SAI360
RISK FROM EVERY ANGLE

GRC Benchmark Report

Table of Contents

Benchmark Objectives

The risk and regulatory landscape in which firms operate is constantly in flux. Not only does this demand a more proactive and forward-thinking risk culture, but it necessitates substantial investment in compliance infrastructure and internal controls. This commitment is both financial and temporal, which in itself brings inherent risks as firms pivot their finite capital and human resources away from traditionally revenue generating initiatives to focus on long-term sustainability.

Amidst these challenges, benchmarking serves as a useful tool, offering senior managers a sense of perspective from which they base future decisions. Without such transparency, firms are often left to work in isolation, confined to their relative echo chambers. By embracing common challenges and best practices, we can collectively elevate compliance standards. This collaborative approach not only fosters a culture of transparency and continuous improvement but also contributes to the overarching regulatory objective of reducing systemic risk.

This survey is part of a co-creation Governance, Risk and Compliance (GRC) project between The Hague University of Applied Sciences, Peter Konings of Johnson Controls, Thought Leader Global and SAI360. The survey seeks not only to understand current practices but also to facilitate a comparative analysis across organizations, providing a basis to benchmark corporations that fall within the profile of those surveyed.

Educational Aspects

Researchers from The Hague University of Applied Sciences (THUAS) Law faculty have developed comprehensive reports on the regulatory legal frameworks within the designated GRC priority areas, furnishing the theoretical underpinning for the Benchmarking project across each of these sectors. In addition to these analytical reports, the students have created a professional checklist. This tool compiles critical information that acts as a measure of corporate performance within the specified GRC domains. It has been seamlessly integrated into the survey, serving as a resource for evaluating and understanding corporate adherence and best practices in these areas.

Profile of Survey Respondents

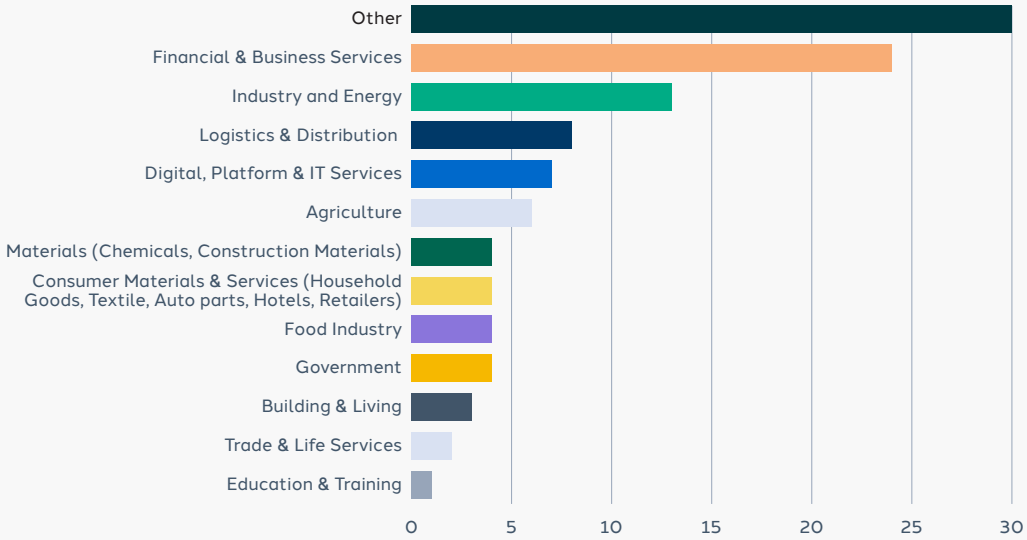
Firmographics

The broadening of regulatory scope mirrors the expansion of operational and financial risk as firms become more globalized and dispersed, yet at the same time more interconnected. The demographic of survey responses is well representative of this dynamic, encompassing 110 risk and regulatory professionals from a diverse tapestry of sectors, ranging from financial services, to food and drink and energy and agriculture.

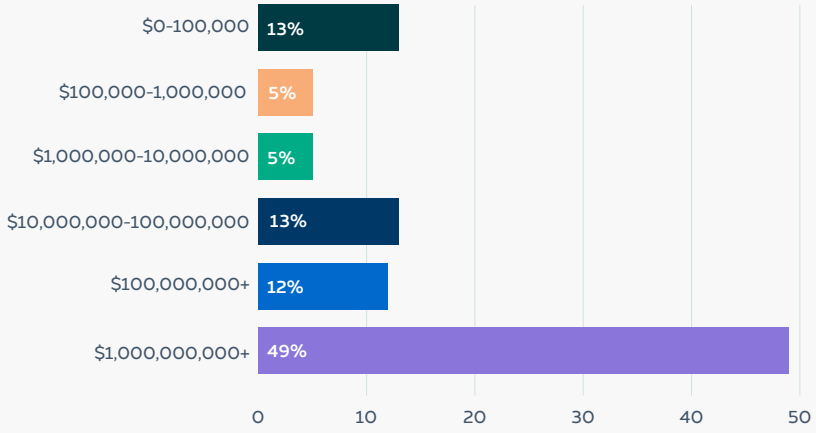
Whilst the survey responses are weighted more heavily toward larger firms - exceeding a $1 billion valuation and 250 employees - we see a strong representation from smaller and mid-market players. Geographically, the majority of responses emanate from North America and Europe, but there is notable participation from the United Kingdom and Asia-Pacific (APAC).

