Deloitte.

Internal Audit Hot Topics

2024

Internal Audit Hot Topics:

2024 Risks and Opportunities

- Vision and purpose
- Enterprise trust
- Resilience
- Disruptive technology
- Building a digital backbone
- Controls modernization
- Environmental, Social, and Governance (ESG)
- Human capital management

Source: https://kx.deloitte/documents/view/83303

Internal audit's role in

Vision and purpose

Our view

Resilience and value are not created by accident. Many of the companies that have successfully weathered the storm over the last few years and have come out stronger on the other side have done so—on purpose. A significant body of evidence shows that an integrated purpose strategy can provide organizations with a "purpose premium," driving long-term value and creating competitive advantage. Among other benefits, leading with purpose can deliver new revenue streams, faster growth, and an enhanced ability to attract and retain talent.

While most often considered in the context of the broader organization, the idea of a "purpose premium" also applies to the internal audit function. Internal Audit 4.0, Deloitte's market-leading framework for helping internal audit functions set their stretch targets, envisions the future function to be purpose-driven and digitally powered. That is because internal audit has a largely untapped opportunity to accelerate engagement around purpose.

By aligning its role and remit with the organization's purpose, internal audit can maximize its impact by working in a more intentional way to support specific, purpose-driven, organizational outcomes; attracting top talent, who, research has shown, would prefer to work for purpose-driven organizations and teams; and ensuring innovation efforts are purpose-driven.

The path to becoming purpose-driven starts with a single step. Whether its saving money for customers, improving health and well-being, creating a sustainable future, or some other noble goal, every organization, every function, and every person has a purpose. Can you articulate yours?

Source: https://kx.deloitte/documents/view/83303

Data points

Companies anticipate a wide range of benefits from being more purpose-driven in relation to sustainability, with the following business outcomes ranking among their Top 3 responses: talent attraction and retention (52%), gains in efficiencies (52%), enhanced trust with stakeholders (51%), brand/reputation enhancement (49%), and risk reduction (48%).

News item

Recently, the Institute of Internal Auditors (IIA) recognized purpose as part of its international professional practices framework (IPPF). As part of a multi-year refresh project, the content from six elements of the IIA's current IPPF (Mission, Definition, Code of Ethics, Core Principles, Standards, and Implementation Guides) has been incorporated into a draft of the proposed Global Internal Audit Standards™ and organized into five domains that more clearly indicate key roles and responsibilities. One of those domains is the Purpose of Internal Auditing, which emphasizes elements of the current definition and mission of internal audit.

Warning signs

Necessary evil: If internal audit is widely perceived as an unpleasant policing function, then it probably has failed to articulate its purpose or value to the broader organization clearly.

Revolving door: High turnover or lack of employee engagement within internal audit can be a sign that leaders are not articulating and communicating the function's purpose to their own teams.

Follow the leader: It is easy for internal audit to fall into a routine of following the same working practices that everybody else uses. If your internal audit function is no different than any other in the industry, then it may be missing an opportunity to maximize its impact with purpose.

Stuck on status quo: Ways of working need to be intentional in order for internal audit to make a purpose-driven impact in the context of the broader organization's purpose. Value does not happen by accident. It is designed.

Getting the fundamentals right

Start at home: Articulate internal audit's purpose and the value the function delivers to stakeholders in the context of the broader organization's purpose. This is the top-down force that shapes everything internal audit does, including how it works and where it invests to innovate.

Plan with purpose: Identify risks to achieving the organization's purpose and incorporate them into the internal audit plan.

Walk the talk: Consider how the internal audit function can support the broader purpose of the organization. For instance, if the broader purpose is sustainability-related, internal audit could think about reducing its emissions footprint by traveling less.

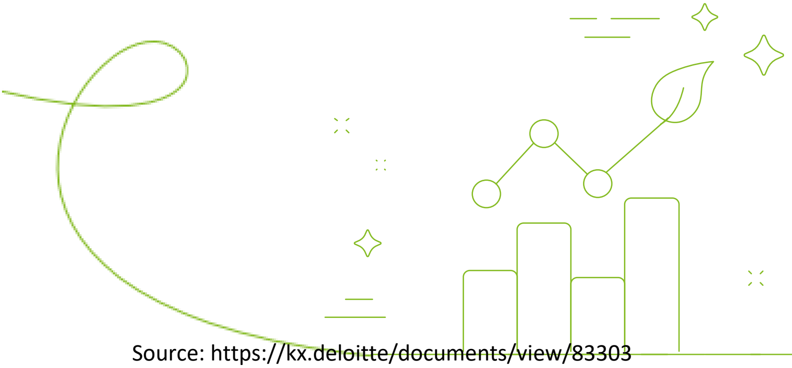
Taking the next steps

Align and refine: Make sure the three lines are aligned around purpose, clarifying roles and responsibilities where necessary.

Form an opinion: Develop a point of view about whether the organization is achieving its purpose and identify any behaviors or communications that contradict the organization's purpose statement.

Mind the gap: Develop recommendations to close the gap between leadership and employee perceptions around the organization's purpose.

Envision the possibilities: Consider the attributes of a future internal audit function that is living and delivering on the organization's broader purpose as well as its own.



Source: https://kx.deloitte/documents/view/83303

Internal audit’s role in

Enterprise trust

Our view

Trust is to an organization like electrolytes are to an athlete. Without it, an organization will struggle to compete. Leaders increasingly grasp this concept. Recent Deloitte research indicates 94% of boards believe building trust is important to the organization’s performance and highly trusted companies outperform low trust companies with up to 4X amplification of market value.

