ORACLE

2021 SURVEY

New benchmarks for security, risk, and audit

100% of respondents say they need to improve risk management and audit

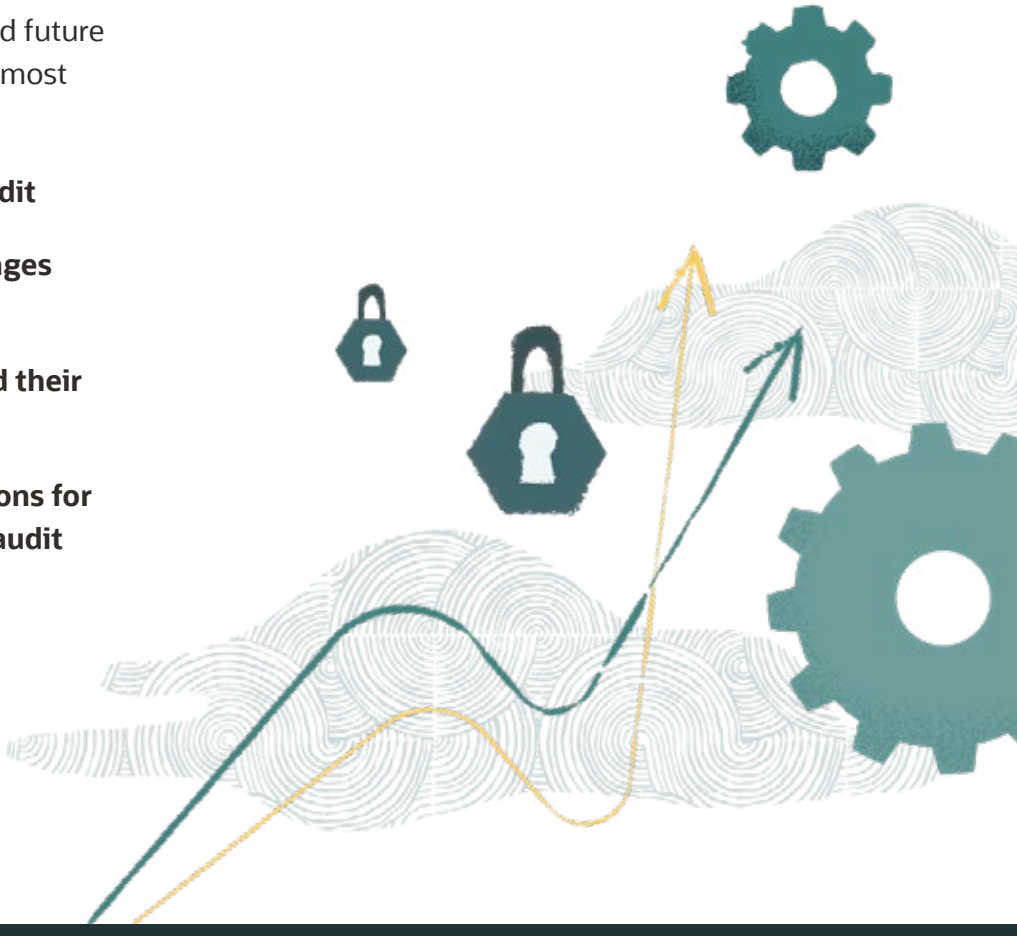
As the business landscape continues to redefine itself in a post-pandemic market, data is increasingly becoming an operating currency. On-premises systems for financial business processes, functions, and planning do not have the advanced technology, data processing power, and real-time access necessary to optimize this data and produce actionable, accurate results. This is particularly damaging when it comes to security, risk, and internal audit.

Oracle recently conducted a survey, in partnership with Aberdeen Research, to take an in-depth look at risk management and internal audit, including companies' strategies, technology solutions, and future plans. In this report, we'll share our most critical findings on:

- **The current state of internal audit**
- **Specific pain points and challenges within the audit process**
- **Technology solutions in use and their intrinsic benefits**
- **The use of modern cloud solutions for risk management and internal audit**

This survey looks specifically at the internal audit function because it has traditionally taken extensive time and resources to conduct—especially when manual processes are used to verify each transaction.

With the proliferation of data and cloud technology, organizations have a unique opportunity to turn internal audit into a security asset, helping to ensure the organization is not exposed to unnecessary risks including cyber threats, operational and fraud risks, and audit weaknesses.