Participant Firmographic Overview

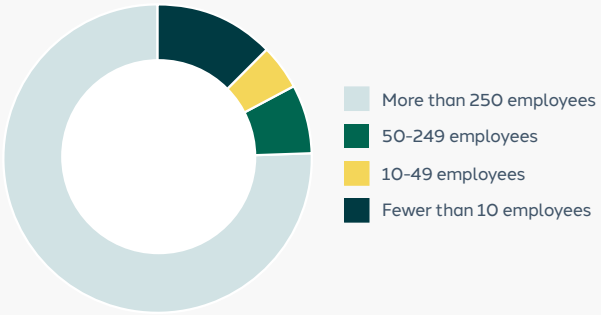
INDUSTRY OF OCCUPATION



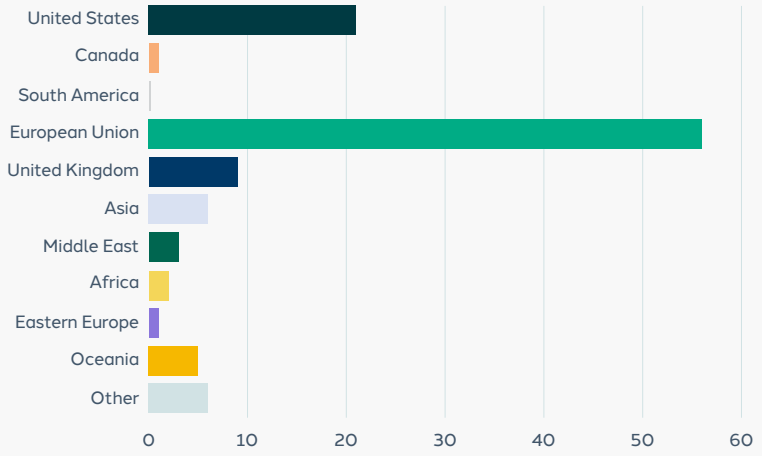
FIRM MARKET CAP



NO. OF EMPLOYEES



LOCATION OF HEADQUARTERS



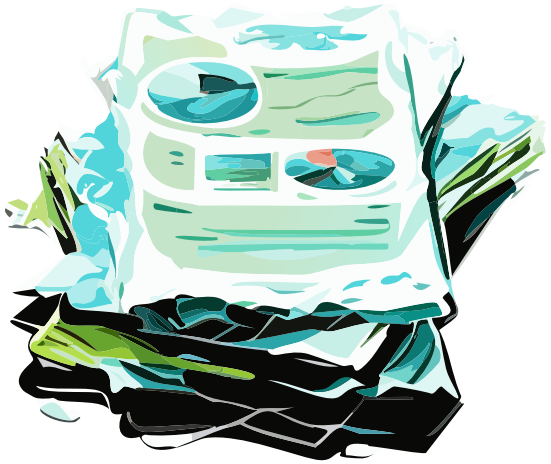
Compliance Personas

Given the slight skew in responses toward larger firms, it follows logically that the majority of these organizations have established specialized departments dedicated to Enterprise Risk Management (ERM), Compliance, Environmental, Social, and Governance (ESG), and Ethics. Despite facing a degree of criticism for its simplicity in assigning responsibilities for risk management, the "Three Lines of Defense" (3LoD) model still reigned supreme amongst our respondents.

77.2% OF COMPANIES SURVEYED APPLY A **RISK GOVERNANCE MODEL**, SUCH AS THE AS 3LoD

The establishment of dedicated departments for ERM, ESG and compliance isn't solely a function of regulatory demands; it facilitates a strategic advantage. It is no secret that the mounting regulatory pressure and evolving operational risks are proving difficult for organizations to manage. By building specialized risk and compliance functions, firms can proactively manage and mitigate compliance and operational risks more effectively, positioning themselves for sustainable long-term growth and resilience.

DEDICATED RISK AND COMPLIANCE FUNCTIONS



44.3% OF COMPANIES SURVEYED SPEND MORE THAN **1 000 000 USD ON THE COST OF COMPLIANCE.**

The Cost of Control

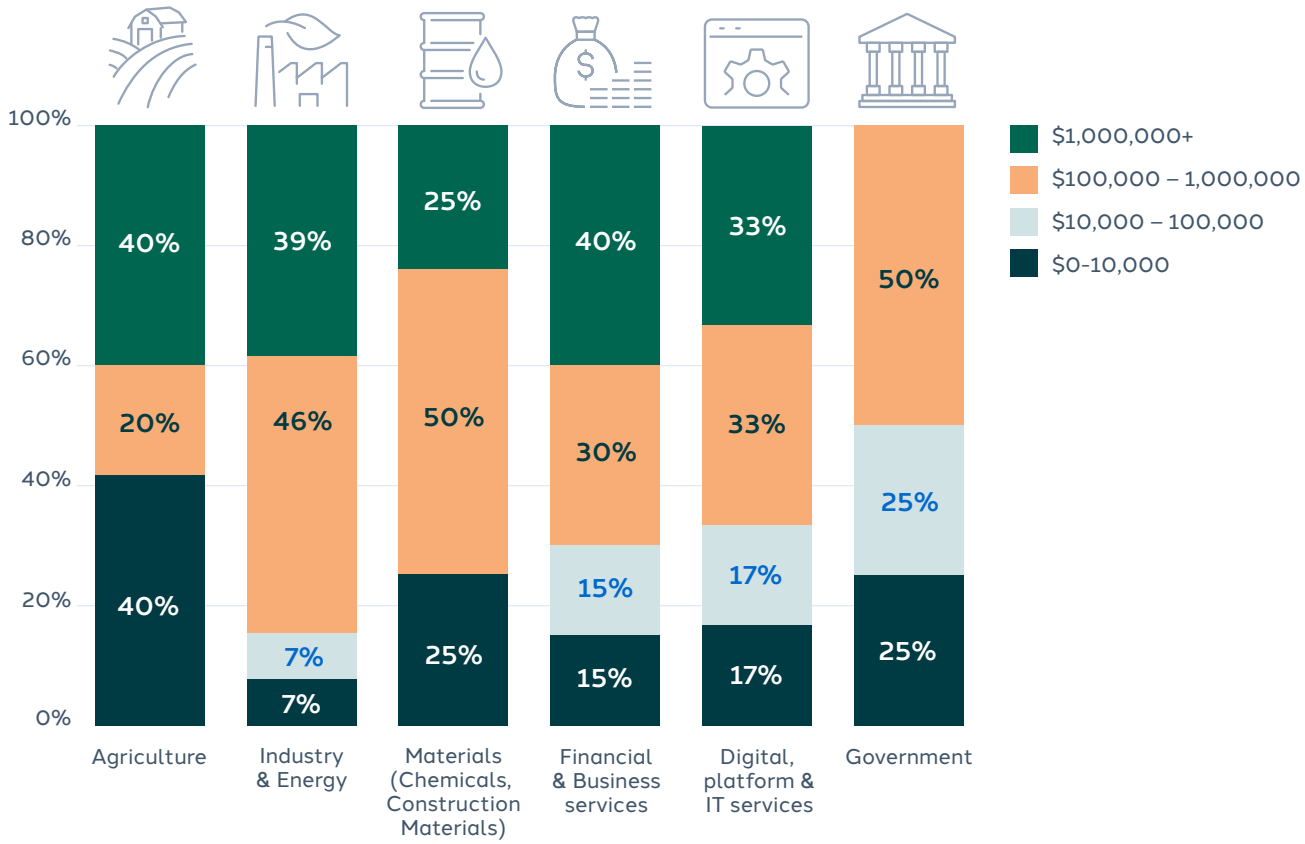
44.3% of respondents estimated their annual cost of compliance to be in excess of $1 million per annum. This figure encompasses a wide array of expenses, including but not limited to internal audit, financial compliance, business compliance, IT compliance, IT security, as well as all associated tools, templates, and the cost of external auditors. We have already alluded to the significant investment that firms make to ensure regulatory compliance, but this figure underscores the expectations placed on entities to meet regulatory demands and mitigate risk throughout their organization. But it also begs the question; is this capital being allocated efficiently? Later in the report we explore the possibility for innovation in compliance practices, evaluating some of the opportunities for companies to streamline their internal controls, adopt new technologies, and potentially reduce costs while maintaining or even enhancing their compliance effectiveness.