But what exactly is trust? At its core, trust is the foundation of a meaningful relationship between an entity and its stakeholders at both individual and organizational levels. Trust is built through actions that demonstrate a high degree of *competence* and the right *intent*. Often seen as a nebulous concept, trust actually can be defined, quantified, measured, and intentionally cultivated both as means of enhancing performance and mitigating risk. Deloitte, for instance, has identified 18 domains and 90+ drivers for measuring trust.

Simply put, stakeholders today expect organizations to do the right things and to do them well. These expectations run the gamut, from safeguarding customers’ private data to taking a strong stance on environmental, social, and governance (ESG) issues; and from providing safe working conditions to being transparent about vulnerabilities and risks. Meeting these stakeholder expectations consistently—by displaying capability, reliability, transparency, and humanity—engenders trust. Failing to meet them poses risks to the organization. Like any other performance-related attribute, trust indicators need to be monitored for gaps, analyzed for risks and opportunities, and ultimately assured. Considering these factors, along with its broad enterprise view, internal audit is a natural fit for advising on trust and accelerating a trust agenda.

Source: https://kx.deloitte/documents/view/83303

Data points

- Organizations impacted by trust events fall **26-74%** behind industry peers in value and their market cap falls by **20-56%.**
- 79% of employees who highly trust their employer feel motivated to work.
- Out of customers who highly trust a brand, **88%** bought again and **62%** buy almost exclusively from that brand.

News item

According to the Edelman Trust Barometer, businesses and governments have historically low levels of trust, creating new opportunities to gain competitive advantage for those who can reverse this trend. With new data at its core, The Four Factors of Trust gives practical guidance to measure and build trust in critical stakeholder relationships. Trust ultimately comes down to just Four Factors that make up Deloitte’s HX TrustID™.

Warning signs

Free to be me: Psychological safety—the freedom to be oneself or to raise issues without threat of retaliation—must be present in order to build trust. Yet, this component is lacking in many organizations due to organizational culture, leadership structures, and the personalities involved.

Not my problem: If you do not see clear lines of ownership or accountability for trust, the organization is unprepared to build it.

Blind eye: Ignoring issues surfaced through customer and employee surveys is a quick way to lose trust.

Crisis mode: If leaders take a defensive stance when something goes awry, they do not see trust as a proactive strategy to avert or diffuse a crisis.

Getting the fundamentals right

Start the dialogue: Affirm trust measurement as a strategic priority and a key tenant of organizational culture.

Find meaning: Define trust within the enterprise and industry context. What will we measure? How do we bring it to life? Whose trust matters? Which areas of the organization are at risk for losing trust?

Work it: Embed trust throughout internal audit's ways of working—in hindsight, insight, and foresight.

Do not rush: Trust must be built consistently over time. Exploring, diagnosing, prioritizing, and acting on trust should become part of the DNA of every organization embedded in how a company operates, rather than a one-time exercise.

Taking the next steps

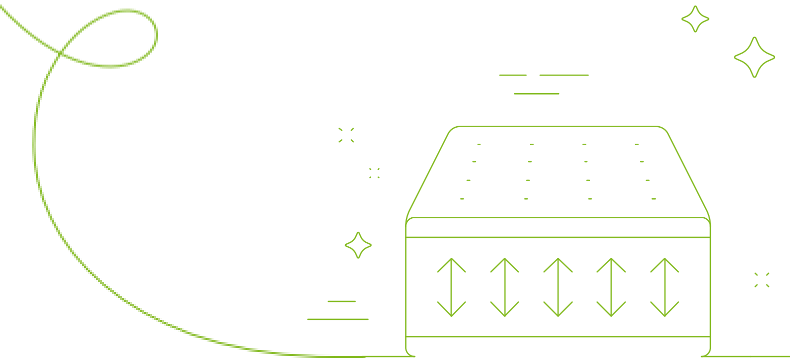
Plan ahead: Strategize on how to engage on trust throughout the risk assessment. Determine how to report effectively on trust and related trends.

Measure up: Make trust measurement a strategic priority within your internal audit plan, supported by a structured framework to quantify trust across your internal audit services: assure, advise, anticipate, and accelerate.

Set the stage: Assess trust through standalone internal audit reviews at points in time, or through an integrated audit approach.

Read the room: Leverage internal questionnaires and external sensing to enrich your understanding of trust across different stakeholder groups, including employees, customers, suppliers/partners, and/or investors.

Source: https://kx.deloitte/documents/view/83303



Internal audit's role in
Resilience

Our view

Since the 1970s, the lean philosophy has dominated a great deal of corporate thinking. While the idea of creating needed value with fewer resources and less waste has been a boon for efficiency and cost optimization, it has largely been a detriment to resilience. The COVID-19 pandemic exposed the downside of costing out diversity and redundancy in the relentless pursuit of efficiency. After experiencing critical supply shortages, resilience was suddenly on the tip of everyone's tongues and at the top of many priority lists.

Despite the renewed emphasis, many organizations are no more resilient today than they were in 2020. The reasons for this are many, but they all boil down to a fundamental misunderstanding. Unlike business continuity, disaster recovery, or information security, resilience is not a risk-and-control discipline: It is an outcome of executing risk-and-control disciplines well and in concert with one another.

Resilience does not happen by accident. It requires alignment of language, definitions, and goals. Without that alignment, organizations can find themselves peddling hard but going nowhere fast. Internal audit can help organizations shift into gear by asking:

- What do you want to make resilient? The "what" can be products, services, benefits, processes, facilities, and more. No organization can make everything everywhere resilient all at once. Instead, it needs to identify the "essential outcome" it provides, i.e., things that in absentia would cause harm, rather than inconvenience, to stakeholders.
- How resilient are these things today? Many companies still have significant points of exposure within their supply chains, technologies, and third-party providers. Internal audit can help senior leadership to dig in and understand where the ticking time bombs are within the business architecture.
- How resilient do you want them to be? No impact is unrealistic in a severe disruption, but by better understanding how much impact the organization is willing to tolerate, you can make better choices before, during and after disruption. Internal audit can help the organization to determine its impact tolerance, which in turn can inform investment decisions about how much resilience to build.