About the survey

Audience

Aberdeen reached out to 212 global decision-makers at enterprise companies (defined as $500M in annual revenue and above), including: chief financial officers (CFOs), chief information security officers (CISOs), director level employees in finance and IT (security and control), and heads of digital transformation.

Key takeaways

Security, risk, and audit process maturity is tied to overall enterprise maturity.

There is a disconnect between C-level perspectives and views of other leaders with security, risk, and audit responsibilities.

Lack of executive sponsorship, expertise, and technology are preventing companies from modernizing their risk management operations.

80% **of respondents say security, risk, and audit processes are a top priority for their business**

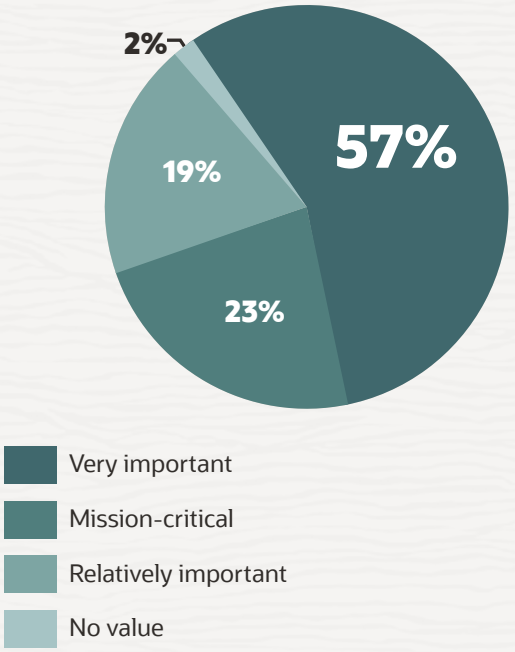
The state of internal audit

Across the board, companies are spending valuable time and effort on internal audits.

For most of these organizations, auditors are tasked with tracking down data in numerous places and verifying it against processed reports. The challenges of a post-pandemic, hybrid workplace have created a need for solutions to help employees across the enterprise share and access the same data seamlessly and support a remote workforce. Companies that can accomplish this quickly will be more agile and accurate in their audit processes. They can also enable finance to partner with internal audit teams to better understand how their risks are being managed. Internal audit becomes a valuable, connected part of risk management, providing increased transparency and confidence in how the business is truly functioning.

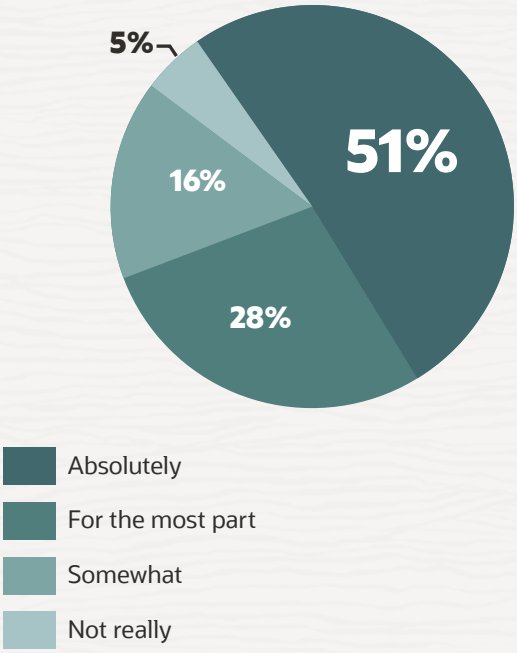
Our respondents had varied experiences and success—especially over the past year—with risk assessment operations and audit controls. Overall, respondents examined the current state of their internal audit, financial and security controls, and the relationship between relevant processes.

