

Deloitte.








내부감사:

2022년 리스크 및 기회

Table of contents

-  04 | Introduction
-  06 | Third-party risk management (TPRM)
-  10 | ESG (environmental, social, and governance)
-  14 | Counter fraud
-  18 | Mergers & acquisitions
-  22 | Psychological safety

-  26 | Cybersecurity
-  30 | Diversity, equality, and inclusion
-  34 | Assurance by design
-  38 | Bullying & harassment
-  42 | Automation

목차

-  04 | 서문
-  06 | Third-party 리스크 관리 (TPRM)
-  10 | ESG (환경, 사회 및 지배구조)
-  14 | 부정행위 대응
-  18 | 인수합병
-  22 | 심리적 안정

-  26 | 사이버 보안
-  30 | 다양성, 평등성 및 포용성
-  34 | 설계를 통한 검증
-  38 | 따돌림 및 괴롭힘
-  42 | 자동화

On risk, opportunity, and internal audit



Risk

Risk is often thought of as inherently negative, but a more-nuanced view perceives a complex duality. Parallels can be found in literature—like Jekyll and Hyde, risk and opportunity inhabit the same body—and in science—like Newton's Third Law, for every risk there is an equal opportunity.

There's little doubt why the negative aspect of risk predominates. In recent years, the world has witnessed an unprecedented confluence of multiple threats, many of which have spawned, entwined with, and/or exacerbated the others. A severely truncated list includes the global pandemic, climate change, labor shortages, supply chain disruptions, cyber threats, and political and social upheaval. Considered in the aggregate, these and other threats have shaken the very foundations upon which society and business are built.



Opportunity

Yet opportunity shadows risk at every turn. Consider, for example, the realm of ESG—environmental, social, and governance. Organizations face intense regulatory and societal pressures to abide by high standards, and failure can lead to significant financial, regulatory, and reputational damage. Yet if businesses get ESG right, they can do great things, both in terms of making positive contributions to key global issues and, of equal importance, in creating a competitive advantage in the marketplace.



Internal audit

Internal audit (IA), like risk itself, is often misunderstood. The profession has historically suffered from unfavorable perceptions, often being seen as a policing body or as a group of scolds who swoop in to report on what went wrong. However, a more progressive and expansive definition of internal audit also contains a duality: essential providers of both assurance and advisory services. Internal audit is rightfully wary of the multitude of risks, and the function will always be charged with protecting their organizations through assurance. But truly evolved internal audit groups will also seek to help management navigate future challenges and make more-informed decisions, taking full advantage of the concurrent opportunities that every risk offers.

In this publication, we present a collection of key risks and opportunities that we believe organizations should have on their radar—and internal audit in their audit plans.

The list is by no means comprehensive; nor will every topic apply to every organization. It's incumbent upon each entity to evaluate, rank, and prioritize these risks and opportunities in relation to their own unique profile and circumstances. (This concept of risk-ranking to focus on the risks that matter most is addressed in more detail in our publication, "[Internal Audit 3.0: The future of internal audit is now.](#)")

While the current environment has surely triggered many feelings of powerlessness and uncertainty, this paper can serve as a counterweight: a motivating and organizing influence; an incentive to get your house in order, your priorities straight, and your action plan initiated. Risks are plentiful but the opportunities are even greater. And internal audit can be the difference maker. Internal audit functions that embrace the risk/opportunity and assure/advise dualities will help their organizations emerge stronger from these unprecedented times.

리스크, 기회 및 내부감사에 대하여



리스크

리스크는 흔히 본질적으로 부정적인 것으로 여겨지지만, 좀더 미묘한 관점에서 보면 복잡한 이중성이 인식됩니다. 지킬 박사과 하이드처럼 리스크와 기회는 동일한 인격체에 존재하는 것이나, 뉴턴의 제3법칙처럼 모든 리스크에는 균등한 기회가 존재하는 것처럼 리스크의 이중성은 과학과 문학에서도 발견됩니다.

리스크의 부정적인 측면이 왜 압도적인지에 대해서는 의심의 여지가 없습니다. 최근 몇 년 간 전 세계에서 전례 없는 여러 위협의 융합을 목격하였으며, 그 중 많은 위협이 다른 위협과 함께 생성되거나 얽히고 악화되었습니다. 아주 협소하게 보더라도 전세계적인 팬데믹, 기후변화, 노동력 부족, 파괴된 공급망, 사이버 위협, 정치적이면서 사회적인 격변을 포함하고 있습니다. 이러한 위협은 전체적으로 사회와 기업의 토대가 되는 기반을 흔들어 놓았습니다.



기회

그러나 기회는 언제나 리스크를 동반합니다. 예를 들어 ESG의 영역인 환경, 사회 및 지배 구조를 생각해 보십시오. 기업은 높은 기준을 준수해야 할 강력한 규제 및 사회적 압력에 직면해 있으며, 이러한 압력으로 인해 재정적, 규제적 측면의 손상이 클 뿐만 아니라 평판도 크게 손상될 수 있습니다. 하지만 ESG를 올바르게 구축하면 주요 글로벌 문제에 긍정적인 기여를 하고 시장에서 경쟁우위를 확보하는 데 중요한 역할을 할 수 있습니다.



내부감사

내부감사 또한 리스크와 마찬가지로 오해받는 경우가 많습니다. 내부감사라고 하는 전문적인 분야는 과거 경험상 좋지 않은 인식으로 시달려 오고 있으며, 흔히 감시기관이나 울바르지 못한 것을 지적하는 집단으로 여겨지고 있습니다. 그러나 내부감사에 대한 보다 점진적이고 광범위한 정의는 검증 및 자문 서비스의 필수불가결한 제공자라는 이중성을 포함합니다. 내부감사는 항상 수많은 리스크를 적절히 경계하며, 이 기능은 검증을 통해 그들의 조직을 보호하는 책임을 집니다. 그러나 진정으로 발전한 내부감사 그룹은 모든 리스크에 공존하는 기회를 최대한 활용하여, 경영진이 향후 과제에서 올바른 길로 향할 수 있도록 돕고 그들이 보다 정보에 입각한 의사결정을 내릴 수 있도록 지원할 것입니다.

본 발간물은 기업이 관심을 가져야 할 주요 리스크와 기회, 그리고 감사 계획에서의 내부감사를 제시합니다.

본 발간물에서 다루는 것은 결코 모든 것을 포괄하고 있지 않으며, 모든 주제가 모든 기업에 적용되는 것 또한 아닙니다. 기업의 각자 상황에 부합하게 이러한 리스크와 기회를 평가하고, 배열하며, 우선순위를 정하는 것은 각 기업이 수행할 의무입니다. (가장 중요한 리스크에 초점을 맞추는 리스크 등급의 개념은 "[Internal Audit 3.0: The future of internal audit is now](#)"에서 더욱 자세히 다루고 있습니다.)

현재의 환경이 분명 많은 무력감과 불확실성을 촉발시켰지만, 본 보고서가 업무를 원활하게 수행하고 우선순위를 바로잡고 실행계획을 착수하는 데 동기부여를 제공하며 영향력을 미치는 균형추로서의 역할을 할 것입니다. 위험부담이 크지만 기회는 더욱 큼니다. 그리고 내부감사는 차별점이 될 수 있습니다. 리스크 및 기회를 포괄하고 이중성을 검증 및 자문하는 내부감사의 기능은 전례 없는 시대에서 기업이 더욱 강하게 부상할 수 있도록 지원합니다.



Internal audit's role in

Third-party risk management (TPRM)

Don't fight fires. Install fire-proof doors.

Our view

Back when every business was seen as an island, internal audit had it easy: Most aspects of the enterprise were handled in-house, and IA's worries ended at the company's front door.

Today, the front door has not just been flung open, it's been knocked down, with companies often outsourcing more functions than they retain. Meanwhile, these third parties—vendors, distributors, suppliers, and the like—also maintain their own webs of relationships (yes, even third parties have third parties) creating a massive ecosystem of fourth and fifth parties and beyond that requires, at a minimum, full awareness, if not active oversight.

Assurance of TPRM across the extended enterprise requires some baseline data. Start by asking management for its inventory of all third-party relationships. (Spoiler alert: There likely isn't one.) How quickly can a report on the entire landscape of relationships and associated risks be produced?

(Hint: If the answer is six months, you have a problem.) How many third-party failures has the organization experienced over the last year? (Expected reply: More than you think.)

Every third-party (and beyond) relationship carries its own set of risks, and for most organizations, investing in technology will be key to mitigating them. Internal audit should be prepared to advise management and the audit committee on appropriate technology for monitoring third-party risk, such as real-time alert and trend analysis tools.

Additionally, provide guidance to your stakeholders on the advantages of outsourcing TPRM. Developing capabilities in-house can be costly and demanding, as TPRM is a niche field that requires specialized expertise. The same motivations that drive a company to engage in third-party relationships in the first place apply to outsourced oversight of TPRM: efficiency, proficiency, rigor, auditability, and an independent perspective are among the benefits to be realized.

News item

In 2021, a large bank was assessed a US\$1 million penalty and hit with additional testing and training requirements due to a failure to properly report financial data to the federal regulator. While the bank had hired a third-party service provider to handle the process, the vendor made persistent errors that the bank failed to properly supervise and correct in a timely manner.

Data points

According to Deloitte's "Future of M&A Trends" survey:

51%

More than half of organizations faced one or more third-party risk incidents since COVID-19.

13%

were high-impact incidents that severely compromised financial performance, impaired customer service, or seriously breached regulation.

10%

were not sure whether they had suffered a third-party incident or not.



Third-party 리스크 관리 (TPRM) 에 대한 내부감사의 역할

화재를 진압하지 마십시오. 방화문을 설치하십시오.

우리의 견해

모든 기업을 고립된 존재로 여기던 시절, 내부감사는 간단하게 이루어졌습니다. 대부분의 업무는 내부적으로 처리되었고, 내부감사에 대한 걱정은 쉽게 해결했습니다.

오늘날에는 기업의 문호는 일반적으로 그들이 보유하는 것에 비하여 많은 기능을 아웃소싱하면서 단순히 개방하였다기 보다는 무너져 내렸습니다. 한편, 납품, 유통, 공급업체 등의 third party 또한 자체적인 관계망을 유지하여 적극적인 감독까지는 아니더라도 최소한 완전한 인식이 필요한 제4자 및 제5자로 구성된 대규모 생태계를 구축합니다 (Third party 마저도 third party를 보유합니다).

전반적으로 확장된 기업의 TPRM(Third-party risk management, Third-party 리스크 관리)에 대해 검증하기 위해서 기준이 되는 데이터가 몇 가지 필요합니다. 우선 경영진 측에 모든 third-party 관계를 포함하는 명단을 요청하십시오. (스포일러 주의: 아마 그러한 명단이 존재하지 않을 가능성이 큼니다.) 기업의 전반적인 관계 및 리스크 관련 보고서가 얼마나 신속하게 작성될 수 있습니까?

(힌트를 제공하자면, 만약 답이 6개월인 경우에는 문제가 됩니다.) 지난 해 기업이 third party로 인해 손해를 몇 차례 경험했습니까? (생각보다 많다는 답변이 예상됩니다.)

모든 third-party (및 그보다 확장된) 관계에는 리스크가 수반되며, 대부분의 조직에서 기술에 투자하는 것이 리스크를 줄이는 키가 될 것입니다. 내부감사는 경영진과 감사위원 회에게 실시간 경고 및 트렌드를 분석하는 장치 등 third-party 리스크 모니터링에 적합한 기술에 대해 조언할 준비가 되어 있어야 합니다.

더불어 이해관계자에게 TPRM(Third-party 리스크 관리)를 아웃소싱 하는 것에 대한 장점을 안내하십시오. TPRM이란 전문 지식이 필요한 틈새 분야이기 때문에 내부적으로 역량을 발전시키는 것은 비용이 많이 들고 부담될 수 있습니다. 기업이 처음 third party를 사용할 때 적용하는 효율성, 능숙도, 엄격성, 감사가능성과 독립적인 관점 등의 동기가 TPRM에 대한 감독을 아웃소싱 할 때에도 동일하게 적용됩니다.

뉴스거리

2021년에 어느 대형 은행이 연방 규제기관에 재무보고를 제대로 하지 않아 백만 달러의 벌금을 부과받았고 추가적인 검사와 필수 교육 등으로 타격을 입었습니다. 업무 과정에서 은행이 제3의 용역업체를 고용하였는데, 용역업체가 지속적으로 오류를 발생시켰고, 은행은 그것을 올바르게 감독하거나 적시에 바로잡지 못하였습니다.

데이터 포인트

델로이트의 "Future of M&A Trends" 설문조사에 의하면:

51%

기업의 절반 이상이 코로나 19 이후 한 건 이상의 third-party 리스크와 관련한 사건에 직면했습니다.

13%

13%는 재무성과를 심각하게 저하시키거나, 고객 서비스를 손상시키거나, 규정을 심각하게 위반한 영향력이 큰 사건이었습니다.

10%

10%는 third party로 인한 손해를 경험했는지조차 확실하지 못했습니다.