Source: https://kx.deloitte/documents/view/83303

Data points

52%

of surveyed senior executives say there is a common understanding/definition of resilience within their organizations.

67%

of surveyed senior leaders say resilience in their organizations has been impacted by regulatory change.

59%

The three most cited barriers to achieving greater resilience were scarcity of talent (59%), closely followed by competing strategic priorities and lack of organizational understanding of resilience (tied at 57%).

News item

The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025. DORA seeks to unify the approach of financial entities towards Information Communications Technologies (ICT) risk management, to streamline previous ICT regulations, with the overarching goal of strengthening the operational resilience of the financial services sector in Europe.

Through the EU Critical Entities Resilience (CER) Directive, the European Commission (EC) aims to enhance and harmonize Member States' and organizations' resilience plans and responses. Member States will have until October 2024 to transpose the CER Directive into national legislation and until July 2026 to identify Critical Entities and to define their resilience strategies, national frameworks for conducting risk assessments, and other elements of national and cross-border resilience.

Warning signs

Eggs in one basket: Does your organization outsource or offshore certain business processes to a single shared services center? While great cost-efficiencies can potentially be gained, management should consider if a centralized strategy eliminates diversity and redundancy that might be useful, inadvertently creating a major point of potential failure.

Math problems: When embarking on significant operational change, management often fails to factor in the impact upon resilience in their business cases. Whether going live with a new product, undertaking a massive new IT migration, or doing major business restructuring, the potential costs and benefits will not add up unless the net resilience gain or loss is taken into account.

Excuses, excuses: Regulators in a number of industries want to see resilience be a part of any change the board considers. Using complexity as an excuse for not knowing where the weaknesses are does not cut it anymore.

Getting the fundamentals right

Anticipate and assess: An organization should have the ability to understand the risks to high-priority products, services, and "essential outcomes," and have some sort of risk-sensing in place. The idea is that if something goes wrong, what does the organization need to achieve at a minimum to continue to function at an acceptable level for its stakeholders?

Design for resilience. Like any desired outcome, resilience rarely happens by accident. Companies should deliberately architect themselves to be resilient rather than retrospectively trying to fit resilience in. This means avoiding major points of failure in how critical services and products are delivered, including setting standards or controls to ensure that dual sourcing, and succession planning for critical staff are in place.

Plan and prepare. Should controls fail, the organization should have a plan for continuing to deliver critical products and services, and for safeguarding their customers and stakeholders throughout the disruption.

Respond and recover. An organization must mobilize quickly in a crisis. This means being agile and flexible enough to redirect resources as necessary, and having robust post-event or post-crisis review processes in place so people can learn lessons.

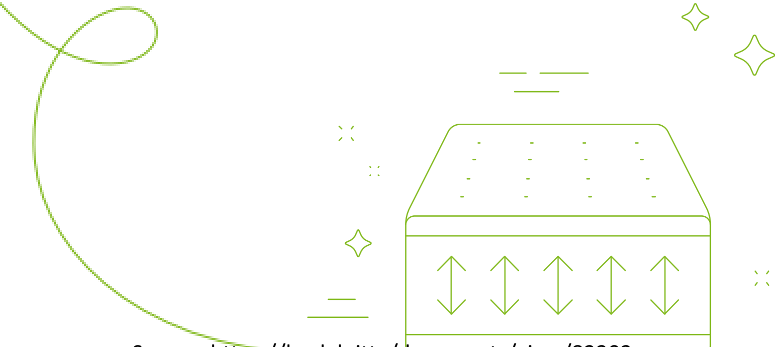
Taking the next steps

See it like it is: Unlike business continuity, disaster recovery, or information security, resilience is not a risk-and-control discipline. You can put resilience on your audit plan, but understand that it is not going to be risk-and-control specific. It is about helping the organization to identify what is critical.

Speak the same language: Things can get confusing when you are doing an audit on third-party risk management, for instance, and the procurement team is talking about what is critical in one way; and the disaster recovery team another way; and the business continuity group in yet another way. Internal auditors can help their organizations come to a common understanding of what is critical, so they can point to duplications or synergies between different audits and help management to connect the dots on what the resilience outcomes might be.

Arrive early: If given a seat at the table upfront, internal audit can be a critical friend to management in illuminating blind spots and providing a check and challenge to different aspects of resilience programs right from the outset.

Got governance? There should be a single accountable body for resilience; a set of minimum requirements; and proper reporting that can inform senior management/board decision-making.



Source: https://kx.deloitte/documents/view/83303

Internal audit’s role in

Disruptive technology

Our view

Disruptive technologies, such as the cloud, artificial intelligence (AI), and machine learning (ML) are nothing new. Companies across industries have been using algorithms and automation to process transactions, enhance customer service, and support executive decision-making for years. What is new is the pace of change.

As the latest development in the quickening evolution of disruptive technologies, generative AI (GenAI) is changing the scope of the conversation. The main difference between “traditional AI” and GenAI is that the output is of a higher complexity in the latter. Rather than just a number or a label, the output can be high-level chatbot answers, multi-page business documents, movie scripts, videos, images, and more. Simultaneously, more mature disruptive technologies, such ascloud applications and infrastructure, are becoming increasingly sophisticated—often by embedding GenAI and machine learning into their solutions—even as companies seek to cost-optimize their cloud portfolios and align them with enterprise strategy.

These developments all point to the potential for elevated risks. What does the rapid evolution of disruptive technologies such as AI mean, for example, for the workforce and broader environmental, social, and governance (ESG) objectives? What data governance and security risks do these technologies present? What is the company’s ethos around deploying them?