Cost of Compliance by Industry[1]

The Agriculture and Materials sectors show a diversified distribution of compliance costs, yet a significant number of firms in these categories manage to contain expenses under $100,000, possibly due to less stringent regulatory demands or more streamlined compliance procedures.

The Industry and Energy sector stands out for its high compliance costs, with a notable portion of firms allocating over $1 million annually to meet regulatory demands. The sector's significant regulatory scrutiny, rooted in its environmental, public health, and safety impacts, mandates strict adherence to a host of regulations. Additionally, the inherent operational complexities - managing hazardous materials and sophisticated equipment - necessitate extensive compliance infrastructure.

COST OF COMPLIANCE BY INDUSTRY



[1] These industries have been highlighted in particular due to their statistical significance. They were well represented amongst respondents (minimum n=7) which allows for a more accurate cost breakdown in percentage terms.

Financial Services Spotlight

The study highlights that while compliance costs generally increase with a firm's size, financial services firms show varied spending within size categories. This suggests some firms manage compliance capital more effectively than others do.

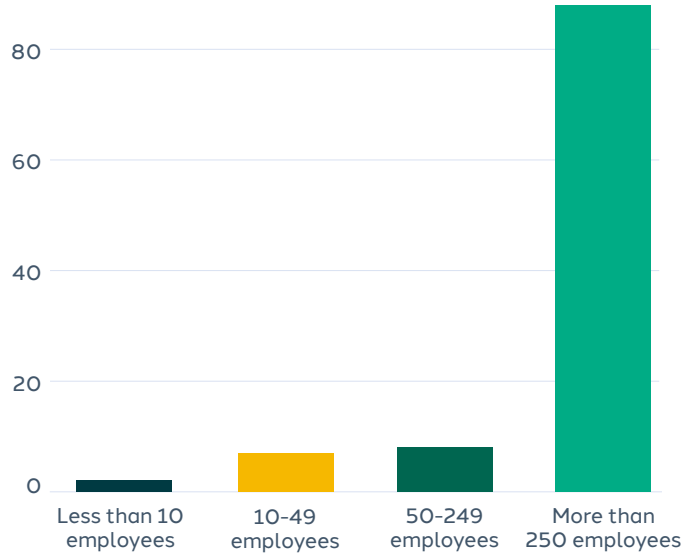
- **Room for improvement**
  67% of large institutions (>250 employees) spend $1 million plus annually on compliance. This highlights the high costs associated with managing more complex operations. Interestingly, 22% spend between $100,000 and $1 million. Yet only 11% spend below $100,000, indicating widespread significant expenditure. This scenario suggests opportunities for cost reduction and efficiency gains through automation and advanced technology to potentially improve compliance effectiveness and risk management.
- **The relative compliance burden on small firms**
  Small banks face significant compliance costs due to strict anti-money laundering and capital requirement regulations. With 25% of small firms (those under 10 employees) spending $10,000 to $100,000 on compliance, the financial burden is obviously a hindrance. This all only underscores the need for more cost-effective and better scalable solutions.

Sales Value vs Compliance FTE

"Sales Value per Compliance Full-Time Equivalent (FTE)" measures company revenue against the compliance department's size. It also assesses the efficiency and productivity of compliance roles. Higher values suggest effective compliance contributions to profitability within regulatory limits. Lower values indicate potential for operational review and efficiency improvements, potentially prompting a compliance operations review.

Overall, the data shows that over 57% of firms achieve over $100 million revenue per compliance FTE, with many surpassing $500 million. However, a significant number still don't reach economies of scale, likely due to reliance on manual processes that fail to leverage automation to augment human capability. These are less efficient and increase the risk of non-compliance. Some firms fall below $50 million revenue per FTE, suggesting a need for automation to enhance efficiency and compliance.

COMPLIANCE FTE VS. COMPANY SIZE



Compliance FTE

On average, our respondents have 66 dedicated full-time staff across internal audit and compliance functions. Particularly amongst larger institutions, the status quo remains to leverage people first and tooling second, despite the increasing availability and sophistication of compliance technologies. This reliance indicates that, while technology plays a crucial role in enhancing efficiency and accuracy in compliance processes, the judgment, expertise, and oversight provided by human professionals remain indispensable.

However, it also highlights potential opportunities for optimization. The substantial investment in personnel underscores the potential benefits of integrating more advanced technologies into compliance functions. As we will come to discuss, many firms have yet to fully leverage technological solutions, such as artificial intelligence (AI), machine learning (ML), and automation tools, which can significantly reduce the burden on human resources. These technologies can automate routine tasks, improve risk identification and management, and enhance the overall effectiveness of compliance programs.

Interestingly, the smaller and mid-market firms amongst our sample maintain minimal FTE which could suggest a strategic inclination toward a more technology-first approach to risk and compliance. The FinTech sector serves as a good example; many of these “neobanks” have a diverse pool of technological talent in-house which heavily influences their strategic focus. It’s an unforgiving race to scale for many, so having compliant innovation as a focal point allows for competitive differentiation and risk mitigation.