For more info on third-party risk management (TPRM)

- Deloitte: [Third-party risk management survey 2021](#)
- Deloitte: [The challenge of third-party risk management](#)
- Wall Street Journal: [Manage third parties with cutting edge technologies](#)

Warning signs

- **Party time:** Does your third party use third parties? If, for example, your payroll vendor subcontracts some services, you may discover you've lost control over the personal data of your employees.
- **Vendor venom:** Employee grumbling about the reliability or performance of external vendors may be an indicator of third-party contract violations that should be further investigated.
- **Management misconceptions:** Management often think they can do TPRM on a shoestring. They think they can do it quickly. And they think they can do it without technology. They can't. They can't. And they can't.
- **Expanding borders:** Many third-party relationships exist with companies in other jurisdictions. If your vendors operate in an environment with lax regulatory standards, potentially corrupt business practices, or a variety of ESG (environmental, social and governance) concerns, your risk exposure may exceed your risk appetite.

Getting the fundamentals right

- **Send lawyers:** Most third-party relationships are governed by contracts that specify rights and obligations. Your general counsel was likely involved in drawing up the agreements and can be a valuable resource in interpreting them.
- **Widen the lens:** Does the current TPRM program truly encompass all third parties, or is it limited to suppliers? Does it cover all risk domains, such as antibribery, business continuity, and ESG aspects?
- **Make the case:** Examine the business case for engaging in third-party relationships and its alignment with the overall business strategy.
- **Pull the chain:** How far down the supply chain should you go? Risk assess whether and how intently 4th-party and beyond providers should be monitored.
- **Eye the little guy:** Risk does not diminish in parallel with the contract value of your third-party relationships. Your reputation risk is the same with a 10K vendor as a 1M vendor. That small company that you spend a few thousand on can cost you millions.

Taking the next steps

- **Get a jump:** Get your team involved in the vendor selection process to vet providers and head-off potential problems before they arrive.
- **Install "fire doors":** Make the case to the audit committee for additional technology resources. Here's an opening statement: "Rather than fighting fires, management should be installing fireproof doors."
- **Act suspicious:** Anticipate ways in which managers may try to circumvent internal controls that govern third-party relationships. Advise management on the means of strengthening.
- **Look on the bright side:** Don't just flag weaknesses in third parties; as part of your work, strive to identify areas to obtain additional value from the relationships.
- **Flag the penalties:** Determine if a defined process exists (and is followed) for escalating concerns, obtaining remedies, and extracting penalties for contract non-performance, quality issues, or other breaches.



Third-party 리스크 관리 (TPRM)에 대한 더욱 자세한 정보는

- 델로이트: [Third-party risk management survey 2021](#)
- 델로이트: [The challenge of third-party risk management](#)
- 월 스트리트 저널: [Manage third parties with cutting edge technologies](#)

위험신호

- **포개진 시간:** 귀사의 third party가 하도급업자를 활용합니까? 예를 들어 귀사의 급여장부를 담당하는 용역업체가 서비스의 일부를 하도급한다면, 임직원 개인정보에 대한 통제력을 상실할 것을 발견할 수도 있습니다.
- **공급업체 원한:** 외부 공급업체의 신뢰도나 성과에 대한 직원의 불만은 추가적인 조사가 필요한 third-party 계약 위반에 대한 지표가 될 수 있습니다.
- **경영진의 착각:** 흔히 경영진은 적은 예산으로 신속하게 기술을 사용하지 않고 third-party 리스크를 관리할 수 있다고 생각합니다. 절대로 불가능합니다.
- **국경 확장:** 다른 지역에서 활동하는 기업들 간에도 수많은 third-party 관계가 존재합니다. 공급업체가 규제기준이 느슨한 환경이나 비즈니스상 비도덕적인 관행 혹은 다양한 ESG(환경, 사회 및 지배구조) 문제가 있는 환경에서 운영되고 있다면, 위험노출 수준이 리스크 수용범위를 초과할 수 있습니다.

기초 다지기

- **변호사 파견:** 대부분의 third-party 관계는 권리와 의무를 명시한 계약에 종속됩니다. 귀사의 법률자문이 계약서를 작성하는 과정에 관여했을 것이며, 법률자문은 계약서를 해석하는 데 있어서 중요한 자원이 될 수 있습니다.
- **시야 확장:** 현재의 third-party 리스크 관리 체계가 진정 모든 third party를 아우릅니까, 혹은 공급업체에만 국한되어 있습니까? Third-party 리스크 관리 체계가 뇌물, 사업의 연속성과 ESG 측면 등 모든 리스크 영역을 커버하고 있습니까?
- **사례 입증하기:** Third party와 관련된 기업의 사례를 분석하고 전체적인 사업전략과도 연계하여 살펴보세요.
- **사슬 끌어올리기:** Supply chain은 어느 단계까지 내려가야 합니까? 리스크는 제4자 및 그보다 확장된 관계자를 얼마나 세심히 감시해야 하는지를 평가합니다.
- **소규모 기업 의심하기:** 리스크는 third party와의 계약금액수준과 병행하여 감소하지 않습니다. 평판리스크는 공급업체와의 계약관계가 만 달러이든, 백만 달러이든 동일하게 적용됩니다. 당신이 수천 달러를 지출하는 소규모 기업 때문에 수백만 달러의 비용이 들 수 있습니다.

다음 단계 수행

- **사전에 해결하기:** 공급업체 선정 단계에서 팀원들을 참여시켜 그들이 공급업체를 조사하고 문제가 발생하기 이전에 미리 해결할 수 있도록 하십시오.
- **"방화문" 설치하기:** 감사위원회에 추가적인 기술 자원이 필요하다는 것을 입증하십시오. 다음과 같이 이야기를 시작해 보는 것입니다. "경영진은 화재를 진압하기보다는 방화문을 설치해야 합니다."
- **의심하기:** Third-party 관계를 관리하는 책임자가 내부통제를 회피하려는 방법을 예측하십시오. 이를 강화할 수단에 대해 경영진에게 조언하십시오.
- **긍정적으로 생각하기:** Third party의 취약점을 지적하는 데서 그치는 것이 아닌 업무의 일환으로 그러한 관계를 통해 추가적인 가치를 얻을 수 있도록 노력하십시오.
- **페널티 표시하기:** 문제점을 지적하고, 해결책을 얻으며, 계약불이행, 품질문제, 기타행위위반에 대한 페널티를 부과하기 위해 정해진 절차가 존재하는지 (그리고 준수되고 있는지) 파악하십시오.



Internal audit's role in

ESG (environmental, social, and governance)

Although mandated ESG reporting has yet to arrive in many jurisdictions, adoption is imminent in several major economies.

Our view

Internal audit has always had a lot on its plate, but now the serving must be sustainably cultivated, fair-labor harvested, and carbon-neutral transported. It's enough to give a CAE indigestion.

Internal audit groups in large multinationals may find it relatively painless to accommodate environmental, social, and governance (ESG) issues in their audit plans. But for smaller and mid-sized organizations, the alphabet soup of ESG standards and frameworks—GRI, SASB, TCFD, IIRC, and more—may be intimidating. For these groups, we offer this reassurance: You already know more than you think. Yes, there are new requirements, but just as you absorbed COSO, IFRS, FCPA, and other standards, you can handle this.

Fundamentally, ESG assurance is still accounting, albeit using other metrics—such as gallons of water, carbon emissions, and workforce diversity.

Although mandated ESG reporting has yet to arrive in many jurisdictions, adoption is imminent in several major economies. Internal audit should not delay in tackling the issue, as the stakes are simply too high, with pressure exerted by regulators, investors, customers, third-party affiliates, and society at large. The benefits for getting it right may be significant, as "high ESG performance" may translate to better access to capital, talent and business opportunities."

For IA functions just starting on their ESG journey, one early challenge will be identifying responsible parties within the organization. Oftentimes, we find the CFO pointing to investor relations, who look to HR, which passes the buck to legal, who redirects to marketing. Effective coordination among these groups and a focal point of responsibility will be critical to progress.

News item

The COP26 climate talks in Glasgow [led to agreements](#) on phasing out coal power, cutting methane emissions, "greening" the financial services sector, and stopping deforestation. However, not every country was a signatory, with some major CO2 emitters declining to sign. Full adoption, compliance, and accountability remain significant hurdles.

Data points

- Female representation on corporate boards [varies dramatically](#) throughout the world: Australia-34%; Canada-31%; France-43%; Germany-25%; India-17%; Japan-11%; Netherlands-26%; UK-34%; US-28%.
- [World leaders](#) for ESG metrics include Denmark for environmental performance, Finland for absence of discrimination, and Singapore for regulatory quality. The United States does not currently appear in the top 10 in any of these categories.



ESG (환경, 사회 및 지배구조)에 대한 내부감사의 역할

여전히 많은 국가에서 ESG 보고의무가 시행되지 않았지만 여러 경제대국에서 관련 법안의 제정이 임박했습니다.

우리의 견해

본 주제와 관련하여 내부감사에 대한 의견이 항상 분분하지만, 이제 지속가능하게 양성하고 공정한 기회를 부여하고 탄소중립을 지향해야만 합니다. ESG는 최고감사책임자가 소화불량을 일으키기에 충분합니다.

다국적 대기업들의 내부감사 그룹은 감사 계획에 환경, 사회 및 지배구조 (ESG) 문제를 수용하는 것이 비교적 수월하다고 생각할 수 있습니다. 그러나 중소기업들에게는 ESG 기준과 체계(GRI, SASB, TCFD, IIRC 등)와 같은 이해하기 어려운 약어가 겁을 먹게 할 수 있습니다. 우리는 중소기업들이 그들이 생각하는 것보다 훨씬 많은 것들을 알고 있다는 확신을 주어야 합니다. 그렇습니다, ESG에는 새로운 요구사항들이 존재하지만 중소기업들이 COSO, IFRS, FCPA 등 다른 기준을 수용했듯이 본 문제도 해결할 수 있습니다. 기본적으로 ESG 검증이 대량의 수자원, 탄소배출량 및 조직다양성과 같은 다른 측정 기준을 사용하기는 하지만 여전히 회계와 관련되어 있습니다.

여전히 많은 국가에서 ESG 보고의무가 시행되지 않았지만 여러 경제대국에서 관련 법안의 제정이 임박했습니다. 감독 당국, 투자자, 고객, third-party 계열사 및 사회전반의 압력으로 인한 이해관계가 지나치게 높기 때문에 내부감사가 더이상 본 문제를 미루어서는 안 됩니다. "ESG에서 우수한 성과를 거두면 더 나은 자본, 인재 및 사업기회를 얻을 수 있다"는 점에서 ESG 의무를 올바르게 수행하는 것이 중요할 수 있습니다.

ESG 여정을 한창 시작하는 내부감사 그룹의 초기 과제 중 하나가 바로 조직 내 책임자를 파악하는 것입니다. 우리는 CFO로부터 IR담당자로, IR담당자에서 인사관리자에게, 인사관리자로부터 법무부서로, 법무부서에서 마케팅부서로 문제가 전가되는 광경을 흔히 목격합니다. 그룹 간의 효과적인 협력과 책임에 초점을 맞추는 것은 진전에 있어 매우 중요합니다.

뉴스거리

글래스고에서 개최된 COP26(Conference of the Parties, 당사국총회) 기후협약은 석탄발전의 단계적 감축, 메탄 배출 감소, 금융서비스 "녹색화" 및 삼림 벌채 중단에 대한 [합의를 이끌어냈습니다](#). 그러나 일부 주요 이산화탄소 배출국에서 서명을 거부하는 등 모든 국가가 서명국이었던 것은 아닙니다. 모두의 참여, 규정 준수 및 책임이 여전히 중요한 관문으로 남아 있습니다.

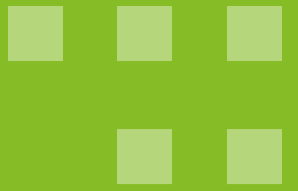
데이터 포인트

- 기업의 이사회에서 여성이 차지하는 비율은 전 세계적으로 [매우 다양합니다](#). 호주(34%), 캐나다(31%), 프랑스(43%), 독일(25%), 인도(17%), 일본(11%), 네덜란드(26%), 영국(34%), 미국(28%)으로 나타났습니다.
- [세계적으로](#) ESG 지표상 선도하는 국가는 환경성과 부문에서 덴마크, 차별이 없는 핀란드, 규제품질 부문에서 싱가포르로 나타났습니다. 미국은 현재 어떠한 항목에서도 상위 10위권 내에 위치하지 않는 것으로 나타났습니다.



For more info on ESG (environmental, social, and governance)

- Deloitte: [Finding the value in environmental, social, and governance performance](#)
- Wall Street Journal: [ESG and the role of internal audit](#)
- Wall Street Journal: [Five steps to building credible climate commitments](#)



Warning signs

- **Marketing hype:** If your marketing department makes claims that are at odds with your ESG audits, reins will need to be quickly pulled in.
- **Outdated policies:** Organizational policies around business travel, remote working, diversity and inclusion, corporate governance, and more should be reviewed and updated to reflect the current business environment and ESG goals.
- **Siloed approaches:** Organizations may literally or figuratively be all over the map, with standards, priorities, and rigor varying by geography or business unit.
- **Divorced from strategy:** ESG considerations should be married to the business strategy. A harmonized approach will further the company's objectives; a disjointed approach can drag down performance.