In answering these questions and more, internal audit has a key role to play in creating and protecting value by assuring, advising, anticipating, and accelerating the organization’s ability to both manage the related risks and take advantage of the opportunities posed by disruptive technologies. For instance, internal audit can help the board and management understand which GenAI and other disruptive technologies are leveraged in the organization and what risks they present. It can also provide assurance over existing controls and governance structuresor advise management on their options if those structures do not yet exist. In addition, an effective governance and controls framework can create value by enabling the organization to scale and drive adoption of these technologies more quickly. There is also an opportunity to turn the technology lens on the internal audit function itself, considering if upskilling is necessary to enable practitioners to audit algorithms, and if intelligentsolutions can be leveraged to improve efficiency and surface more insights for the business.

Naturally, the rate of adoption of disruptive technologies will differ for each company, and so will the ability of internalaudit to respond to the risks posed based on its maturity and philosophy. Nonetheless, GenAI stands poised to rock the business world. The challenge for auditors will be how to keep pace with the shifting risk landscape to deliver insightful assurance and valuable advice.

Source: https://kx.deloitte/documents/view/83303

Data points

42%

of surveyed CFOs say their companies are experimenting with GenAI.

15%

of surveyed CFOs say they are building GenAI into their strategies

>50%

of surveyed CFOs cite impact to risk and internal controls (57%), data infrastructure and technology needs (52%), and investment needs (51%) among their top three concerns regarding GenAI.

News item

In June 2023, the European Commission changed its draft artificial intelligence rules to include a ban on the use of AI technology in biometric surveillance and for generative AI systems like ChatGPT to disclose AI-generated content. The amendments to the proposed landmark law, which aims to protect citizens from the dangers of the technology, could set up a clash with EU countries opposed to a total ban on AI use in biometric surveillance. The proposed rules and the controversies around them illustrate the thorny ethical issues posed by certain GenAI use cases.

Warning signs

Who is the boss? Uncertainty around who owns the risk can indicate a precarious situation where everybody is doing something but nobody is in charge.

Random acts: If tactical actions are being taken and you can't see the connections between them, the organization may not have appropriate policies, standards, and guidelines in place to effectively manage AI and cloud risks.

Lofty expectations: Sometimes organizations assume that cloud services automatically deliver cost and sustainability benefits, only to be surprised by larger-than-expected bills and mounting stakeholder concerns about energy consumption. Be prepared to ensure the responsible use of cloud resources to minimize environmental impact and maximize cost optimization.

Mum is the word: During the risk assessment process, it is important for auditors to pose questions about the adoption of AI and automation broadly. If you do not ask, you do not receive.

Getting the fundamentals right

Start the conversation: Begin with an initial education or awareness session around AI risks at the senior leadership level, and then double-click down into the organization more broadly.

Survey the landscape: Determine if AI tools or other disruptive technologies are already being deployed within the organization, and if so, where.

Never stop learning: Auditors are being challenged to keep up with the pace of technology so they can effectively engage the business in this domain.

Get out the map: Advise on setting up or refining an AI governance framework and implementation roadmap, inviting cross-functional input to ensure that risks across the entire organization are considered as solutions are rolled out.

Taking the next steps

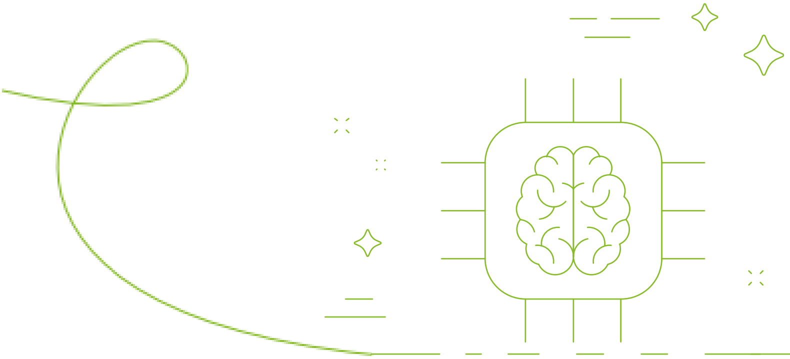
Familiarize: Learn about the underlying technologies that make GenAI possible, as well as the current capabilities and limitations.

Strategize: Develop a strategy for GenAI and harmonize it with the enterprise's existing AI strategy as well as internal audit's digital transformation plan.

Democratize: Bring together a cross-disciplinary team of people to democratize discussions about the potential use cases of disruptive technologies and associated risks.

Acclimatize: Adapt legacy technology risk frameworks to consider challenges around bias and misinformation, attribution, transparency, and enterprise accountability related to the new GenAI topography.

Source: https://kx.deloitte/documents/view/83303



Internal audit's role in

Building a digital backbone

Our view

Advanced digital capabilities, such as generative artificial intelligence (GenAI), are making news. Despite the glitziness of the new capabilities, the concept of "adopting digital" within the internal audit function is not about implementing fancy tools; it is about accelerating the flow of data through revised methods and upskilled talent. Like a human backbone, digital hardware and software can be linked together to form a spinal column through which signals travel unimpeded.

Many internal audit functions have started their digital journeys by leveraging analytics capabilities. Yet, most still use these digital tools in a limited way, such as for inquiries or data sampling. To date, few functions view digital broadly enough to systematically move toward building a digital backbone—a spine capable of automating processes and driving efficiencies and insights across the entire audit lifecycle.

Imagine a world where: risk taxonomies are integrated into the digital backbone, and risk assessments flow end-to-end throughout the audit lifecycle; enhanced insights are available across each audit phase; team members have visibility into a portfolio of audit findings and their current statuses; automated controls testing reduces manual activities to almost zero; and quantitative key risk indicators (KRIs), qualitative interview insights, and experienced auditor inputs are combined into a dynamic annual planning process.