4 in 5 respondents believe their financial leaders strongly value risk, compliance, and audit processes



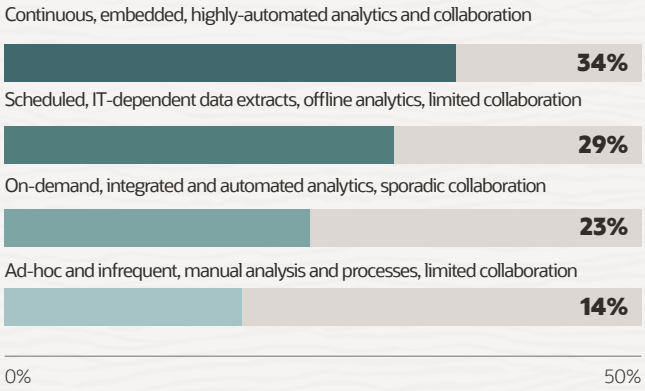
Question: To what degree do CFOs and other financial leaders at your organization value the risk, compliance, and audit processes as being a critical component of addressing overall governance and risk management?

100% of respondents say that their risk, compliance, and audit processes can be improved



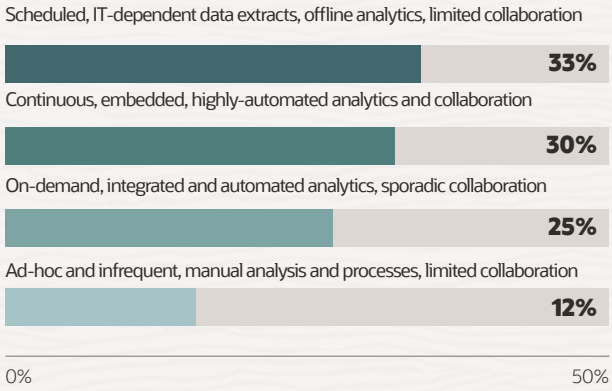
Question: Do you feel that your risk, compliance, and audit processes need to be improved in order to address critical risk management challenges?

Only 1 in 3 companies have continuous, embedded, highly-automated risk, compliance, and audit processes



Question: Which best describes your risk, compliance, and audit processes?

The maturity of internal controls varies from continuous and highly-automated to ad-hoc and manual



Question: Which best describes how data-driven and automated your internal controls are?

Top findings

Four out of five respondents think their financial leaders strongly value security, risk, and audit processes. Furthermore, 57% of respondents believe their leadership regards these processes as very important to the overall health of the organization. The correlation between security, risk, and audit processes is tied to overall organizational maturity (as defined by an organization's ability to immediately act on the data it receives).

79% **of our respondents—regardless of role—noted that improvement was considered either critical or among their organization's main priorities.**

C-level executives were more likely to view continuous audit process improvement as a top priority (61%). By way of comparison, only 42% of those outside the C-suite held a similar view that continuously improving risk management and audit programs was a top priority. There is a disconnect between C-level perspectives and views of other leaders with security, risk and audit responsibilities. Where the former sees a massive opportunity to grow in digital enterprise maturity, the latter group has run into a perceived lack of resources.

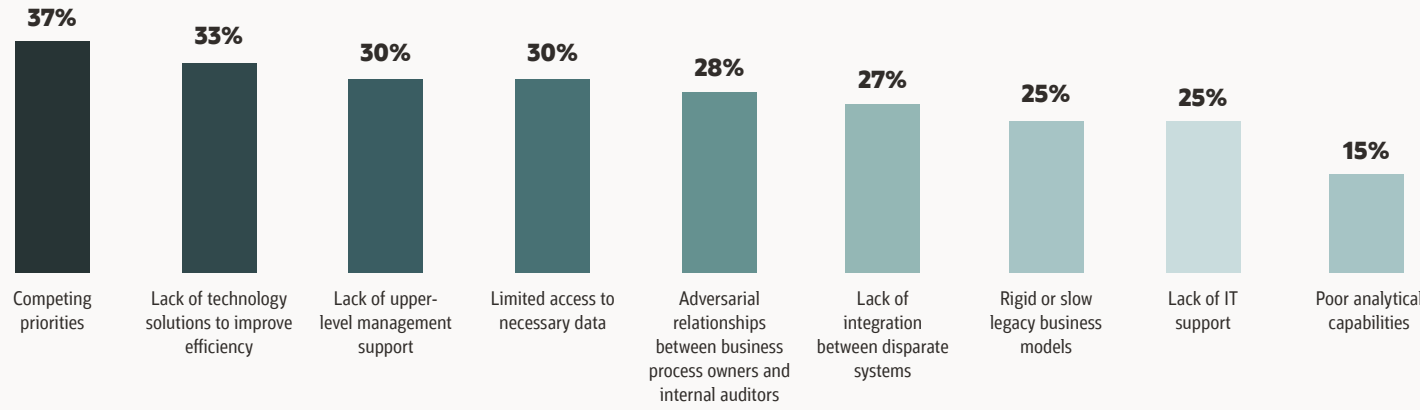
Only one in three companies have continuous, highly automated processes for audit and risk management. Companies further along in their digital transformation tended toward continuous embedded automation and process controls (30%). However, 33% of respondents cited IT-dependent data extracts and limited collaboration as roadblocks to automated, analytics-driven results.

