharing concerns, ideas or observations that could affect your company's performance or ethical standing. It's not about criticizing for the sake of it; it's about proactive problem-solving.

Before diving into how to manage internal risks by listening, it's crucial to understand the bedrock of what you're trying to build: an environment where people are not just allowed, but encouraged, to speak their minds.

Create windows where your walls are

Think of your organization as teeming with risk managers. More often than not, they're the first to spot red flags, sometimes even before your dedicated risk team.

However, if your organization is full of walls, there's mountains of data you're going to miss that plays a vital part in identifying and handling risk. If you try to turn those walls into windows, where transparency and open communication are valued, you'll see so much more across your business.

Why speak-up culture matters:

- It's powered by a resource you already have: your people
- It facilitates faster problem-solving on companywide issues
- It can increase employee engagement and improve morale
- When you listen and act on feedback, it builds trust across your organization

Whistleblowing: a gift, not a curse

People who raise concerns with management, commonly known as whistleblowers, often get a bad rap. Historically, they've been seen as nuisances, snitches or even traitors, especially when we think of big scandals involving whistleblowers taking insider info to the press.

However, whistleblowers who report internally when they have concerns are effectively an early warning system. They aren't going to the press – they're telling you they think something is wrong. Sure, you've got meetings, maybe even a suggestion box or two. But have you established a culture where people genuinely feel they can voice their concerns?

To meet global whistleblowing regulations and support a speak-up culture, you must create avenues where employees can report issues they've noticed without fearing a proverbial slap on the wrist.

To meet global whistleblowing regulations and support a speak-up culture, you must create avenues where employees can report issues they've noticed without fearing a proverbial slap on the wrist. Even so, culture also needs softer touch points alongside reporting channels guides in your code of conduct on how to raise concerns.

A starting point can be as simple as dedicating five minutes in your weekly team meeting for risk discussions. A reward system for constructive feedback, such as making processes safer or more efficient, can also encourage more people to come forward.

Here are a few more tips for normalizing how and why people should raise concerns within your organization:

- Use and regularly highlight an internal communication tool specifically for employees to raise concerns or check policies
- Talk about issues noticed or reported, and how they were handled, openly in company communications
- Implement a regular speak-up segment in team meetings, initiated by management where possible
- Train managers to actually listen for wider issues during these segments, rather than just noting what individuals say

The perils of ignoring your staff can't be stressed enough. It's not just about keeping talent; it's about listening to those who are tuned in to the realities you can't see from your boardroom. When your team members feel unheard, you really risk them becoming someone else's team members.

Losing your people to mistrust and poor morale isn't just a team loss. It's a massive internal risk management failure.

Thinking tactically about tech

Internal risks – especially people-based ones – can be elusive. So, how do you go about detecting them? Employee surveys are one way to start, but you need to dig deeper. Tech can help.

Modern risk assessment platforms, designed to flag internal issues, can offer you useful insights not visible from the CCO's office. They can sift through data, including reports submitted by employees, pick up on inconsistencies and alert you to looming problems through pattern detection.

- **Whistleblower helplines** – Digital platforms that provide an anonymous, secure way for employees to report any issues. These are essentially your early warning systems for employees to ring the bell. As the mouthpiece of speaking up, they are where people go to tell you what's up.
- **Incident management platforms** – These aren't just for data breaches. Use them to log and manage all your reports of internal risks flagged by your team, ensuring every voice is heard and responded to in line with regulatory requirements.
- **Collaboration portals** – Think of these as your organization's internal social media. They encourage open dialogue and can serve as less formal platforms or forums for raising red flags, discussing problems and ideating solutions, helping to normalize the act of speaking up.
- **Employee feedback tools** – These can go beyond the traditional annual review, but they are more of a periodic prompt to your people rather than only offering an open-ended portal to raise concerns. Real-time feedback platforms allow employees to raise concerns as they occur, letting you nip potential issues in the bud.
- **Audit solutions** – While they're great for financial checks, consider using them for social audits on your company culture. They can help you track how often concerns are raised and how swiftly they are addressed, providing a tangible measure of the health of your speak-up culture.

As a final point, data mismanagement is a sneaky carrier of risk that thrives in a culture of silence. Whether it's due to poor procedures or a sheer lack of oversight, when data isn't handled correctly, it's not just about potential financial losses or wasted time. External audits that find these mistakes can quickly land you in hot water with regulating bodies – you're far better off finding them yourself so you can strategize how to manage them better.

Employee input can be a rich source of qualitative data to fill the gaps your quantitative surveys leave. Make sure your tech tools are calibrated to treat this data with the gravity it deserves, flagging trends, common concerns and patterns that quantitative data might miss – the applications for this sort of information are infinite.

Risk is a bigger picture than your organization

Many of the emerging risks you face every day touch the remit and responsibilities of one or more of your employees.

A strong speak-up culture is your first line of defense against a range of risks, especially internal risks. Furthermore, the human element of risk management should never be underestimated. While we've examined various categories of risks, they often intersect and are magnified through human behavior, for better or worse.