Comparing Automation across Compliance and Internal Audit

To what extent are companies adopting new technologies and automation within compliance? The use of automation serves as an indicator of where companies might be feeling the most pressure, and accordingly investing resources. Technological advancements like data mining, process mining, and AI provide a snapshot of the current tech landscape in compliance functions.

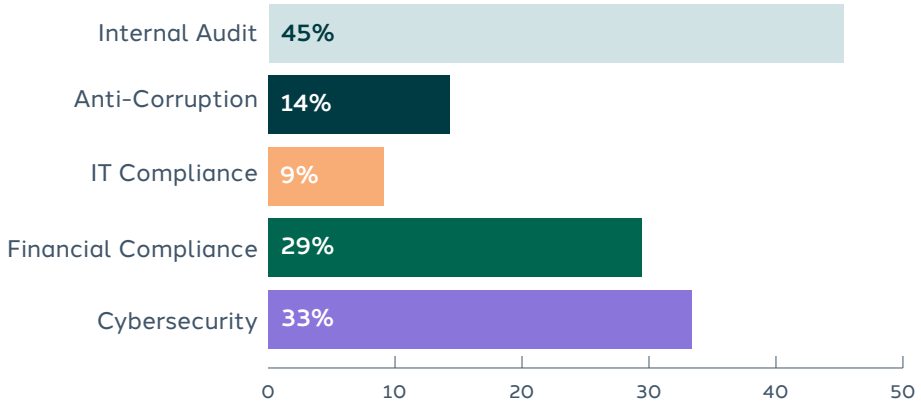
To obtain a representative view of the technological landscape, we evaluated the use of three increasingly sophisticated technological brackets: data mining, process mining, and AI.

Data Mining

Data mining uses machine learning, statistics, and database systems to find patterns and insights in large data sets, aiming to transform data into a structured form for further use.

Our findings reveal varying levels of data mining use across compliance areas. Internal Audit leads in maturity, likely due to Internal Audit's need for data analysis to spot risk patterns, ensure regulatory compliance, and identify operational issues. Anti-Corruption has the lowest adoption at 14.29%–perhaps surprising given a long-standing regulatory focus on this risk area.

FIRMS USING DATA MINING ACROSS COMPLIANCE FUNCTIONS



Process Mining

Process mining uses algorithms on event log data to uncover process trends, patterns, and operations within an information system. It aims to discover, monitor, and enhance actual processes by analyzing event data, filling the gap between traditional process analysis and data-centric techniques like ML. Process mining addresses questions beyond mere data storage and analysis, providing insights into process efficiency and effectiveness.

Such questions include:

- What's the best step order?
- Where are deviations from the designed process?
- What steps hinder process performance?
- Which non-compliant process behaviors demand addressing?

Process mining is most common in Financial Compliance and Cybersecurity, with 31.25% and 33.33% adoption rates, respectively. These areas involve large data volumes and complex workflows. They're ideal candidates for the efficiency improvements offered by process mining.

However, Anti-Corruption sees lower process mining adoption at 12.24%. This may be because its reliance on qualitative data and complex human interactions might not align well with current process mining technologies.

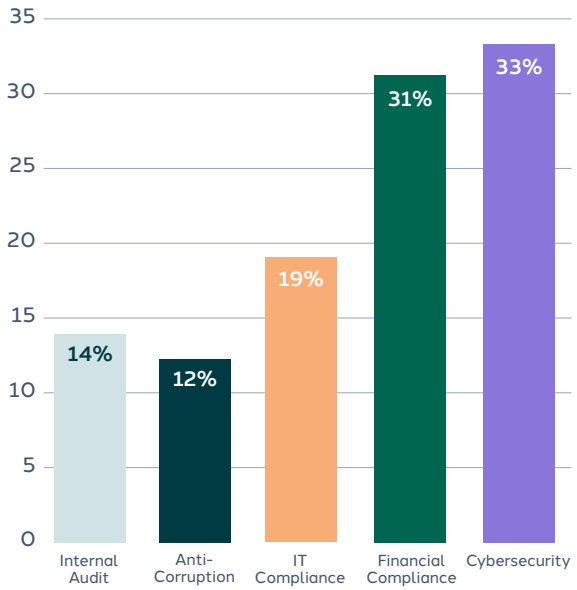
Internal Audit's use of process mining is only 13.95%. This is despite its benefits for insight into operations and efficiency. This low rate, contrasted with high data mining use, suggests room for growth in employing process mining to enhance audit functions by comparing actual to expected process performance.

Artificial Intelligence and Deep Learning

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. AI systems can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. AI is an umbrella term that encompasses various subfields, including machine learning ML, where machines learn from data to improve their accuracy in performing tasks.

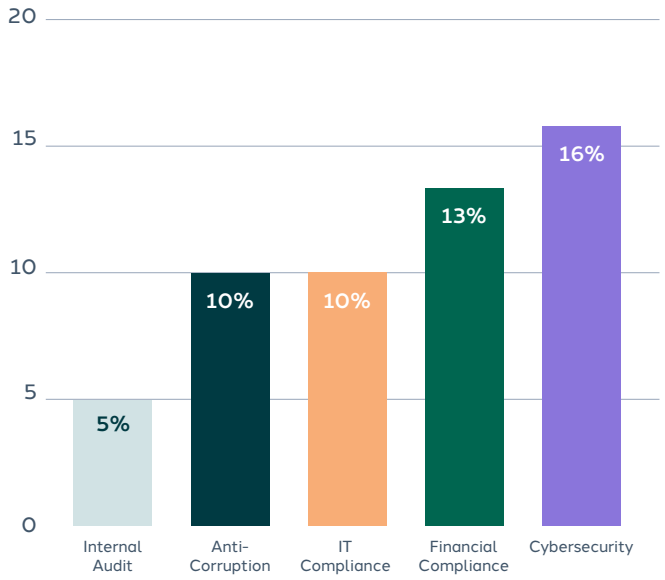
Deep Learning is a specific subset of machine learning inspired by the structure and function of the brain called artificial neural networks. It involves feeding a computer system a lot of data, which it then uses to make decisions about other data. This data is fed through neural networks, which are complex algorithms modeled on the human brain. They have various layers (hence "deep") for processing data, which enable the machine to go "deep" in its learning, making connections and weighting input for the best results.

