ORACLE

How CFOs can use audit to secure strategic outcomes and make big moves

Introduction

To compete in today's business environment, finance teams must continuously innovate and find new areas for growth. But making big, innovative moves is easier said than done when disruption and uncertainty challenge the integrity of financial processes and underlying operations. A rapidly expanding remote workforce adds to the complexity, amplifying existing vulnerabilities and introducing new risks.

Companies cannot move forward until they know what could potentially hold them back—and create significant damage down the road. "You can't be bold until you know what risks you're facing, and until you've found opportunities to mitigate them," said Amrita Ahuja, chief financial officer at Square. As a player in the digital payments industry, Square is focused on delivering new products and services to help businesses and individuals interact with their money.

Even the most agile, forward-thinking companies are challenged by the changing regulations and cyber-threats that can prevent digital transformation and growth. They move forward anyway—overcoming these challenges by taking a risk-based approach to decision-making and aligning their organizations around their enterprise risks.

This modern approach to risk management creates a risk-intelligent culture that gives company leaders like CFOs and their teams the confidence to make big moves without compromising security or the integrity of their financials.

Most companies, however, agree that they are not doing enough when it comes to modernizing risk management. In a [2021 survey](#) of finance and security executives from Aberdeen Research:

100% of respondents admitted that their security, risk, and audit processes could be improved.

And although 79% of respondents believe that improving these processes is important, the survey revealed key challenges such as competing business processes and a lack of efficient technology solutions.

So what does modern risk management look like? Security, risk, and audit controls are embedded in critical enterprise resource planning (ERP) processes, connecting IT, finance, operations, and audit teams so they can support ongoing change while maintaining control. This enables a continuous, collaborative cycle for risk prevention and response.

> "You can't be bold until you know what risks you're facing, and until you've found opportunities to mitigate them."
>
> **Amrita Ahuja**
> CHIEF FINANCIAL OFFICER, SQUARE

Watch the video: See the big moves Square is making in the global payments industry (8:15)

Making audit more efficient and effective to take on the unknown

Internal audit has always been critical in helping organizations manage their risk frameworks to protect their assets, reputation, and financial integrity. A big move can produce non-compliance risks that can lead to substantial fines, or damage a company's brand. Increasing public and regulatory scrutiny make internal audits all the more important.

Helping organizations meet their strategic priorities or undertake a big move in a complex business environment with ever-changing regulatory mandates, however, requires a fundamental shift in how internal audits are conducted.

Efficient financial audits automate manual, labor-intensive tasks so internal audit teams can spend more time on value-add activities like analyzing and helping to prevent risk. Automation and digitization of the audit function is integral for efficiency, but in order for audits to also be effective, companies must use:

- Embedded risk intelligence in critical business processes
- AI and machine learning (advanced analytics) for real-time continuous monitoring and analysis
- A single source of enterprise truth through a shared data repository

These tools help match controls to risks so finance and audit can refine and improve them. A continuous cycle of refinement driven by audit helps companies to continually improve. Internal audit can help reduce risks and improve controls—resulting in cost and risk management benefits across the enterprise. Audits become data-centric, accelerated, and collaborative—rather than adversarial —helping the business to identify and mitigate risks, and respond to evolving regulations, markets, and business models. The outcome is transformative: proactive risk management, stronger controls, and a more secure enterprise.

This approach to audit is scalable; as the business grows, the need for additional audit resources is minimal, and existing resources can continue to focus on more strategic work. It also supports digitized, virtual, self-service audits by external auditors, streamlining the process, reducing costs, and ensuring appropriate access. Automation eliminates duplicate audit activities and reduces the need for requests for information and clarifications. Business process owners and auditors can work in parallel, reducing audit cycle times. And, with a single source of data, internal and external auditors work off of the same data—increasing integrity and quality.

Such was the case for Skechers. As the company experienced rapid growth—going from a $815M US company to a $4.5B global enterprise—its Vice President of Internal Audit, Ashwat Panchal, was able to not only save employees valuable time (and the company money) while ensuring localized compliance, but he accomplished this with an increase in internal audit headcount of only two employees.

Watch the video:
See how Skechers transformed internal audit (1:35)