Whether it's on a screen or part of an interaction, in your day-to-day operations, it's far more likely someone will notice potential or actual risk faster than your processes or occasional auditors will. Can these people tell you? What would put them off telling you? And if they do raise a concern, what will you do next?

NAVEX is trusted by thousands of customers worldwide to help them achieve the business outcomes that matter most. As the global leader in integrated risk and compliance management software and services, we deliver our solutions through the NAVEX One platform, the industry's most comprehensive governance, risk and compliance (GRC) information system.

For more information, visit NAVEX.com and our blog. Follow us on X and LinkedIn.

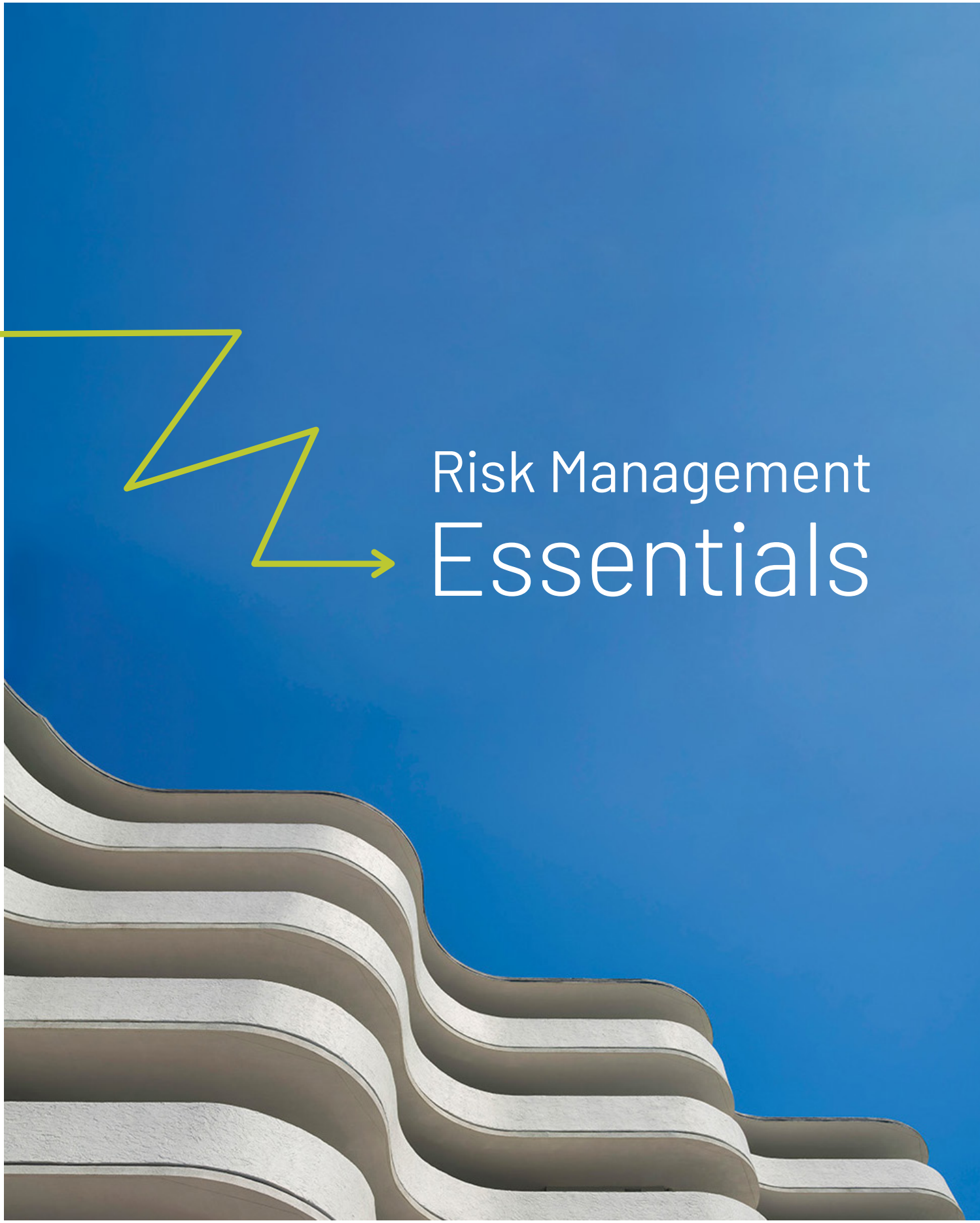
AMERICAS

5500 Meadows Road, Suite 500
Lake Oswego, OR 97035
United States of America
info@navex.com
www.navex.com
+1 (866) 297 0224

EMEA + APAC

4th Floor, Vantage London
Great West Road
Brentford, TW8 9AG
United Kingdom
info@navex.com
www.navex.com/uk
+44 (0) 20 8939 1650

NAVEX®



Risk Management Essentials

NAVEX®

Contents

Introduction

The most important part of risk management is understanding that no risk management strategy, approach or mindset is foolproof.

