NAVEX

Navigator Series

Risk Resilience Guide

Seizing the initiative on risk management

Contents

Special thanks to:

Kristy Grant-Hart, Matt Kelly, Kyle Martin, Michael Rasmussen, Mark Robertson, Jan Stappers, Michael Volkov

NAVEX | Navigator Series

The Navigator Series offers expert guidance on building and enhancing risk and compliance programs. From foundational insights to deep dives on specific topics and regions, our research-backed materials provide the roadmap to program success.

The Risk Management Challenge is Real

Many businesses fail to take a holistic approach to risk prevention

When it comes to risk management, many organizations are missing the point. They are too focused on reactive measures such as firefighting urgent problems, instead of identifying and monitoring risks to proactively mitigate their exposure. In short, they are taking a checkbox approach with a focus on ad-hoc cures, rather than holistic prevention.

With the scale of the task at hand, and the rapid pace at which obligations can shift, it's little wonder businesses choose to prioritize their responsibilities on a case-by-case basis. But by failing to install a systematic process for risk management, organizations are leaving themselves vulnerable.

Major compliance regulations are being introduced and updated with stiffer penalties

1977
- **U.S.** - Foreign Corrupt Practices Act (FCPA)

1993
- **France** - Law Sapin I

2002
- **U.S.** - Sarbanes Oxley

2010
- **U.K.** - UK Bribery Act
- **Spain** - Spanish Criminal Code
- **U.S.** - Dodd-Frank

2015
- **Germany** - German Act on Combatting Corruption
- **Netherlands** - Dutch Criminal Code

2016
- **France** - Law Sapin II
- **South Korea** - Improper Solicitation and Graft Act

2017
- **Argentina** - Criminal Liability Statute
- **Mexico** - General Law of Administration Responsibilities
- **Peru**- Legislative Decree 1352

2018
- **Russia** - Russian Criminal Code
- **India** - Prevention of Corruption Act
- **UAE** - Penal Code
- **China** - Anti-Unfair Competition Law
- **Malaysia** - Anti-Corruption Act

2019
- **Italy** - Bribe Destroyer Act
- **Saudi Arabia** - Anti-Bribery Law
- **Australia** - Corporate Crime Bill

2022
- **EU** - Digital Markets Act

2023
- **EU** - Digital Services Act Cyber Resilience Act
- **Germany** - Supply Chain Due Diligence Act (LkSG)

2024
- **EU** - AI Act
- Corporate Sustainability Reporting Directive
- **U.K.** - Economic Crime and Transparency Act
- **U.S.** - Corporate Transparency Act

That's because risk is dynamic. Regulations change, third-party vendors become problematic, and operational vulnerabilities shift. A supplier that passed a sanctions check six months ago might fail it today. Without sufficient ongoing monitoring, it's easy to see how a business might, for example, fail to detect unethical labor practices in its supply chain that could have profound consequences for the organization.

Growing pressure calls for new approaches

As risks increase, the pressure is on risk and compliance leaders to find a new approach. It's more important than ever to go beyond a "check-the-box" philosophy at a time when rules are continually changing, enforcement regimes are stepping up pressure, regulators are collaborating across borders, and the financial and reputational risks associated with third-party failures are escalating.

The solution? Compliance program operational risk management

Despite the scale and breadth of the challenge, there is a way forward.

With a systematic approach, organizations can reduce the impact of regulatory failings and better protect their businesses through compliance program operational risk management. This approach centers on an ongoing process:

- Horizon-scanning for emerging vulnerabilities
- Triaging the greatest risks
- Learning from post-crisis reviews
- Working through theoretical scenarios
- Constant, proactive monitoring for evolving and changing risks

Regulatory pressure is mounting

With an alphabet soup of new legislation worldwide, organizations operating across borders are experiencing significant challenges to comply. For example, there's a global push towards protecting the human rights of workers throughout global supply chains, with new regulations including the German Supply Chain Act, the Norwegian Transparency Act, Canada's Bill S-211 and the EU's Corporate Supply Chain Due Diligence Directive.

At the same time, companies continue to grapple with global privacy regulations like the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act. Then there's a new swath of legislation to govern the use of artificial intelligence (AI), as signaled by the arrival in 2024 of the groundbreaking EU AI Act.

Regulators are also putting an emphasis on operational resilience. This includes the EU Digital Operational Resilience Act (DORA), requiring impacted financial industry organizations to develop compliant internal frameworks that address several technology-related risks including those involving third parties. Internationally, legislation is growing more centralized in moving risk management forward.

How this report will help

This report explores the reality of operational risk management, what it looks like and how implementation might take shape. Starting with a focus on regulatory risk and third-party risk management, we take a look at the scale of the challenges organizations are facing and offer up operational risk management as a best practice to address these risks.

Over the following pages, we share insights on how to use data for proactive risk management and outline how businesses can move from simply reacting to regulatory requirements in favor of a more proactive approach.

In short, this report guides readers through not only how to build a risk program that works, but how to keep it working in a changing environment.

Key terms

Regulatory risk
The risk that organizations will be negatively affected if they fail to comply with regulations set by global and local regulatory authorities. Organizations can be subject to thousands of regulations, which differ by region and change over time. New regulations regularly come into effect, which further adds to the complexity and increases the risk of being non-compliant. If organizations fail to comply, they face regulatory enforcement and fines, as well as reputational damage. Examples of such rules include:

- U.S. Department of Justice Evaluation of Corporate Compliance Program (ECCP) guidance
- U.S. Foreign Corrupt Practices Act
- U.K. Bribery Act
- German Supply Chain Due Diligence Act
- U.S. Securities and Exchange Commission requirements for publicly traded companies
- EU General Data Protection Regulation
- U.S. Treasury Office of Foreign Assets Control sanctions programs

Third-party risk management (TPRM)
The process of managing and mitigating the risks posed by parties external to the organization. These parties can include vendors, suppliers, partners and service providers. Relationships with these parties can leave the organization vulnerable to cybersecurity, operational, financial, reputational, compliance and strategic risks, all of which must be managed as part of third-party risk management practices.

Operational risk management (ORM)
The process of managing risks in an ongoing, systematic way. Organizations adopting this approach identify, assess, mitigate and monitor risks on a continuous basis, dedicate resources in proportion to risk level, and assess risks based on up-to-date operational data. For the purposes of this guide, we'll speak largely to compliance program operational risk management, which involves overall compliance risk as well as regulatory and third-party risk within the context of operational risk management.

IT risk management (ITRM)
The process of managing risks related to information technology. This includes risks around IT infrastructure, systems, data and processes, including cybersecurity threats, system failures, data breaches and regulatory non-compliance. The goal is to protect information and technology assets while supporting business objectives.

