The Pulse:

Risk & Compliance

BROUGHT TO YOU BY:

nintex

IFP

nintex

At Nintex, we are transforming the way people work, everywhere.

Nintex is the global standard for process intelligence and automation. Today more than 10,000 public and private sector organizations across 90 countries turn to the Nintex Process Platform to accelerate progress on their digital transformation journeys by quickly and easily managing, automating and optimizing business processes.

We are committed to fostering a workplace that supports amazing people in doing their very best work every day. Our core values, deliver on our commitments, don't wait, and operate with respect and consideration, are not just words. We use them to guide our daily work, measure our success, and continuously ideate and improve.

Visit our site

Executive Summary

Effective risk and compliance management is vital for companies that want to protect their business, reputation, and stakeholder interests.

They must be able to identify, assess, and mitigate the risks associated with compliance in order to ensure all regulatory laws, standards, and policies are being met.

However, in 2023, cyberattacks and data breaches posed a significant challenge to many organizations. As such, leaders are now turning their focus towards better risk and compliance management in the year ahead, recognizing the need for more proactive measures.

By understanding the key areas of concern and the opportunities for automation, organizations can endeavor to bridge these gaps and streamline their risk and compliance processes for greater efficiency and effectiveness.

With that in mind, we conducted a study to explore the evolving landscape of technology adoption within risk and compliance, looking towards the future to discover top priorities for 2024 and beyond.

Here’s what we found out.

Survey demographics

Insights For Professionals surveyed over 100 UK-based IT and cybersecurity leaders across a range of sectors. The survey focused on those with IT, Business Process, Digital Transformation, Risk, and Compliance-related job titles.

Company size

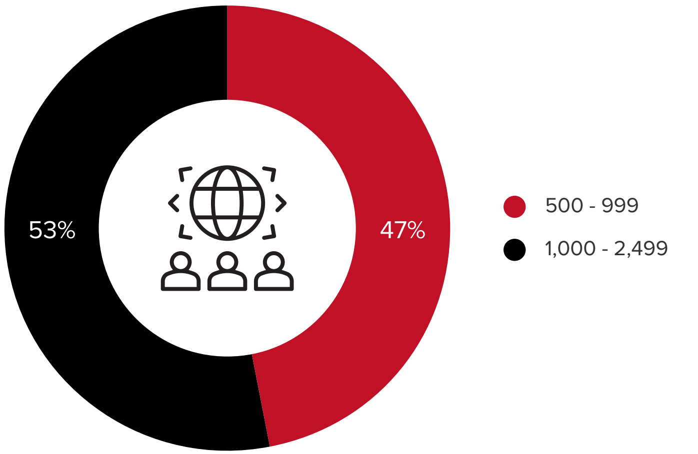
All respondents worked in companies with a workforce of between 500 and 2500 employees.

The biggest group of participants came from companies with 1000 to 2,499 employees at 53%. This was followed by organizations of between 500 to 9999 employees at 47%.

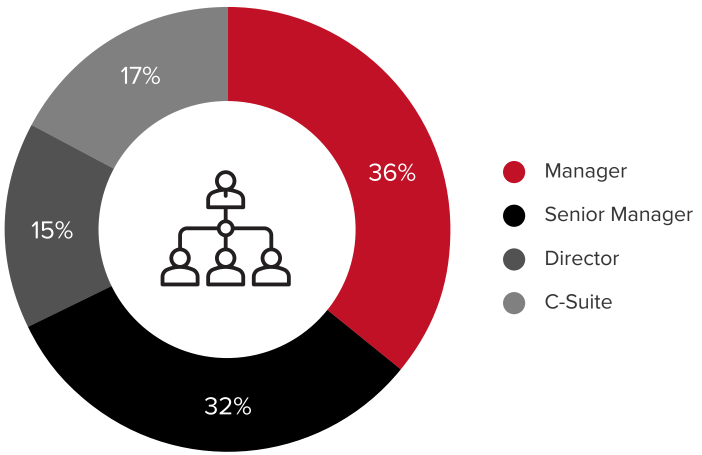
Seniority level

The majority (68%) of our respondents occupied Manager-level (Manager and Senior Manager) positions. While 32% held positions at the Director level or higher and 17% occupied C-Suite roles.

Company size



What is your authority level?