Risk is unavoidable. It's an unwavering, unwanted companion accompanying every decision, strategy, activity and daily operation. It's an inevitable part of life and doing business – and much like having a lifejacket on a boat, you can only be prepared for whatever challenges come your way to limit the damage it can do.

Many risks are predictable but insidious. Countless organizations suffer from the impact of information silos, disconnected systems and disjoined communication between "risk owners". All of these seem minor and common until they get in the way of you handling more immediate, spreading damage from other risks that arise. Most damaging of all is the lacking the ability anticipate risk until it's already at the door.

A proactive strategy involving thorough screening and due diligence can help avoid many risk-related dilemmas. Continuity plans should be ironclad, regardless of where your primary risks lie – and there should always be an understanding that risk is always alive and evolving.

Your organization's broader goals and ethos rely on risks being identified, not thriving unchecked. Effective risk management involves exploring diverse solutions, from risk transfer to mitigation, and periodically reviewing what you have found, what went wrong, and the results of your efforts to continuously improve.

When devising a risk management strategy from the bottom up, there are many places to start. But whether risk assessments take up half your servers or if your last audit resides in a dusty filing cabinet in the corner, understanding where your risks lie must be a vital part of your organization's strategy for survival.

This eBook is your guide to crafting a risk management strategy that not only safeguards your operations, but also positions you to find new successes and opportunities to lead and face risk head-on.

Risk is unavoidable. It's an unwavering, unwanted companion accompanying every decision, strategy, activity and daily operation.

Risk Management Essentials
Turning "Oh No" Into Opportunity

From small mom-and-pop shops on the corner to global conglomerates, risk is an ever-present companion in the workplace and in life. It's in the decisions you make, the strategies you adopt, and the daily operations you oversee.

Most importantly, risk is unavoidable. But think of it this way: just like having a lifejacket aboard a boat, the precautions in place to foresee and navigate risks are just as crucial as knowing what to do if you fall overboard.

In other words, the true measure of an organization's effectiveness isn't in its ability to avoid risk completely, but in its determination to quickly face it, get back up, learn, and adapt.

David vs. Goliath: which is the risk?

Take a look at powerhouse names like Apple and Netflix. These global juggernaut brands didn't just sidestep risk – they barreled into it and used it to their advantage.

Apple ventured into uncharted waters with the first iPhone, entering a market dominated by established manufacturers and brands. While some might say the market for success was slim, it pushed forward with a unique approach to marketing its products and redefined smartphones and desktop technology. Netflix, taking the emerging concept of digital content consumption into stride as a pioneer, evolved from LoveFilm DVD rentals into streaming right into our living rooms.

In the wider B2B sphere, there's BlackBerry. Once the go-to for business communications handheld devices, they saw a decline in interest as touch-screen smartphones evolved. When its once-dominant market share slipped away, BlackBerry pivoted with the challenge. They ventured into cybersecurity – a move that transformed their trajectory. They are now a familiar name in the cybersecurity software space.

Key benefits of effective risk management

So, what can effective risk management mean, generally speaking?

- **An enhanced field of vision** – More perspective opens up more doors – Netflix, Apple and BlackBerry are good examples. By not just focusing on immediate achievements, instead anticipating hurdles and building up the resources you need to respond to them, your organization is equipped to gauge challenges and seek out solutions.
- **Resilient operations** – Picture your organization as a smoothly running machine. Effective risk management ensures you face fewer disruptions, making operations seamless and efficient.
- **Stakeholder dependability** – Trust is earned over time. Everyone recognizes that risks are a fact of life. By acknowledging your unique risks and planning for them, you assure stakeholders of your organization's resilience and long-term viability. Proactively discussing these risks fosters trust far better than an unexpected crisis announcement and rushed damage control.

Regularly reviewing and auditing suppliers for compliance with current legislation and ethical practices is a must for third-party risk management.

- **Active sustainability efforts** – Whether making small strides or massive leaps towards a green future, it's undeniable that regulations are getting stricter, and customers globally are becoming more eco-conscious. Recognizing and addressing the environmental and regulatory risks positions you ahead in reducing your corporate footprint.

Third-party risk: the linchpin of risk management

Risk management isn't just about theory or preparation. It involves having a full view of your unique business risks and how they interact. Third parties are a major element of any approach around risk, as all risks will have threads across your operation – but third-party risks are largely invisible on a day-to-day basis.

Though the inner workings of your third-party suppliers aren't accessible to you in the same way as your internal operations, your suppliers share your spotlight. Their actions reflect on your organization as a result. Regarding third-party risk, there are two major points to keep in mind:

Supply chain vigilance

Regularly reviewing and auditing suppliers for compliance with current legislation and ethical practices is a must for third-party risk management.

For instance, imagine discovering that a key supplier was recently fined for non-compliance with new legislation. If they are willing to improve and take immediate steps to rectify the issue and take steps to limit the damage, an option to limit disruption might be to collaborate with them to ensure compliance with that legislation to the standards you (and the law) expect.