Regulatory Risk Management

The volume of regulation that companies must navigate continues to escalate, with the pace of change creating real challenges for compliance. Forward-thinking organizations are seizing the initiative

1

Global regulation is increasing at an unprecedented pace

1,255

ESG regulations introduced globally since 2011

Source: ESG Book, 2023

33%

increase in regulations related to AI in the EU between 2022 and 2023

Source: Statista, 2024

Approximately

40%

of sustainable finance policies worldwide were created in the past five years

Source: Statista, 2024

2

Some organizations are struggling to keep up with the rate of change

£21.6bn of funds were reported to the Office of Financial Sanctions Implementation as frozen as a result of U.K. financial sanctions

Source: Office of Financial Sanctions Implementation, 2023

Two-thirds of organizations have experienced compliance issues in the past three years

Source: NAVEX State of Risk & Compliance Report, 2024

3

Very few are taking an optimal approach to risk

Only

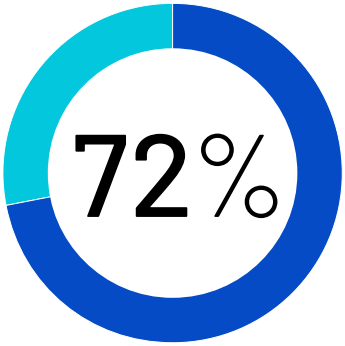
29%

of businesses take the optimal risk-based approach, stratifying risk and applying different levels of due diligence based on risk evolution throughout the engagement

Source: NAVEX State of Risk and Compliance Report, 2023

4

But ambitious organizations are investing in risk management and reaping the benefits



of organizations are planning to increase spending on technology to monitor and detect risks

Source: PwC Global Risk Survey, 2022

75%

plan to increase spend on data analytics to support risk management

Source: PwC Global Risk Survey, 2022

In the past 12 months...

40%
of organizations have achieved more robust compliance with regulatory standards

31%
have improved their identification and tracking of potential risks

30%
have greater integration of risk management across business functions

Source: PwC Global Risk Survey, 2023

Navigating global regulation

Global organizations are dealing with more regulatory change than ever before

Organizations face a significant challenge when it comes to keeping pace with an increasingly complex international regulatory landscape. Among the recent developments that businesses are working hard to digest are new whistleblowing requirements in the EU, a fast-evolving sanctions landscape, increased legislation relating to environmental impact, enhanced privacy rules, and growing regulatory oversight of third-party suppliers.

Global firms are dealing with 234 regulatory change events every business day, coming from 1,374 regulators around the world, to use a 2023 Thomson Reuters figure.

The risks associated with running afoul of these rules are significant. For example, the maximum penalty for non-compliance of the EU AI Act – which prohibits certain uses of AI – is 7% of an organization's worldwide annual turnover or EUR 35 million, whichever is greater.

And there are plenty of examples of companies feeling the heat. In 2017, a large telecoms company was fined a combined penalty of $1.19 billion for conspiring to violate U.S. sanctions by illegally shipping U.S.-origin items to Iran. In 2023, a $300-million civil penalty was imposed on an American data storage company for breaching U.S. export controls related to selling hard-disk drives to an overseas tech business.

Industry focus: financial services

Financial institutions face a vast array of compliance risks

450,000
average number of exposed files within financial services organizations, the highest of any industry

$5.9m
average cost per data breach in the financial industry

95%
of breaches are financially driven

Source: NAVEX

An ineffective response

Overwhelmed by complexity and the speed of regulatory developments, compliance managers often resort to a checkbox approach to regulatory change, addressing issues as they arise rather than taking a strategic outlook. Instead of responding systematically and effectively, too often teams find themselves racing to keep up.

This reactive mindset creates problems. Businesses can find themselves failing to adjust quickly enough to emerging risks, failing to allocate enhanced resources to high-risk areas, and producing risk assessments that are not properly informed by continuous access to operational data.

Nowhere is this more apparent than when it comes to sanctions screening: a third-party supplier might be green-lit one day, only for it to fall afoul of fast-shifting rules six months later.

Matt Kelly, editor and CEO of Radical Compliance, says, "Increasingly, agencies are using economic sanctions as a policy and enforcement weapon; Russia and its invasion of Ukraine put that issue on steroids. But for a long time before that, sanctions were becoming the go-to tool to push diplomatic objectives, forcing large companies to pay really close attention to who all their customers are and whether they know who all the sanctioned entities are in any jurisdiction in which they are doing business."

For breaching the sanctions regulations involving Ukraine/Russia, Cuba, Iran and Syria, one major technology player was forced to pay more than $3.3 million in civil penalties in order to resolve 1,339 violations.

Industry focus: healthcare

The healthcare industry has particularly strict compliance rules

553

large-scale breaches were reported on the U.S. Department of Health and Services Office for Civil Rights (OCR) breach portal in 2023

15%

of breaches on the OCR portal involved unauthorized access or disclosure of protected health information

$68,928

maximum civil monetary penalty per HIPAA violation

Source: NAVEX

35%

of businesses rank compliance and regulatory risk as their greatest threat to growth

Source: PwC Pulse Survey, 2022

Global firms are dealing with

234 **regulatory change events every business day**

Source: Thomson Reuters Cost of Compliance Report, 2023

> "The leaders who really get it understand that building a culture of ethics and compliance is incredibly valuable."
>
> Michael Volkov, CEO of the Volkov Law Group

A new approach is needed

A better response is one that aligns regulatory compliance with the organization's risk appetite and its operations. Businesses should be thinking about how they can accomplish their strategic objectives and assess the uncertainties or risks that prevent them from achieving those outcomes. Then, ultimately, they need to know how those uncertainties can be mitigated.

Michael Volkov, CEO of the Volkov Law Group, says, "The first questions are, what do people in your organization know, and what is your risk tolerance? In other words, are you comfortable living with potential bribery risks overseas if it may give you more business, or are you going to fight to instill a culture of ethics, compliance and integrity?"

Assuming the latter, he says, "Ethical and compliant organizations perform better over the long run financially, the research shows. The leaders who really get it understand that building a culture of ethics and compliance is incredibly valuable. That is absolutely the best internal control against regulatory risk that there is – you can't watch over every employee every day, but you want to trust them to do the right thing."

Too often, compliance is seen as more important than ongoing monitoring. According to the NAVEX 2024 State of Risk and Compliance Report, compliance is most often ranked as the number-one consideration for organizational decision-making, while the number-two response broadly describes compliance program operational risk management.

Industry focus: government

Breaches in the public sector waste taxpayer money and disrupt essential services

Only
12%
of money from detected frauds was recovered by the U.K. government in 2021

26%
increase in the yearly cost of a data breach in the public sector

16%
of data breaches in public administration are due to collusion (multiple parties working in concert)

Source: NAVEX

The shift to a systematic methodology

Businesses need to adopt a continuous, systematic process of addressing regulatory risks. This calls for a shift in business culture towards a regular reassessment of the risk landscape related to regulatory pressures. Generally, this transition starts as a cultural dynamic among leaders, recognizing its importance, collaborating to have informed conversations about addressing it and, in many cases, investing in tools that can help support those operations.

Recognizing that each business activity carries a different level of risk, and that a certain level of risk may be acceptable depending on the context, is an example of operational risk management in practice. Constant, proactive monitoring for emerging and changing risk should also be a feature, along with ongoing reviews of how effective tools are proving to be.

Kyle Martin, vice president, product management – risk governance at NAVEX, says, "You have to document what you're doing, test what you're doing, then evaluate it, validate that it works over and over again, and then verify it before repeating that whole loop again."

Compliance should have a seat at the table and learn to speak the same language as other business units that manage organizational risks, such as HR and information security.

"The compliance team has to not only be much more risk-aware in the day-to-day operations, but also have that relationship with the chief technology officer, the chief information security officer and the chief human resources officer," says Martin. "By having a seat at the top table, you can talk risk and you can talk about the impact on the business, both in terms of the downside and the upside. There are things we have to mitigate, but also things we might be able to take advantage of."

Shared technology can be used to ensure all business units are looking at cases and risks in the same way. This can include internal reporting, which provides a real-time view of potential misconduct that may violate various regulations, as well as training, third-party risk screening and more. Indeed, compliance practitioners say the top reason they turn to technology is to reduce risks, not merely to meet regulatory requirements.