The biggest cybersecurity issues facing organizations in 2023

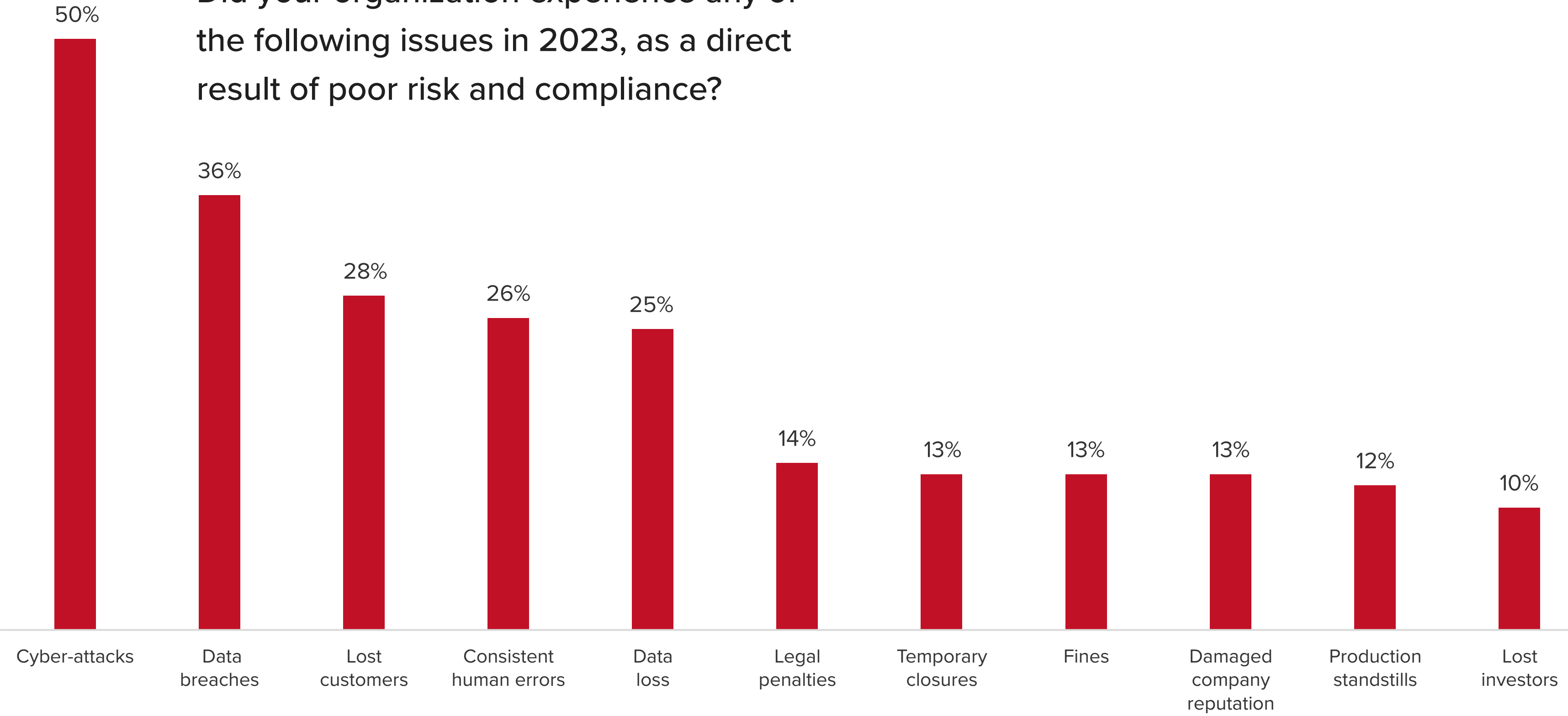
In order to understand the impact of poor risk and compliance management, we asked respondents to identify the biggest security issues they faced in 2023.

The findings revealed that half (50%) of organizations experienced a cyberattack last year. Not only that, but 36% suffered a data breach and 25% lost valuable data.

As a result of these security issues, 28% suffered a loss of customers, followed by consistent human errors (26%), and legal penalties (14%).

Further to this, 13% of those surveyed faced temporary closures, fines, and found that their company reputation was damaged in the process.

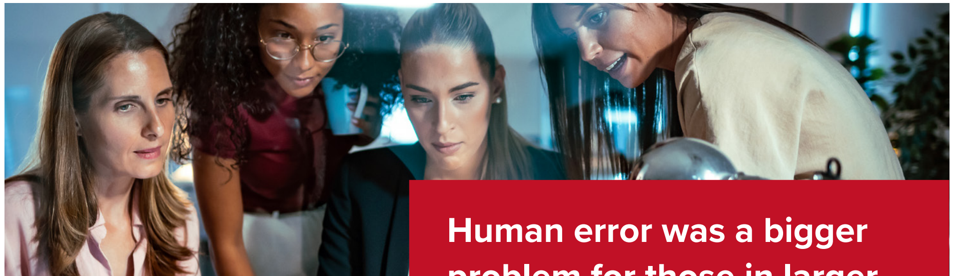
Did your organization experience any of the following issues in 2023, as a direct result of poor risk and compliance?



Interestingly, human error was a bigger problem for those in larger organizations (1,000-2,499 employees) with 30% revealing they saw consistent problems in this area, compared to 22% in smaller companies.

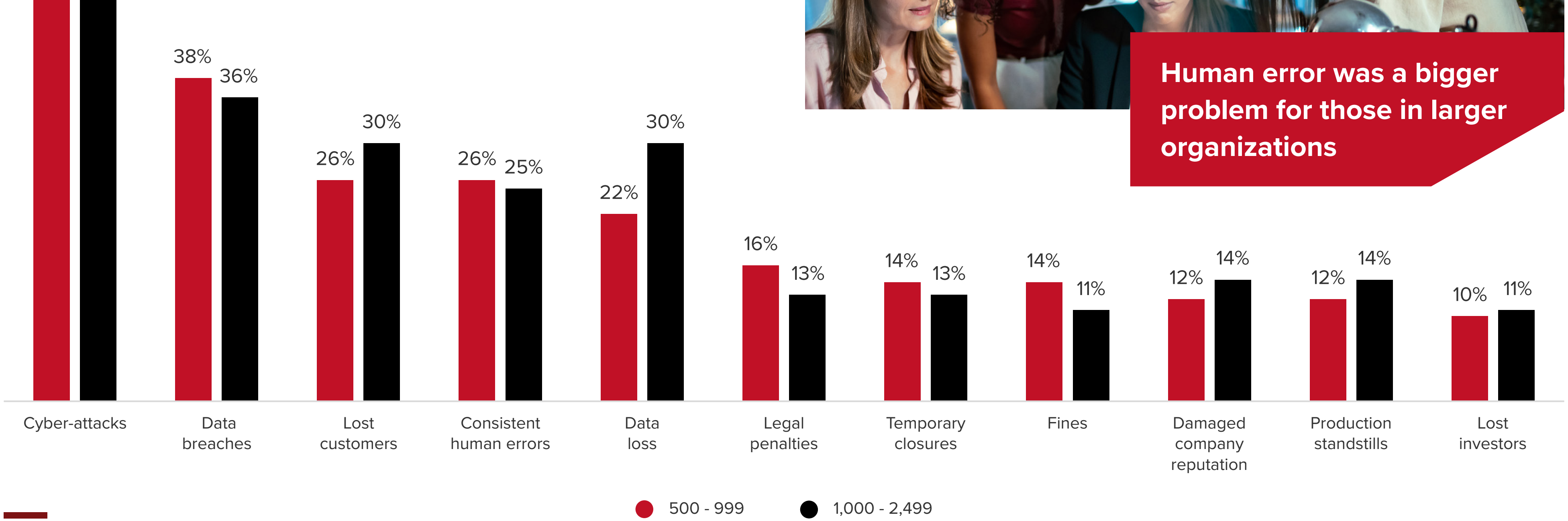
It's clear then, that successful cyberattacks and security breaches can have significant consequences for organizations, including financial losses, reputational damage, and operational disruptions.