Challenges within the internal audit process

What are the roadblocks to creating symbiotic priorities? As our survey uncovers, seamlessly integrating applications, functions, and people requires a one-stop solution. Security, risk, and audit functions are often spread across a variety of humans and applications, all with an eye toward greater collaboration internally.

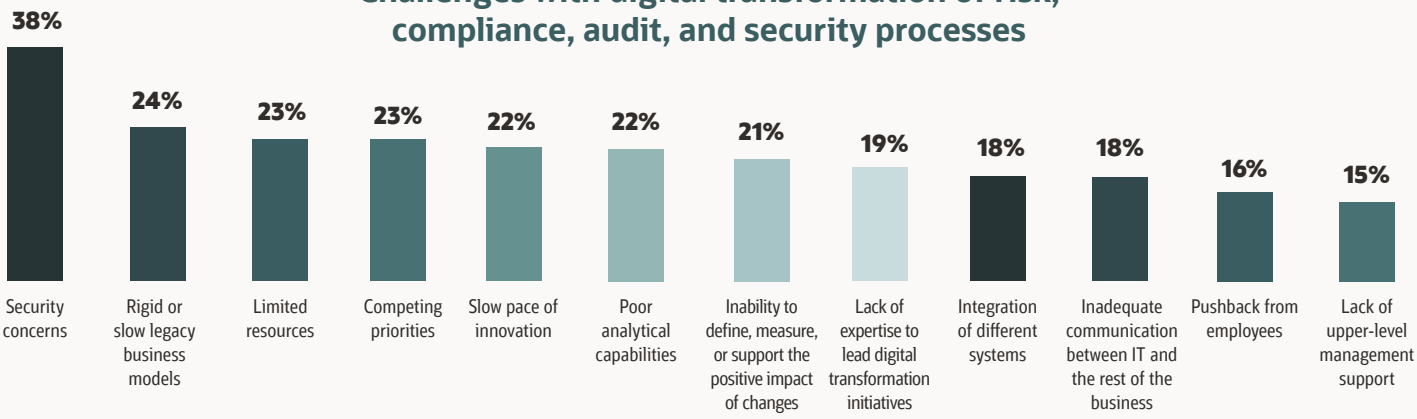
Integrating and embedding risk management within your critical enterprise resource planning (ERP) processes can help reduce roadblocks to your business goals and speed decision-making.

Risk, compliance, audit, and security process challenges



Question: What are the top three challenges your organization faces with managing your current risk, compliance, audit, and security processes?*

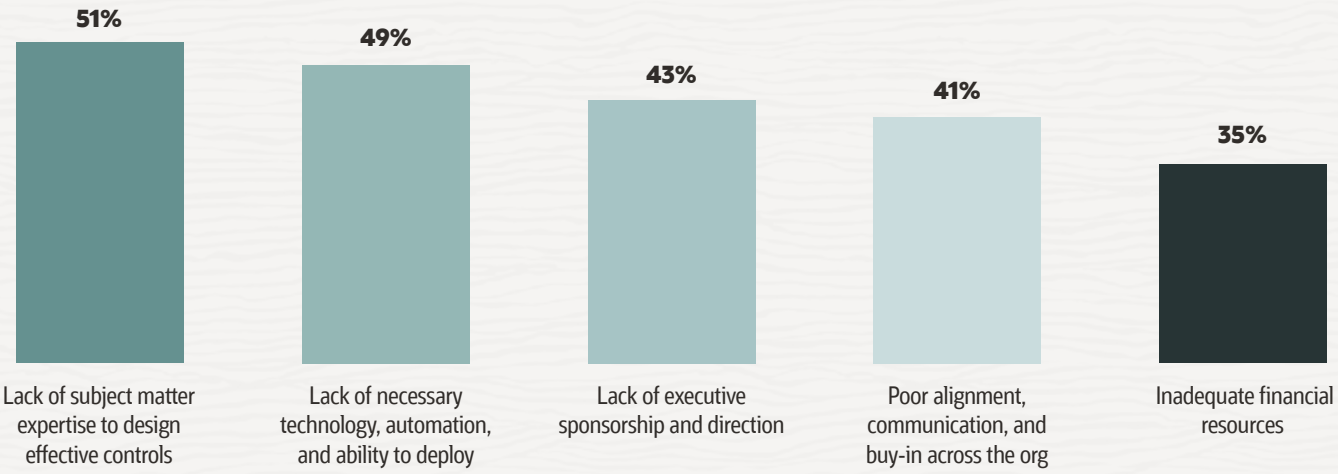
Challenges with digital transformation of risk, compliance, audit, and security processes