Solving the problem

This approach provides the tools and leadership needed to manage risks in a more agile way. A holistic regulatory compliance program is organic and operates in real time, helping to achieve the goal of compliance program operational risk management.

"The compliance team has to not only be much more risk-aware in the day-to-day operations, but also have that relationship with the chief technology officer, the chief information security officer and the chief human resources officer."

Kyle Martin, vice president, product management – risk governance, NAVEX

Risk reduction is a big driver of risk and compliance solutions

Top reasons for adopting new risk and compliance automation and technology solutions

Source: NAVEX State of Risk & Compliance Report, 2024

Sanctions are a great example. Employees, and perhaps key vendors, can receive training to make them aware of the importance of potential sanctions in relationships across their supply chain. Perhaps there's a supplier who's violating a rule, and maybe an employee or third-party worker raises a red flag by anonymously using the internal reporting system provided to all employees. Compliance program operational risk management here means providing the leadership and tools to be agile in approaching this challenge.

Compliance professionals can champion this change

It can be a challenge to shift course and transition to a more systematic approach, but compliance professionals can champion the change.

Kristy Grant-Hart, CEO at Spark Compliance Consulting, is an expert at transforming compliance departments into on-demand business assets. She says the cultural challenge can come from silos and fiefdoms – both of which have the potential to derail the creation of operational risk management systems. "The tone from the top needs to be crystal clear in support of openly sharing information between functions."

Compliance professionals need to highlight the vast, interconnected nature of regulatory risk to help justify investment, says Grant-Hart. "Bring in stories of it going wrong, especially from your industry, because that helps drive the message that the risk is not just theoretical," she says.

"And explain the consequences of things going wrong. For instance, in Europe, the use of banned AI applications could cost the company up to 7% of global turnover. For GDPR, your exposure is 4% of global turnover. Compare that to the investment and it starts to add up."

The volume of regulations organizations must navigate is potentially vast, depending on the nature of their operations, so simply keeping up will almost always be an enduring challenge. Getting organizational silos on the same page about a compliance program operational risk management approach is achievable and any risk or compliance professional can be the champion in this conversation.

IN CONCLUSION

When navigating regulatory risk, organizations face a challenging, complex and fast-moving landscape of evolving risk factors. Rather than simply keeping up with obligations, businesses must adopt a more strategic, systematic and ongoing process. By being more proactive, businesses can focus on their greatest risks, learn from past errors, scenario-plan and respond to emerging and changing threats.

The primary goal of operational risk management is to reduce risks to acceptable levels and ensure business continuity. Organizations should assess their current practices and identify how new approaches might bring positive results.

To learn more about NAVEX regulatory and third-party risk management solutions, click here.

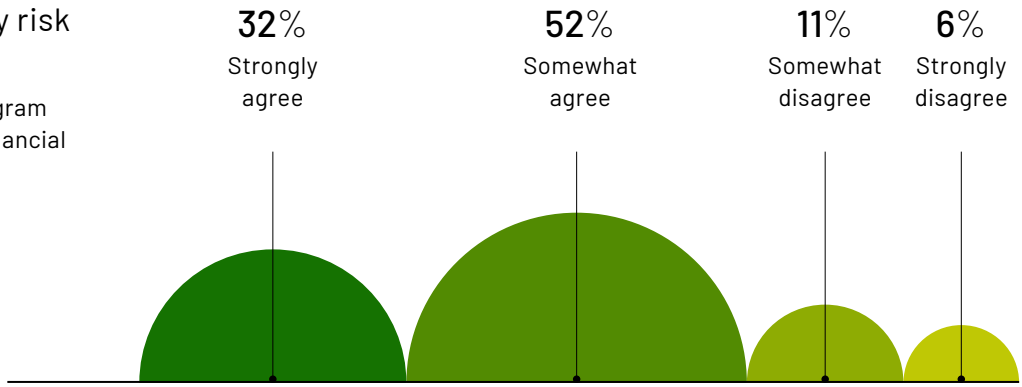
Third-Party Risk Management

As supply chains scale in geographic reach and complexity, the potential for business disruption created by third parties is a growing concern. Organizations that prioritize third-party risk management have much to gain

1

Confidence in third-party risk management is mixed

Our third-party due diligence program significantly reduces our legal, financial and reputational risks



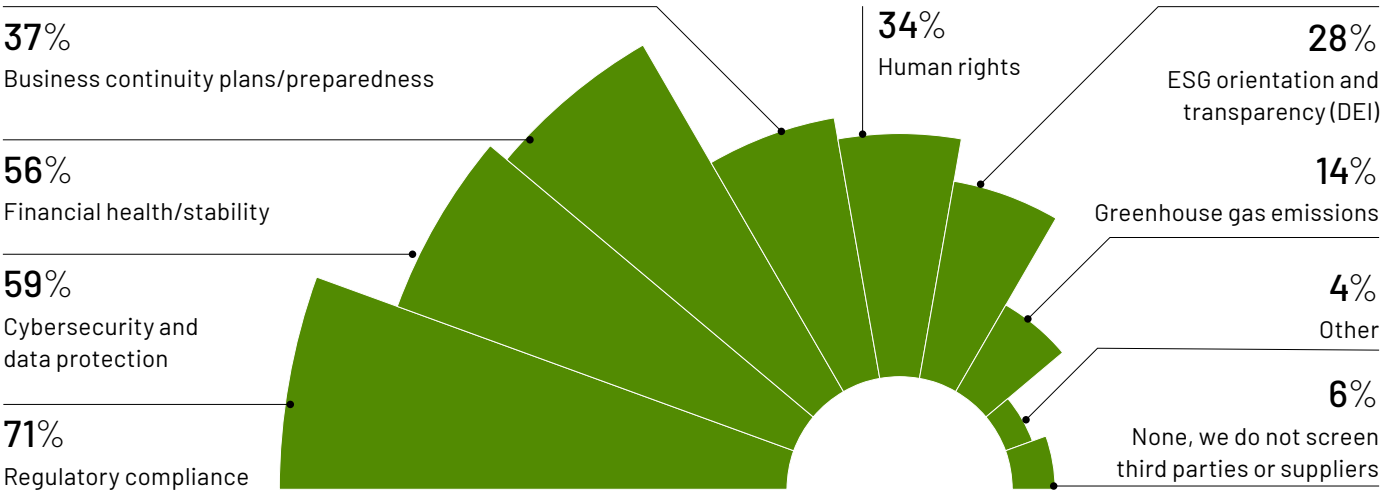
Figures represent multiple response options. See full report for details.