FIRMS USING PROCESS MINING ACROSS COMPLIANCE FUNCTIONS



We see an understandably cautious approach to AI adoption across all compliance and risk functions, with the highest utilization in cybersecurity at a mere 15.79%. As AI technology evolves, its applications in risk management and RegTech are becoming more prominent, with use cases such as predictive analytics for fraud detection, automated compliance monitoring, and ML for anti-money laundering (AML) activities gaining traction. Despite the increasing number of solutions, the "hype" often surrounding AI's capabilities contributes to skepticism. Many firms remain hesitant to fully rely on AI, preferring a hybrid model in which humans oversee and work in tandem with AI systems to ensure a balanced and reliable approach to compliance.

FIRMS USING AI ACROSS COMPLIANCE FUNCTIONS



Monitoring Compliance Performance

The subsequent segment of our report delves into the mechanisms by which firms evaluate their compliance efficacy.

Retrospective Key Performance Indicators

A majority, 70%, of the surveyed entities rely on internal audit outcomes as a principal metric for assessing compliance performance. Furthermore, over half of the respondents, at 52%, consider the duration of remediation – the time span required to address and resolve compliance issues - as a critical performance indicator.

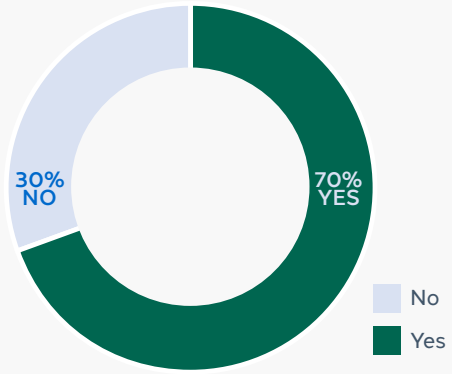
Employing lagging indicators, such as the length of remediation periods, implies that firms may only recognize suboptimal performance upon breaching established risk thresholds. This method of oversight could potentially expose organizations to heightened risks, calling into question whether current strategies effectively preempt compliance failures or merely respond to them.

Moving the Needle

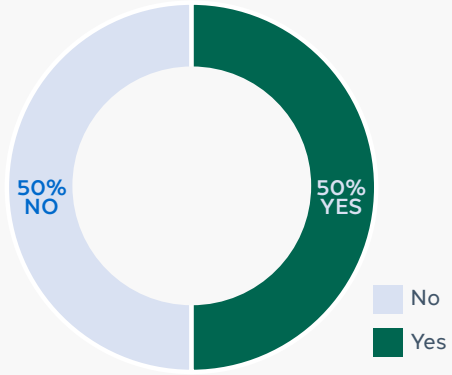
Firms should consider ways in which they can take a more proactive approach to compliance reviews, leveraging real-time data or forward-looking metrics to ensure they are improving their internal controls and processes by measuring their effectiveness before an incident occurs. Through the integration of technology, companies have the potential to monitor their risk exposure as a key performance indicator (KPI), ensuring it remains below a predefined threshold consistently;

- **Compliance training completion rates**
  Monitoring the percentage of employees who have completed mandatory compliance training within a given timeframe can be a lead indicator of a company's commitment to compliance culture.
- **Risk management software**
  Operational risk management software can help firms identify and assess their key operational risks. Such solutions enable leaders to conduct comprehensive risk assessments that take into account huge volumes of internal and external data and overlay advanced analytics to extract quantifiable insights in real-time. By analyzing data on risks, compliance, and performance, both across the organization and its third and fourth parties, these tools can help businesses make data-driven decisions that improve their operations and enhance their compliance.

DOES YOUR ORGANIZATION USE INTERNAL AUDITS AS A KPI?



DOES YOUR ORGANIZATION USE REMEDIATION DAYS RESULTS AS A KPI?



Enterprise Risk Management (ERM)

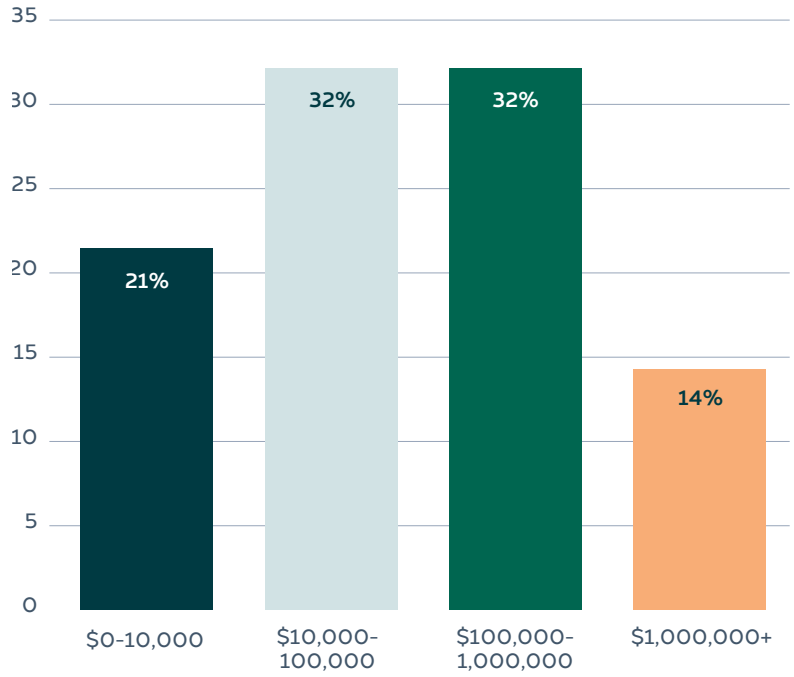
The subsequent section of this report examines the current state of firms' ERM programs, specifically amongst larger firms (>250 employees). Although the adoption of ERM practices by smaller firms can enhance their resilience, decision-making, and ability to achieve strategic objectives, ERM is a more embedded practice within larger firms, and there are several reasons why this is the case:

- **Complexity and scale of operations**
  Larger organizations typically have more complex operations and a wider geographic presence, which expose them to a broader spectrum of risks, including strategic, operational, financial, and compliance risks. ERM provides a structured framework to identify, assess, manage, and monitor these risks comprehensively.
- **Resource availability**
  Implementing an ERM framework requires significant resources, including technology, skilled personnel, and financial investment. Larger firms are more likely to have the necessary resources to establish and maintain an effective ERM program.
- **Stakeholder expectations**
  Shareholders, investors, and other stakeholders of larger firms have higher expectations regarding risk management. They demand transparency and assurance that the company is managing risks effectively. ERM enables firms to meet these expectations by providing a clear and comprehensive view of the organization's risk profile.