However, when ethical issues compound legal breaches and the risk of further reputational or financial damage, you need to look at the bigger picture. Is this the first time they have had such issues? Has their communication with you been immediate and clear on what they will do next? Has your data privacy been affected?

Depending on the severity of the issue and the context of what it means to their, and your, organization, cutting ties might be the best way forward to maintain your integrity and reduce extended risks.

Ironclad continuity plans should be built into your risk management strategy regardless, whether your main risks lie with third-party suppliers or outside the business completely – as the world recently experienced with COVID-19.

Of course, a more proactive strategy that involves thorough screening and due diligence as part of a third-party risk management strategy will help you to avoid these dilemmas.

Diversification

In a volatile market, heavily relying on a single revenue stream, vendor or key figure to drive growth can make or break an organization, from one department to the entire operation. Proactively identifying and venturing into new, complementary markets, identifying silos and taking steps to limit the impact of realized risk can serve as a buffer. For example, diversification can stabilize revenue flow, ensuring business continuity even when one segment faces challenges.

The same concept applies to supply chains, as well as subject matter experts and vendors of assets, software or resources your organization needs to survive. Putting all your eggs in one basket means being absolutely certain that the basket is 100% bulletproof 100% of the time. Who can guarantee that? If you can't, if one line of revenue is disrupted, what plans are in place to keep the business afloat?

Prioritizing risks: what matters most?

Understanding and prioritizing risks is half the battle. The next step is taking action. Here's how to navigate this:

1. Strategic alignment: Before deciding on a risk action, ensure it aligns with the organization's broader goals and ethos. Every action taken, even in risk management, reflects on your company's identity, reputation and brand.

2. Diverse solutions: Sometimes, risks can be avoided; other times, they need to be accepted. There are various strategies at play – from transferring the risk (like insurances) to mitigating it (like backup plans). Understand the pros and cons of each, including what other factors might impact them.

3. Review periodically: After action is taken, always circle back to see the results. Was the risk managed effectively? What could have been done better? Regular reviews ensure that the organization is always learning and improving.

A risk by any other name

Whether it's the tech titans like Apple or security pioneers like BlackBerry, there's a consistent narrative: embrace risk to chart new realms of innovation and growth and work out which risks are pitfalls vs. which are propellers.

Managing risk is really about building a comprehensive understanding of your surroundings, having the tools to monitor, measure, and manage, and then making informed choices that drive your business forward.

NAVEX

Risk Management Essentials
Navigating the Tightrope of Third-Party Risks

Let's talk tightropes

Picture this: a daring tightrope walker maneuvers gracefully across a thin wire. Suspended high above a bustling circus, each step is deliberate, each movement a calculated risk.

In many ways, managing third-party risks mirrors this high-stakes performance. Every decision carries weight – and one misstep could result in a dangerous fall.

So, how do you maintain this precarious equilibrium? Is your organization the tightrope walker or the tightrope?

What is third-party risk management?

Before we dive too deep, let's set the stage by defining third-party risk management.

Far from simply being a subcategory of general risk management, it's a unique, multifaceted discipline. Imagine a chess match, but instead of only trying to checkmate your opponent, you're also working together first to defeat a common enemy.

Here, vigilance isn't optional. It's a necessity.

Third-party collaboration can offer specialized skills, open doors to new products and markets, and boost growth. Every organization, from a small organic grocery chain to a multinational tech conglomerate, knows this. However, in the same way a glass of expensive wine can leave a sour taste in your mouth, third-party associations without the proper screening and audits in place can become a vulnerability faster than you can say "data breach".

Third-party risks are as prevalent and varied as any internal risk – and even more unpredictable since they're wrapped up in another entity's actions and the veil of all the other operations and processes you don't have insight into. Sweeping these risks under the rug? Big mistake.

Subcategories of third-party risk

Navigating third-party risk isn't a one-size-fits-all endeavor, so there isn't one single field to watch out for pitfalls underfoot.

Let's break the major risk areas down:

Cybersecurity – With the increasing number of cyberattacks every week, there's no glossing over how big a risk cyberthreats are to anyone, anywhere. The best crisis management processes in the world can't prevent a risk brought through the front door by a partner you thought you could trust.

Evaluate and press the buttons of security measures like you would your own, keeping in mind you may not have access on a daily basis – and the cyberthreat landscape is always one step ahead. Some of these factors are easy to check, while others are more subtle. For example, are your partners using outdated software? Do they regularly train their staff in cybersecurity best practices?

Compliance – Regulatory pitfalls are everywhere. Your third-party partners need to meet the same local, regional and international standards that you do. Why? Because if they slip up, you're implicated too. Use compliance management systems to continuously monitor their activities, identify where risk areas lie and assess risk on an ongoing basis.

Financial – The financial stability of your third-party partners can directly impact your operations. If suppliers or vendors suddenly go bankrupt or face cashflow problems, you're left holding the empty bag. Ensure you regularly review your third parties' financial health through credit reports, audits and other financial assessments to confirm cash flow is healthy from A to Z.