Source: NAVEX State of Risk & Compliance Report, 2024

2

Compliance is the top criteria for screening third parties

Aspects reviewed when screening third parties

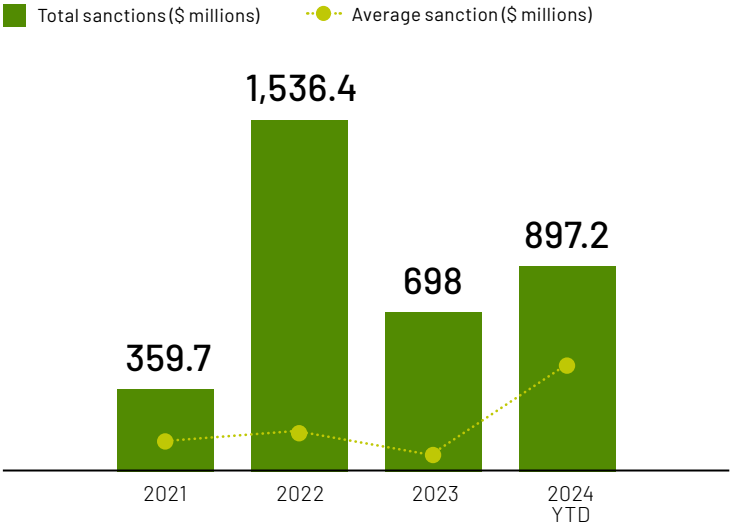


Source: NAVEX State of Risk & Compliance Report, 2024

3

Sanctions are increasing

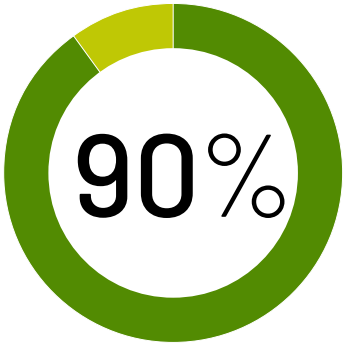
The total and average monetary sanctions imposed on entities and individuals per year due to FCPA-related enforcement actions



Source: Stanford Foreign Corrupt Practices Act Clearinghouse, 2024

4

But organizations are putting more emphasis on their third-party risks



of organizations are investing to improve their TPRM program's effectiveness

Source: EY Global Third-Party Risk Management Survey, 2023

5

And those who invest in managing the risks see the benefits

To what extent have you seen the following benefits from the maturation of your TPRM program?

Source: EY Global Third-Party Risk Management Survey, 2023

The evolving third-party risk landscape

Third-party networks are getting bigger and have the potential to cause more harm

All organizations have to deal with some form of third-party risk, and for most companies the scale and scope of that risk continues to increase. Supply chains are typically crossing more borders and touching more areas of a company's business.

Third-party risk management is a uniquely challenging obligation for most organizations, because even the smallest companies now often rely on external providers for HR management, payroll and other core software operations. Technology and systems availability is vital, with few organizations capable of even functioning should their internet service provider go down, while physical supply chain operations within certain industries are as important as ever.

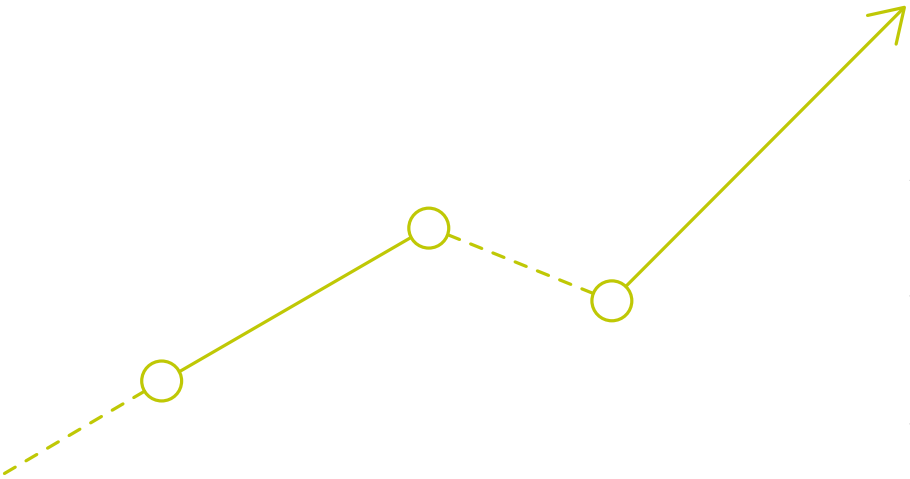
For the largest companies, thousands upon thousands of third-party suppliers may be providing products, raw materials, software, labor and other services. And those third parties have third-party exposures of their own. This creates significant threats and concerns. In fact, 31% of chief risk officers and risk management leaders rank third-party risk as their greatest threat to growth, according to a PwC survey.

Matt Kelly, editor and CEO of Radical Compliance, says, "The challenge is that third parties are now posing more types of risk. A great example would be the recent outages caused by the Crowdstrike failure in August 2024. For most companies, that was not a compliance breach, but it caused severe operational disruption and was a horrendous third-party risk failure. The sort of damage that can happen is huge, and that raises important questions that regulators will ask."

31%

of chief risk officers and risk management leaders rank third-party risk as their greatest threat to growth

Source: PwC Global Risk Survey, 2023



The risk management difficulty

The challenge of managing these risks is increasing. Regulators are only getting stricter in demanding that organizations ensure they are engaged with ethical supply chains. Recent examples of new laws scrutinizing third-party relationships include the EU's Corporate Sustainable Due Diligence Directive and the German Supply Chain Act – both of which add new compliance burdens for companies with complex supplier networks.

And it's not just regulations driving the issue. Organizations have an interest in ensuring reliability from their critical vendors, whether that be the supply of a given raw material or the protection of sensitive data. In an era of increased connectivity and disparate, remote workforces, third parties also pose a significant risk to business operations given the threat they pose to insecure devices and unprotected networks.

Jan Stappers, director of regulatory solutions at NAVEX, says, "As we move towards an evermore global economy, fewer and fewer organizations do everything in-house and companies are increasingly responsible for who they do business with and where they source their raw materials from. Consumers, too, are demanding more transparency about the supply chain behind the goods they buy."

While regulatory fines imposed on the back of third-party failings are a big threat, the biggest third-party risk for most businesses is reputational, Stappers asserts. "Fines are fines and you can budget for those, but that reputational risk can really slam the goodwill and value of a brand that has been so carefully built up over years or even decades."

"Reputational risk can really slam the goodwill and value of a brand that has been so carefully built up over years or even decades."

Jan Stappers, director of regulatory solutions, NAVEX

The wrong approach

Despite a growing recognition of these challenges, organizations too often take a checkbox approach to managing third-party risks. Instead of being methodical and agile in identifying, assessing, mitigating and monitoring risks, companies find themselves taking a reactive, fire-fighting approach, simply meeting their responsibilities as issues crop up.

There are several problems with this. First, without vendor tiering (categorizing third-party vendors based on the level of risk they pose to an organization), there is no recognition that some vendors do not warrant the same level of scrutiny as others. Further, during initial vendor screening, organizations can apply too little, or too much, scrutiny to a vendor because they have failed to adequately consider their own risk profile.

Another issue organizations struggle with is simply the volume of vendors and the need to enforce sometimes hundreds of contracts while grappling with a lack of resources.

Third-party screening can also throw up false positives if it is not sufficiently sophisticated to bring forward only real concerns.

Despite this, according to the NAVEX 2024 State of Risk and Compliance Report, only 36% of organizations use a risk-based approach with third parties, while a quarter use the same approach regardless of risk level, meaning they are often doing either too much or too little than is appropriate for the risk level.

Michael Volkov, CEO of the Volkov Law Group, says, "You need to build a third-party risk management system that is in accordance with your culture. It's not just a one and done, 'We do a due diligence deep dive and we're set'. It's more than that. It's building a relationship and understanding the risk associated with each third-party relationship, because they are all different. If they are helping you to sell to state-owned enterprises overseas, there's a bribery risk. If they are helping you source materials, there may be a sanctions risk. Third party is such a broad term that encapsulates lots and lots of relationships in the outside world."