Getting the fundamentals right

- **Brief the team:** Familiarize your IA team with recognized 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 (TCFD).
- **Check the status:** Analyze the current ESG disclosure process for internal controls: Are controls in place and sufficient? Are findings reported to the board?
- **Offer input:** Provide input on ESG risk indicators. Help assess how ESG risks have been considered within the organization's enterprise risk management process. Is ESG integrated into the broader business strategy?
- **Review the reports:** Determine how management has identified the key issues to disclose and whether they have aligned those topics to recognized standards.
- **Assess independently:** Use standalone assessments to understand appropriate policy, control landscape, and responsibilities.

Taking the next steps

- **Go emerald, not ecru:** Keep a watchful eye out for "greenwashing." Greater scrutiny has slowed the trend, but many organizations still make flimsy claims about their green profile rather than reflecting their true color.
- **Nurture knowledge:** Initiate training as needed to fill knowledge gaps, both within IA and throughout the organization at large. Cover awareness, deep dive sessions, and holistic views.
- **Build credibility:** Upgrade internal audit's qualifications with ESG-related certifications and accreditations earned through professional organizations.
- **Fund the team:** Invest in resources with the right experience and skillset to understand, recognize, and assess ESG risks. Consider creating ESG-dedicated position(s) within internal audit to allow for specialized expertise and increased focus.
- **Integrate ESG:** Include ESG risks within each audit program to inquire about ESG aspects within each function. Report on ESG throughout each audit report.



ESG (환경, 사회 및 지배구조)에 대한 더욱 자세한 정보는

- 델로이트: [Finding the value in environmental, social, and governance performance](#)
- 월 스트리트 저널: [ESG and the role of internal audit](#)
- 월 스트리트 저널: [Five steps to building credible climate commitments](#)



위험신호

- **과도한 마케팅:** 마케팅 부서에서 ESG 감사와 상충되는 주장을 하는 경우, 신속히 통제력을 확보할 필요가 있습니다.
- **오래된 정책:** 출장, 원격 근무, 다양성 및 포괄성, 기업 지배구조 등 기업의 정책을 검토하고 업데이트하여 현재의 사업환경과 ESG 목표를 반영해야 합니다.
- **고립된 접근:** 기업이 따르는 기준, 우선순위 및 규칙의 엄격성은 지역과 사업부에 따라 문자 그대로이든 비유적이든 매우 다양할 수 있습니다.
- **전략에서 분리:** ESG 고려사항과 사업전략이 결합되어야 합니다. 조화로운 접근법은 기업의 목표를 높이지만 일관성이 없는 접근법은 성과를 저하시킬 수 있습니다.

기초 다지기

- **팀원에게 간략히 설명:** 귀사의 내부감사 그룹이 Global Reporting Initiative(GRI, 지속가능보고서에 대한 가이드라인을 제시하는 국제기구), SASB(Sustainability Accounting Standards Board, 지속가능회계기준위원회), GHG(Greenhouse Gas, 온실가스) 프로토콜 및 TCFD(Task Force on Climate Related Financial Disclosure, 기후변화 관련 재무정보 공개 협의체)와 같은 합의된 ESG 보고기준 및 체계에 익숙해 지십시오.
- **상태 확인:** 내부통제에 대한 현행 ESG 공시절차를 분석하십시오. 통제가 적절하고 충분히 운영되고 있습니까? 발견사항이 이사회에 보고되고 있습니까?
- **의견 제의:** ESG 리스크 지표에 대한 의견을 제시하십시오. 기업의 전사적 위험관리 프로세스 내에서 ESG 리스크를 어떻게 고려하는지 평가할 수 있도록 지원하십시오. ESG가 보다 광범위한 사업 전략에 통합되고 있습니까?
- **보고서 검토:** 경영진이 공시할 주요 이슈를 어떻게 식별했는지, 주제를 합의된 기준에 따라 올바르게 조정했는지 판단하십시오. landscape, and responsibilities.
- **독립적으로 평가:** 적절한 정책, 통제환경 및 책임을 이해하기 위해 독립적인 평가를 사용하십시오.

다음 단계 수행

- **담갈색이 아닌 에메랄드 색상:** "그린워싱(위장환경주의)"을 주의 깊게 보십시오. 더 많은 정밀조사는 추세를 늦추었지만, 여전히 많은 기업이 본인의 실제 활동을 반영하기보다 친환경적인 모습으로 외면을 포장하며 설득력 없는 주장을 하고 있습니다.
- **지식 쌓기:** 내부감사와 기업전반에서 지식격차를 메우기 위해 필요한 교육을 시작하십시오. 의식, 심층 조사, 전체론적 관점에서 교육을 시행하십시오.
- **신뢰도 구축:** 전문적인 조직을 통해 취득한 ESG 관련 자격 및 인증으로 내부감사 능력을 개선하십시오.
- **자금 지원:** ESG 리스크를 이해하고 인식하며 평가하는 데 적합한 경험과 기술을 갖춘 자원에 투자하십시오. ESG에 대해 전문적인 지식을 갖추고 집중력을 높일 수 있도록 내부감사에서 ESG에 전념하는 자리를 마련하는 것을 고려하십시오.
- **ESG 통합:** 각 부서의 ESG 측면을 질문하기 위한 각각의 감사 프로그램 내에 ESG 리스크를 포함하십시오. 각각의 감사보고서에 ESG에 대해 보고하십시오.



Internal audit's role in Counter fraud

A maxim for medicine also rings true for business: Prevention is better than cure.



Our view

Every country has its sensationalist, tabloid news outlet. And every executive and CAE hopes to never see their company splashed across that front page.

Indeed, there's no more surefire way to attract unwanted publicity than to suffer a case of insider fraud. But the damage extends well beyond titillating headlines. Fraud hurts not only the reputation of the business, but also the careers of those on whose watch the deceit occurred. Financial consequences, regulatory penalties, customer loss, and competitor gains are all common outcomes. And, in extreme cases, fraud can present an existential crisis for the organization itself.

The problem pervades across industry lines. While financial services and the public sector are generally more focused on this risk, due in large part to the strict regulatory environments they operate in, most other industries lag. Start-ups in particular can struggle with fraud and its aftermath.

Oddly, despite the prominence of the issue, many organizations operate in a state of denial. But this "out of sight/out of mind" posture belies a key factor: fraud, by its nature, involves deception. There are no flashing lights that say "look here." Fraudsters cover their tracks and will do their best to direct your attention elsewhere. So when organizations say, "We don't have a fraud problem," the standard response perhaps should be, "Yes you do. You just haven't found it yet."

What's true in medicine also rings true in business: *Prevention is better than cure*. The best way to minimize fraud losses is to prevent fraud from occurring in the first place.



News item

When the German financial technology company Wirecard disclosed that more than \$2 billion in cash had vanished from its books, the fallout was swift and severe: the stock price plummeted by more than 90%; the CEO resigned; the company filed for insolvency; and several executives were arrested on accounting fraud charges.



Data points

According to the [Association of Certified Fraud Examiners](#):

5%

On average, organizations lose 5% of their annual revenues to fraud.

\$4.5T

More than US\$4.5 trillion is lost due to fraudulent activity each year.

14 mos.

The typical fraud case lasts 14 months before it is detected.



부정행위 대응 에 대한 내부감사의 역할

예방이 치료보다 낫다는 의학적 명언은 사업에도 적용됩니다.



우리의 견해

어느 국가이든 황색언론이 존재하기 마련입니다. 그리고 모든 경영진과 최고감사책임자는 결코 그 신문의 1면을 그들의 기업이 장식되지 않기를 바랍니다.

사실 내부자 부정행위보다 원치 않는 공공의 주목을 끄는데 더 확실한 방법은 없습니다. 그러나 그 피해는 신문의 헤드라인을 자극하는 것 이상으로 확산됩니다. 부정행위는 기업의 평판 뿐만 아니라 부정행위를 지켜보는 개인의 경력 또한 손상시킵니다. 재무적인 결과, 규제 위반 페널티, 고객 이탈 및 경쟁업체가 취하는 이익은 모두 예상 가능한 결과입니다. 그러나 극단적인 경우에는 부정행위가 조직 자체의 실존 위기를 초래할 수 있습니다.

문제는 산업 전반에 확산되어 있습니다. 대체로 금융 서비스와 공공 부문이 엄격한 규제 환경으로 인해 이러한 리스크에 더욱 집중하고 있으나 그 밖의 대부분의 산업은 뒤쳐집니다. 특히 스타트업 기업은 부정행위와 그 후유증으로 어려움을 겪을 수 있습니다.

문제가 부각되었음에도 불구하고 이상하게도 많은 기업들이 이러한 사실을 부정합니다. 그러나 "눈에 보이지 않으면 마음도 멀어진다"는 자세는 본질적으로 부정행위가 속임수를 수반한다는 중요한 사실을 나타냅니다. "여기 보세요" 하며 번쩍이는 불빛 같은 것은 없고, 부정행위를 저지르는 이들이 흔적을 감추고 다른 곳으로 주의를 돌리기 위해 최선을 다할 뿐입니다. 따라서 기업이 "우리에게는 부정행위가 존재하지 않습니다." 라고 말할 때 "그렇습니다. 아직 발견하지 못했을 뿐입니다." 라고 답변해야 합니다.

예방이 치료보다 낫다는 의학적 명언은 사업에도 적용됩니다. 부정행위에서 발생하는 손실을 최소화하는 최고의 방법은 애초에 부정행위가 발생하지 않도록 예방하는 것입니다.



뉴스거리

독일의 금융 기술 기업 Wirecard가 20억 달러 이상의 현금이 장부에서 사라졌다고 발표했을 때, 결과는 신속하고 가혹했습니다. 주가가 90% 이상 폭락했고, CEO가 사임했으며, 회사는 파산을 신청했고, 임원 몇 명은 회계 부정혐의로 체포되었습니다.



데이터 포인트

[Association of Certified Fraud Examiners\(공인부정조사사협회\)](#)에 의하면:

5%

기업은 평균적으로 연수익의 5%를 부정행위로 잃습니다.

\$4.5T

부정행위로 인해 매년 4조 5천억 달러 이상의 손실이 발생하고 있습니다.

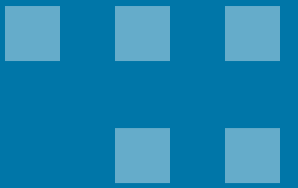
14 mos.

전형적인 부정 사례는 발견되기 전 14개월 동안 지속됩니다.



For more info on counter fraud

- Deloitte: [The nature of fraud is changing](#)
- Deloitte: [Building confidence in your fraud risk framework](#)
- Wall Street Journal: [Five actions to fortify whistleblower plans](#)



Warning signs

- **Extravagant lifestyle:** If the assistant to the junior bookkeeper is driving to work in a top-of-the-range Mercedes-Benz, you might want to recheck their journal entries. An employee living beyond their means is the most common sign of fraudulent activity. (It may seem obvious but it still occurs.)
- **Personal problems:** Certain personal issues can also be an early warning sign for potential fraud, including financial difficulties, divorce, and addiction. According to the [Association of Certified Fraud Examiners](#), "In 63% of cases, the fraudster exhibited red-flag behavior associated with his or her personal life."
- **Work woes:** Some workplace behaviors can also be an indicator of underlying fraud. Among the top concerns: unusually close relationships with vendors or customers; strained colleague interactions; and poor performance evaluations.



Getting the fundamentals right

- **Survey the landscape:** To get a real handle on the risks your organization is facing, conduct a thorough and comprehensive fraud risk assessment. The results should drive subsequent activities—where to focus, spend your time, and invest. This is not a five-minute, one-off exercise: speak to stakeholders, do anonymous surveys, hold workshops, and regularly refresh and challenge the outputs.
- **Pass the test:** It's surprising how many organizations have fundamental gaps or weaknesses in basic internal controls. To deter fraud, adhere to the basics: segregate duties; limit access; set maximum authorizations; conduct background checks; rotate job responsibilities; enforce mandatory vacations.
- **Shore up the infrastructure:** Establish robust fraud reporting mechanisms for use by employees and contractors, allowing for anonymous referrals. Often these involve the use of third-party hotlines; however it is vital that reports received are triaged and appropriate follow-up action taken.



Taking the next steps

- **Mind the gaps:** Once you understand your key risks, correlate them with existing controls to identify gaps, weaknesses, and quick wins. Start closing those gaps. Some will require longer-term fixes; others will be straightforward without requiring a big investment.
- **Train the troops:** With the risks identified and the reporting mechanisms established, anti-fraud training can commence. Be sure to highlight the true cost of fraud, the warning signs, and the reporting mechanisms. Communicate a policy of zero tolerance.
- **Deputize stakeholders:** Your best defense is your stakeholders: employees, middle management, and third parties. Educate them on the threats and key risks. Help them understand how to detect and flag emerging issues. Don't completely open the kimono, though. Keep sensitive information about your best fraud detection techniques under wraps.