Question: What are the top three challenges your organization faces with digital transformation of risk, compliance, audit, and security processes?*

*percentage of respondents who rated each challenge as one of their top three

Barriers to establishing continuous improvement for risk, compliance, audit, and security processes



Question: What are the top three barriers preventing your organization from establishing continuous improvement for risk, compliance, audit, and security processes?*

*percentage of respondents who rated each challenge as one of their top three

Top findings

For risk processes overall, challenges include competing priorities (37%); lack of technology solutions to improve efficiency (33%); lack of upper-level management support (30%); and limited access to necessary data (30%). While these numbers may seem contrary to the broad C-level support noted in Section I, the responses show that there is an active disconnect between perceived priorities. Our research supports this as a potential pain point as fragmented organizations begin to resume hybridized models of working.

When it comes to digital transformation, the top two challenges cited—security concerns (38%) and rigid or slow legacy systems (24%)—validate the need for risk and audit solutions that handle multi-faceted operations, are embedded within business processes, and leverage a single source of data.

While limited budget, competing priorities, and slow pace of innovation all scored nearly identically as challenges, they are part and parcel of the larger challenge—lack of speed and technological resources.

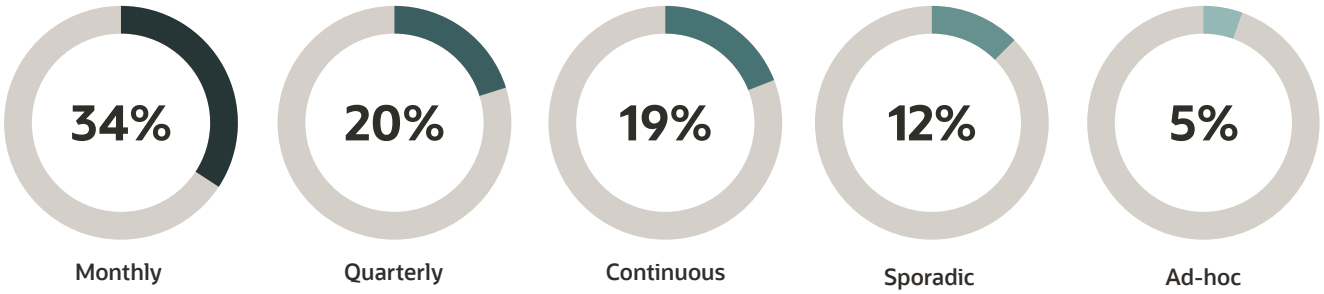
Interestingly, a lack of financial resources is not the largest roadblock to continuous improvement for our respondents, coming in at 35%. Larger concerns include a lack of subject matter expertise (51%), lack of necessary technology and automation (49%), lack of executive buy-in (43%), and poor communication across the organization (41%).

Technology adoption and performance

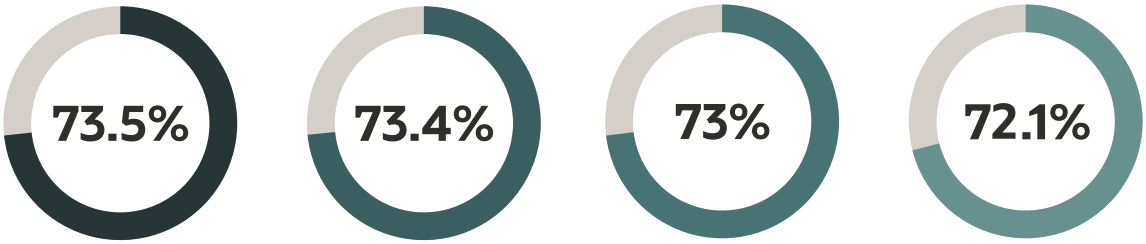
Fragmented workplaces are seeing potential solutions come and go without unifying under one system, causing great confusion and potential mistakes down the line.