Most organizations do not use a risk-based approach with third parties

Source: NAVEX State of Risk & Compliance Report, 2024

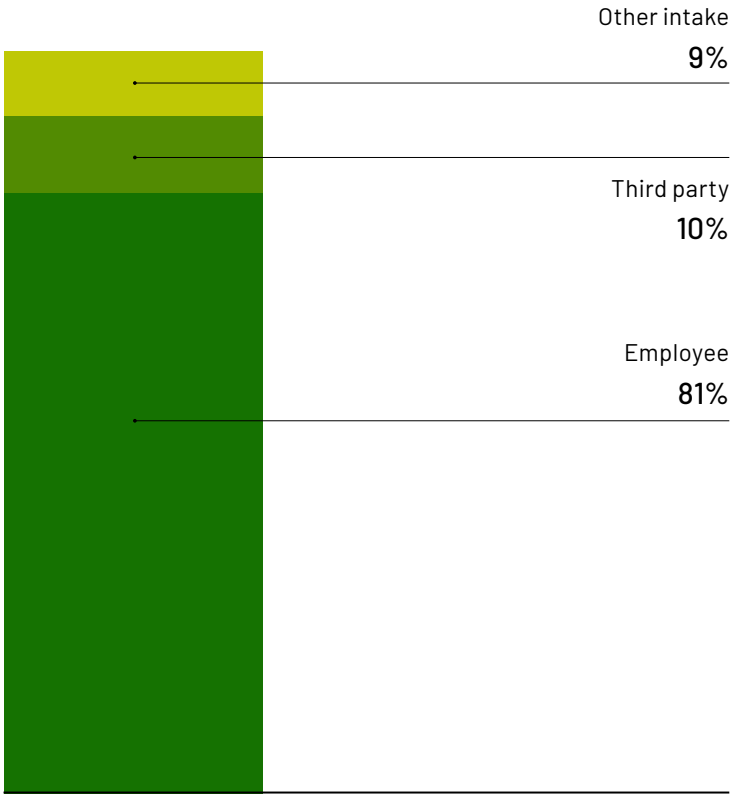
Embracing compliance program operational risk management

To tackle these issues, the solution for most organizations is a shift to stronger, more proactive compliance program operational risk management – a business strategy where real-time awareness of risk across the organization's operations informs high-level decision-making.

Operational risk is the risk a company faces while attempting to run day-to-day business activities, which includes third-party risk management. Vendors are a critical part of operations, therefore managing those vendors appropriately is key to effective compliance program operational risk management.

Internal reporting systems are valuable for managing third-party risks

Internal reporting system reporter types



Source: NAVEX Whistleblowing & Incident Management Benchmark Report, 2024

What does this approach involve? When focusing on third-party risk management, organizations need to have a proper due diligence solution in place to pursue a risk-based approach, as required by the U.S. Department of Justice and other regulators. This solution should help the business to understand the regulatory issues third parties can present, with screening to uncover anti-bribery concerns, human rights violations, sanctioned entities and so on, which is crucial to avoiding regulatory enforcement.

A compliance program operational risk management approach also embeds ongoing monitoring of third parties, typically enabling external partners to use the internal reporting system to flag issues.

"Technology has a huge role to play here," says Mark Robertson, associate general counsel and compliance officer at NAVEX. "There's a lot of valuable information out there and being able to capture that and use it in your program is extremely valuable."

He adds, "Beyond that, organizations really need to be honest with themselves about what they truly have visibility of and what they can actually tackle in their oversight and monitoring practices, so that they are not trying to do so much that it becomes paralyzing. The key is to identify the material risks and address them in a focused and manageable manner."

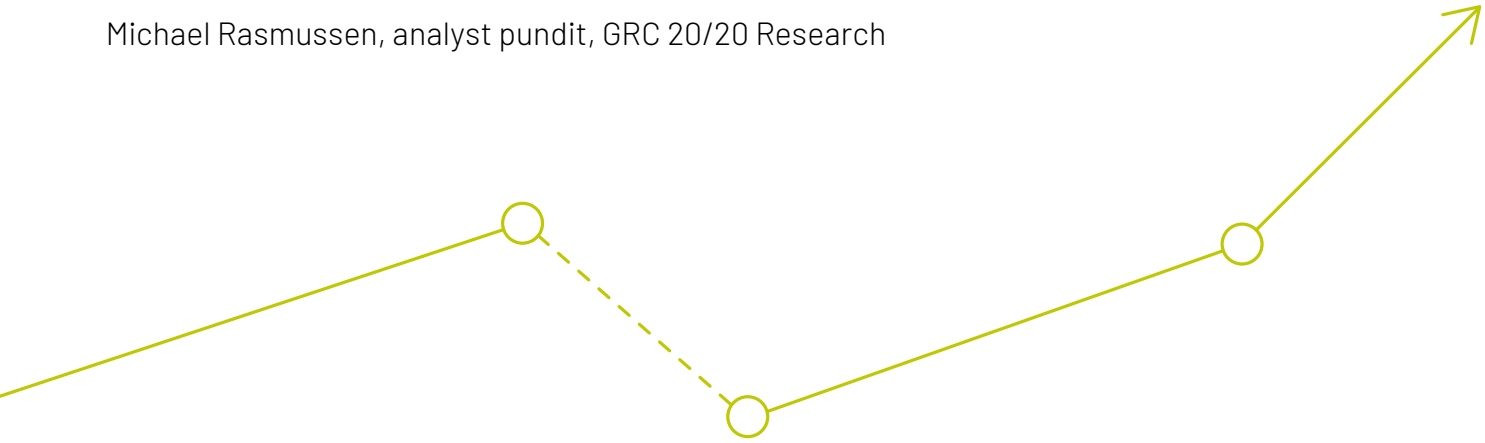
Unlocking a smooth, efficient process

This approach provides the tools, processes and leadership to better deal with third-party risks, solving many of the problems encountered as a result of the fast-growing third-party risk universe.

Technology can significantly enhance the effectiveness of the approach. Digital tools can screen third parties against databases to uncover any and all issues an organization

"The answer is a holistic third-party risk program, stretching from onboarding and initial due diligence, through ongoing continuous monitoring, to managing issues, audits and onsite inspections, right up to offboarding."

Michael Rasmussen, analyst pundit, GRC 20/20 Research



should be aware of, flagging those issues for further review. If additional action is needed, organizations can conduct enhanced due diligence to gather the appropriate context into each risk and understand the ownership structure of third parties, which is particularly important with the continued focus on sanctions.

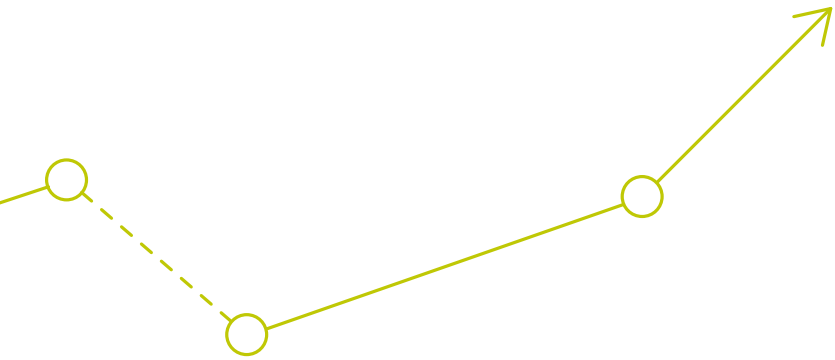
When it comes to ongoing monitoring, platforms exist to aggregate data points from across organizations, as well as from assessments, audits, authoritative sources and external systems, to keep leadership fully informed on issues as they arise and develop.

The existence of best-in-class internal reporting tools, accessible to third parties, is also key to success in a challenging risk environment. According to the 2024 NAVEX Whistleblowing and Incident Management Benchmark Report, on average 10.3% of internal reporting system activity is attributable to third parties, showing that an internal reporting system is a valuable tool for ongoing risk management beyond the organization, including in the supply chain.