부정행위 대응에 대한 더욱 자세한 정보는

- 딜로이트: [The nature of fraud is changing](#)
- 딜로이트: [Building confidence in your fraud risk framework](#)
- 월 스트리트 저널: [Five actions to fortify whistleblower plans](#)



위험신호

- **사치스러운 생활방식:** 만약 주니어 장부 담당자의 조수가 최고급 메르세데스 벤츠를 타고 출근한다면, 기업 장부를 재차 확인해 보는 것이 좋습니다. 신분에 맞지 않는 생활을 하는 직원은 부정행위의 가장 흔한 징후입니다. (진부한 이야기일 수도 있지만 여전히 발생하는 사례입니다.)
- **개인 문제:** 경제적 어려움, 이혼 및 중독을 포함한 특정한 개인의 문제는 잠재적인 부정행위에 대한 사전 경고 신호일 수도 있습니다. [공인부정조사사협회\(Association of Certified Fraud Examiners\)](#)에 의하면, "부정행위 사례 중 63%가 사생활과 관련하여 주의를 기울일 만한 행동을 보였다"고 합니다.
- **업무상 난제:** 직장 내에서 보이는 행동의 일부 또한 부정행위를 암시하는 보편적인 지표가 될 수 있습니다. 가장 우려되는 사항으로는 공급업체 혹은 고객과 비정상적으로 긴밀한 관계, 동료 간의 부자연스러운 관계, 저조한 성과평가 등이 있습니다.



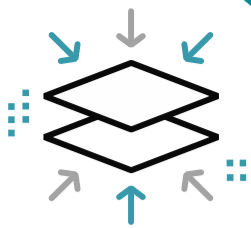
기초 다지기

- **전체 상황에 대한 조사:** 기업이 직면한 위험을 확실하게 파악하기 위해 부정행위에 대해 철저하고 포괄적인 리스크 평가를 수행하십시오. 그 결과로 어디에 집중하고, 어디에 시간을 쓰고, 어디에 재원을 투자할지 등과 같은 후속활동을 이끌어야 합니다. 이는 5분만에 종료되는 일회성 행위가 아닌, 이해관계자와 대화하고, 익명의 설문조사를 수행하며, 워크숍을 개최하고, 정기적으로 결과를 업데이트하고 이의를 제기하는 과정이 되어야 합니다.
- **테스트 통과:** 많은 기업이 기본적인 내부통제에 근본적인 빈틈과 결함을 가지고 있다는 것이 놀랍습니다. 부정행위를 방지하기 위해 업무를 분장하고, 접근을 제한하며, 최대 권한을 설정하고, 배경을 조사하고, 업무를 순환시키고, 강제 휴가를 시행하는 등의 기본에 충실하십시오.
- **인프라 강화:** 익명의 의견을 허용하는, 직원과 거래처가 사용할 수 있는 강력한 부정행위 보고체계를 구축하십시오. 본 과정은 흔히 third-party 핫라인을 사용하는 경우가 많지만, 접수한 의견을 분류하고 적절한 후속 조치를 취하는 것이 중요합니다.



다음 단계 수행

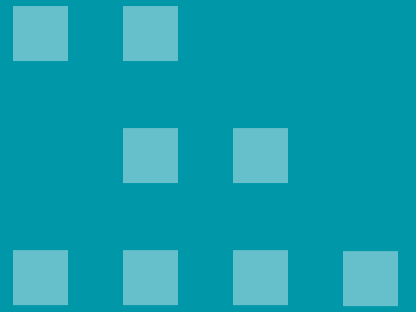
- **차이점을 인지:** 주요 리스크를 이해한 후, 차이점과 취약점 그리고 즉각적인 성과를 파악하기 위하여 기존의 통제와 연관시키십시오. 차이점을 줄이기 시작하십시오. 장기적인 수정이 필요한 리스크가 있는가 하면, 큰 투자가 필요없는 간단한 리스크도 있습니다.
- **부대 교육:** 리스크가 파악되고 보고체계가 구축되면 부정행위를 방지하는 교육을 시작할 수 있습니다. 부정행위로 인해 실제로 발생하는 비용, 위험 신호, 그리고 보고체계를 강조하십시오. 무관용 정책을 제시하십시오.
- **이해관계자 대행:** 최고의 방어책은 직원, 중간 관리자 및 third party와 같은 이해관계자입니다. 이들에게 위협과 주요 리스크를 교육하십시오. 새로운 이슈를 감지하고 표시하는 방법을 이해할 수 있도록 지원하십시오. 그러나 경계를 완전히 낮추지는 마십시오. 최상의 부정행위 적발 방법에 대한 민감한 정보는 비밀로 하십시오.



Internal audit's role in

Mergers & acquisitions

Dealmaking will increase in the post-pandemic economy.
Internal audit can help transactions succeed.



Our view

M&A executives are sending [clear and strong signals](#) that dealmaking will be an important lever as businesses recover and thrive in the post-COVID-19 economy. Just as consumers are reopening their wallets after the pandemic shutdown, companies and private equity investors have accumulated plenty of capital that they are ready to spend. But for the deal to be a long-term winner, with a laser focus on value and risk from the get-go, internal audit must be a key player: pre, post, and everything in between.

Among the thornier issues will be IT system integration. It's not uncommon to find dozens of IT systems among merging companies, all of which will need to be evaluated for compatibility and redundancy. The initial M&A announcement will likely include a rosy assessment of potential synergies, but as the closing date nears, those synergy models may suddenly shrink. There will be intense pressure to make initial projections work, and IT systems is often where the ball is dropped.

Another concern will involve accounting processes. During the transition service agreement (TSA) period, accounting and internal control processes can fall through the cracks, resulting in potentially damaging financial reporting issues. Many companies underestimate the effort required to separate or integrate their systems. It's essential to get the right skillsets involved, rather than just throwing resources at the problem.

And finally, not only must CAEs worry about the overall integration effort, they may also have to contend with the merging of two distinct internal audit groups. The IA functions will need to reconcile differences in vision and role, operating models, workpaper documentation, tools and technology, and more. This IA integration cannot be a back-burner issue: since internal audit will be advising on the overall integration, it is essential for credibility that it have its own house in order. Start early and move quickly are the keys to success.

News item

In 2001, dot-com darling America Online merged with cable-and-content stalwart Time Warner to create a potential media behemoth. But unrealized synergies, clashing cultures, and a bursting dot-com bubble led AOL/Time Warner to suffer a nearly [US\\$99 billion loss](#) in 2002, earning this M&A deal the sobriquet of "[the worst merger of all time](#)." While the deal is now over twenty years ago, the learnings still apply.

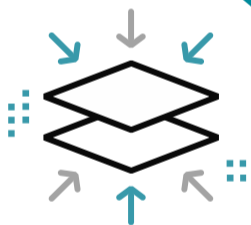
Data points

According to Deloitte's "[Future of M&A Trends](#)" survey:

61%
of US dealmakers expect M&A activity to return to pre-COVID-19 levels within the next 12 months.

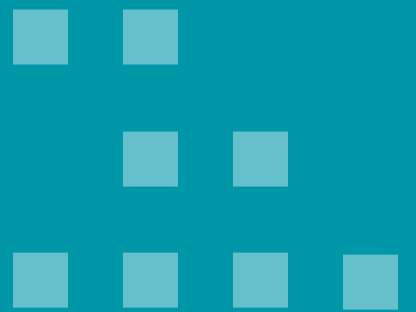
51%
Cybersecurity threats are top of mind for 51% of respondents as companies manage deals virtually.

 Uncertain market conditions, translating business strategic needs into an M&A strategy, and valuation of assets are deemed the biggest challenges to M&A success.



인수합병에 대한 내부감사의 역할

포스트팬데믹 시대에는 딜메이킹이 증가할 것입니다.
내부감사가 딜을 성사시키는 데 도움이 될 수 있습니다.



우리의 견해

M&A 경영진은 포스트코로나 경제에서 사업이 회복하고 번창할 때 딜메이킹이 중요한 수단일 것이라는 [명확하고 강력한 신호](#)를 보내고 있습니다. 팬데믹으로 인한 봉쇄조치 이후 소비자가 다시 지갑을 여는 것처럼 기업과 사모투자자도 지출할 준비가 된 자본을 충분히 축적해 두었습니다. 그러나 거래가 장기적으로 승리하려면, 시작부터 가치와 리스크에 초점을 맞춘 내부감사가 핵심이 되어야 합니다. 즉, 내부감사가 거래 이전, 이후, 그리고 그 사이의 모든 순간에서 핵심이 되어야 합니다.

IT 시스템 통합 또한 곤란한 문제들 중 하나입니다. 합병이 이루어진 기업들 사이에서 IT 시스템을 여럿 발견하는 것은 드문 일이 아니며, 모든 시스템은 호환성 및 불필요한 중복성의 측면에서 평가되어야 합니다. 당초 인수합병(M&A) 발표에는 잠재적인 시너지에 대한 장밋빛 전망을 기대하지만 마감일에 가까워질수록 시너지가 급격히 위축될 수도 있습니다. 초기의 예측이 제대로 작용하도록 하는 강력한 압박이 있을 것이나, IT 시스템에서 종종 실패하기도 합니다.

또 다른 문제는 회계와 관련된 것입니다. TSA (Transition Services Agreement, 이전 서비스 합의) 기간 동안 회계 및 내부통제 프로세스가 제대로 작동하지 않아 재무보고와 관련한 문제가 발생할 수 있습니다. 많은 기업이 시스템을 분리하거나 통합하는 데 필요한 노력을 과소평가합니다. 문제를 해결하는 데 자원을 마구 투입하는 것이 아닌, 올바른 기술을 도입하는 것이 중요합니다.

마지막으로 최고감사책임자는 합병 과정에서 전반적인 통합 뿐만 아니라 두 개의 구분된 내부감사 팀을 병합하는 문제를 두고 고민해야 할 수도 있습니다. 내부감사 기능은 비전 및 역할, 운영 모델, 조서 문서화, 도구 및 기술 등의 차이를 조정해야 합니다. 내부감사는 전반적인 통합에 있어 자문 역할을 하고, 신뢰도를 위해 제대로 처리되어야 할 필요가 있으므로 내부감사 통합이 후순위가 되어서는 안 됩니다. 일찍 시작하고 신속하게 움직이는 것이 성공의 열쇠입니다.

뉴스거리


2001년 닷컴 버블 열풍 속 America Online은 견조한 케이블 및 콘텐츠 기업 Time Warner와 합병하여 미디어 계의 잠재적인 거물이 되었습니다. 그러나 실현되지 않은 시너지와 문화 충돌 그리고 닷컴 버블의 붕괴로 인해 America Online과 Time Warner는 2002년에 [990억 달러 가까이 손실](#)을 입었고, 당 M&A 거래는 "[역대 최악의 합병](#)"이라는 별명을 얻었습니다. 20년이 더 지난 거래이지만, 그 교훈은 여전히 유효합니다.

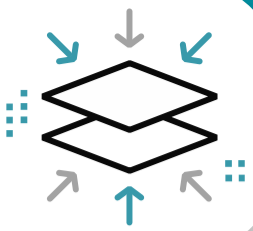
데이터 포인트

딜로이트의 "[Future of M&A Trends](#)" 설문조사에 의하면:

61%
미국의 딜메이커 중 61%가 향후 12개월 이내에 M&A 활동이 코로나 19 이전의 수준으로 되돌아갈 것으로 예상하고 있습니다.

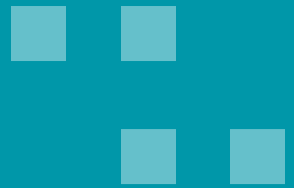
51%
응답자 중 51%가 기업이 사실상 거래를 관리할 때 사이버 보안 위협을 가장 중요하게 생각하는 것으로 나타났습니다.

 불확실한 시장 상황, 사업 전략적 요구사항을 M&A 전략으로 전환, 자산의 가치평가 등이 성공적인 M&A의 최대 과제로 여겨집니다.



For more info on mergers & acquisitions

- Deloitte: [M&A trends survey: The future of M&A](#)
- Deloitte: [M&A: The intersection of due diligence and governance](#)
- Deloitte: [Regulatory realities amid the M&A market's momentum](#)



Warning signs

- **Fundamental mismatches:** Flat vs. hierarchical org charts. Methodical vs. unstructured decision-making. Conservative vs. flamboyant leadership. Some cultural hurdles may be steep to leap.
- **Insufficient rationale:** Achieving economies of scale is often cited as a driver of M&A deals, but if you merge two companies with flawed strategies, poor leadership, or ruthless competition, the only thing you'll be scaling up is likelihood of failure.
- **ESG issues:** Does the acquired company have a patchy ESG (environmental, social and governance) record? Is the deal going to set your own ESG program back a number of years?

Getting the fundamentals right

- **Do due diligence:** As potential deals are evaluated, internal audit should ensure that all process areas are covered; assess existing internal control environment; and review material issues from recent audits.
- **Suss out synergies:** Dealmakers sometimes present an overly optimistic picture of potential synergies. Take an independent look and report findings to the board. Follow up for a year or more post-transaction to see where synergy is and is not being realized.
- **Insert IA:** Internal audit should join the blueprinting sessions, focusing its risk-and-control lens and asking tough questions. (In some deals, internal audit may be shut out of the blueprinting, but once the deal is announced, the function should push to be involved.)
- **Day 1 duties:** Internal audit has a uniquely broad view of the organization—who's who, how the company is connected, where the new company fits in. That knowledge should be utilized as part of Day 1 readiness planning and support.