Over the past 12-18 months, increasingly fragmented workplaces have led to increasingly fragmented processes, bringing with them a new set of organizational challenges. The problem boils down to confidence. More than ever, businesses are demanding cloud-based data and information tools to restore confidence in their financial numbers and overall outlook. Our research shows that many organizations feel they experience at least some reduction in efficiency due to not having the right technology in place. With that comes the ambivalence created by outdated information and slow reactions to market conditions.

Frequency of risks and controls analysis monitoring



Current performance in key compliance and risk management metrics*



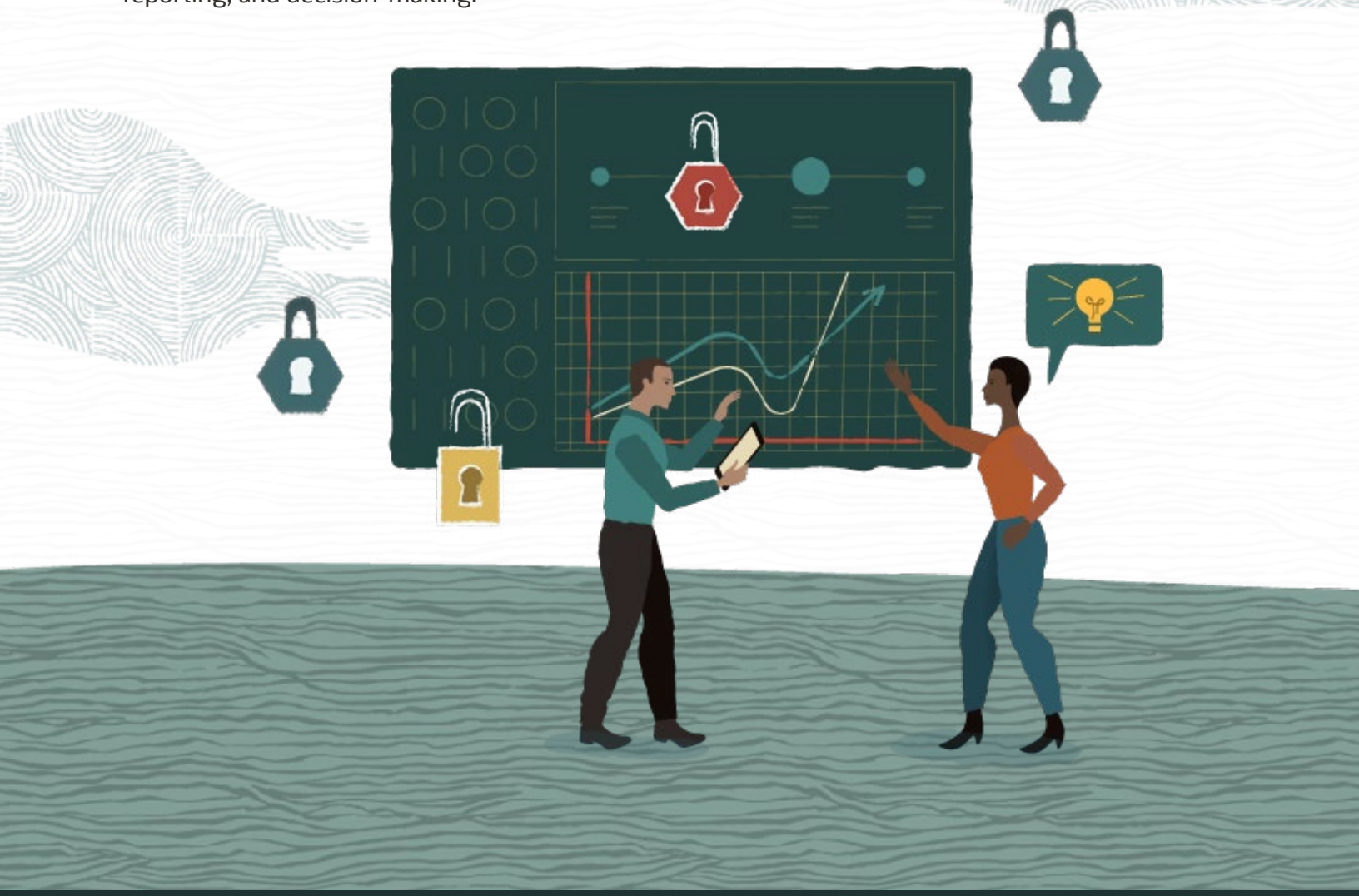
*weighted average

Top findings

One in five (19%) companies surveyed have continuous analysis monitoring for risks and controls. However, 34% of companies are monitoring risk on a monthly basis.