Implementation challenges

It can be a challenge for organizations to drive implementation of a new compliance program operational risk management approach to third-party risks. The key is to take the first steps, secure senior-level buy-in, and be clear on the risk appetite and objectives of the program.

A common pitfall is trying to address all regulations from day one, without strategic prioritization. Particularly with third-party risk management, more and more regulations



are coming into effect than ever before, so organizations are advised to start with the areas in which they are most active and follow those requirements, before then expanding the program from there.

Michael Rasmussen, analyst pundit at GRC 20/20 Research, says, "The answer is a holistic third-party risk program, stretching from onboarding and initial due diligence, through ongoing continuous monitoring, to managing issues, audits and onsite inspections, right up to offboarding."

He adds, "Organizations need to build out that strategy, and it is a collaborative process across multiple departments. Procurement might lead it, Compliance might lead it, because third-party risk is broad and involves many parts of the business. The key is to define that process across the lifecycle."

Senior leadership must also champion the change. Without a top-down culture for establishing these programs, they will fail. Only 30% of boards are highly engaged in their organizations' compliance programs, according to the NAVEX 2024 State of Risk and Compliance Report, but top-level buy-in is a key determinant of success.

IN CONCLUSION

In dealing with third-party risk, businesses face an escalating challenge characterized by increased scrutiny across an ever-expanding roster of external relationships. Many organizations take a reactive approach, simply coping with issues as they emerge, rather than being methodical in their identification, assessment, mitigation and monitoring of risk.

A compliance program operational risk management approach starts with a proper due diligence solution, encompasses sophisticated ongoing monitoring of third-party suppliers, embeds incident management through internal reporting tools accessible to third parties, and follows through all the way to strategic offboarding. The proper prioritization of risks is critical, as is the adoption of technology tools alongside full leadership support.

Organizations should review their current third-party risk management solutions and consider how to optimize new approaches. To learn more about NAVEX regulatory and third-party risk management solutions, click here.

Compliance Program Operational Risk Management

As the risk landscape that organizations must navigate continues to evolve, many businesses feel overwhelmed and are struggling to keep up with the pace of change. Embedding proper compliance program operational risk management processes offers a solution to take charge and oversee risk more effectively

1

Leaders are unprepared for the rapidly evolving risk landscape

5x

increase in leaders who feel unprepared for regulatory risk in 2024 versus 2023

Source: BDO Global Risk Landscape Report, 2024

Only

30%

of boards are highly engaged in their organizations' compliance programs

15%

of senior executives have impeded compliance personnel from effectively implementing their duties

Source: NAVEX State of Risk & Compliance Report, 2024

Percentage of organizations unprepared for regulatory risks

Source: BDO Global Risk Landscape Report, 2024

2

Some organizations are struggling to adapt to the rate of change

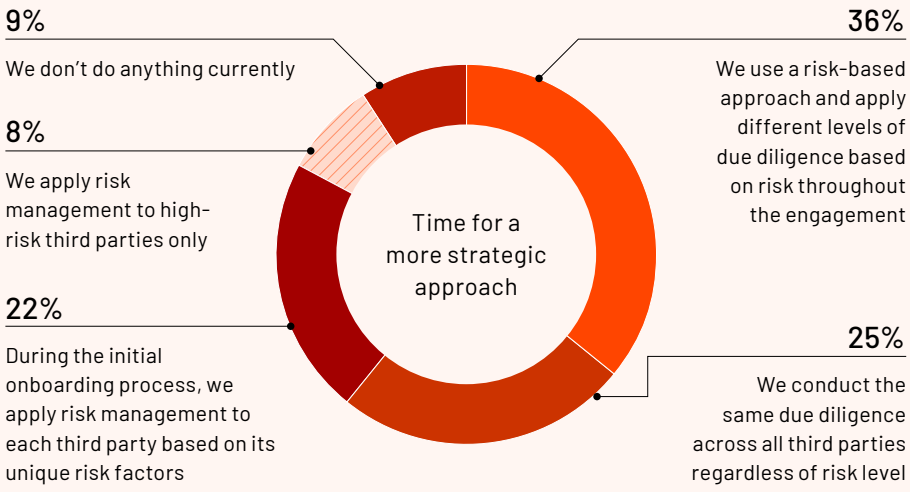
Only

36%

of organizations use a risk-based approach with third parties

1/4

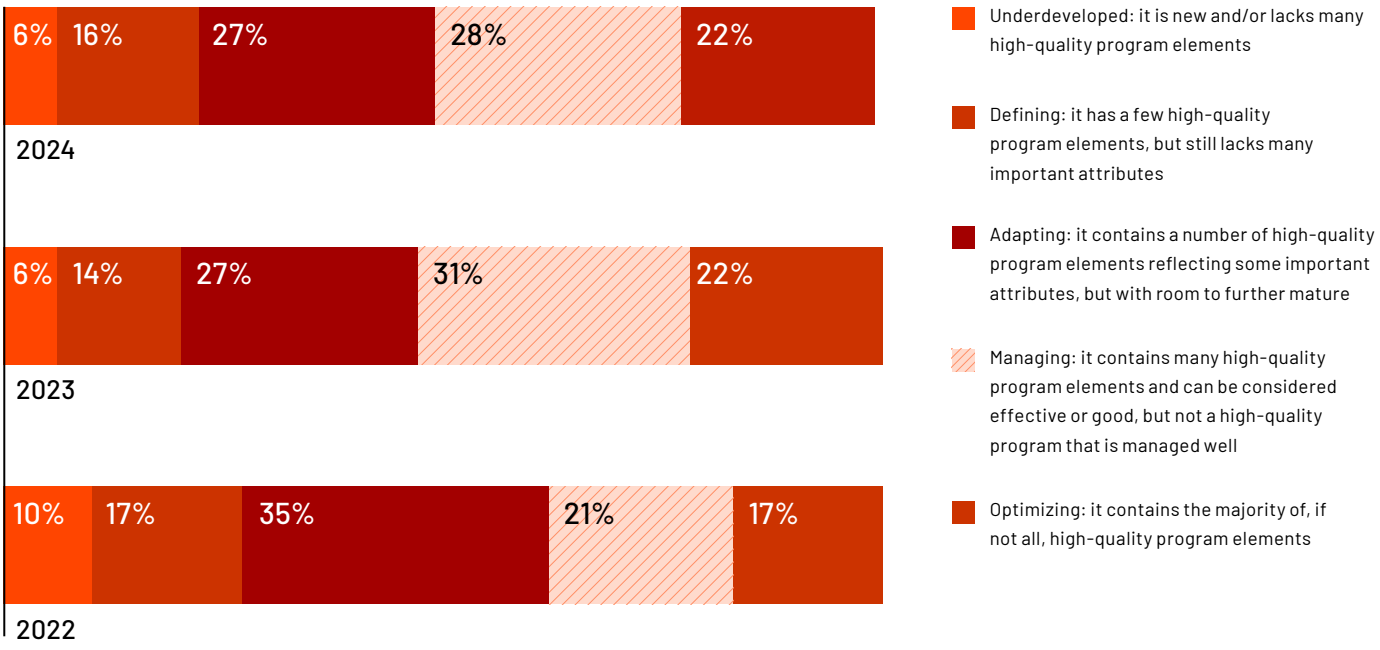
use the same approach to all third parties regardless of risk level