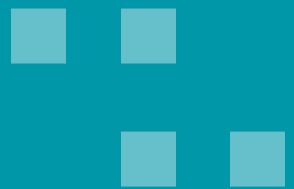
Taking the next steps

- **Compare and counsel:** Get a handle on processes, controls, and technology at the target company. Identify current states; carve out synergies and determine redundancies; identify what is covered by the TSA.
- **Find the exit:** Examine the TSA and recommend changes as needed. Track TSA end dates and assess how the company is preparing for a timely exit without extending the TSA to cover shortfalls.
- **Look back:** Conduct post-transaction assessments to ascertain lessons learned that can be applied to deals going forward.
- **Contemplate compliance:** If the deal pushes the acquiring company into new markets, additional regulatory and reporting requirements will come into play. Assess early to avoid non-compliance and missed deadlines and the headaches they bring.



인수합병에 대한 더욱 자세한 정보는

- 델로이트: [M&A trends survey: The future of M&A](#)
- 델로이트: [M&A: The intersection of due diligence and governance](#)
- 델로이트: [Regulatory realities amid the M&A market's momentum](#)



위험신호

- **근본적인 차이:** 수평적 조직문화와 수직적 조직문화, 체계적인 의사결정과 비체계적 의사결정, 보수적인 리더십과 진보적인 리더십 등 도약하기에 무리가 있는 문화적 장애물이 있을 수 있습니다.
- **불충분한 근거:** 규모의 경제를 달성하는 것이 M&A 거래를 추진하는 요인으로 흔히 언급되지만, 전략에 결함이 있고 형편없는 리더십과 무자비한 경쟁을 하는 두 기업을 합병한다면, 여러분이 확장하게 될 유일한 것은 실패의 가능성이입니다.
- **ESG 관련 이슈:** 인수한 회사가 적절하지 않은 ESG(환경, 사회 및 지배구조) 이력을 가지고 있습니까? 이번 거래로 인해 귀사의 ESG 프로그램이 몇 년 전으로 후퇴할까요?

기초 다지기

- **실사 실시:** 잠재적인 거래에 대하여 평가할 때 내부감사는 기존의 내부통제 환경을 평가하고, 최근 감사에서 중요하게 거론되는 이슈를 검토하는 등 모든 프로세스 영역을 포함하는 것을 보장해야 합니다.
- **시너지 검토:** 딜메이커는 종종 시너지를 지나치게 긍정적으로 표현합니다. 시너지를 독립적으로 살피고 이사회에 발견사항을 보고하십시오. 거래 이후에도 1년 이상 추적하여 어느 부분에서 시너지가 실현되고 있는지와 실현되고 있지 않는지 확인하십시오.
- **내부감사 투입:** 내부감사는 리스크와 통제의 관점에 초점을 맞추고 어려운 질문을 하며 상세한 계획을 설립하는 단계에 참여해야 합니다. (일부 거래의 경우 계획하는 단계에서 내부감사가 배제될 수 있지만, 거래가 발표된 후에는 내부감사 기능이 포함되어야 합니다.)
- **1일차 업무:** 내부감사는 그 담당자가 누구인지, 기업이 어떻게 통합될 것인지, 새 기업이 어떻게 자리를 잡을 것인지 등 기업에 대해 독특하며 광범위한 관점을 가지고 있습니다. 이러한 사고(思考)는 1일차 준비 계획과 지원의 일환으로 활용되어야 합니다.

다음 단계 수행

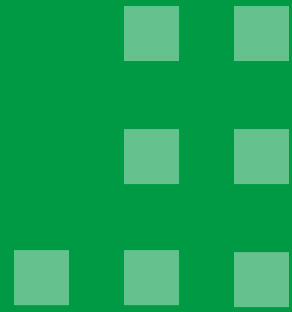
- **비교 및 진단:** 인수대상 기업의 프로세스와 통제기능, 기술에 대해 파악하십시오. 현재의 상태를 파악하고, 시너지를 창출하고, 불필요한 중복을 감별하며, TSA(이전 서비스 합의) 단계에서 이루어지는 사항을 파악하십시오.
- **출구 모색:** TSA(이전 서비스 합의)를 점검하고 필요에 따라 변경할 사항을 권장하십시오. TSA 종료 기한을 확인하고, 기업이 부족분을 채우기 위해 TSA를 연장하지 않고 적절한 시점에 어떻게 빠져나올지를 검토하십시오.
- **되돌아보기:** 거래 후 평가를 수행하여 향후 거래에 적용할 교훈을 파악하십시오.
- **컴플라이언스 고려:** 만약 이번 딜로 인해 인수기업이 새로운 시장에 진출한다면 추가적인 법적 규제와 보고 요건이 적용될 것입니다. 이러한 것들을 사전에 평가하여 규정에 대한 불이행과 기한 초과 및 그로 인해 발생하는 문제를 예방하십시오.



Internal audit's role in

Psychological safety

The old adage, "Safety first," takes on a new meaning for internal audit.



Our view

It has become something of a business bromide to state that work environments should embrace openness, collaboration, and learning, but in fact hard data exists to back the claim. In a two-year study on team performance conducted by Google, the highest-performing teams all adopted the concept of "psychological safety"—the notion that mistakes are a precursor to success and that those who make them should be supported, not punished. Google concluded that when teams have the freedom to engage in strategic risk-taking in a supportive environment, their collective confidence, creativity, and productivity will rise.

The Google study is compelling, but before internal audit starts championing psychological safety for the organization at large, perhaps a look inward is warranted. Is the IA group contributing in a positive or negative way to the psychological safety levels of the organization? To determine the answer, begin with a single-question poll of internal stakeholders: "How does it feel to be audited by us?"

The replies may come as a shock: for most auditees, undergoing an internal audit is akin to an invasive medical test—necessary and important perhaps, but loathed and dreaded nonetheless.

For internal audit, then, psychological safety begins at home. Take steps to make your function less an adversary, more an advisor. Don't just spotlight the bad, also celebrate the good. Don't only scrutinize the past, but envision the future.

To advance psychological safety, IA teams can adopt the statement known as "The Prime Directive": "Regardless of what we discover, we understand and truly believe that everyone did the best job they could, given what they knew at the time, their skills and abilities, the resources available, and the situation at hand." (Norm Kerth, Project Retrospectives: A Handbook for Team Review)



(Historical) news item

Early in his career, American inventor Thomas Edison was fired by Western Union after a failed experiment damaged company property. The termination was short-sighted on the part of his employer, as Edison went on to file over 1,000 patents, inventing the electric light bulb, phonograph, motion picture camera, and many other devices. Years later, Western Union, after neglecting to create a work environment where it was safe to fail, wound up purchasing the rights to one of Edison's inventions.



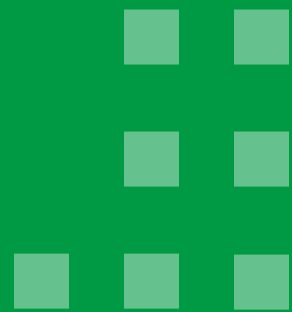
Data points

- Deloitte's 2020 Global Audit Committee survey found that 86% of audit committee chairs said that management is encouraged to present issues and findings to the audit committee, but institutional barriers often prevent this from happening.
- Deloitte's 2018 Global Chief Audit Executive research survey revealed that only 33% of CAEs believe their internal audit function is viewed very positively.
- The resource site Internal Audit 360 found that IA reports "do not usually communicate the positive aspects of the internal control and governance environment."



심리적 안정 에 대한 내부감사의 역할

내부감사에서 "안전제일"이라는 옛말은 새로운 의미를 내포합니다.



우리의 견해

업무 환경이 개방성, 협업과 학습을 구현해야 한다는 의견은 이 분야에서 상투적인 이야기가 되었지만, 실제로 이러한 주장을 입증하는 신빙성 있는 데이터가 존재합니다. 구글이 팀 성과를 주제로 2년 간 수행한 연구에 의하면 최고의 성과를 거둔 팀은 모두 "심리적 안정" 개념을 적용하였는데, 이는 실수가 성공의 근원이며 실수를 저지르는 이들은 처벌이 아닌 지원을 받아야 한다는 개념입니다. 구글은 지원하는 환경에서 전략적인 위험감을 자유롭게 허용하는 것이 조직원의 집단 자신감, 창의성, 생산성을 향상시킨다고 결론을 내렸습니다.

구글의 연구가 설득력 있지만, 전반적으로 내부감사에서 조직의 심리적 안정을 호소하기 이전에, 기업의 내면을 관찰하는 것이 필요합니다. 내부감사 그룹이 기업의 심리적 안정 수준에 긍정적인 방식으로, 혹은 부정적인 방식으로 기여하고 있습니까? 답을 찾기 위해 우선 내부 이해관계자에게 "우리에게 감사 받는 기분이 어떠한지" 질문하십시오.

대부분의 피감사자에게 있어, 내부감사를 받는 것이 의료행위와 유사하게 필수적이고 중요함에도 불구하고 혐오스럽고 두렵다는 답변은 충격으로 다가올 수도 있습니다.

그렇다면 내부감사를 위한 심리적 안정은 내부에서부터 시작해야 합니다. 내부의 그룹이 적이 아닌 조연자가 될 수 있도록 당신의 기능을 조정하십시오. 단지 단점만 부각하는 것이 아닌 장점도 주목하십시오. 과거에만 얽매이지 말고, 미래를 그리십시오.

심리적 안정을 향상시키기 위해, 내부감사 그룹은 "The Prime Directive(프라임 디렉티브)"라고 알려진 주장을 다음과 같이 적용할 수 있습니다. "무엇을 발견하는 상관없이, 우리는 당시 그들이 보유한 지식과 능력, 유효한 자원 및 상황을 고려했을 때 모두가 최선을 다했다고 이해하고 진심으로 믿습니다." (노만 커스(Norm Kerth)의 Project Retrospectives: 팀 리뷰를 위한 핸드북(A Handbook for Team Review) 中)



(역사적) 뉴스거리

미국의 발명가 토마스 에디슨은 그의 경력 초기에 실험 실패로 회사 자산을 손상시킨 후 웨스턴 유니온에서 해고되었습니다. 이후 에디슨이 전구, 축음기, 영화 카메라 등 많은 다른 장치를 발명하며 특허를 1,000건 이상 출원했기 때문에 고용주 입장에서 그를 해고하는 것은 근시안적이었습니다. 몇 년 후 실패를 수용하는 작업환경을 구축하는 것을 간과했던 웨스턴 유니언이 에디슨의 발명품 중 하나에 대한 판권을 구매하게 되었습니다.



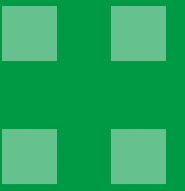
데이터 포인트

- 딜로이트에서 진행한 2020년 글로벌 감사위원회 설문조사에 의하면 86%의 감사위원장은 경영진이 감사위원회에 이슈와 조사결과를 보고하려는 태도를 보이지만, 제도적 장벽이 이를 막는 경우가 많았다고 답했습니다.
- 딜로이트에서 진행한 2018 글로벌 최고감사책임자 설문조사에 의하면 33%의 최고감사책임자만이 자사의 내부감사 체계가 매우 긍정적으로 평가된다고 생각하는 것으로 나타났습니다.
- 리소스 사이트 Internal Audit 360에 의하면 내부감사 보고서가 "일반적으로 내부 통제 및 지배구조 환경의 긍정적인 측면을 전달하지 못한다"고 합니다.



For more info on psychological safety

- Deloitte: [Optimizing internal audit: Developing top-flight teams](#)
- Deloitte: [Creating resilience through psychological safety](#)
- New York Times: [What Google learned from its quest to build the perfect team](#)



Warning signs

- **Excitable execs:** If your audit reports spark eruptions from the c-suite and tremors in the trenches, it may be safe to surmise that psychological safety has not yet been attained across the organization.
- **Averted gazes:** A lack of camaraderie or bonhomie between internal audit and other business units may be a sign that relations are strained, making an environment of psychological safety harder to establish.
- **Misconstrued mission:** If the perceived purpose of internal audit (within and outside the function) is to "provide assurance and advisory services," rather than to "help the organization succeed," then the foundation upon which psychological safety is based, needs shoring up.

Getting the fundamentals right

- **Audit thyself:** Ask your stakeholders how it feels to be audited. If auditees find your audits off-putting or uncomfortable, or if they perceive you more as police and less as advisor, some recalibration may be in order.
- **Watch your language:** Analyze the tone you use in reporting to management and the audit committee. How helpful is it in terms of facilitating good outcomes and creating a positive environment? Consider rephrasings to avoid emotive and accusatory language.
- **Influence the influencers:** Identify influential stakeholders and talk to them about potential steps to create an environment where people have a positive response to audits. How can rough areas be smoothed?