When it comes to performance in key compliance and risk management metrics, there is room for improvement. On average, nearly 25% of respondents' external financial reports are not on time or accurate.

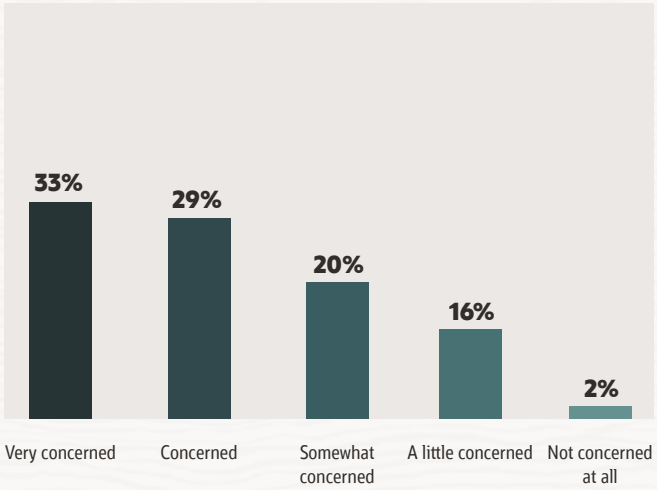
These findings underscore the need for improvement, revealing a lower-than-ideal rate of success in terms of output, compliance, reporting, and decision-making.



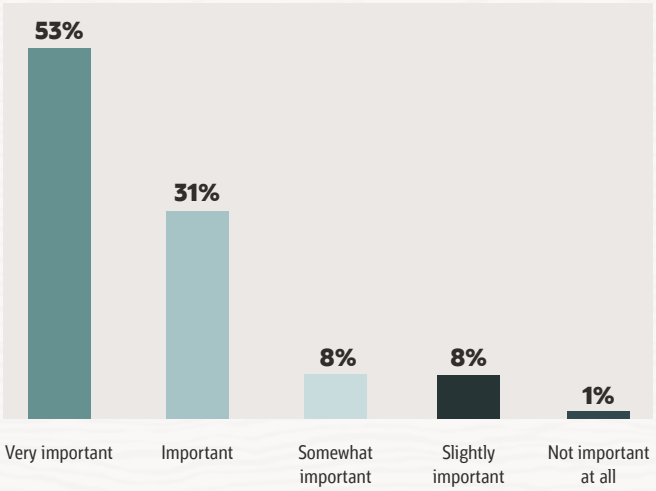
The modern approach to risk management

The ideal risk management framework embeds internal controls into critical ERP processes, and connects IT, finance, operations, and audit for collaboration and fast risk identification and remediation—all leveraging a single, shared source of data in the cloud. This framework promotes a comprehensive, enterprisewide view of risks, necessary for efficient risk-based decisions, fast response, and continuous compliance. Modern risk management also leverages advanced technology like AI to support real-time monitoring and analysis.