These scenarios represent the art of the possible. While they may seem distant for many, now is the time to get on the road to seamless connectivity by making sure that the technologies you are acquiring, fit together. Only through an intentional approach to embracing digital will you be able to architect an integrated platform capable of carrying your internal audit function forward into a real-time, continuous future.

Data points

Bigger technology investments often bring increased scrutiny. Leaders should be thoughtful in allocating capital and articulating value, yet 61% of respondents in the Deloitte 2023 Global Technology Leadership Study find it difficult to quantify the benefits of individual technology investments. Furthermore, their biggest challenge with measuring technology's impact is quantifying the softer, less tangible benefits that are key to a function like internal audit, such as agility, innovation, or insights.

News item

When a large computer equipment company needed to expedite the development of internal-audit-related automations but did not want to distract their subject matter experts from their critical work, they deployed a Deloitte Automation and Analytics Development Pod. Composed of handpicked professionals, the Pod quickly established an operating and technology model that enabled team members to leverage their deep knowledge of internal audit procedures while developing automations within the client's technology infrastructure. Working closely with key internal audit stakeholders, the Pod was able to produce automations and tangible results in a matter of months, ultimately providing development scale without the normal operational overhead.

Source: https://kx.deloitte/documents/view/83303

Warning signs

Spreadsheet dread: If your risk assessment process is laborious, then you are likely missing an opportunity to leverage technology to improve efficiencies.

Tech disconnect: Disparate platforms (i.e., “vertebrae”) used for risk assessment, planning, audit execution, issue remediation, and continuous monitoring can indicate the lack of a formal architecture for building a digital backbone.

My way or the highway: Limited process standardization can mean your internal audit function is ill-prepared for automation.

Analytic blinders: Digital has become synonymous with analytics within many internal audit functions, but it offers so much more. Make sure your organization sees past the valuable, but narrow, capabilities of analytics to embrace the full potential of an integrated digital backbone.

Getting the fundamentals right

Put process first: It is important to focus on making the process more effective, rather than just implementing the technology itself. Ultimately, a digital transformation should help internal audit functions anticipate risks, assist the business in understanding those threats, and devise preventative measures.

Mindset matters: Whether you are a small or large function, the mindset and willingness to experiment with digital tools is paramount. Promote innovation, encourage ideas, and make it safe for people to learn through trial and error.

Inform to transform: You cannot move toward continuous auditing without continuous learning. In digital transformation, attaining data literacy and keeping up with business changes and emerging risks is often more challenging than selecting and implementing the right technology solutions.

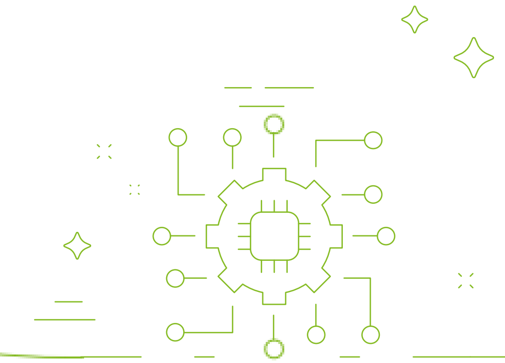
Taking the next steps

Systematize and prioritize: More mature internal audit functions have demonstrated the benefits of applying a systematic and methodical approach to digital innovation, taking the time to assess their ways of working to identify and prioritize opportunities.

Try, try again: Intentionally pilot proof of concepts and measure Return on Investment (ROI) to guide purpose-driven technology investments—those that not only deliver targeted improvements but also serve as vertebrae in an increasingly strong, yet flexible, digital backbone.

Believe to achieve: People need to quickly experience the benefits of digital transformation in order to build momentum for the long haul. Leveraging technology to document risk assessments, input data, calculate risk ratings, and provide visibility across the audit department can be a good place to start in encouraging buy-in and helping people envision the art of the possible.

Source: https://kx.deloitte/documents/view/83303



Internal audit's role in Controls modernization

Our view

An ounce of prevention is worth a pound of cure. Yet, when it comes to controls modernization, internal audit typically provides assurance retroactively, after the controls have been designed, implemented, and tested, and in some cases, found to be ineffective or inefficient.

Understandably, some internal audit departments may be hesitant about commenting upfront on the control program undertaken by the first and second lines. While internal audit has an obvious duty to remain independent, this does not preclude advising management on how to achieve the shared ambition of the organization, which is making sure the end-to-end control program is understood, owned, and operated in an efficient and sustainable manner. For internal audit, or the organization at large for that matter, there is no success in reactively producing a hefty report calling out dozens of deficiencies.

Internal audit can maximize its impact and value contribution by engaging with the first and second lines to share leading practices related to control program modernization. But, how can internal audit participate in a way that preserves its independence and avoids stepping on toes? Start by focusing on the risks. This includes helping management to truly understand what the risks are as well as to determine the risk appetite. For example, companies often try to boil the ocean when designing controls, rather than discerning what is non-negotiable versus what is tolerable. Internal audit is often in the best position to perform this assessment because of its overarching view of the risk landscape, and its seat at the audit committee table, which gives it a sense of the organization's appetite around risk and control from the very top of the organization.

Modernizing the control environment and achieving greater levels of efficiency and effectiveness requires both greater automation and a recognition by the organization that internal audit can advise management and anticipate risks, in addition to providing traditional assurance. In short, it is about internal audit intervening earlier as a change agent, not acting after the fact as an insurance policy and supporting the shared ambition of the organization (i.e., how the first line supported by the second line can understand, own and operate the controls better).