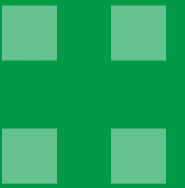
Taking the next steps

- **Revamp the reports:** Strive to tell the story better. Consider separating control environment issues from the rest of the report, recognizing that a poor control environment can be a temporary anomaly due to factors such as implementing new processes or expanding into a new market or country.
- **Accentuate the positive:** Celebrate positive behaviors both within your reports and via separate means, such as internal newsletters, awards, or other recognition. Such actions not only benefit the recipient, but also shine some reflected glow on internal audit itself.
- **Help shift the view of the audit committee:** As a primary consumer of internal audit's reports, the audit committee plays a key role in enabling psychological safety: leading by example, setting the tone, and responding to audit findings as an opportunity for learning and improvement rather than as an occasion for criticism and reprimands.



심리적 안정에 대한 더욱 자세한 정보는

- 델로이트: [Optimizing internal audit: Developing top-flight teams](#)
- 델로이트: [Creating resilience through psychological safety](#)
- 뉴욕 타임즈: [What Google learned from its quest to build the perfect team](#)



위험신호

- **예민한 경영진:** C 레벨의 경영진과 전면에서 감사보고서를 주제로 격동의 불꽃이 튀고 있다면, 아직까지 심리적 안정이 기업 전체에서 확보되지 않은 것으로 추정해도 무방합니다.
- **외면:** 내부감사와 타 사업부 사이의 동료애 혹은 친밀감 결핍은 부자연스러운 관계를 의미하며 심리적 안정 환경을 구축하기 어려움을 나타내는 신호일 수 있습니다.
- **잘못된 임무 해석:** (기능 내외부에서) 내부감사의 인식된 목적이 "조직의 성공을 돕는 것"이 아닌 "검증 및 자문 서비스를 제공"하는 것이라면, 심리적 안정이 기반이 되는 토대를 강화해야 합니다.

기초 다지기

- **스스로를 감사:** 이해관계자에게 감사 받는 기분이 어떤지 질문하십시오. 그들이 내부감사를 냉정하게 느끼고 불편해하거나 조언자가 아닌 경찰로 인식한다면, 일부 재정비가 필요할 수 있습니다.
- **언행에 주의:** 경영진 및 감사위원회에 보고 시 사용하는 어조를 분석하십시오. 어휘를 구사하는 방식이 긍정적인 환경을 구축하고 우호적인 결과를 초래하는데 얼마나 도움이 됩니까? 감정적이고 비난하는 언어를 피하기 위해 표현을 바꾸어 이야기하는 것을 고려하십시오.
- **인플루언서에게 영향 미치기:** 이해관계자를 파악하고 그들과 감사에 긍정적인 반응을 보이는 환경을 조성하기 위한 잠재적인 단계에 대하여 논의하십시오. 어떻게 거친 부분을 순조롭게 진행할 수 있습니까?

다음 단계 수행

- **보고서 개편:** 이야기를 더 나은 구성으로 전달하기 위해 노력하십시오. 새로운 절차를 도입하거나 새로운 시장, 국가로 확장하는 등의 요인으로 인해 허술한 통제환경이 일시적인 예외사항이 될 수 있음을 인지하여, 통제환경과 관련된 이슈를 보고서의 나머지 부분과 분리하는 것을 고려하십시오.
- **긍정적인 면을 강조:** 긍정적 행동을 보고서 이외에도 사내 소식지, 수상내역, 기타 인증내역 등의 별도의 수단을 통해 축하해 주십시오. 이러한 대응은 당사자에게 유익할 뿐만 아니라 내부감사 자체를 돋보이게 할 것입니다.
- **감사위원회에 대한 관점을 전환하도록 지원:** 내부감사보고서의 주 소비자로서 감사위원회는 심리적 안정을 실현하는 핵심적인 역할을 수행합니다. 예를 들어, 감사결과를 비판과 비난 보다는 학습과 개선의 기회로 여기도록 분위기를 잡고, 대응합니다.



Internal audit's role in Cybersecurity

Emerging tech equals emerging threats.



News item

Despite frequent and highly publicized data breaches, news reports publicize only a fraction of all cyberattacks. According to [Security magazine](#), "over half of business owners admit to concealing a data breach."



Data points

- 43% of cyberattacks target small business.
- 64% of companies have experienced web-based attacks.
- 9.7M healthcare records were compromised in September 2020 alone.
- 75B By 2025, 75 billion Internet of Things (IoT) devices will be online.



Our view

Q: What is a chief audit executive's biggest cybersecurity fear?

A: Everything that management thinks is under control.

The CAE's anxiety is well-justified. Here's an abbreviated list of things management typically underestimates:

- How many former employees still have logon rights
- Number of third-party vendors with access to corporate IT systems
- Amount of cloud accounts the company uses
- Total cyber breaches the company has experienced

When correcting these misconceptions, CAEs should pay particular attention to the following issues:

Cloud: Complexity increases as companies outsource services to the cloud, introducing multi dependencies on third parties (supply chain risk), resulting in a wider attack surface. IA needs to leverage cyber cloud skills to address risk in this modern-day, complex IT environment. While the cloud enhances the ability to quickly leverage new capabilities such as AI, machine learning, blockchain, and data lakes, these services also bring a concurrent set of risks.

Consider approaches such as a risk-based "assurance by design" cloud migration strategy; take advantage of native cloud services; and embed security and engage in a multi-cloud strategy. For IT IA, cloud assurance will be a multi-year journey—not one audit and done.

Privacy: With regulators and investors ratcheting up the pressure, privacy must be top of mind for CAEs. Internal audit first needs to understand all the places where personal data resides, and then should pose some challenges to management: Do we need and use all the personal identifiable information(PII) we collect? Does everyone who has access to the data actually require it? Do we have sufficient safeguards to protect PII? Do we have decredentialing processes for former employees? Has remote working impacted data privacy?

Talent: Attracting and retaining cloud and cybersecurity specialists represents a significant challenge for internal audit but winning the talent wars is compulsory. When talking to the technology team about their systems and controls, IT internal auditors who lack "street cred" will be written off for being checklist-driven and failing to add value. Some solutions to the talent crunch may be found in longevity bonuses, training opportunities, career path enhancements, or outsourcing IT IA to a reputable third party.



사이버 보안에 대한 내부감사의 역할

새롭게 부상하는 기술은 새로운 위협을 의미합니다.



우리의 견해

Q: 사이버 보안에 있어 최고감사책임자의 최대 두려움은 무엇입니까?

A: 경영진이 생각하는 모든 것이 통제된다는 사실입니다.

최고감사책임자가 불안감을 느끼는 것은 당연합니다. 경영진이 일반적으로 과소평가하는 사항은 다음과 같습니다.

- 얼마나 많은 퇴사자들이 여전히 로그인 권한을 가지고 있는지
- 기업의 IT 시스템에 접근할 수 있는 third-party 공급업체 수
- 기업에서 사용하는 클라우드 계정 수
- 기업이 경험한 총 사이버 위반 수

이러한 오해를 바로잡을 때 최고감사책임자는 다음 문제에 특히 주의를 기울여야 합니다.

클라우드: 기업들이 서비스를 클라우드 업체에 아웃소싱하면서, third party에 대한 다중 의존성(공급망 리스크)이 도입되고, 공격을 받을 수 있는 영역이 확장되면서 복잡성은 증가됩니다. 오늘날의 복잡한 IT 환경에서 리스크를 극복하기 위해 내부감사는 사이버 클라우드 기술을 활용할 필요가 있습니다. 클라우드가 인공지능(AI), 머신 러닝, 블록체인, 데이터 레이크 등 새로운 기능을 신속하게 도입할 수 있는 역량을 강화하는 반면에, 이러한 서비스들은 리스크도 유발하였습니다.

리스크를 기반으로 한 "설계를 통한 검증"의 클라우드 마이그레이션 전략과 같은 접근법을 고려하고, 네이티브 클라우드 서비스의 장점을 활용하며, 보안을 강화하고, 멀티 클라우드 전략을 도입하십시오. IT 내부감사에서 클라우드 검증은 한 번의 감사로 마무리되는 것이 아닌 수년간의 여정이 될 것입니다.

프라이버시: 규제당국과 투자자가 지우는 부담감과 함께 프라이버시는 최고 감사책임자에게 최우선 고려사항이 되어야 합니다. 우선 내부감사 측면에서 개인 데이터가 보관된 위치를 모두 파악한 후, 경영진에게 다음과 같이 몇 가지 문제를 제기해야 합니다. 우리는 수집한 개인식별정보(PII)를 모두 필요로 하고 사용하고 있습니까? 접근권이 있는 사용자 모두가 실제로도 데이터를 필요로 합니까? 개인식별정보를 보호하는 안전장치를 확보하였습니까? 퇴사한 직원들의 접근권한을 해지하는 절차가 존재합니까? 원격근무가 개인 정보 보호에 영향을 줍니까?

인재: 내부감사에서 클라우드 및 사이버 보안을 담당하는 전문가를 유지하고 유지하는 것이 중요한 과제이지만 인재 전쟁에서 승리하는 것 또한 필수적입니다. 시스템과 통제장치에 대해 기술진과 대화할 때 "누구에게나 통하는 신뢰"가 미흡한 IT 내부감사인은 체크리스트에만 치중하고 부가가치를 창출하지 못한다는 이유로 해고될 것입니다. 우수한 인재 관련 해결책은 장기 보너스를 지급하거나, 교육의 기회를 제공하고, 경력을 향상시키며, 공신력 있는 third party에게 IT 내부감사를 아웃소싱하는 방법에서 찾을 수 있습니다.



뉴스거리

지속적인 데이터 위반이 이목을 모으고 있지만, 수많은 사이버공격 중 공론화되는 사건은 극히 일부로 나타납니다. [Security magazine](#)에 의하면, "반 이상의 기업인이 데이터 침해를 감춘다는 사실을 인정한다"고 합니다.



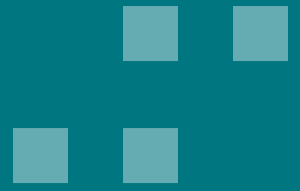
데이터 포인트

- 43% 사이버 공격 중 43%가 중소기업을 대상으로 이루어집니다.
- 64% 기업 중 64%가 인터넷 기반의 공격을 받은 경험이 있습니다.
- 9.7M 2020년 9월에만 970만 건의 의료 기록이 손상된 것으로 나타났습니다.
- 75B 2025년에는 750억 개의 사물인터넷(IoT) 기기가 온라인 형태로 이루어질 것입니다.



For more info on cybersecurity

- Deloitte: [Cybersecurity and the Role of Internal Audit](#)
- Deloitte: [Assurance in the Cloud](#)
- ISACA: [Cloud Computing for Auditors](#)



Warning signs

- **Cyber silence:** If your IT group has reported no attempted cyberattacks, the problem may be a lack of detection capability rather than the absence of bad actors.
- **Cloud control:** If your current cloud migration strategy hasn't developed standards or a cloud-based risk catalog for services to be consumed, you may be leaving risks on the table where your organization has responsibility to implement controls to restrict user access, customize interfaces, or encrypt data, leading to a cloud control problem.
- **Undefined domains:** Clear delineation of responsibilities should exist between the cloud provider and customer. Left undefined, a lack of clarity in this area can give a false sense of security to all parties.

Getting the fundamentals right

- **Train up:** Evaluate the existing cloud and cyber skillset of your team. Address gaps by recruiting, training, and/or outsourcing as needed. Consider creative approaches to attract and retain valuable staff.
- **Follow a framework:** Establish a holistic, risk-based program that is built on a tested cloud and cyber framework. Using the framework as a guide, deliver both assurance and advisory services to gauge cyber capabilities and program maturity.
- **Query providers:** Before settling on a cloud provider, ask for evidence of infrastructure resilience, service downtime, performance, and other metrics. Review the corresponding system and organization controls (SOC) report, if available. Inquire about regulatory compliance and independent controls assessments. Observe red flags and pursue remedies or alternatives if needed.

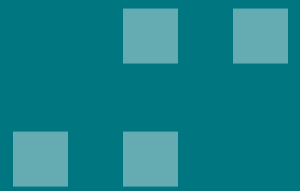
Taking the next steps

- **Embrace the future:** Broaden your audit plan to encompass emerging risks, including IT and data governance; pace of change issues; unbounded IT infrastructure; and new technologies such as AI, RPA, blockchain, virtual and augmented reality, and IoT.
- **Prepare for grilling:** Given recent high-profile cyberattacks and data losses, and the SEC and other regulators' growing expectations, it is critical for internal audit to understand cyber risks and prepare for the questions and concerns expressed by the audit committee and the board.
- **Cross the border:** Regulatory requirements around data privacy vary by jurisdiction. Conduct a comprehensive review that maps areas of operation—both physical and virtual—against local laws and regulations.