A playbook for third-party risk management

Data is a global currency, and some countries want to keep their citizens' data squarely under their control. Russia's data privacy law, passed in 2022, provides new rules for personal data processing and cross-border data transfer. It establishes mandatory requirements for data controllers and processors, including a new requirement on data breach notification.

Your next move is to create a clear-cut plan that lays out how you'll identify, assess, monitor and respond to third-party risks. Think of this as your treasure map: it outlines the terrain, warns you of pitfalls and guides you to your destination – which is nothing less than robust risk management!

The following points are your directions to get you through the maze of complexities that come with dealing with third parties:

1. Identify and classify – This is your first filter. Separate the wheat from the chaff by understanding the nature and degree of risk each third-party brings:

- **High-risk** – These entities require extensive audits and frequent check-ins
- **Medium-risk** – Adequate due diligence is enough
- **Low-risk** – Minimal oversight is required – just don't get complacent

2. Conduct due diligence – You're the detective; your third parties are the subjects. Use tools like background checks, credit reports and compliance certificates to verify credentials and screen partners for concerns.

3. Monitor and review – Ever heard of the saying "trust but verify"? In other words, to scan while you sustain, implement automated governance, risk and compliance solutions to track performance metrics and flag risks and anomalies. Known risks mean you're aware of what to watch out for; no risks on your radar means there's something (or several things) you aren't seeing.

4. React and revise – If you discover a risk, don't just put a band-aid on it. Dig deep, find the root cause and revise your approach to either prevent it from reoccurring or manage it to avoid damage, escalations or losses to your organization.

Data is a global currency, and some countries want to keep their citizens' data squarely under their control.

Tools and technologies

Technological advancements have changed the world – including how organizations can manage third-party risks. From automated oversight to real-time auditing, today's tools are light-years ahead of clunky manual processes that struggle to sort a mountain from a molehill.

Whether you're a seasoned pro or new to the field, there's a suite of digital solutions designed to make your life easier and your strategies more effective:

- **AI-based analytics platforms** – Your secret weapon for sniffing out third-party vulnerabilities, these platforms use advanced algorithms to detect potential external risk areas before they escalate.
- **Contract management systems** – Keep track of every term and condition with your external vendors. These systems make sure compliance is upheld and financial agreements are clear, agreed in advance and subject to airtight non-disclosure agreements and data security. If you've ever been burned by the fine print, you know how vital contract management is. These systems help you monitor and manage every agreement with third-party vendors, ensuring compliance is maintained, and any financial implications are clear from the get-go.
- **Collaboration portals** – Secure spaces to share sensitive information and collaborate on risk assessments with your third parties.

- **Risk management software** – When risks can change in days rather than weeks, the adaptability of an integrated risk management can't be underestimated. Automated alerts for periodic assessments and can help you keep you on top of the risk admin work that keeps current data feeding into the system.
- **Audit solutions** – Get real-time snapshots of third-party compliance. These tools alert you to potential issues before they blow up, helping you keep your eyes on any potential problems on the horizon.

The view from the tightrope

Managing third-party risk is more than a one-time task. It's an ongoing act of agility, awareness and adjustment on both your part and the part of your partners and suppliers.

As you contemplate the path ahead, remember that it's always better to be proactive than reactive. There are both internal and third-party risks in your organization's future – that's a fact. It's how you manage them that keeps your organization safe.

Risk Management Essentials
The Human Touch

Everyone plays a role in managing risk

Risk management isn't one team's concern, so keep those communication lines open. A collective understanding of potential risks sets a strong foundation. Conduct surveys, engage in brainstorming sessions and encourage a culture where everyone feels empowered to voice their concerns and share their insights.

Elements to consider for effective risk management collaboration across different teams:

1. Operations and supply chain: It's all about maintaining a smooth flow. By staying in close communication with suppliers and anticipating potential delivery issues, teams can ensure there are no unexpected interruptions. It's beneficial to always have a backup plan, so when hiccups do arise, you're already steps ahead.

Beyond the operational and strategic benefits, understanding the emotional and psychological implications of risk can pave the way for deeper, more impactful decisions focused on how risk affects people inside and outside your business.

2. IT and cybersecurity: A proactive approach goes a long way. By staying informed about the latest cyber threats and conducting regular system checks, IT teams can keep the company's data and infrastructure safe. This isn't just routine – it's the most important risk factor of running a business in the digital age, so the whole organization has to be aware of and invested in managing this area of risk.

3. Human resources: The wellbeing of the team affects the whole organization. Regular check-ins, surveys and addressing any concerns promptly can help avoid larger issues and people-related risk down the road. Recognizing and acting on these insights keeps morale high, talent retained and operations smooth sailing.

4. Sales and marketing: Feedback from the field is gold. By actively listening to customers and keeping an eye on competitors, these teams offer early warnings about market shifts and any problems in important client relationships that might crop up. This real-time information can be crucial for adjusting strategies quickly when needed.