It has also become apparent that organizations need to fortify their risk and compliance practices if they hope to effectively combat these threats and safeguard their operations in the future.



Human error was a bigger problem for those in larger organizations

Did your organization experience any of the following issues in 2023, as a direct result of poor risk and compliance?



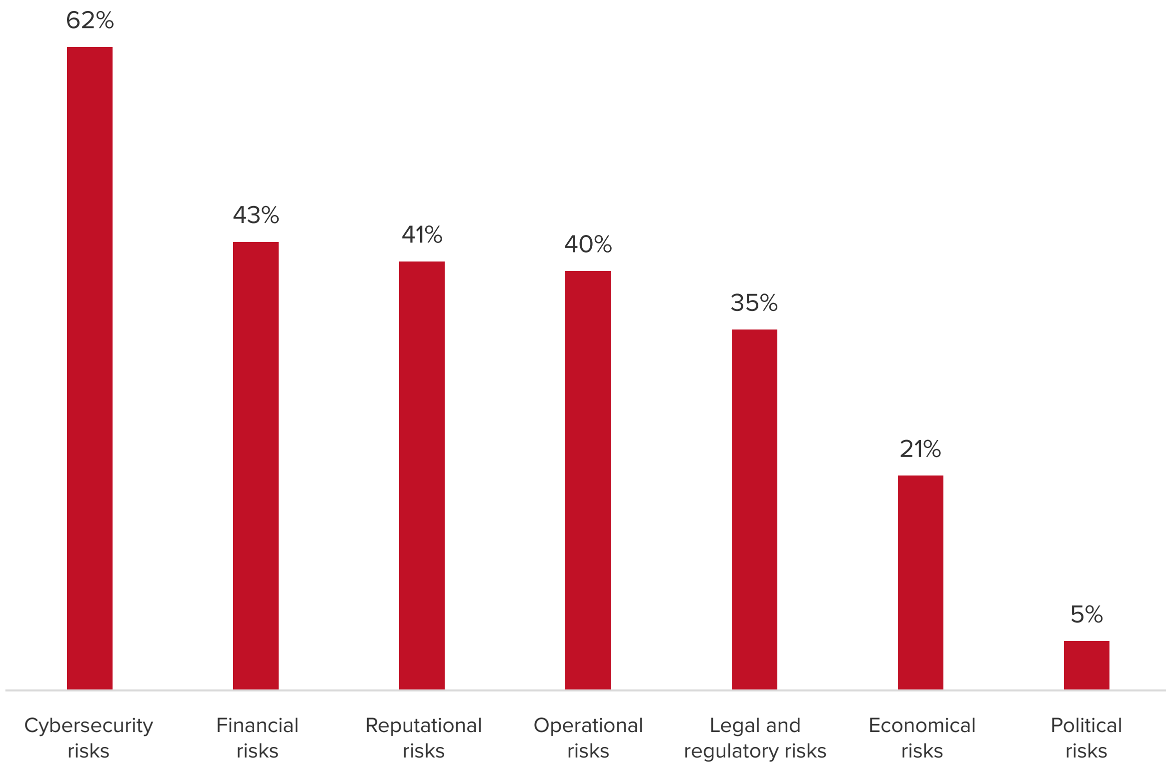
Key areas of concern for 2024

Having experienced a plethora of security issues last year, cybersecurity risks remain a key concern for almost two-thirds (62%) of companies in 2024, and this figure reflects the rising threat of cyberattacks in today's landscape.

However, cyberattacks clearly aren't the sole focal point in the realm of risk and compliance, with financial (43%), reputational (41%), operational (40%), and legal (35%) risks also appearing high up on the list.

This comes as no surprise, as successful attacks can have a significant impact on organizations, their customers, and their future.

Which areas of risk and compliance are you most concerned about in 2024?