사이버 보안에 대한 더욱 자세한 정보는

- 델로이트: [Cybersecurity and the Role of Internal Audit](#)
- 델로이트: [Assurance in the Cloud](#)
- ISACA: [Cloud Computing for Auditors](#)



위험신호

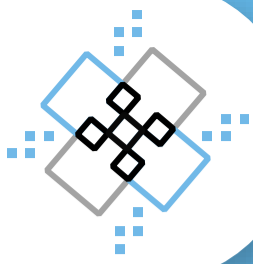
- **사이버 사일런스:** 귀사의 IT 그룹에서 사이버 공격을 당한 경험이 없다고 보고하는 것은 범인이 없는 것이 아니라 공격을 감지하는 능력이 부족할 가능성이 있습니다.
- **클라우드 통제:** 현재 클라우드 마이그레이션 전략에서 사용할 서비스에 대한 기준이나 클라우드 기반 리스크 목록을 개발하지 않았을 경우, 기업이 사용자 접근을 제한하거나, 인터페이스를 커스터마이징하거나, 데이터를 암호화하는 통제를 구축해야 하는 리스크를 떠안게 되어 클라우드 통제 문제로 이어질 수 있습니다.
- **정의되지 않은 도메인:** 클라우드 제공자와 고객 사이의 책임을 명확히 표시해야 합니다. 확실하게 정의되지 않고 방치될 경우, 모든 이해관계자에게 안전에 대해 잘못된 인식을 제공할 수 있습니다.

기초 다지기

- **교육:** 팀에서 사용하는 기존 클라우드와 사이버 기술을 파악하십시오. 필요에 따라 채용, 교육, 아웃소싱을 통해 공백을 채우십시오. 귀중한 직원을 영입하고 유지할 창의적인 방안을 고려하십시오.
- **체계 준수:** 검증된 클라우드와 사이버 체계에 전반적인 리스크를 기반으로 하는 프로그램을 구축하십시오. 본 체계를 기준으로 사용하여, 사이버 역량과 프로그램의 성숙도를 측정하기 위한 검증 및 자문 서비스를 제공하십시오.
- **질문 제공자:** 특정 클라우드 공급사를 결정하기 이전에, 인프라의 복원력과 서비스 중단 시간, 성능 및 그 밖의 지표에 대한 증거를 요청하십시오. 가능하다면 해당 SOC(System and Organization Controls, 시스템 및 조직 컨트롤) 보고서를 검토하십시오. 규제 준수 및 독립적인 통제 평가 방법에 대해 문의하십시오. 경고 신호에 주의하고 필요한 경우 해결 방법이나 대응책을 추구하고하십시오.

다음 단계 수행

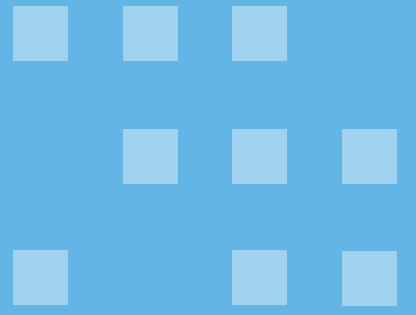
- **미래를 수용하기:** IT 및 데이터 거버넌스와 변화의 속도, 끝없는 IT 인프라와 AI, RPA, 블록체인, 가상/증강 현실, IoT 등의 신기술과 같은 새로운 리스크 항목들을 포함하여 감사계획을 확장하십시오.
- **질문 공세에 대비:** 최근 세간의 이목을 끄는 사이버 공격과 데이터 손실, 그리고 SEC 및 기타 규제기관의 기대치가 증가하는 것을 감안했을 때, 내부감사에서 사이버 리스크를 이해하고 감사위원회와 이사회에 질문과 우려사항에 대응하는 것이 상당히 중요합니다.
- **국경 너머:** 개인 정보에 대한 규제요건은 국가별로 상이합니다. 기업이 영위하는 물리적 지역과 가상의 장소를 매핑하고 현지 법률 및 규정을 전체적으로 검토하십시오.



Internal audit's role in

Diversity, equality, and inclusion

Internal audit has both an opportunity and an obligation to foster a diverse and inclusive culture.



Our view

Historically, internal audit has been primarily a quantitative operation, focusing on hard data and measurable outcomes and steering clear of qualitative issues that lack distinct KPIs. Those days are gone.

Current events and trends—including reckonings around racism, injustice, and inequality—have pushed internal audit into a new realm: diversity, equality, and inclusion (DEI). While this represents a non-traditional area for the function, numerous factors—both lofty and pragmatic—compel internal audit to take stock of DEI initiatives across the organization and play a role in advancing them:

- Discriminatory practices are inherently objectionable. Internal audit has both an opportunity and an obligation to help an organization to foster a diverse and inclusive culture.
- A diverse workforce and inclusive culture are essential components of successful organizations, correlated with improved job performance, reduced turnover, and decreased absenteeism.

- Diversity, equality, and inclusion are critical attributes for job-seekers, and organizations that embrace DEI will have an advantage in recruiting and retaining top talent.

Internal audit, with its broad perspective on risk and its extensive relationships across the organization, is uniquely suited to help organizations assess their current state of DEI and advise on appropriate paths forward. This includes serving as catalysts by advising on risk indicators and KPIs; assessing whether DEI programs are meeting their intended objectives; and reporting results to the board, committees, and senior leaders.

Internal audit should be on the lookout for—and advise against—any quick-fix or shallow solutions proposed or enacted by management. If the DEI initiative seems like a band-aid approach, employees and the marketplace will quickly take note.



News item

In 2018, a UK tribunal ruled that a luxury brands firm had a "blind spot on race." In a discrimination case brought by an employee, the Central London Employment Tribunal cited multiple offenses by the company, including a biased recruitment process, inadequate equality and diversity training, and unwarranted covert surveillance of the worker.



Data points

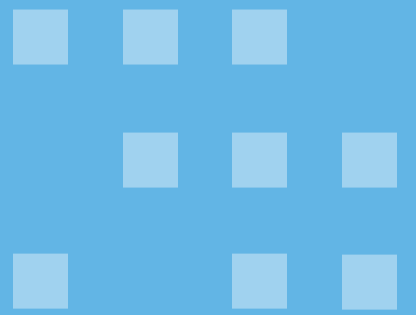
In a 2019 Deloitte survey, [64% of respondents](#) said they had experienced or witnessed bias in the workplace within the prior 12 month a significant weakness in the culture of many organizations. Yet about [70% percent of internal audit groups](#) do not assess organizational culture as part of their audit plan.



다양성, 평등성 및 포용성

에 대한 내부감사의 역할

다양하고 포용적인 문화를 조성하는 것은 내부감사의 기회이자 의무입니다.



우리의 견해

역사상 내부감사는 하드데이터 및 측정 가능한 결과물에 집중하고 명확한 KPI(Key Performance Indicators, 핵심성과지표)가 결여된 질적인 문제를 피하면서 주로 양적 운영에 매진하였습니다. 이러한 날들은 모두 지나갔습니다.

최근의 인종, 차별 및 불평등에 대한 견해를 포함한 사건들과 추세는 내부감사를 다양성(Diversity), 평등성(Equity) 및 포용성(Inclusion) (이하, DEI)이라는 새로운 영역으로 밀어붙였습니다. 이는 기능적으로 기존의 방식에서 벗어난 관점을 제시하며, 기업 전반적으로 내부감사가 이상적이면서 현실적인 다양한 요소를 통해 DEI에 대한 계획을 분석하고 성사시키는 역할을 하도록 요구합니다.

- 차별적인 관습은 본질적으로 불쾌합니다. 내부감사는 조직이 다양하고 포용적인 문화를 조성할 수 있도록 도움 기회와 의무가 있습니다.
- 다양한 인적자원과 포용적인 문화는 업무성과를 향상시키고 이직률과 결근율을 감소시키는 성공적인 기업의 필수 구성요소입니다.

- 다양성, 평등성 및 포용성은 구직자가 견뎌야 할 중요한 자질이며, DEI를 수용하는 기업은 최고의 인재를 채용하고 유지하는데 유리합니다.

기업전반의 리스크 및 광범위한 관계를 전체적으로 고려하는 내부감사는 기업이 DEI의 현황을 평가하고 적절한 경로에 대해 조언하는 기능에 최적화되어 있습니다. 이는 리스크 지표 및 KPI에 대해 조언하고, DEI 프로그램이 계획한 목적을 달성하고 있는지 평가하며, 이사회, 위원회 및 고위임원에게 결과를 보고하는 촉매제 역할을 하는 것을 포함합니다.

내부감사는 경영진이 제안하거나 제정한 일시적이고 피상적인 해결책에 경계하며 주의를 기울이고 이에 대해 조언해야 합니다. 만약 DEI 계획이 급박한 응급조치와 같이 보인다면 직원들과 시장은 빠르게 주목할 것입니다.



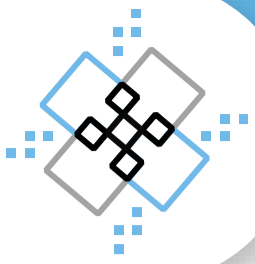
뉴스거리

2018년에 영국의 법원은 어느 명품 브랜드 기업에게 "인종주의의 맹점"이 존재한다는 판결을 내렸습니다. 어느 직원이 고발한 차별사건에서 런던 중앙 고용재판소는 편파적인 채용 절차, 평등성 및 다양성에 대한 부적절한 교육, 근로자에 대한 비밀스러운 부당한 감시 등 기업의 다양한 위법 행위를 인용했습니다.



데이터 포인트

2019년 딜로이트의 설문조사에서 [응답자의 64%](#)가 지난 12개월 이내에 직장에서 편견을 경험 혹은 목격했다고 답변하여 많은 조직문화의 심각한 취약성을 드러냈습니다. 그럼에도 대략 [70%의 내부감사 그룹](#)은 조직문화를 감사 계획의 일부로서 평가하지 않는 것으로 나타났습니다.



For more info on diversity, equality, and inclusion

- Deloitte: [The inclusion imperative for boards](#)
- Wall Street Journal: [Internal audit's role in driving diversity, inclusion](#)
- Wall Street Journal: [Board diversity improves but key goals decades away](#)



Warning signs

- **Redundant resignations:** Resignations and the reasons behind them may offer clues into whether diversity or inclusion problems exist. If root causes for resignations reveal a pattern, evaluate for underlying cultural issues.
- **Social scuttlebutt:** Negative postings on job boards or social media may be a harbinger of DEI problems. Initiate regular site scanning to stay attuned to the trends; automated tools or a third-party contract can make this process less burdensome.
- **Damning demographics:** Your organization's demographic data can shine a light on bias or discriminatory practices. Scrutinize board, c-suite, and senior leader composition; hiring, promotion, and termination practices; salary, bonus, and benefit awards; and other metrics.

Getting the fundamentals right

- **Start small:** Develop a culture assessment to determine the existence and scope of DEI initiatives. Document what your organization is currently doing to understand, communicate, and shape its corporate culture.
- **Incorporate risks:** Include DEI risks in your audit plan. Assess current DEI initiatives to determine if they are meeting their objectives. Inform stakeholders on DEI improvement opportunities and progress in each audit report.
- **Aid and abet:** Help leadership understand the implications of an unhealthy organizational culture as viewed through a risk lens. Provide input on training, communications, and policies.
- **Ask questions:** To understand employees' perceptions and experiences and to identify potential risks, develop as part of the audit plan a standard questionnaire to guide interviews with stakeholders. Conduct interviews with a diverse sampling of employees.

Taking the next steps

- **Facilitate improvement:** Assess the methods used to monitor, measure, and report on the program and evaluate whether any improvements can be made.
- **Validate statistics:** If your organization publishes DEI statistics to the marketplace, provide assurance on accuracy and controls.
- **Tap tools and tech:** Leverage innovative tools and technologies, such as risk sensing, to assess DEI issues and identify potential risks.
- **Reconcile realities:** Develop recommendations to close the gap between leadership perceptions and employee realities in corporate culture.



다양성, 평등성 및 포용성에 대한 더욱 자세한 정보는

- 델로이트: [The inclusion imperative for boards](#)
- 월 스트리트 저널: [Internal audit's role in driving diversity, inclusion](#)
- 월 스트리트 저널: [Board diversity improves but key goals decades away](#)



위험신호

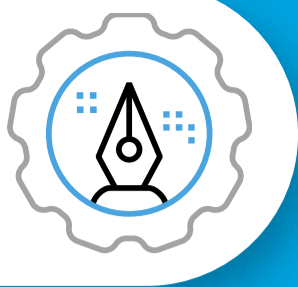
- **불필요한 사직:** 직원 사임과 그 배후에 있는 이유를 파악하면 다양성 및 포용성 문제 유무에 대한 단서를 확보할 수 있습니다. 사임의 근본적인 원인에 대한 규칙을 파악했다면, 문화에 대한 기저 문제를 분석하십시오.
- **SNS상의 소문:** 취업 게시판 혹은 소셜미디어에 게재된 부정적인 게시물이 DEI 문제의 징후일 수 있습니다. 트렌드에 대응하기 위해 사이트를 정기적으로 훑어보기 시작하십시오. 자동화 도구나 third-party 업체를 통해 본 절차에 대한 부담을 경감할 수 있습니다.
- **불가피한 인구통계학적 지표:** 기업의 인구통계학적 데이터는 편견 혹은 차별적 관행을 규명할 수 있습니다. 이사회, C 레벨의 경영진 및 리더의 구성과 채용, 승진 및 계약기간 종료에 대한 관행, 급여, 상여금 및 복리후생 제도와 그 이외의 것들을 면밀히 검토하십시오.