ERM Budgets

There is a significant variance of ERM budgets amongst larger firms. Most surprisingly, a portion of these businesses maintain extremely low capital allocation, with around 20% directing less than $10,000 annually. Given the size of these firms, such modest budgeting for ERM activities is surprising. This could be due to various reasons: ERM programs may still be maturing, firms might perceive their risk as low, or they may prioritize other investments. In any case, it's essential for companies to recognize the potential pitfalls of underinvestment in ERM. The following sections evaluate how this capital allocation translates to performance.

ERM BUDGETS FOR FIRMS WITH OVER 250 EMPLOYEES



Time Taken to Resolve Issues

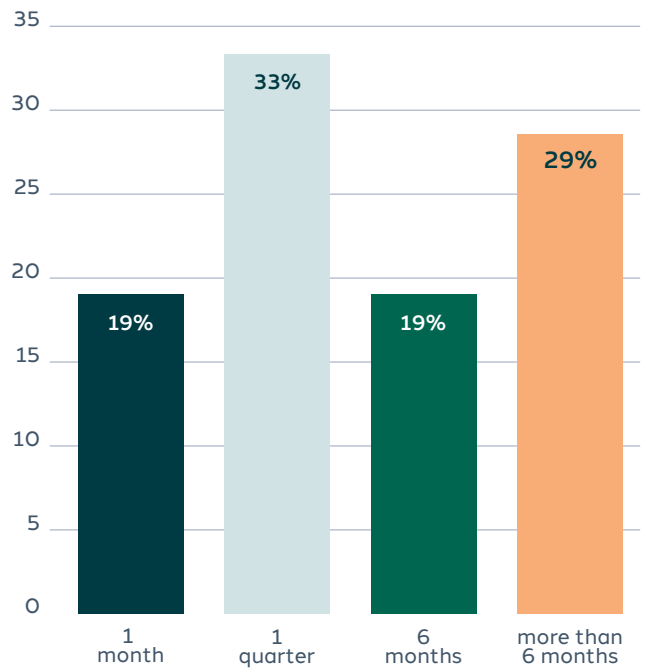
There is a significant variance in response times for large firms to respond to risk exceeding their defined appetite. The slight majority of respondents (33.3%) take circa one quarter to address such issues, which could be indicative of a systematic, and potentially automated, approach to risk resolution. However, we see nearly as many firms (28.57%) seemingly struggling to resolve any breaches of their risk tolerance within six months.

This variation may be influenced by a number of factors, from resource allocation, to automation and inherent risk exposure. Whatever the case may be, the data shows room for improvement for many, highlighting the need for a balanced investment in people, processes and technology to foster timely and effective risk management practices.

Taking more than six months to respond to issues that exceed the defined risk appetite can be problematic for firms for several reasons:

- **Increased exposure**
  The longer a risk remains unaddressed, the greater the potential for damage. These may include financial losses, reputational damage, and regulatory non-compliance penalties.
- **Stakeholder confidence**
  Investors, customers, and partners may lose confidence in a firm's ability to manage risk effectively if they perceive the firm as slow to react to significant risk events.
- **Resource strain**
  Prolonged issues can tie up resources for an extended period, preventing them from being used in other critical areas of the business.

TIME TAKEN TO RESPOND TO ISSUES



Evaluating the Correlation between ERM Budgets and Remediation Time

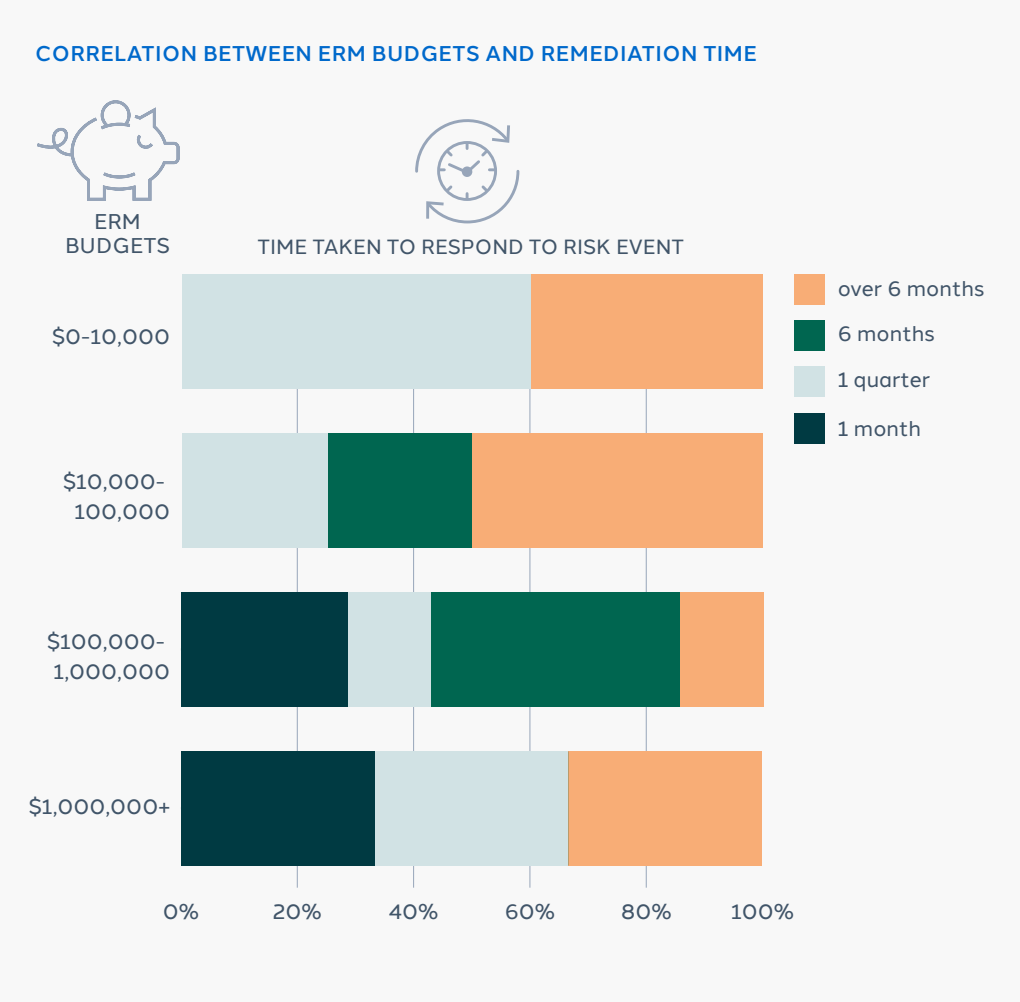
Although the data highlights a correlation between increased ERM spending and a reduction in remediation time, it is far from directly proportional. It is clear that higher ERM budgets do not necessarily correlate with quicker response times. In fact, firms with the most substantial budgets (over $1 million) exhibit an equal distribution across all timeframes for responding to risk events. This could indicate that while ample resources are available, the effectiveness of risk response may be influenced by other factors such as organizational agility, the complexity of decision-making processes, or perhaps the extent to which firms are leveraging technology.