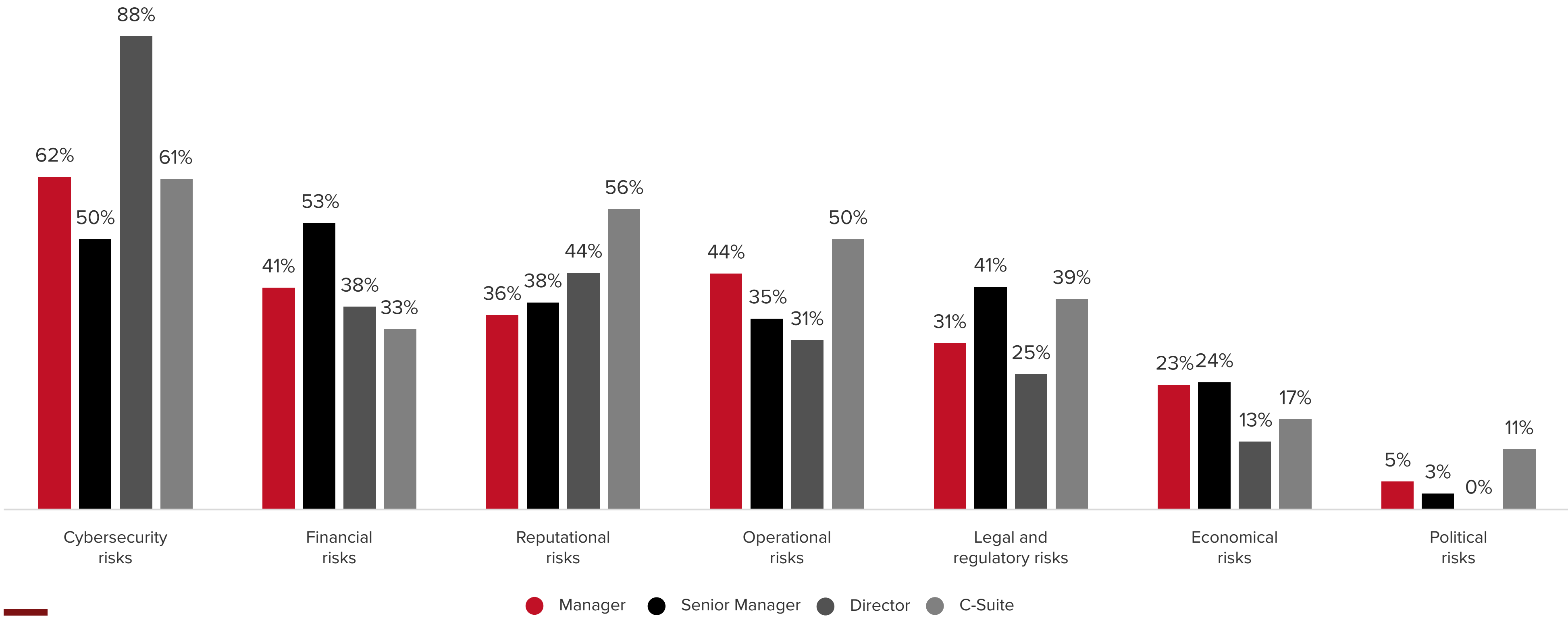
Priorities based on position

Drilling down into this data, it became apparent that almost 9 in 10 respondents (88%) at a Director level highlighted cybersecurity risks as their biggest concern, significantly above the average.

Meanwhile, C-Suite level respondents were increasingly concerned about reputational (56%) and operational (50%) risks. Again, above the average.

For Senior Managers, financial risk was identified by more than half (53%) as their biggest area of concern. These statistics point to differing priorities across our respondents when it comes to risk and compliance management, depending on their authority level within their organization.

Which areas of risk and compliance are you most concerned about in 2024?



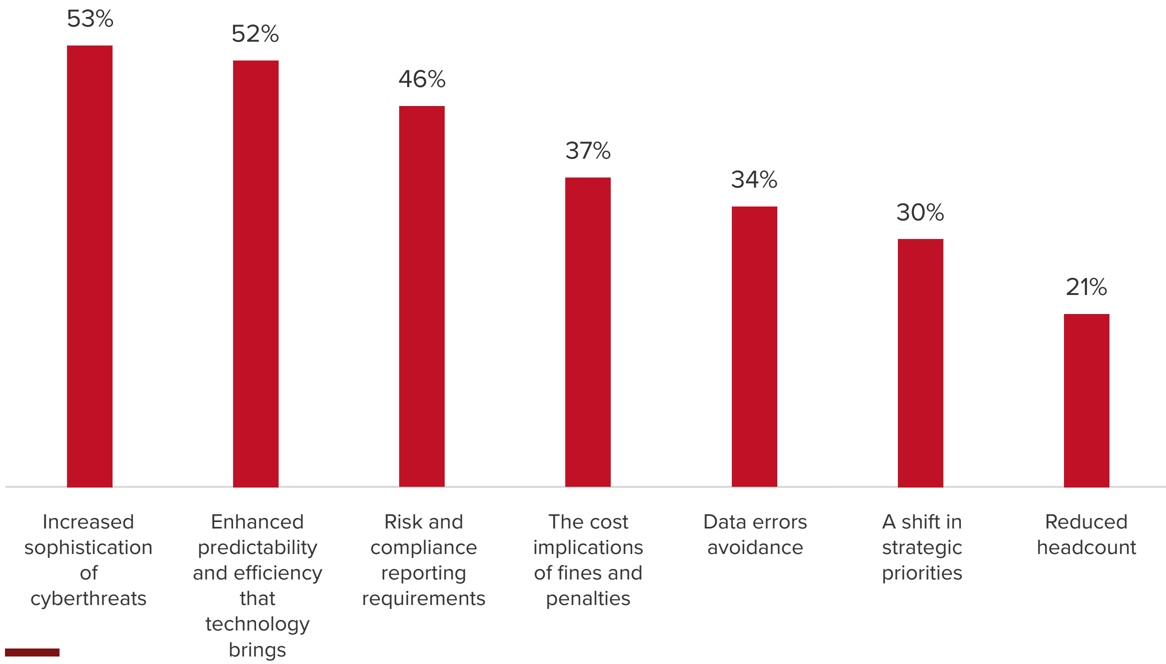
Drivers for investment in risk and compliance technology

With half (50%) of organizations experiencing a cyberattack in 2023, it stands to reason that leaders are keen to prevent this from happening again. With that in mind, investing time and resources in tackling and mitigating these issues is key.

Some of the other key drivers for investment in this area include the increased sophistication of cyberthreats (53%) and the enhanced predictability and efficiency that technology can bring (52%).

This was followed closely by the various risk and compliance reporting requirements (46%) organizations are faced with, and the cost implications of fines and penalties (37%).

Which of the following are drivers for technology investment into risk and compliance?