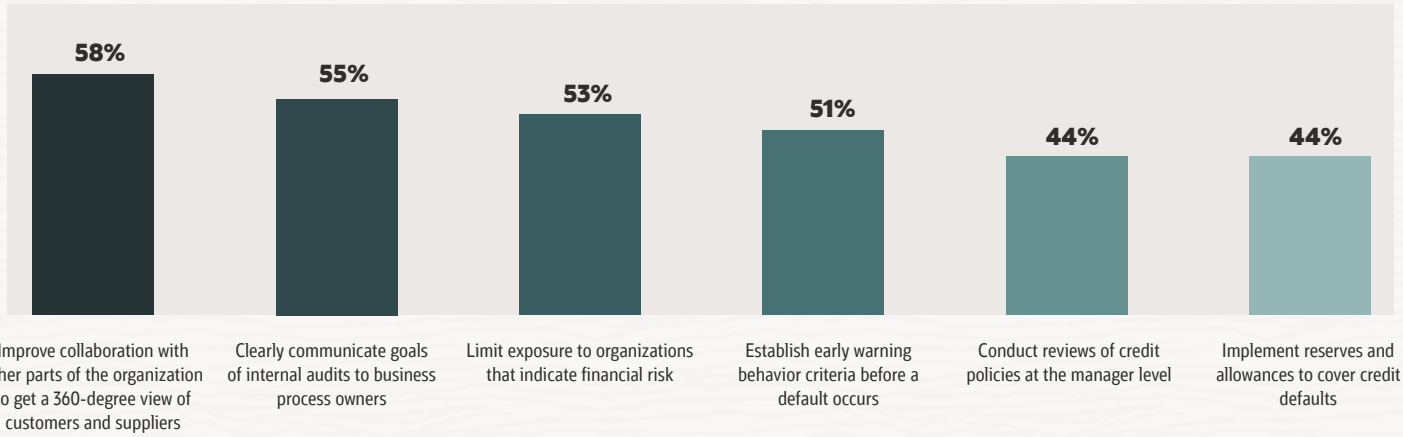
Level of concern about the growing complexity of risks coupled with degradation of internal controls



Importance of updating business continuity practices to avoid operational disruptions



Actions being taken to minimize cash leakage



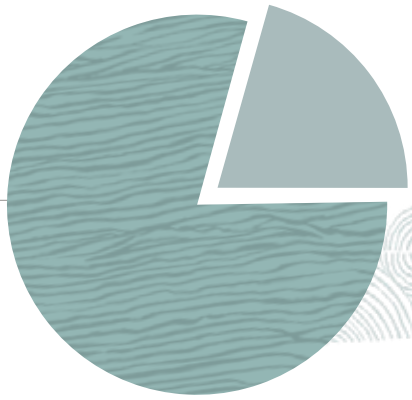
Top findings

Among the leaders we surveyed:

82% reported being at least somewhat concerned about growing risk complexity.

Across the board, however, anticipated risk complexity—and confidence in an organization's ability to handle that complexity—was directly proportional to overall maturity in digital adoption and risk management. Increased collaboration was cited as a proactive step for 58% of respondents, along with improving communication between both internal and external stakeholders at 55%. Other high-scoring actions included limiting exposure to risk and establishing early warning behavior in risk processing (53% and 51% respectively). This lends credence to the overarching issue of diminished collaboration and communication capabilities within these organizations.

84% of leaders see updated continuity practices as important.



There are many qualifications for a solid data integration strategy. Many applications solve a variety of problems at the issue level, but they fall short when it comes to enhancing the operations of an already remote workforce. Cloud-based ERP and embedded risk management eliminate the need for multiple systems across categories, featuring automatic separation of duties, compliance reporting, digitized user access workflows, continuous financial monitoring, and more. Better yet, a comprehensive repository of data reduces the number of hours spent on audits. The real bonus is that AI and machine learning monitor every transaction, alerting you to potential problems.

The future of internal audit

When determining what solution is right for your business, consider its ability to maintain consistency across the cloud to keep your organization and finance department aligned. At the forefront of that solution is a single source of truth, offering embedded security, risk, and audit controls within your business processes. Consistent risk management frameworks across your cloud applications can help you move faster and with better alignment.

Oracle Risk Management and Compliance was developed to address pain points felt by managers and executives around the globe. It includes transaction monitoring to strengthen financial controls and prevent fraud, a secure platform that remote workers can access with ease and minimal risk, streamlined workflows for a seamless audit, and secure asset management to ensure separation of duties (SOD).

Finance leaders are now looking ahead to make strategic decisions, with confidence, by managing risk and compliance with innovative technology such as AI and the cloud.

The future of audit is here. Read our finance starter kit to learn how to build a risk-intelligent culture.

Get starter kit

ORACLE