The data does indicate a minimum threshold of expenditure required for firms to reduce their remediation time to one quarter. This may be due to the inherent investment required to procure, implement and maintain technological solutions – both those developed in-house or purchased from third-party vendors. However more research would need to be done to validate this hypothesis.

The data prompts a deeper inquiry into the qualitative aspects of risk management: Are firms with larger budgets investing effectively in proactive risk identification and management tools, or are they simply better cushioned to absorb the impact of risk events? And how do firms across the budget spectrum balance the scale of their ERM investments with the agility required for rapid response to emerging risks?

Identifying Areas for Improvement

The next section of the report explores the specific measures within firms which may highlight areas for improvement. In doing so, we aim to provide targeted data for organizations to explore where they may be able to direct investment to generate better returns on their ERM programs.



Defining Risk Appetites - Fail to Prepare, Prepare to Fail

A risk appetite statement does more than set benchmarks; it serves as an essential tool for decision-making, indicating when actions may be necessary to mitigate risks. Moreover, it acts as a vital communication mechanism, integrating the company's performance and commercial activities within a unified framework.

The findings reveal that 40% of large firms have not delineated a precise risk appetite. This omission can critically hinder an organization's capacity to pinpoint, evaluate, and strategically prioritize risks. Reflecting on the earlier chart, this absence of defined risk thresholds could offer insight into the observed inconsistencies in the returns on ERM investments across these organizations.

For many large organizations, particularly in highly regulated industries like finance, healthcare, and energy, establishing a risk appetite is not just strategic but also a regulatory expectation. Failure to define and communicate risk appetite to regulators, investors and broader stakeholder groups can lead to severe legal, financial and reputational ramifications.

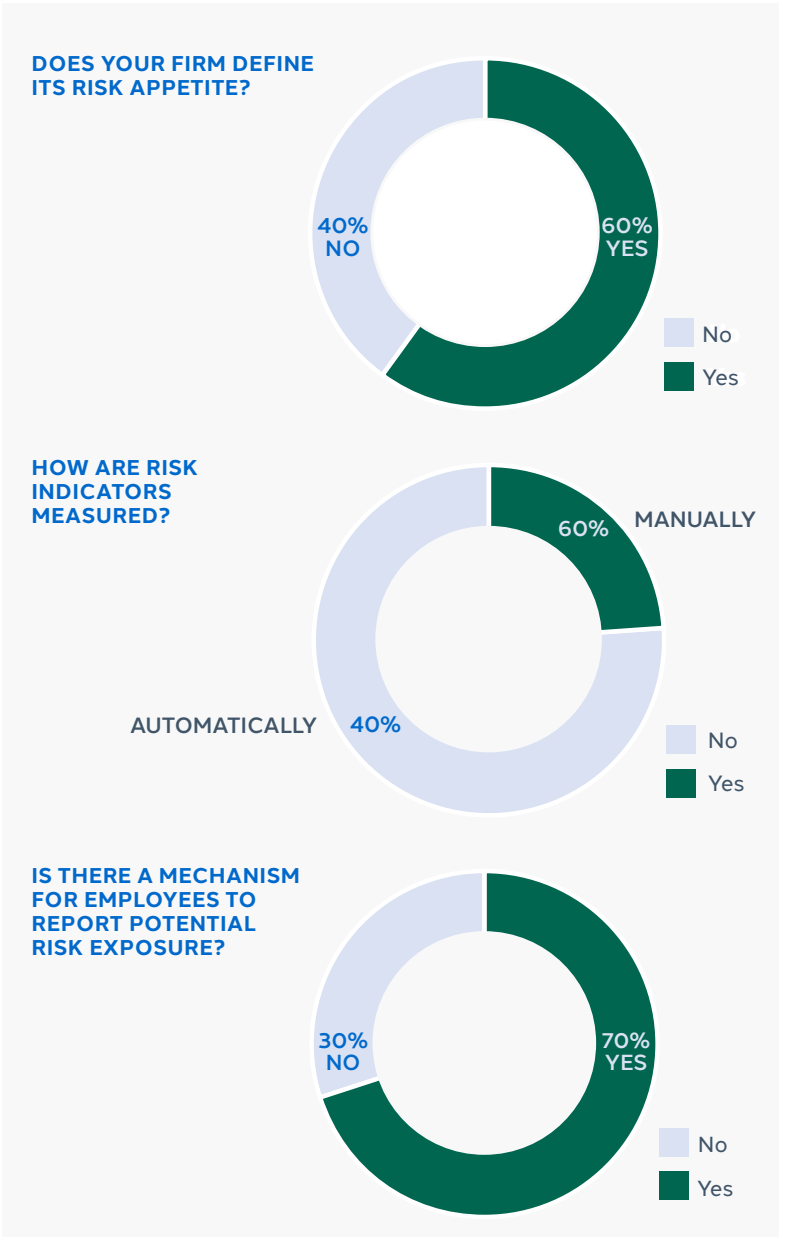
Measuring Key Risk Indicators

Given the earlier observations on the underutilization of automation tools in compliance functions, it is unsurprising that 76% of firms with over 250 employees still rely on manual methods to measure their key risk indicators (KRIs). These indicators encompass a broad range of data points, including technical failures, security incidents, customer attrition, and employee turnover, among others. The increase in risks naturally leads to a surge in data that needs to be monitored, measured, and analyzed. When these tasks are performed manually, firms expose themselves to significant vulnerabilities.