Source: https://kx.deloitte/documents/view/83303

Data points

>66%

of businesses plan to spend more on technology and software in 2023.

$4.7 Trillion

worldwide technology spending projected in 2023.

€1 Billion

European Commission planned investment in AI.

News item

Increasing business complexity and regulatory requirements are driving continual change to the risk environments for many organizations, and historical approaches to risk and controls may not be suited for the current atmosphere of digital transformation, persistent change, and uncertainty. As the business landscape continues to evolve, the risk of accounting and reporting misstatements rises, often due to the inability to respond to internal and external circumstances and adapt quickly to business changes.

Warning signs

Manual maneuvering: Lack of technology enablement, either fully or partially, can point to inefficiencies in the controls program that can be addressed, for example, by automating control performance, control testing, or project management through a governance, risk, and control (GRC) platform.

User dissatisfaction: If users find it difficult to navigate the controls program, for example, due to excessive controls testing and an expanding control landscape, it could indicate an unoptimized environment with an elevated risk of failure.

Many layers: Does the organization have a ongoing process in place to challenge and optimize the control framework, along with methodologies such as a risk assessment? If the control environment is complicated with many layers, probably not.

Risky business: Sometimes control failures can be overlooked because they do not impact the business in a big way. In aggregate, these "little things" can add up, indicating the organization is trying to control for too many risks. The ineffective use of risk-based approach may result in exposure to material weaknesses and misaligned resources.

Getting the fundamentals right

Engage early: Advise upfront on how to make the controls program risk-driven. For example, update methodologies and testing strategies using a risk-based versus a compliance mindset.

Take a bite: Define the risk appetite so the first and second lines do not bite off more than they can chew.

Go beyond: Encourage the business to challenge existing orthodoxies to go beyond the basics of a controls program. For example, consider designing continuous controls monitoring to provide assurance instead of relying upon transactional controls.

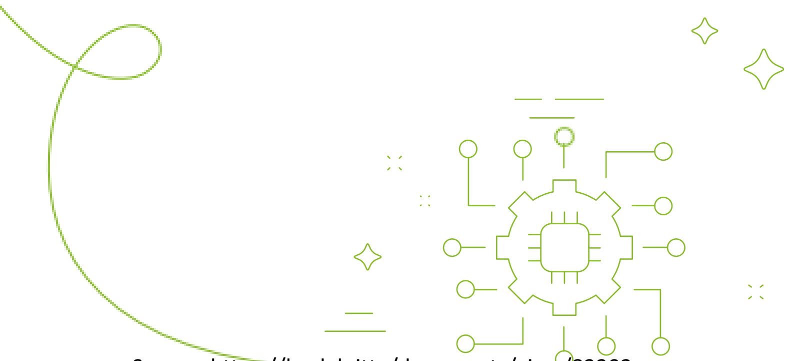
Assure by design: Align stakeholders and control owners to expectations, requirements, and strategic priorities in an assurance-by-design process.

Taking the next steps

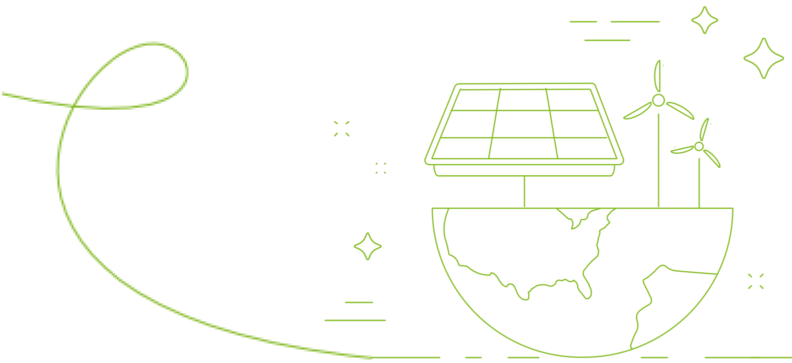
Level set: Make sure all stakeholders within the three lines truly understand the risk landscape and their related roles and responsibilities so they can be responsive to the risks and challenge existing orthodoxies.

Zero in: Ensure management and compliance leaders are laser-focused on mitigating the risk so they are designing the control program optimally to do only what it needs to do.

Challenge the status quo: Ask if business and compliance teams have considered what portions of the control program can be digitized and automated on the path toward modernization and continuous controls monitoring.



Source: https://kx.deloitte/documents/view/83303



Internal audit's role in

Environmental, Social, and Governance (ESG)

Our view

Embracing ESG can be mighty good for business. A substantial body of evidence now demonstrates the strong connection between a company's purpose—the differentiated role it serves in society—and business value. While skeptics remain, they will not be able to resist much longer amid a global regulatory push toward greater levels of ESG reporting and transparency, especially concerning sustainability disclosures. And, therein lies the issue.

As the pressure increases for companies to demonstrate environmental responsibility, social consciousness, and governance effectiveness, so too does the temptation to be less-than-forthcoming about how ESG targets are set and whether or not they are being attained on schedule. In fact, the ever-evolving business vernacular can barely keep up with the expanding range of ESG-related risks. Enter *greenwashing*, making a company's products and activities seem more environmentally friendly or less environmentally damaging than they really are; *bluewashing*, overstating a company's commitment to socially responsible practices; and *pinkwashing*, or using a LGBTQ+-friendly marketing approach, while masking other negative actions. From green to pink to blue, such deceptive practices comprise an entire color palette of risks.

Uniquely positioned to help an organization anticipate such risks, internal audit should incorporate ESG into their audit plans, as well as serve as a trusted business advisor to management. For internal audit functions early in their ESG journeys, getting a lay of the land via a current-state ESG program assessment can be a good place to start.