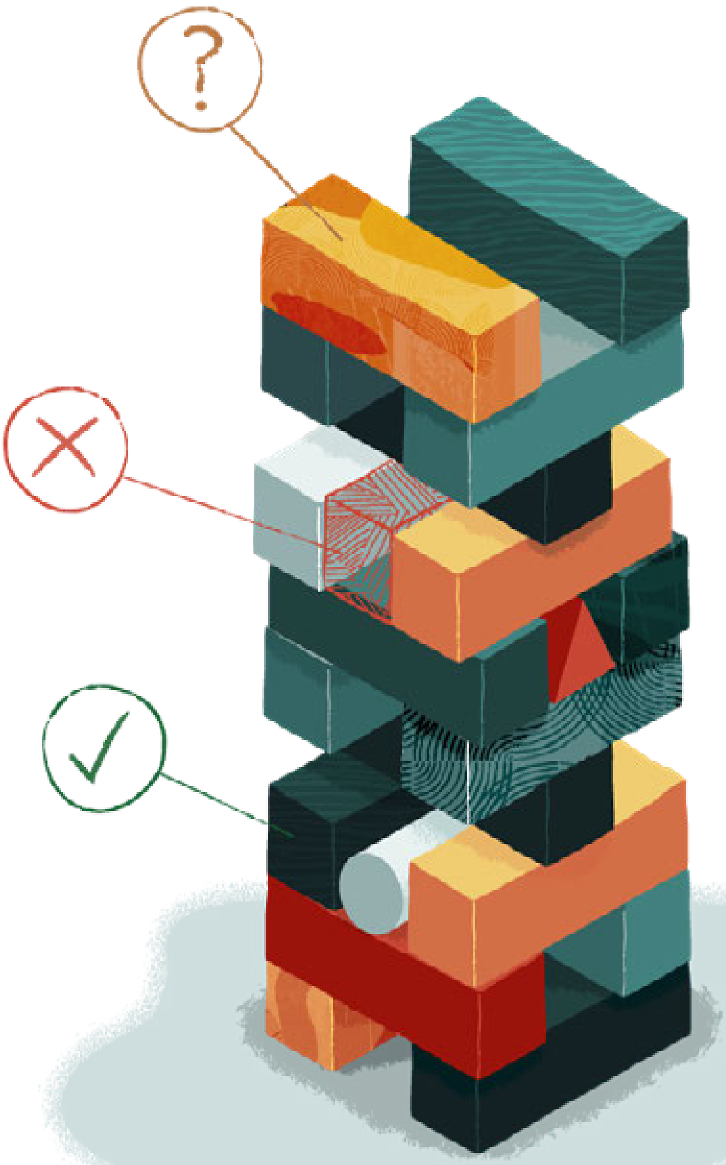
"Six people for a $4.5B company! Without a standardized audit program and a compliance solution agile enough to handle ever-changing, and worldwide, regulatory requirements, I would have to spend 75% of my time on a plane, which would severely impact productivity," said Panchal. His team uses [Oracle Fusion Cloud Risk Management and Compliance] to help mitigate risks across the business.

Avoid growth roadblocks with the right security, risk, and audit controls

When innovative organizations look to make a big move they can use risk management as an advantage—but only when it's coupled with the right controls. Automation of security, risk, and audit controls plays an important role in efficient risk management, but automation alone doesn't ensure the effectiveness of a control. With the right controls, the risk of fraudulent activity, inappropriate access, and a lack of a holistic view of enterprise risk are no longer roadblocks to growth. Controls that are not only real-time and continuous, but predictive in nature, provide organizations with the confidence to seize opportunities to innovate.

When these controls are embedded in ERP business processes, organizations can obtain an enterprisewide view of risks and align their organization around prevention. Controls are no longer manual and periodic, but automated and continuous. This helps drive confident, risk-based decisions.

And, strong internal controls let organizations scale without the need for significant investment. Organizations maximize their ability to future-proof against ever-changing risks, security threats, and mandates (ICFR, GDPR, CCPA, etc.). Ineffective and inefficient controls cannot meet the demands of global, regulatory, or organizational change. This is a growing challenge.



More than half of those surveyed by Aberdeen said they are concerned or very concerned about the growing complexity of risk, coupled with the degradation of internal controls.