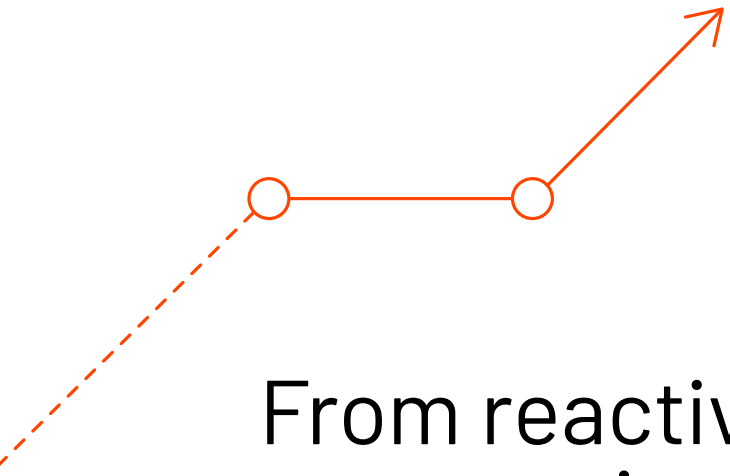
Source: NAVEX State of Risk & Compliance Report, 2024

3

But the future is bright as risk management matures each year



Source: NAVEX State of Risk & Compliance Report, 2024



From reactive to proactive

If compliance program operational risk management feels overwhelming, now is the time for a fresh approach based on more strategic risk assessment, monitoring and mitigation

Many organizations are not managing their risks effectively. Businesses are subject to copious risks from international regulations and disparate third-party networks, but too often wrongly adopt a reactive approach, simply running to address the latest changes, instead of moving toward a more regular, ongoing process of identifying, assessing, mitigating and monitoring for risks.

Too many organizations are still focused solely on meeting requirements as they arise, responding to sanctions updates on a case-by-case basis, for example. They don't allocate their resources according to risk severity, and their risk assessments are not informed by continuous access to operational data.

Regulators are also putting an emphasis on operational resilience. This includes the EU Digital Operational Resilience Act (DORA), requiring impacted financial-industry organizations to develop compliant internal frameworks that address several technology-related risks including those involving third parties. Internationally, legislation is growing more centralized in moving risk management forward.

"Operational risk management really prioritizes your crown jewels — the assets that are most critical to your operation."

Kyle Martin, vice president, product management – risk governance, NAVEX

The shift to proactive compliance program operational risk management

Operational risk management is the process of managing risks in an ongoing, systematic way. Organizations adopting this approach identify, assess, mitigate and monitor risks on a continuous basis, dedicate resources in proportion to risk level, and assess risks based on up-to-date operational data.

The term "compliance program operational risk management" highlights the role compliance has to play in this broader risk management approach.

"Operational risk management really prioritizes your crown jewels — the assets that are most critical to your operation," says Kyle Martin, vice president, product management – risk governance at NAVEX. "It, by nature, forces you to categorize and better understand risk, to think about business continuity and recovery time objectives. It allows you to take a more quantitative approach, putting dollar values on assets and reputational harm, so that when you go to the board you are speaking a language that makes sense to everybody."

Compliance program operational risk management

Regular ongoing process of identifying, assessing, mitigating and monitoring for risks

Dedicating more resources to the greatest risks

Risk assessments informed by continuous access to operational data

Checkbox approach

One-off approach to meeting requirements, leaving the organization vulnerable to changes

Giving the same attention to all risks (inefficient)

Risk assessments using out-of-date or incomplete information

Compliance program management: DOJ guidance

The U.S. Department of Justice (DOJ) Evaluation of Corporate Compliance Programs (ECCP) represents the latest DOJ guidance to federal prosecutors about how to assess the strength and quality of a company's corporate compliance program.

That assessment, in turn, helps determine the size and severity of punishment a company should face in the event of a compliance failure. Many organizations – not just those based in the U.S. – are keen to track closely with U.S. DOJ compliance program guidance.

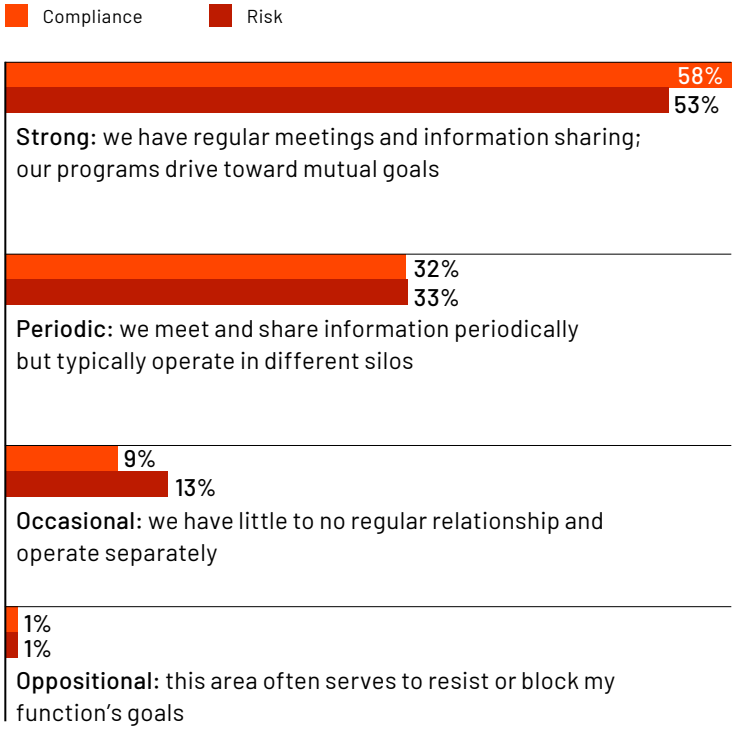
Four pillars of compliance program operational risk management

Organizations need to make cultural, technological and process changes to implement effective operational risk management. But it's not easy. There are four elements that must be in place for effective compliance program operational risk management:

Pillar 1: Effective communications

A first step is to ensure different parts of the business are speaking the same language when it comes to operational risk management. For example, the metrics cybersecurity professionals are using to measure success will be different to those of the legal department, but both divisions should be talking to each other on a regular basis and involving others like HR and compliance.

Nearly half of risk and compliance professionals typically operate in silos



Source: NAVEX State of Risk & Compliance Report, 2024

Pillar 2: Risk management solutions

Risk management solutions are an important element of any compliance program operational risk management program, given their ability to automate and streamline regulatory risk management, third-party risk management and others, and integrate those with operational risk management.

For organizations overwhelmed by disconnected data sources and fast-moving, complex risk landscapes, risk management solutions can provide a reassuring element of clarity and control. The best tools enable businesses to highlight their challenges, build organization-wide understanding of risk management principles and fully integrate assessments and workflows to monitor and flag issues based on standards clearly tailored to the business footprint.

By embedding efficient risk management tools, organizations can stop worrying about blind spots and instead shine a light on potential risks before they become issues. They can effectively track and escalate risk management concerns at the touch of a button, and can embrace best practice templates and workflows to save time and effort.

Pillar 3: Data analytics and reporting

Data analytics and reporting tools also have a fundamental contribution to create smooth and successful compliance program operational risk management. Data analytics can be used to identify trends, predict risks and ensure both are handled effectively, particularly when aligned with customizable dashboards and reports that deliver usable insights to aid decision-making.

"Data analytics is so critical," says Kristy Grant-Hart, CEO at Spark Compliance Consulting. "It isn't realistic to manage the third-party environment without it, other than in a very small company. Continuous monitoring is important for organizations and regulators. The ability to produce the kind of reports that actually flag risk is important. For third-party management, we need to be sure it isn't a one-and-done exercise."