This reliance on manual processes for tracking KRIs likely contributes to the previously identified delay - often exceeding six months - in firms' responses to risks. The time gap between the occurrence of a risk event and its detection, compounded by the possibility of human error, underscores the inefficiencies of manual risk management. This situation highlights the critical need for enhanced automation in risk identification and management processes to mitigate vulnerabilities and accelerate response times.

Reporting Mechanisms

On the employee engagement front, 70% of these firms have implemented a reporting mechanism for employees to flag potential risk exposures. This is a positive sign that firms are encouraging a culture of risk awareness and open communication. However, the 30% without such mechanisms may be missing critical insights from their frontline staff, which can be essential in early risk identification and mitigation.



Risk Assessment Length

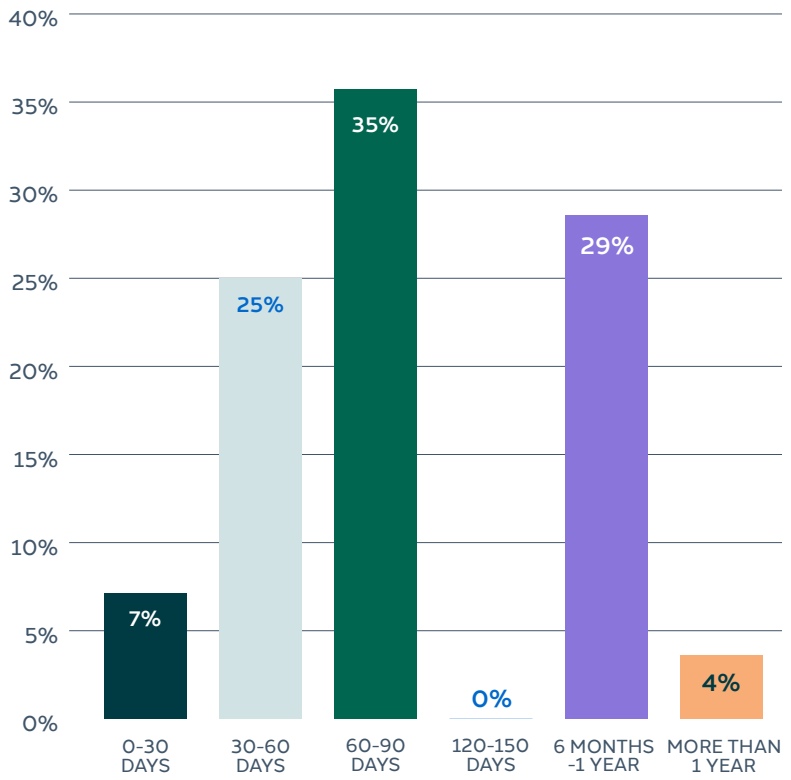
Conducting an enterprise-wide risk assessment requires the collective involvement of various stakeholder groups to identify critical services, map their dependencies and qualify and/or quantify associated risks. Regulators require such assessments to be reviewed on a regular basis, often annually.

The data points to a noteworthy 28.6% of firms taking six months to a year to conduct ERM risk assessments, and a further 3.6% taking more than a year. Taking six months to a year, or even more, to complete risk assessments can be problematic for firms, especially when periodic evaluations are needed annually.

The issue is twofold:

- **Rapidly evolving risks:** In a business landscape where risks evolve swiftly due to new technologies, market volatility, and geopolitical changes, a risk assessment process that spans several months may result in outdated findings by the time it is completed. Risks that were emerging at the start of the assessment could become pressing threats by its end, leaving the firm exposed and its risk mitigation strategies misaligned with the current risk profile.
- **Regulatory expectations:** Regulators often expect firms to have an up-to-date understanding of their risk environment and to be agile in their risk management practices. A prolonged assessment cycle could result in regulatory scrutiny if a firm cannot demonstrate that it is monitoring and mitigating risks effectively and continuously.

HOW LONG DOES IT TAKE TO COMPLETE RISK ASSESSMENT?



Conclusion and Next Steps

This year's GRC Compliance Benchmark Report, produced in partnership with The Hague University of Applied Sciences, Peter Konings of Johnson Controls, Thought Leader Global and SAI360, has afforded us an opportunity to conduct a systematic evaluation of the current compliance landscape, laying the groundwork to continue a more longitudinal analysis of trends over time.

The inaugural findings bring to light the persistently high costs associated with compliance, a perpetual challenge which ultimately stems from compounding regulatory and operational risks and widespread underutilization of technology across the spectrum of compliance activities. With that said, we saw a huge breadth of results, with some firms deploying capital far more efficiently and achieving admirable results. This highlights a burgeoning cohort of organizations that are strategically embracing technological advancements to refine and expedite compliance processes.

It's particularly encouraging to see such results amongst larger firms who have had a notoriously difficult time grappling with embedded legacy systems and manual processes. It's clear that a deepening financial commitment to ERM is not enough, rather, firms must carefully consider how and where money is spent to ensure they see a worthwhile return on investment in the long term.

By pivoting toward a more technology-driven approach, firms can optimize their compliance budgets and enhance their overall risk posture. This transition is not merely about cost savings; it's about enabling a proactive, dynamic approach to risk management that can provide a competitive edge in today's complex business environment.

As we look ahead, the message is clear: there is ample room for improvement, and the time for action is now. Firms that choose to invest in and prioritize GRC technology will likely find themselves leading the pack, armed with the agility and foresight to navigate the complexities of modern enterprise risk.

SAI360 RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.
Visit www.sai360.com.

154350 0424