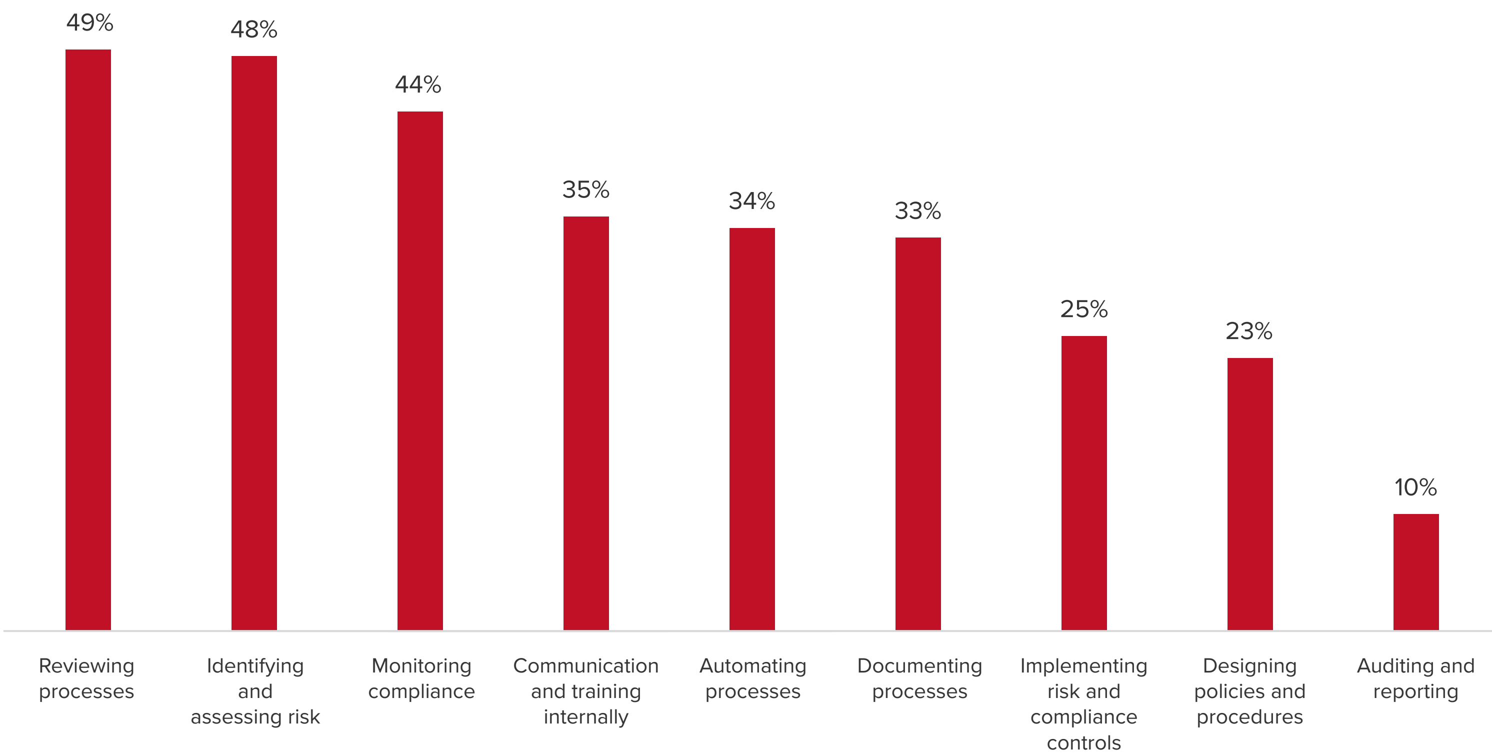
Understanding where leaders are spending their time

Sophisticated threats, enhanced predictability, efficient tools, and risk and compliance reporting are some of the key reasons leaders want to invest in new technology and processes.

But in order to understand which areas these companies are currently focusing on and what they need to do in the future, respondents were asked where they currently spend most of their time when it comes to achieving risk and compliance standards.

The top three results reflect the fact that **reviewing, assessing, and monitoring risk** and **compliance** are the foundations of any comprehensive risk management strategy.

Where do you spend most of your time when it comes to achieving risk and compliance standards in your business?