When internal employees or individuals outside the organization lean into an internal reporting system, for example, it can be the first signal of a sanctions violation or a regulatory failing. That first line of defense generates real-time risk signal data that can be used for incident reporting and for better identification, assessment, mitigation and monitoring of risk moving forward.

Michael Volkov, CEO of the Volkov Law Group, says, "Chief compliance officers are now setting up systems to monitor real-time activity through data. The key to this is collecting the right data, monitoring the right data, and finding anomalies in activity that warrant follow-up or testing. And by testing I don't mean deep-dive results, I mean sampling techniques. I urge everybody to use statistical sampling."

"Data analytics is so critical. It isn't realistic to manage the third-party environment without it."

Kristy Grant-Hart,
CEO at Spark Compliance Consulting

Pillar 4: Organizational culture

Often a business can find its culture to be a challenge in maturing compliance program operational risk management, but getting culture right will allow organizations to reap the benefits.

A common problem is a lack of shared mindset, with different parts of the business adopting different approaches and programs hindered by silos. These issues can only be solved by getting everybody on the same page, using the same protocols and tools when vetting new third-party vendors or assessing regulatory exposures.

It's important that leaders are talking about and addressing regulatory challenges regularly, ensuring the intensity of vetting is appropriate for the level of risk a vendor represents, and that all of these things are given the right level of focus with a tone from the top that encourages collaboration.

Jan Stappers, director of regulatory solutions at NAVEX, says, "The cultural differences among people are really important to keep in mind, because in some cultures people are totally comfortable with people simply bearing more responsibilities the more senior they become. They are surprised to hear that at the junior level employees also have responsibilities."

He adds, "It may be necessary to start with a cultural self-assessment, to make sure your communications land and key messages are picked up."

So many risk management challenges boil down to culture. If a certain business division has a hunger for control, such as IT buying software for the business without going through mainstream procurement procedures, that will be a stumbling block. Leaders need to build trust across divisions and move toward operational risk management in lockstep across the business.

IN CONCLUSION

As organizations struggle to keep up with an expanding and increasingly complex risk landscape, many continue to rely on reactive checkbox approaches to risk management. With too much focus on meeting requirements when they arise, rather than strategically categorizing, prioritizing and mitigating the risks that matter most, issues can fall through the gaps.

Strengthening a compliance program operational risk management approach, which is continuous, systematic and agile, and puts the focus on ensuring business continuity, is the best way forward. But it can be a challenge. Organizations need to invest in the right tools and processes, embrace tech-driven risk management solutions, lean into data analytics and reporting, and above all ensure business-wide buy-in.

Businesses are encouraged to review their current risk management practices and consider how to optimize new approaches. To learn more about NAVEX regulatory and third party risk management solutions, click here.

Conclusion

In a riskier operating environment, a simple shift in approach can strengthen resilience

Regulatory and third-party risks are increasing, and organizations are struggling to keep up, leaving them vulnerable. Despite the danger, many businesses are still using a reactive approach to risk management, addressing challenges as they arise rather than adopting a strategic view that properly prioritizes the risks that matter most.

The solution is to strengthen the compliance program operational risk management, recognizing that risk is part of doing business, security is necessary, and the most effective way forward is focusing on the greatest priorities and constantly monitoring for emerging and changing risks. The aim of compliance program operational risk management is to bring potential threats down to acceptable levels and ensure business continuity, delivered through a continuous process of identifying, assessing, mitigating and monitoring risks.

At a glance

- Regulatory compliance is a baseline, but if operational resilience is the goal, then an organization will need a full lifecycle approach
- Organizations must be aware of the continuous nature of risk. Regulations change, vendors evolve, threats emerge geopolitically and digitally. One-and-done screening is not enough
- Without a business-wide, systematic approach to risk management, businesses will not allocate sufficient resources to high-risk areas and will fail to keep risk assessments up to date
- Senior leadership has a critical role to play in embedding a culture from the top that supports ongoing, integrated and meaningful compliance program operational risk management
- Regulatory and third-party risk management success has a real-world impact in minimizing practices like child labor – there is a moral and reputational case for success

Five things you can do now

01
Form a cross-functional committee tomorrow to start evaluating risk impact and likelihood for the business

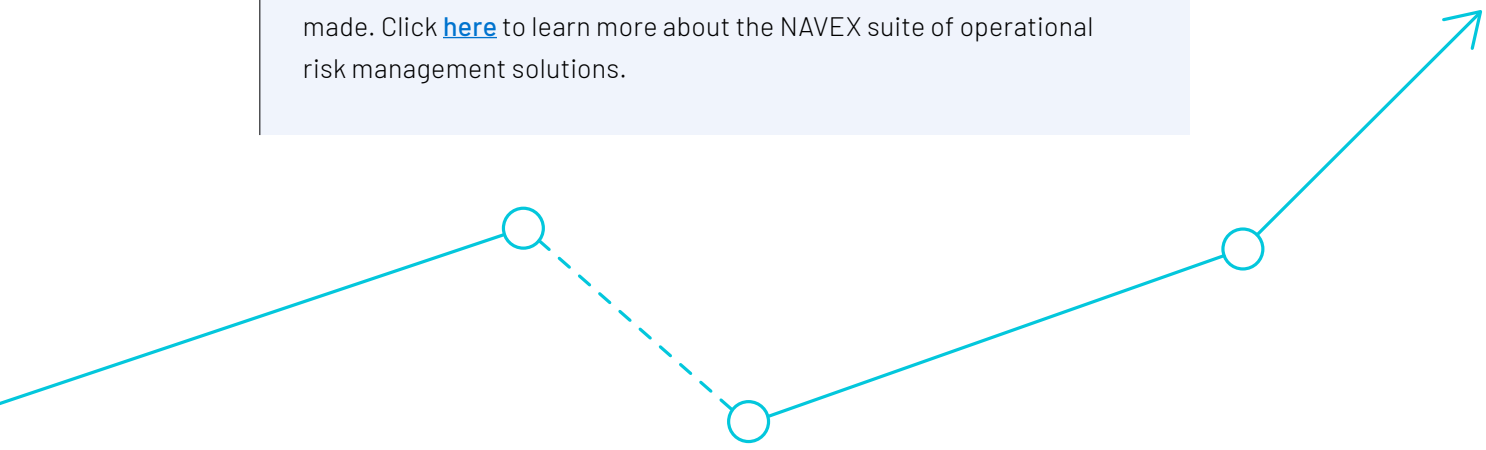
02
Incorporate a constant data feed on regulatory change into risk management processes

03
Centralize issue management with a single location for audit findings and a clear process for employees to report issues

04
Create an incident response plan for third-party failures

05
Perform a gap analysis against a recognized framework – don't let perfect get in the way of better

Now is the time to assess your current risk management practices to see where you can do better. There are always improvements to be made. Click here to learn more about the NAVEX suite of operational risk management solutions.



NAVEX | Navigator Series

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 LinkedIn.

Legal disclaimer
This content is informational. It is not and should not be relied upon as legal advice. Please consult your attorney for advice relating to your specific circumstances.

AMERICAS

5885 Meadows Road, Suite 500
Lake Oswego, OR, 97035
United States

info@navex.com
www.navex.com
+1 (866) 297 0224

EMEA + APAC

London
1 Queen Caroline St.
London W6 9YN
United Kingdom

info@navex.com
www.navex.com/en-gb/
+44 (0) 20 8939 1650