5. R&D and product development: Innovation doesn't exist in a vacuum. Regular brainstorming sessions can help the team anticipate industry challenges, ensuring the next big thing is truly groundbreaking and not just a fleeting idea. It also gives you a starting point to check your sales and marketing is in alignment with the reality of your product.

Risk management – thinking about human impact

Beyond the operational and strategic benefits, understanding the emotional and psychological implications of risk can pave the way for deeper, more impactful decisions focused on how risk affects people inside and outside your business.

For example:

Embracing vulnerabilities: Going beyond accepting risks at face value and avoiding the action that leads to it in the future. Imagine a leading software company receiving feedback on its latest release. The release saves overhead, is more secure and is easier to update, but feedback from users is overwhelmingly negative. Instead of deflecting or ignoring this feedback and waiting for the customer base to get used to it, the organization could openly admit areas for improvement and open up new means to receive feedback and prioritize which features are causing the most complaints. By actively addressing and refining those issues, they not only enhance their product but also reinforce trust over time with their users.

Changing strategies: Being adaptable doesn't just mean rolling with the punches, and confronting risk sometimes requires taking risks. Think of a small online retail business that starts to see a decline in sales because of changing consumer preferences. Instead of sticking to their tried-and-true inventory, they delve into market research, putting more effort into exploring and updating their product range based on customer desires. Nimbleness turns a potential risk into an opportunity for growth.

Empathy in action: It's not just about managing a brand's image; it's about recognizing and valuing the human experiences intertwined with the business. When an organization faces backlash for a decision, they might initiate community-focused events or forums, not simply as a PR move for damage control, but as a gesture to listen to and understand concerns to avoid a repeat. By actively engaging, they demonstrate a commitment to their values and create an opportunity to strengthen trust.

Analyzing risks: more than just numbers

When diving into risk analysis, remember that risks aren't just abstract concepts – they have real-world implications. Here's how to go about it:

1. The power of data: Data-driven analysis forms the backbone of understanding risks, but it goes further than statistics and percentages. Qualitative data is a powerful form of data that helps you measure the impact of your organization's actions on people. Collecting relevant data of this nature, for example from past incidents, market studies, product reviews and feedback loops, can help you get a full view of potential risks from all relevant data sources.

2. Tools and techniques: Employing tools like SWOT analysis – i.e., looking at your strengths, weaknesses, opportunities and threats – and putting together risk matrices can give you a structured way to visualize and weigh risks. But remember, it's not just about the tools. The interpretation of the results, and perceptions of those results, are just as crucial.

Consultants and experts around risk are a useful avenue for making sure you are getting the most of your data, and that you are aligned with the real risk landscape of your business. However, much of the actions already embedded within your business – such as employee satisfaction surveys, downtime assessments or the nature of complaints concerns reported by employees – are all great risk indicators to include in your risk management processes.

3. Embrace subjectivity: While quantifying risks is important, some risks might be more subjective based on intuition or experience. These insights, especially from seasoned team members and completely fresh eyes, can provide valuable perspectives and suggestions you may not have considered before.

Embracing the full spectrum of risk

Managing risk is as much about understanding people, their strengths and how to keep them safe as it is about process from a purely operational point of view. Though complexities including legal, cybersecurity and financial risks can feel distant from the human impact, organizations don't exist in a vacuum. Every risk impacts a person or people, so reminding yourself of this fact can add depth to your understanding of risk and how best to manage it.

Managing Internal Risks
Why do Internal Risks Matter?

Building risk resilience from the inside

Why bother looking inward when external risks seem so pressing?

The answer is straightforward: you're only as strong as your internal structure. Studying how to manage floods in your neighborhood is only so helpful when your house is on fire.

The role your people play in preventing or enabling risks, for example, cannot be underestimated. Huge scandals in the press don't always start out on the front cover of national newspapers – internal risks can be insidious, starting as small as rumors, a white lie in a meeting, or a statistic or number entered incorrectly.

The culture of your organization makes or breaks your risk management strategy. People raising their concerns when small risks arise, and not staying silent, can be the difference between no issue at all and a much larger risk that spirals out of your control.

Think less "if it happens" and more "how it could happen"

Not seeing risks doesn't mean there are none – it means you're missing something.

When we mentioned earlier that internal risks are insidious, it's really a perfect way to describe them – the changes are so gradual you may not recognize the risk until you're in its headlights. This is where psychological factors like confirmation bias can also play a role. If all your metrics are going green, it's easy to ignore that one red flag waving in the wind.

Secondly, where there are people, there are risks. Humans and human behaviors are messy, and the business of doing business *always* comes with human risks.

Essentially, risks are always present – determining whether risks need to be mitigated, or managed with regular oversight, requires full visibility into the risks facing your organization.

Let's break down the types of internal risks you might be dealing with:

Immediate risks

These risks demand urgent attention and action as they are likely to escalate quickly. They also pose danger for the business, your people, or both. Immediate risks are also the hardest to anticipate, so procedures defining how they should be handled need to be prepared long before they have a chance to happen. Think of these risks as flashing red lights that get the emergency service team on the move ASAP. That emergency service team has to know exactly where to go and what to do.