How are ESG targets set? Who reports to whom? Does the ESG strategy align with the overall business strategy? How does the company monitor progress? And, perhaps most importantly, what happens if things do not go as planned?

Internal audit can accelerate change by evaluating and strengthening data, processes, and internal controls over sustainability information. In this way, ESG strategies, goals, and progress can be communicated transparently and can be relied upon by stakeholders, so the most colorful ESG risks can be avoided and a company's reputation protected.

Source: https://kx.deloitte/documents/view/83303

Data points

78%

of consumers were more likely to remember companies that exhibit a strong purpose.

53%

of surveyed CXOs reported new revenue streams from socially conscious offerings.

2X

growth in consumer-packaged goods (CPG) products marketed as sustainable grew ~2x faster than those not marketed as sustainable and achieved a 5-YR CAGR of 9.43% vs. 4.98% for their conventional counterparts.

News item

In September 2023, the California State Assembly and the California Senate passed the Climate Corporate Data Accountability Act, SB-253, and the Climate-Related Financial Risk Act, SB-261. The bills require public and private companies that do business in California to disclose their greenhouse gas emissions annually, and to report biennially on their climate-related financial risk. Both address investor concerns about dealing with the risks to the global financial system that are posed by climate change. SB-253 and SB-261 established the first official US regulation to mandate reporting disclosure requirements for greenhouse gas emissions and climate risks for large companies.

Warning signs

Marketing magic: If ESG reporting still sits within marketing rather than with the financial reporting and/or sustainability teams, then the organization may be at greater risk for green, pink, or blue washing, or other misleading practices.

Seeing green: When a company raises green funds frequently or for large amounts, internal audit should pay attention. Ethically raised green loans must correspond to specific, qualified projects.

Feeling blue: High staff turnover or increased attrition rates can be a symptom of blue washing and a lack of genuine commitment to diversity, equity, and inclusion (DEI) goals.

Wait-and-see: Some companies still do not see ESG as a priority, even with new regulations coming into force around the globe. ESG reporting is a long journey. Those who hesitate may be left behind.

Getting the fundamentals right

Talk it up: Internal audit should ensure that ESG is incorporated into conversations on risk; added to the internal audit plan; and provide assurance that ESG reporting and the control environment is sound. The aim is not to re-invent the wheel, but to apply the skill sets you already have to ESG.

Get familiar: Brief your internal audit team with well-established ESG reporting standards and frameworks such as the Global Reporting Initiative (GRI), Sustainability Accounting Standards Board (SASB), Greenhouse Gas (GHG) Protocol, and the Task Force on Climate-related Financial Disclosure (TFCD).

Verify actions: While ESG disclosure readiness is paramount, internal audit's role goes beyond assuring the completeness and accuracy of the ESG-numbers calculated by the business; it also involves verifying the actions taken.

Move with confidence: You do not need to be an ESG specialist in order to act. While upskilling is important, internal auditors can immediately add value by applying traditional auditing techniques and bringing professional skepticism to ESG reporting and communications.

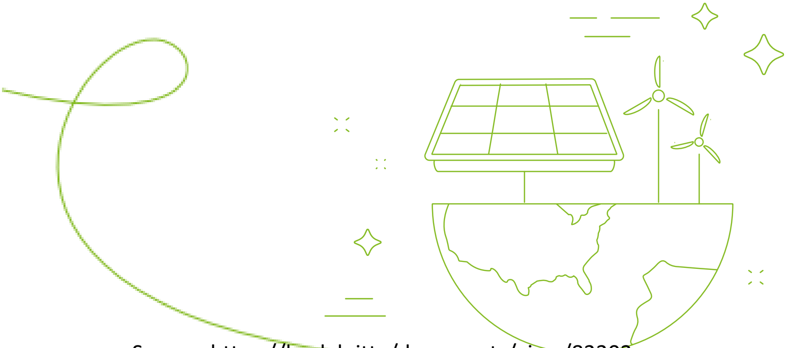
Taking the next steps

Survey the landscape: If internal audit has not been involved in ESG to date, conduct a current state assessment of the organization's overarching ESG efforts to identify potential enhancement opportunities.

Validate metrics: Perform a risk assessment to identify prioritized metrics and execute traditional assurance activities on ESG-related metrics and disclosures to confirm completeness and accuracy.

Zoom in: Deliver ESG-centric internal audits to determine whether ESG-related objectives, activities, and risks are being appropriately identified, considered, assessed, and documented.

Frame the subject: With increased expectations around ESG metrics and disclosures, build a SOX-like framework to identify risks, controls, and test procedures, document process flows, and identify gaps and potential improvement opportunities. Define a controls assessment methodology to determine where to start.



Source: https://kx.deloitte/documents/view/83303

Internal audit's role in

Human capital management

Our view

Just a few years ago, work was generally well-defined. You commuted to a workplace. You stayed there for a certain amount of time. And, you were paid a salary or an hourly rate to perform discrete tasks that were organized into a "job." As described in the Deloitte Human Capital Trends 2023 report, many of the boundaries that used to provide the structure of work have been dismantled. Digital advances have redefined the concept of work as a physical space. Talent shortages are prompting companies to experiment with using skills, not jobs, as the baseline for how workforce decisions are made. And employee demands for more meaningful work, flexible workplace models, and more personalized career paths are pushing companies to focus more on the "S" in environmental, social, and governance (ESG).

Internal audit has a key part to play in helping management and those charged with governance to get their bearings on where the organization stands in this boundaryless world and how it can get to where it needs to be. And, like the flexible jobs of the future, internal audit's role in human capital management (HCM) can be as broad or as narrow as the organization desires. For instance, the internal audit function can assess the maturity of talent recruitment or diversity, equity, and inclusion (DEI) efforts and determine if they are meeting their intended objectives. It can also identify risks, perform culture audits, and advise if programs for addressing deficiencies do not exist or need improvement. And, if an organization publishes "social" statistics to the marketplace, internal audit can provide assurance by independently testing the data for completeness and accuracy.