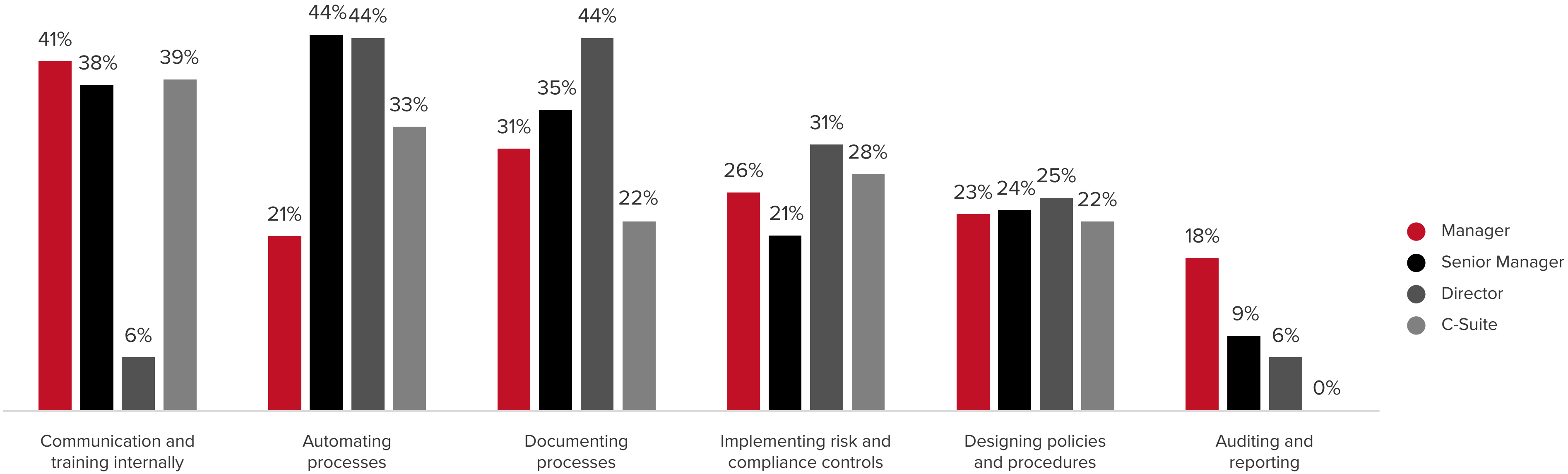
44%

of Directors and Senior Managers have automating processes as a key focus area

Internal communication and training are also crucial for reducing human error, a recognized issue in more than a quarter (26%) of the companies surveyed.

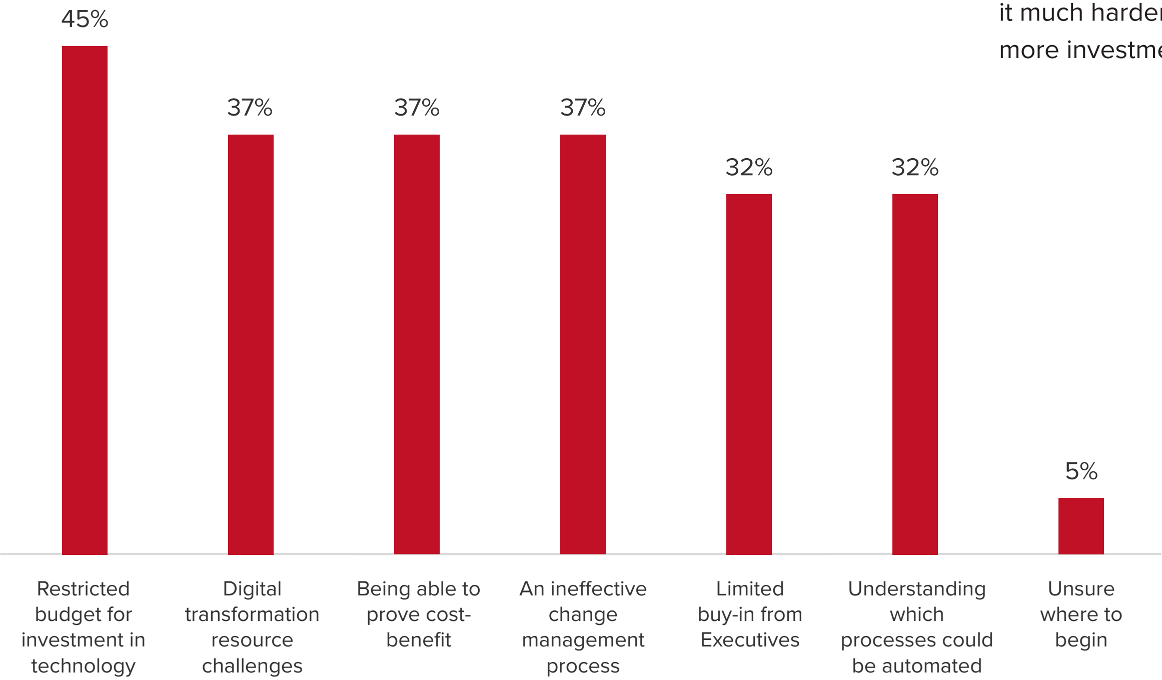
Although automating processes is only a key focus for one in three (34%) businesses, 44% of Directors and Senior Managers highlighted this as the area where they spend most of their time. In contrast, the majority (41%) of Managers concentrated on internal communications and training. This may be indicative of differences in responsibility across the organization when it comes to achieving risk and compliance standards.

Where do you spend most of your time when it comes to achieving risk and compliance standards in your business?



The biggest barriers to automation

What are the biggest barriers you have in your organization preventing you from automating processes to reduce risk?



It's positive to see that the majority of organizations have already taken some steps toward assessing their automation needs and identifying potential starting points for implementation.

However, there are some key barriers that are preventing them from automating more processes as a way of reducing security risks and ensuring compliance.

Resources are a clear problem, with almost half (45%) revealing that they have a restricted budget for investing in this type of technology and a further 37% facing digital transformation resource challenges. Proving cost-benefit (37%) and ineffective change management processes (37%) were also significant hurdles when attempting to automate processes to reduce risk.

The reason for this is that many organizations are still getting to grips with automation and learning what is and isn't possible. This can make it much harder to prove the value of these tools and secure more investment for these areas.

Interestingly, the data revealed that restricted budget and proving cost-benefit were bigger challenges in smaller organizations, with 50% saying they lack budget and 44% struggling to prove why it's a worthy investment. This is unsurprising given that small companies typically have less capital to invest in these areas.

That said, budgets are still an issue for many larger companies, though more are grappling with challenges related to resource allocation for digital transformation (43%) and identifying automation opportunities (41%).

More support is needed

The findings suggest that most organizations are facing a common set of obstacles. While financial constraints may pose a significant barrier to many, it's evident that resource challenges, proving cost-benefit, and ineffective change management processes compound these difficulties further.