Essentially, risks are always present – determining whether risks need to be mitigated, or managed with regular oversight, requires full visibility into the risks facing your organization.

Examples

- Incidents involving gross misconduct, violent assault or harassment
- Illegal activity, such as embezzlement or extortion
- The discovery of a dangerous artifact onsite
- A major data breach

Evolving risks

Risks that aren't unheard of – but can also be managed with good processes and regular review. These are things that could happen but aren't necessarily happening today. These risks often start out small and become larger issues over time, like a weed growing in your garden. They often affect teams and productivity over extended periods, risking attrition, poor morale and negatively impacted productivity if they aren't kept under control. A healthy workplace culture where your people can have open conversations about workplace issues before they become longer-term problems will help manage these kinds of risks.

Examples

- Shifting project goalposts over time beginning to risk meeting your SLAs
- Poor budget management and oversight into spending month-on-month
- Inefficient communication and operations – and a struggling pipeline
- Ongoing resourcing issues and stressed, unhappy employees
- Data or knowledge silos causing delays in your production cycle

Situational risks

These are risks you can't prevent and sometimes can't anticipate. These risks may originate externally, but can have huge internal repercussions for your organization and the communities, regions and industries you work in.

Examples

- Regulatory-related risks including legislative updates or new requirements impacting service or processes internally or with third-parties and suppliers
- An economic downturn forcing you to cut budget areas – this might include employee perks, events or even headcount
- Geopolitical conflict requiring an urgent rethink in the countries you work with or hire from, including, but not limited to sanctions
- Natural disasters or health-related crises in a particular area your business operates

Kickstarting your internal risk assessments: where to start

We've examined the types of risk your organization might face that originate or impact your internal operations. Now the key is to start laying groundwork you can build on as part of your management of internal risks. Once you know where to look, you can more easily identify what steps to take.

- **Start with an internal audit** – Before you can manage risk, you need to know where it exists. Enlist your compliance, finance and HR departments to provide an overview of existing procedures and policies so you can see how risks are handled right now.
- **Employee feedback** – Your team knows your internal workings better than anyone else. Make use of anonymous surveys or open forums to get insights into possible areas of concern.
- **Identify critical assets and processes** – What are the non-negotiables your business absolutely can't function without? Make a list and start from there.
- **Assess historical data** – Look into any past incidents that could point to potential risks. Even small issues can serve as indicators for larger, systemic risks.

- **Prioritize** – Not all risks are created equal. Use the data you've collected to categorize risks by their potential impact and focus on the ones that could hit your organization hardest.
- **Measure consistently** – Ensure all areas of the business that are prioritizing and categorizing risk use the same method to measure risk. Doing so ensures you won't need a Rosetta Stone to decipher the difference between a "red", a "thumbs down", or a numerical scale to evaluate risk levels.

Once you've gathered this initial information, you'll have a solid base to start formulating a more comprehensive risk management strategy. Remember, the goal is progress, not perfection. Every productive day starts with a well-organized to-do list.

The heart of the matter

Whether internal risks manifest immediately or evolve over time, they are a part of your organization's fabric. Being proactive in identifying and managing them not only prevents potential damage but also fortifies your operation against external uncertainties.

Remember, situational risks may come from outside, but their impact reverberates internally. As much as external issues may dominate the headlines, it's the internal mechanisms that often dictate how resilient an organization truly is. Being vigilant in identifying, categorizing and acting on internal risks enables you to steer the ship with precision, even when unexpected storms hit.

Ultimately, your internal operations set the stage for how well you can manage external risks – and that's why your internal compass should point just as clearly as your outward radar.

Managing Internal Risks

How to Listen When People Speak Up

What is a 'speak-up' culture, anyway?

If you're hearing the term 'speak-up' culture and picturing your team doing stand-up comedy at company parties, you've missed the point – although a good laugh never hurts morale.

Speak-up culture is all about creating an open environment where employees feel comfortable sharing concerns, ideas or observations that could affect your company's performance or ethical standing. It's not about criticizing for the sake of it; it's about proactive problem-solving.

Before diving into how to manage internal risks by listening, it's crucial to understand the bedrock of what you're trying to build: an environment where people are not just allowed, but encouraged, to speak their minds.

Create windows where your walls are

Think of your organization as teeming with risk managers. More often than not, they're the first to spot red flags, sometimes even before your dedicated risk team.

However, if your organization is full of walls, there's mountains of data you're going to miss that plays a vital part in identifying and handling risk. If you try to turn those walls into windows, where transparency and open communication are valued, you'll see so much more across your business.

Why speak-up culture matters:

- It's powered by a resource you already have: your people
- It facilitates faster problem-solving on companywide issues
- It can increase employee engagement and improve morale
- When you listen and act on feedback, it builds trust across your organization

Whistleblowing: a gift, not a curse

People who raise concerns with management, commonly known as whistleblowers, often get a bad rap. Historically, they've been seen as nuisances, snitches or even traitors, especially when we think of big scandals involving whistleblowers taking insider info to the press.