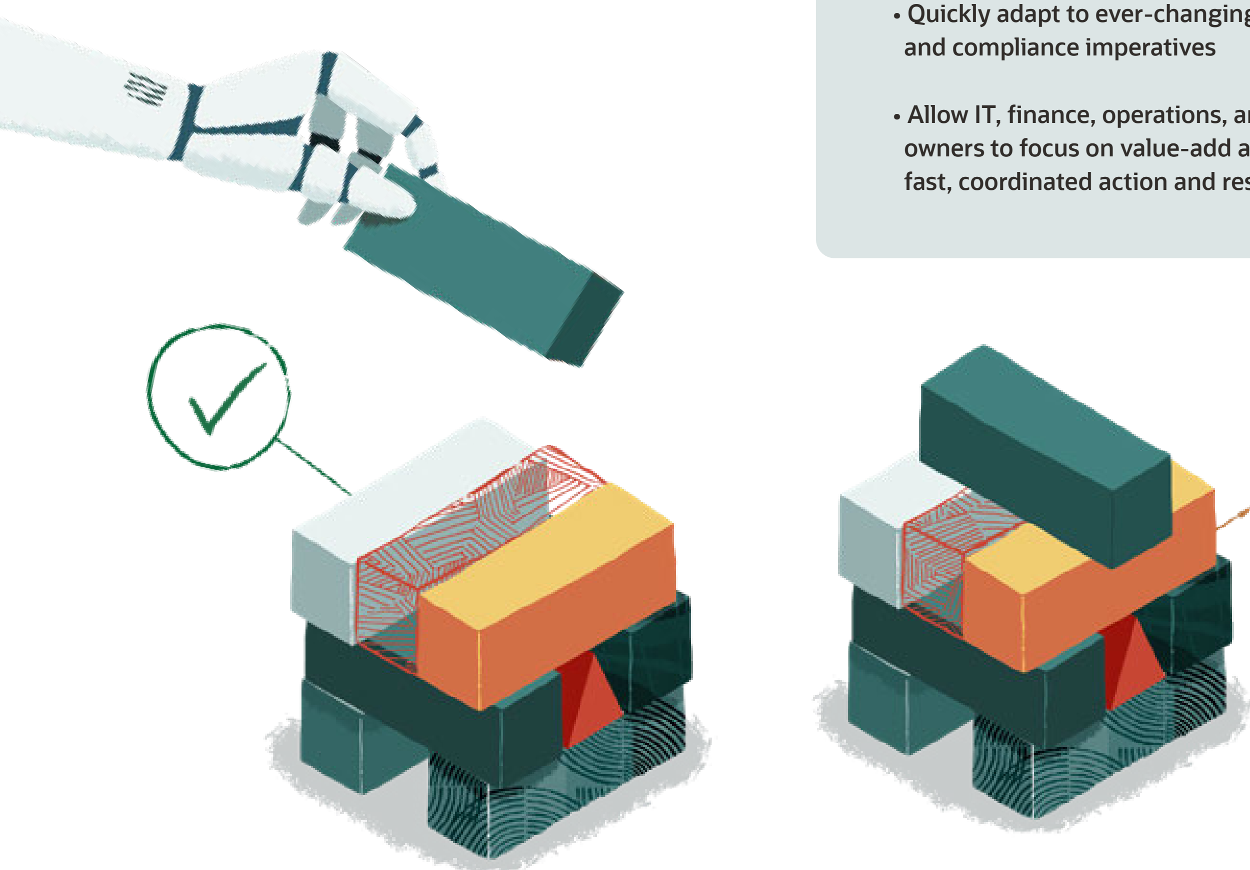
Drive continuous control monitoring and analysis with the power of AI

Today's companies create massive amounts of data. How do you analyze all of this data, especially when companies need to continually monitor their security, risk, and audit data—controlling who can get into their systems and what they can do once they're in? They need to do this at a granular level—something that can only be achieved with artificial intelligence (AI).

Without the advantages of AI-driven continuous monitoring and analysis, security, risk and audit functions become over-extended, increasing the chances of mistakes, making it difficult to use the data to help drive risk-based actions or decisions that can impact business. This cycle influences an organization's appetite for undertaking big moves due to an erosion of trust and confidence. It not only impedes transformation progress but also leaves potentially huge gaps in security; this is a problem for the four out of five companies surveyed by Aberdeen that don't have continuous analysis monitoring for risks and controls.

AI-driven, continuous security and audit monitoring and analysis helps companies:

- Reduce the risk of fraud, error and policy violations, and cash leaks
- Enforce separation of duties (SOD) and prevent external audit failures
- Achieve faster audit cycles and financial reporting
- Prevent unauthorized access to critical ERP processes and sensitive data
- Audit 100% of ERP transactions and configurations
- Quickly adapt to ever-changing security, regulatory, and compliance imperatives
- Allow IT, finance, operations, and audit control owners to focus on value-add activities, and drive fast, coordinated action and response



Rely on a single source of truth for confidence in financial reporting

As data environments become increasingly more complex with massive amounts of data to secure and analyze, the value of data and its reliability, quality, and timeliness of access severely impacts an organization's ability to confidently make the right business decisions. As this data feeds into financial reports, it can ultimately lead to an erosion of trust in financial reporting.

With a centralized risk repository, organizations can implement a scalable, centralized approach to risk management across their enterprise that supports collaboration and information sharing among control owners and governance teams. All risks, policies, and controls are documented in a single risk repository, with separate access for auditors. IT, finance, operations, and audit can add value to the continuous assessment of controls through monitoring, testing, re-evaluation, and certification. Security, risk, and audit no longer act as disconnected teams, all making critical decisions based on data that can be inconsistent, unreliable, and outdated.

For many organizations, data accumulation is very costly when data is stored in disconnected solutions. As organizations become more exposed to regulatory, ethical, and data security risks, bolt-on solutions can compromise data integrity and create lag times in identifying potentially damaging situations. Results can be catastrophic to financial solvency. And, as the collection of sensitive data becomes more prolific, these solutions also increase the potential for data leaks, resulting in significant fines and public scrutiny that can negatively impact brand and reputation.