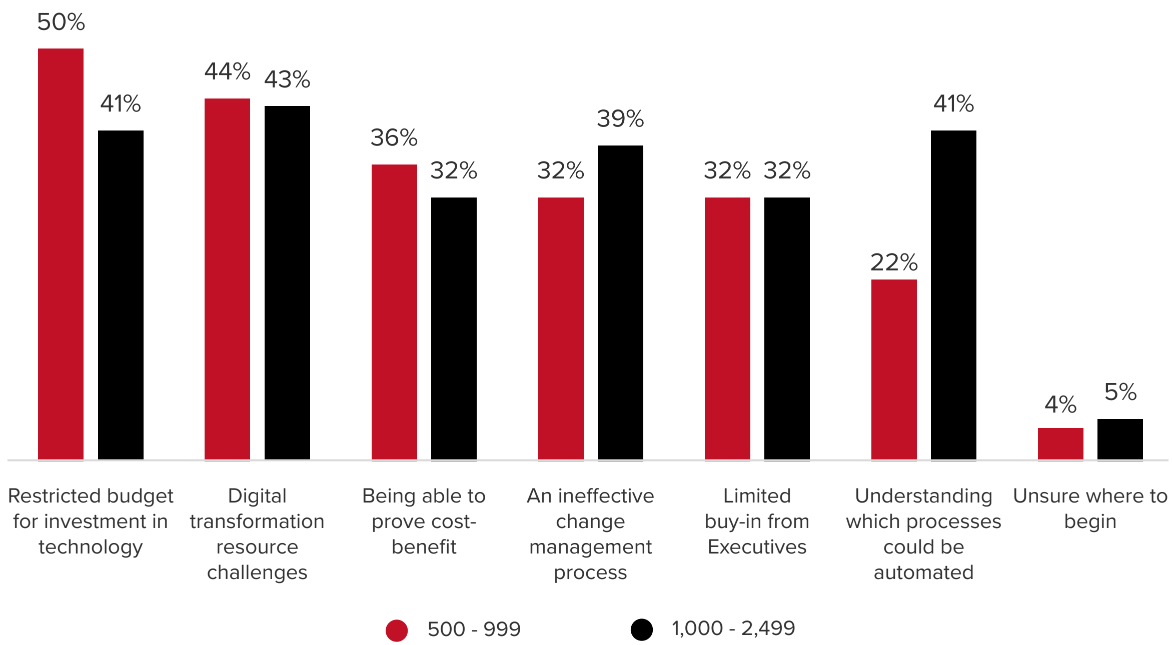
Limited buy-in from executives (32%) and not understanding which processes could be automated (32%) are also preventing companies from automating processes to reduce risk.

Without sufficient support from organizational leaders and a clear understanding of where automation can and will be most effective, initiatives to reduce risks this way may struggle to gain enough traction.

But these initiatives are essential, as automating processes related to risk and compliance can play a pivotal role in combatting cyberattacks, data breaches, and the subsequent fines and loss of customers. This will become more evident in the following section, which elaborates on the advantages of automation in compliance and risk management.

Restricted budget and proving cost-benefit were bigger challenges in smaller organizations

What are the biggest barriers you have in your organization preventing you from automating processes to reduce risk?



The benefits of automating compliance and risk processes

Despite the barriers to automation that many are facing, leaders are clearly aware of the potential benefits of these systems. For one thing, over half (52%) agreed that these technologies can enhance predictability and efficiency across the various areas of compliance and risk.

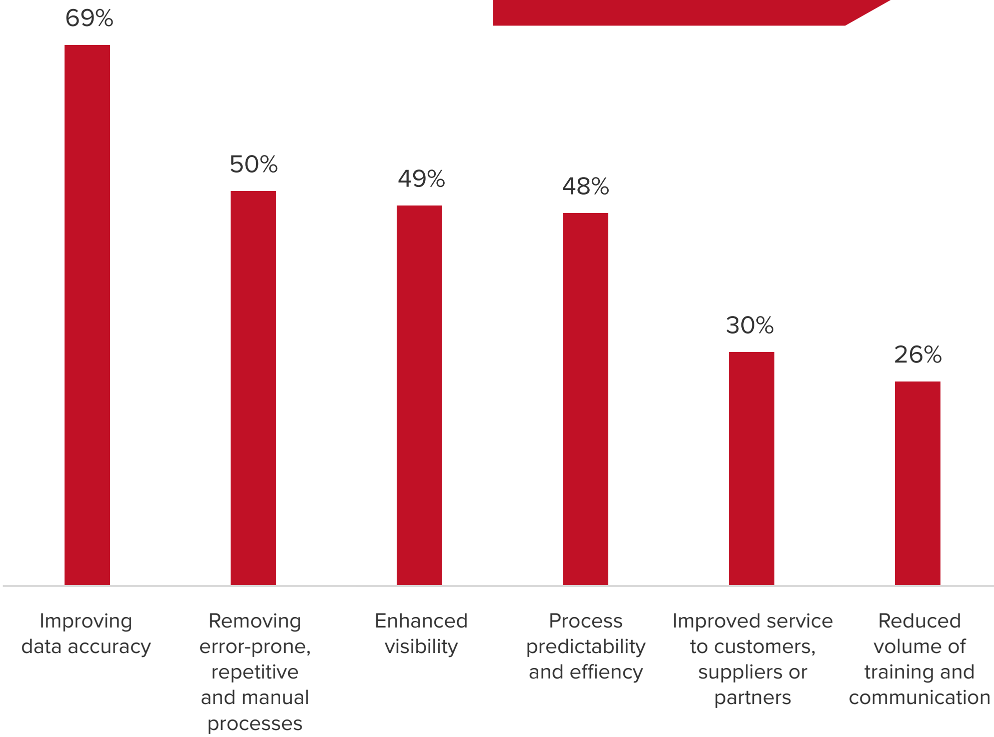
Not only that, but when asked to share the biggest benefits they hope to achieve by automating key processes, improving data accuracy (69%) was highlighted as the biggest potential benefit. This was followed by removing error-prone, repetitive, and manual processes (50%), enhanced visibility (49%), and process predictability and efficiency (48%).