Internal audit, with its broad perspective on enterprise risk and collaborative stakeholder relationships is well-positioned to help organizations assess their HCM programs and to chart a path forward in boundaryless world—a realm that is poised to be more equitable, more technology-enabled, more employee-centric, and critically, more challenging from a risk perspective, especially around talent retention, worker productivity, brand reputation, and cyber security. The question is not whether internal auditors will help shape the future of work; it is only to what degree.

Source: https://kx.deloitte/documents/view/83303

Data points

71%

of CEOs expect talent shortages to continue.

96%

plan to focus on the employee for in-demand talent.

97%

are giving employees greater flexibility in work hours and location.

News item

The US Equal Employment Opportunity Commission (EEOC) filed 143 new employment discrimination lawsuits in fiscal year 2023, representing more than a 50% increase over fiscal year 2022 suit filings. The cases filed by the EEOC challenge workplace discrimination under all of the statutes enforced by the Commission and represent a broad array of issues, including barriers in recruitment and hiring, protecting vulnerable workers and persons from underserved communities, qualification standards and inflexible policies that discriminate against individuals with disabilities, the long-term effects of the COVID-19 pandemic, advancing equal pay, combatting unlawful harassment, and preserving access to the legal system.

Warning signs

Unsocial media: A preponderance of unflattering posts on job boards and recruitment sites can indicate a deeper problem with corporate culture.

Turnover tumult: High rates of attrition can indicate an ineffective human capital operating model that is elevating risk in multiple areas.

Busy signal: Excessive hotline calls can be a cry for help in assessing and addressing HCM risks.

Bad rep: There are places you would not want to work because of their reputation for unfair or discriminatory labor practices. Make sure your organization is not one of them.

Getting the fundamentals right

Model risks: Evaluate the risks associated with the organization’s culture and human capital operating model, taking into account employee engagement, employee behaviors, political environment, and market signals.

Wash, rinse, repeat: Incorporate human capital risks, including DEI and culture risks, into the ongoing internal audit plan.

Lend a hand: Help leadership understand the risks and benefits associated with organizational culture. Provide input on training, communications, and policies.

Build confidence: Provide assurance that management has established effective processes to attract, recruit, hire, and retain diverse candidates, to eliminate bias, and to treat all employees equitably.

Taking the next steps

Shine a light: Assess human capital programs to provide actionable visibility into strengths and weaknesses and to promote continuous improvement.

Take stock: Analyze the organization’s current maturity in key HCM areas—such as infrastructure, talent, culture, brand, analytics, and leadership—that could produce both quantitative and qualitative insights.

Measure up: Advise on metrics tied to specific talent objectives that can be used in evaluations and periodic maturity assessments.

Look closer: Conduct special culture-related audits when the data warrants closer examination (e.g., high attrition rates for specific cohorts), or in response to stakeholder concerns and/or complaints.

Source: https://kx.deloitte/documents/view/83303

Our Team Professionals

Contact us

Alithia Diakatos
Partner
Assurance Leader
Deloitte Greece
Email:
adiakatos@deloitte.gr
Tel: +30 210 6781 186

Pavlos Venizelos
Principal
Assurance | Internal Audit
Deloitte Greece
Email:
pvenizelos@deloitte.gr
Tel: +30 213 0881 696

Eleftheria Psaromanolaki
Senior Manager
Assurance | Internal Audit
Deloitte Greece
Email:
epsaromanolaki@deloitte.gr
Tel: +30 213 088 1627

Michalis Pouspourikas
Assistant Manager
Assurance |Internal Audit
Deloitte Greece
Email: mpouspourikas@deloitte.gr
Tel: +30 213 088 1670

Our Offices

Athens
3a Fragkokklisias & Granikou str.
Marousi Athens GR 151-25
Greece
Tel: +30 210 6781 100
Fax: +30 210 6776 232
www.deloitte.gr

Thessaloniki
VEPE Technopolis
Building Z2 555 35, Pylaia
Tel: +30 2310 406500

Phoenix center
27, Georgikis Scholis av.
570 01 Thessaloniki
Greece
Tel: +30 2310 406500

Heraklion
16b, Dimokratias Av.
713 06
Tel: +30 2816 005700

Ioannina
Science & Technology Park of Epirus
45110 Ioannina, Greece
Tel: +30 210 67 81100

Patras
4, 28th October str.
262 23 Patras, Greece
Tel: +30 2160 039767

Deloitte Certified Public Accountants Societe Anonyme

This document has been prepared by Deloitte Certified Public Accountants Societe Anonyme.

Deloitte Certified Public Accountants Societe Anonyme, a Greek company, registered in Greece with registered number 0001223601000 and its registered office at Marousi, Attica, 3a Fragkokklisias & Granikou str., 151 25, is one of the Deloitte Central Mediterranean S.r.l. ("DCM") countries. DCM, a company limited by guarantee registered in Italy with registered number 09599600963 and its registered office at Via Tortona no. 25, 20144, Milan, Italy is one of the Deloitte NSE LLP geographies. Deloitte NSE LLP is a UK limited liability partnership and member firm of of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of any of each other. DTTL does not provide services to clients. Please see www.deloitte.com/ about to learn more.

DTTL, Deloitte NSE LLP and Deloitte Central Mediterranean S.r.l. do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 411,000 people make an impact that matters at www.deloitte.com.

This document and its contents are confidential and prepared solely for your use, and may not be reproduced, redistributed or passed on to any other person in whole or in part, unless otherwise expressly agreed with you. No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party, who is provided with or obtains access or relies to this document.