For external audit, more data means an increase in scrutiny and documentation to support the data. When external auditors are given controlled access to the same, single data source as finance, operations, IT, and internal audit, their roles become more streamlined, more efficient, and less costly. And, transparency is increased, improving an organization's auditability.

A single source of data helps ensure the integrity and quality of audit. Audit cycle times are reduced as business process owners and auditors can work in parallel.

Despite all of these benefits, Aberdeen research revealed that most companies only provide read-only access of manual processes for external auditors to gather information.

Build a risk-intelligent culture: The framework for modern audit

By championing a risk-intelligent culture, companies aim for real-time, preventative risk management by engaging the organization in analyzing risk.

In order to accomplish this, organizations must pivot from a legacy approach that is task-focused with disconnected security, risk, and audit functions, to a risk-based approach that connects the enterprise around the most critical risks. When ***risks can be connected to strategic business outcomes***, companies can make better business decisions.

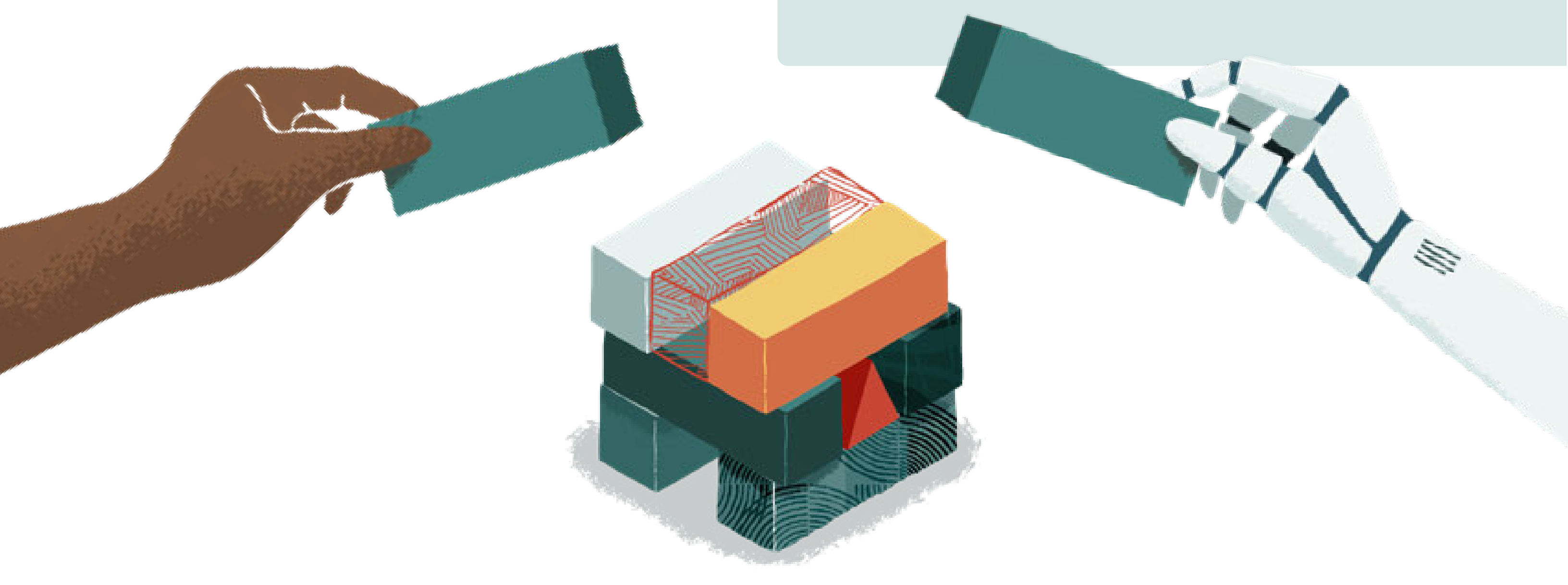
> "An organization that doesn't have a risk framework is going to be reactive. It's going to be their day job."

Rich Christensen
CHIEF ACCOUNTING OFFICER, TRUEBLUE, INC.

Watch the video:
Hear TrueBlue's story (2:56)

7 requirements for modern audit

1. Risk-intelligent culture
2. Embedded risk management in critical ERP processes
3. Continuous monitoring and analysis of security, audit, transaction, and configuration data
4. Automated security, risk, and audit functions
5. Single source of data/truth
6. Single control framework connecting IT, finance, operations, and audit
7. Collaboration through workflows and connected risk functions



How do you get started?

We've created a starter kit for CFOs and other finance leaders looking to build a risk-intelligent culture. It outlines five best practices for risk management and provides the steps to get started using audit to secure strategic outcomes and make big moves.

Read the starter kit