It seems that businesses of all sizes are in agreement when it comes to the top three benefits they were looking to achieve, if they could automate processes for improved compliance and risk management.

69%

highlighted automating processes as the biggest potential benefit

What are the biggest benefits you would hope to achieve if you could automate processes for improved compliance and risk management?



Improving data accuracy is the biggest potential benefit for most leaders

That being said, there were some key differences in what the more senior members of the team were hoping to achieve.

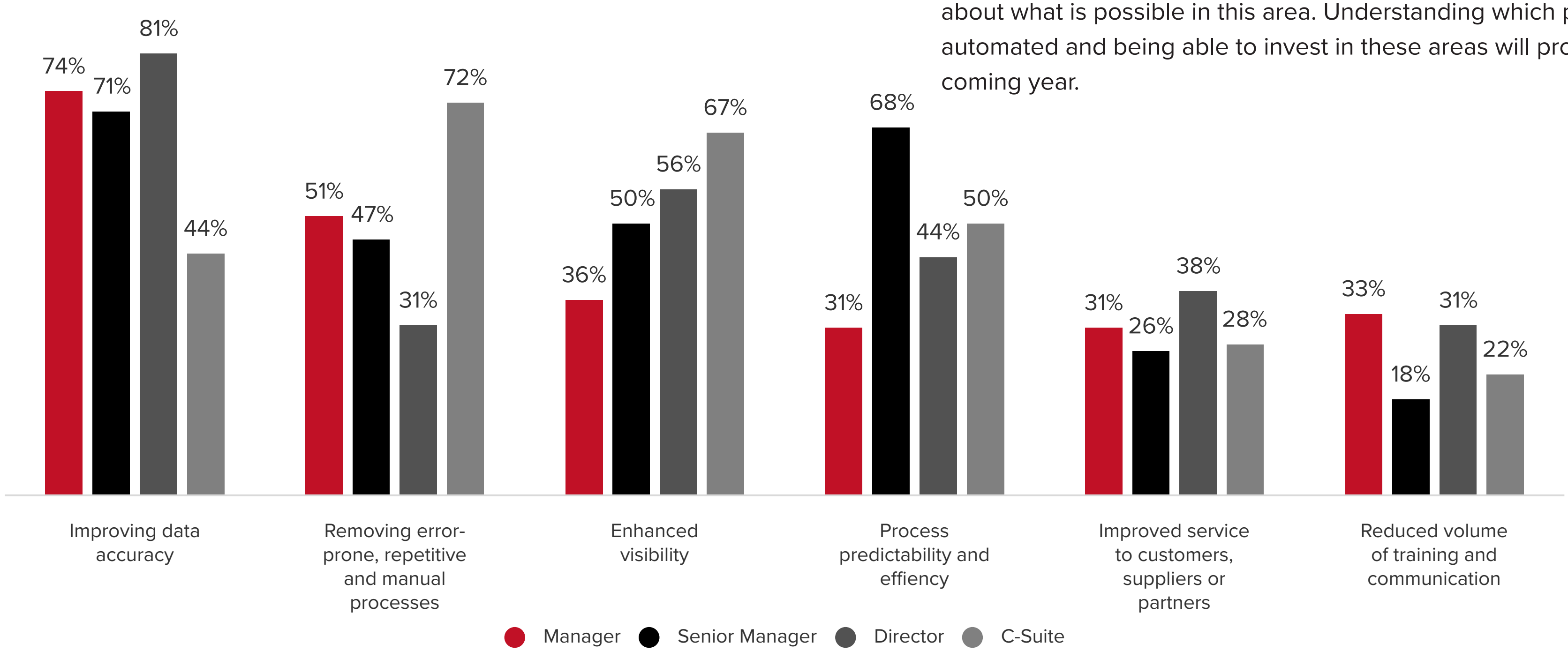
While improving data accuracy was the biggest potential benefit for most leaders, 72% of C-Suite level respondents identified removing error-prone, repetitive, and manual processes as the key benefit of automating different areas of risk and compliance.

Investment and buy-in is going to be crucial

It's apparent from these findings that automation has the potential to improve compliance and risk management in a number of ways. However, leaders are going to have to set aside bigger budgets and more resources to make this possible.

They will also require more buy-in from executives and better education about what is possible in this area. Understanding which processes can be automated and being able to invest in these areas will prove key over the coming year.

What are the biggest benefits you would hope to achieve if you could automate processes for improved compliance and risk management?



Final thoughts

In 2023, far too many organizations were still falling victim to cyberattacks and data breaches, and it's become clear that these are having a huge impact on businesses, leading to financial losses, reputational damage, and operational disruptions.

It comes as no surprise then, that heading into 2024, compliance and risk management is a real priority for many, along with reducing financial, operational, and reputational risks.

Despite this, too many leaders are currently dedicating too much of their time to reviewing, assessing, and monitoring risk and compliance, rather than actually automating these processes.

In fact, only one in three (34%) businesses have made this a focal point of their compliance and risk management strategy so far.

This is most likely due to the financial constraints that pose a significant barrier to many, alongside other resource challenges and the ability to prove cost-benefit.

So, if organizations hope to remove error-prone, repetitive, and manual processes and increase visibility and efficiency, more investment is needed. This requires both financial investment, but also buy-in from executives and leaders who may not currently be aware of the potential benefits automation can bring.

IFP Insights For Professionals

IFP gives you access to the latest business knowledge that's customized for you. We provide high quality, credible and relevant resources for senior professionals in one place.

An easy to access and personalized library to help you when you are researching specific topics, seeking practical advice, or simply want to stay ahead of what's happening in your industry. To do this we gather the best content from suppliers, brands and industry experts, as well as doing our own research.