However, whistleblowers who report internally when they have concerns are effectively an early warning system.

To meet global whistleblowing regulations and support a speak-up culture, you must create avenues where employees can report issues they've noticed without fearing a proverbial slap on the wrist.

They aren't going to the press – they're telling you they think something is wrong. Sure, you've got meetings, maybe even a suggestion box or two. But have you established a culture where people genuinely feel they can voice their concerns?

To meet global whistleblowing regulations and support a speak-up culture, you must create avenues where employees can report issues they've noticed without fearing a proverbial slap on the wrist. Even so, culture also needs softer touch points alongside reporting channels guides in your code of conduct on how to raise concerns.

A starting point can be as simple as dedicating five minutes in your weekly team meeting for risk discussions. A reward system for constructive feedback, such as making processes safer or more efficient, can also encourage more people to come forward.

Here are a few more tips for normalizing how and why people should raise concerns within your organization:

- Use and regularly highlight an internal communication tool specifically for employees to raise concerns or check policies
- Talk about issues noticed or reported, and how they were handled, openly in company communications
- Implement a regular speak-up segment in team meetings, initiated by management where possible

Train managers to actually listen for wider issues during these segments, rather than just noting what individuals say

The perils of ignoring your staff can't be stressed enough. It's not just about keeping talent; it's about listening to those who are tuned in to the realities you can't see from your boardroom. When your team members feel unheard, you really risk them becoming someone else's team members.

Losing your people to mistrust and poor morale isn't just a team loss. It's a massive internal risk management failure.

Thinking tactically about tech

Internal risks – especially people-based ones – can be elusive. So, how do you go about detecting them? Employee surveys are one way to start, but you need to dig deeper. Tech can help.

Modern risk assessment platforms, designed to flag internal issues, can offer you useful insights not visible from the CCO's office. They can sift through data, including reports submitted by employees, pick up on inconsistencies and alert you to looming problems through pattern detection.

- **Whistleblower helplines** – Digital platforms that provide an anonymous, secure way for employees to report any issues. These are essentially your early warning systems for employees to ring the bell. As the mouthpiece of speaking up, they are where people go to tell you what's up.
- **Incident management platforms** – These aren't just for data breaches. Use them to log and manage all your reports of internal risks flagged by your team, ensuring every voice is heard and responded to in line with regulatory requirements.
- **Collaboration portals** – Think of these as your organization's internal social media. They encourage open dialogue and can serve as less formal platforms or forums for raising red flags, discussing problems and ideating solutions, helping to normalize the act of speaking up.
- **Employee feedback tools** – These can go beyond the traditional annual review, but they are more of a periodic prompt to your people rather than only offering an open-ended portal to raise concerns. Real-time feedback platforms allow employees to raise concerns as they occur, letting you nip potential issues in the bud.
- **Audit solutions** – While they're great for financial checks, consider using them for social audits on your company culture. They can help you track how often concerns are raised and how swiftly they are addressed, providing a tangible measure of the health of your speak-up culture.

As a final point, data mismanagement is a sneaky carrier of risk that thrives in a culture of silence. Whether it's due to poor procedures or a sheer lack of oversight, when data isn't handled correctly, it's not just about potential financial losses or wasted time. External audits that find these mistakes can quickly land you in hot water with regulating bodies – you're far better off finding them yourself so you can strategize how to manage them better.

Employee input can be a rich source of qualitative data to fill the gaps your quantitative surveys leave. Make sure your tech tools are calibrated to treat this data with the gravity it deserves, flagging trends, common concerns and patterns that quantitative data might miss – the applications for this sort of information are infinite.

Risk is a bigger picture than your organization

Many of the emerging risks you face every day touch the remit and responsibilities of one or more of your employees.

A strong speak-up culture is your first line of defense against a range of risks, especially internal risks. Furthermore, the human element of risk management should never be underestimated. While we've examined various categories of risks, they often intersect and are magnified through human behavior, for better or worse.

Whether it's on a screen or part of an interaction, in your day-to-day operations, it's far more likely someone will notice potential or actual risk faster than your processes or occasional auditors will. Can these people tell you? What would put them off telling you? And if they do raise a concern, what will you do next?

NAVEX is trusted by thousands of customers worldwide to help them achieve the business outcomes that matter most. As the global leader in integrated risk and compliance management software and services, we deliver our solutions through the NAVEX One platform, the industry's most comprehensive governance, risk and compliance (GRC) information system.

For more information, visit NAVEX.com and our blog.
Follow us on X and LinkedIn.

EMEA + APAC
4th Floor, Vantage London
Great West Road
Brentford, TW8 9AG
United Kingdom
info@navex.com
www.navex.com/uk
+44 (0) 20 8939 1650

AMERICAS
5500 Meadows Road, Suite 500
Lake Oswego, OR 97035
United States of America
info@navex.com
www.navex.com
+1 (866) 297 0224

NAVEX®