기초 다지기

- **작은 것부터 시작하기:** DEI에 대한 계획의 존재 및 범위를 파악하기 위해 문화에 대한 평가를 실시하십시오. 조직문화를 이해하고, 소통하고, 형성하기 위해 기업이 현재 어떤 일들을 하고 있는지 기록하십시오.
- **리스크 포함하기:** DEI와 관련한 리스크를 감사계획에 포함하십시오. 현재의 DEI 계획이 목표를 달성하고 있는지 평가하십시오. DEI를 개선할 수 있는 기회와 진행 상황을 각각의 감사보고서를 통해 이해관계자에게 전달하십시오.
- **도움과 지원:** 리스크에 대한 시각을 통해 살펴본 불건전한 조직 문화가 미치는 영향을 리더가 이해할 수 있도록 지원하십시오. 교육, 커뮤니케이션 및 정책에 대한 정보를 제공하십시오.
- **질문하기:** 직원의 지각(知覺)과 경험을 이해하고 잠재적인 리스크를 파악하기 위해 감사계획의 일환으로 이해관계자와의 표준 설문지를 개발하십시오. 다양한 직원과 인터뷰를 진행하십시오.

다음 단계 수행

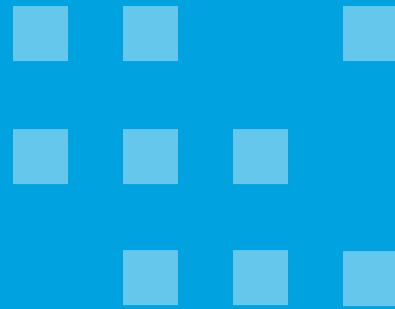
- **개선 추진:** 프로그램에 대한 모니터링, 측정 및 보고 방법을 평가하고 개선이 이루어질 수 있는지 분석하십시오.
- **통계 입증:** 기업이 시장에 DEI에 대한 수치를 공개한다면, 그러한 수치에 대한 정확성 및 통제성을 검증하십시오.
- **도구 및 기술 활용:** DEI에 관한 문제를 평가하고 잠재적인 리스크를 파악하기 위해 리스크 감지 도구와 같은 혁신적인 도구와 기술을 활용하십시오.
- **현실과 조화:** 조직문화에서 지도자의 지각(知覺)과 직원의 현실 간의 차이를 줄이기 위한 권고사항을 개발하십시오.



Internal audit's role in

Assurance by design

For transformations or implementations, controls should be a forethought, not an afterthought.



Our view

If you spent a cool half million for a Lamborghini, you'd surely take full advantage of its massive 12-valve engine, its g-force acceleration, and its multiplicity of bells and whistles.

Yet the same cannot be said for organizations that invest similar sums for enterprise resources planning (ERP) systems. In our experience, a wide array of ERP internal control features are either insufficiently validated and implemented, or go entirely unused. It's the equivalent of buying an expensive Italian sports car and never taking it out of second gear.

Getting your money's worth from your ERP investment begins long before go-live. It starts with adopting a controls-conscious mindset to effectively manage operational and strategic risks across the organization.

That is, rather than consider your ERP system merely as a means of efficiently managing HR, inventory, financials, customers, or supply chain, you should look at it as a tool to manage the many risks associated with these activities.

A controls mindset pertaining to significant company implementations/transformations begins with aligning on the nature and scope of activities performed across the three lines of defense to both efficiently navigate risks and also ensure there are no gaps: the first-line business units, the second-line risk and compliance professionals, and the third-line internal auditors. This coordination/collaboration exercise should not be taken lightly, as it is the foundation upon which a successful ERP deployment or upgrade is built.



News item

In a 2018 audit of a U.S. government agency, almost half of the cited deficiencies were related to its IT systems. Among their findings, the auditors noted that agency didn't implement security controls meant to detect accidental or unauthorized changes to financial data.



Data points

In a recent Deloitte poll, [nearly one-half of all executives](#) said that technology implementations—including ERP, automation, cloud migration and controls related to remote work and associated risks—will drive their organizations to remediate financial processes in the year ahead.



설계를 통한 검증에 대한 내부감사의 역할

개혁 및 구현 시, 사후가 아닌 사전에 통제를 고려해야 합니다.



우리의 견해

당신이 람보르기니를 구매하는 데 몇지게 50만 달러의 거금을 지불했다면 거대한 12기통 엔진이나 중력가속도 등 다양한 부가 기능을 최대한 활용할 것입니다.

그러나 전사적 자원 관리 시스템(ERP)에 유사한 금액을 투자하는 기업을 동일한 맥락에서 볼 수는 없습니다. 경험상 기업의 다양한 ERP의 내부통제 기능은 충분히 검증 혹은 구현되지 않거나, 혹은 전혀 사용되지 않습니다. 값비싼 이탈리아 스포츠카를 구입한 후 2단 기어에서 절대 변속하지 않는 것처럼 말입니다.

ERP에 투자한 것에 대비해 충분한 가치를 얻는 과정은 시스템을 실행하기 훨씬 전부터 시작됩니다. 그 과정은 기업 전체적으로 운영 및 전략적 리스크를 효과적으로 관리하기 위해 통제가 필요하다는 사고방식을 도입하는 것에서 시작됩니다.

즉 ERP 시스템을 단순히 인사, 재고자산, 재무, 고객 혹은 공급망에 대한 효율적인 관리방법으로만 간주하는 것이 아닌 이러한 활동과 관련된 다양한 리스크를 관리하는 수단으로 인식해야 합니다.

중요한 기업의 구현 및 전환에 적용되는 통제에 대한 사고방식은 리스크를 효율적으로 탐색할 뿐만 아니라 차이가 없도록 확실히 하기 위하여, 1차는 사업부 단위, 2차는 리스크 및 컴플라이언스 전문가, 3차는 내부감사인으로서 이루어진, 즉 3차 방어선에 걸쳐 수행되는 활동의 유형 및 범위를 조정하는 것에서 시작합니다. 이러한 조율 및 협업 절차가 성공적인 ERP를 구축하고 개선하는 것에 대한 기초가 되기 때문에 가볍게 여겨서는 안 됩니다.



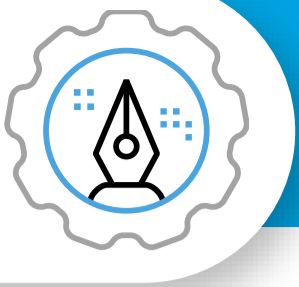
뉴스거리

2018년에 미국 정부기관을 대상으로 진행한 감사에서 발견한 결함 중 대략 절반이 IT 시스템과 관련된 것이었습니다. 발견사항 중에서 감사인은 정부기관이 재무 데이터에 대한 우발적이거나 승인되지 않은 변경을 감지하는 보안 통제를 구축하지 않았다고 주장하였습니다.



데이터 포인트

최근 딜로이트의 설문조사에서 [전체 경영진의 절반에 가까운 인員](#)이 ERP, 자동화, 클라우드 마이그레이션 및 원격근무 등 관련 리스크에 관한 통제를 포함한 기술을 구현하는 것이 향후 1년동안 그들 기업의 재무프로세스의 개선을 이끌 것이라고 답변했습니다.



For more info on assurance by design

- Deloitte: [Assurance by design: Drawing up the control playbook for transformations](#)
- Deloitte: [Modernizing the three lines of defense model](#)
- Wall Street Journal: [Assurance by design – consider control needs up front](#)



Warning signs

- **Unflipped switches:** A surprising number of organizations fail to take advantage of the robust controls built into enterprise resources planning (ERP) software such as SAP and PeopleSoft. Control environments that rely heavily on manual controls may be more susceptible to delays, errors, and fraud.
- **Climbing costs:** Your post-implementation costs could be significantly larger if controls and the associated assurance are not adequately considered upfront.
- **Stubbed toes:** Confusion and inefficiencies may reign if compliance teams are stepping on each other's toes or are unclear as to who is doing what.

Getting the fundamentals right

- **Reach out:** Connect with broad stakeholder groups across the enterprise to help identify needed business process and controls capabilities.
- **Share wisdom:** Advise business leaders to consider not only financial risk but also operational and strategic risk, which will by necessity involve a broader set of controls and capabilities necessary to achieve business objectives.
- **Eye modernization:** Identify opportunities to automate or modernize controls to increase efficiency, reduce error, and automate the provision of assurance.

Taking the next steps

- **Tap expertise:** If your organization is considering a transformative project or system implementation, ensure that control owners engage with risk and compliance and internal audit from the start.
- **Align with the strategy ...:** Take the time to get your three lines of defense aligned. Clarify roles and responsibilities. Defuse tensions and head off turf wars. Think granularly around steps and activities.
- **... and the auditors:** Develop a detailed methodology and strategy around how controls are considered and validated during the implementation, and fully align with the company's auditors to avoid surprises after go-live.
- **Consider owners, not just controls:** Look at control owner readiness, not just control readiness. This involves training the control owners on what they need to do after go-live to meet compliance requirements.



설계를 통한 검증에 대한 더욱 자세한 정보는

- 딜로이트: [Assurance by design: Drawing up the control playbook for transformations](#)
- 딜로이트: [Modernizing the three lines of defense model](#)
- 월 스트리트 저널: [Assurance by design – consider control needs up front](#)



위험신호

- **꺼진 스위치:** 의외로 많은 기업이 SAP, PeopleSoft 등 ERP 소프트웨어에 내장된 강력한 기능을 활용하지 못합니다. 수동통제에 크게 의존하는 통제환경은 지연, 오류 및 부정행위에 더 취약할 수 있습니다.
- **비용 상승:** 통제 및 관련된 검증을 사전에 적절히 고려하지 못하면 구축 이후 상당히 많은 비용이 발생할 수 있습니다.
- **부담된 발가락(서로간의 개입):** 컴플라이언스 팀이 서로의 업무에 개입하거나 누가 어떤 역할을 하는지 불분명할 경우 혼란과 비효율성이 증가할 수 있습니다.

기초 다지기

- **접근하기:** 전체적으로 기업에서 필요한 비즈니스 프로세스 및 통제능력을 파악하기 위해 광범위한 이해관계자 그룹과 가까워지십시오.
- **지식 공유하기:** 기업의 리더에게 재무 리스크 뿐만 아니라 운영 및 전략적 리스크와 같이 비즈니스 목표를 달성하는 데 필요한 광범위한 통제와 역량을 고려하도록 조언하십시오.
- **현대화 주시:** 효율성을 증대하고, 오류를 감소하며, 검증 준비를 자동화하기 위한 통제를 자동화 혹은 현대화할 수 있는 기회를 파악하십시오.

다음 단계 수행

- **전문지식 이용하기:** 기업에서 혁신적인 프로젝트 또는 시스템 구현을 고려하고 있다면, 통제 책임자는 처음부터 리스크, 컴플라이언스 및 내부감사가 참여되도록 하십시오.
- **전략에 맞게 조정...:** 시간을 할애하여 3차 방어선을 조정하십시오. 역할과 책임을 명확히 하십시오. 갈등을 완화하고, 영역 간 갈등을 제거하십시오. 절차 및 활동을 세분화하여 생각하십시오.
- **...감사인에 맞게 조정:** 통제가 어떻게 고려되고 시행 과정에서 검증되는지에 대해 상세한 방법론과 전략을 개발하고, 실제로 실행으로 옮긴 후에도 예상치 못한 사건이 발생하지 않도록 감사인과 충분히 조율하십시오.
- **통제 뿐만 아닌 책임자도 고려:** 단순히 통제를 준비하는 것 뿐만 아니라 통제 책임자의 준비성 또한 살펴보십시오. 이는 컴플라이언스 요건을 충족하기 위해 실행 이후 무엇이 필요한지를 통제 책임자에게 교육하는 절차를 포함합니다.



Internal audit's role in

Bullying & harassment

Toxic culture has emerged as a material root cause of many failing companies. Internal audit can help clear the air.



Our view

Given the preponderance of workplace harassment and bullying stories in the news, we were curious: Why aren't more companies getting out in front of this issue? The excuses were as varied as they were misguided:

- 1 "If you make a big deal of it, you're going to get loads of complaints and reports."
- 2 "We've had a few cases, but they are unrelated and not indicative of our overall corporate culture."
- 3 "We've got a longstanding code of conduct that protects us."

Internal audit has a significant part to play in supporting a company in taking culture risk seriously and minimizing reliance on these misconceptions.

The purpose of internal audit is not to be a moralizer, referee, or sheriff, but rather as facilitator, observer, and advisor. Culture risk can be assessed by triangulating data points from various sources including surveys, interviews, focus groups, risk sensing tools, analytics, and compliance /conduct programs. Analyzing a combination of qualitative and quantitative sources allows a comprehensive picture to be built to anticipate and mitigate potential problem areas.

The benefits of proactively addressing culture issues can be manifold. For example, in an environment where competition for top talent is fierce, organizations that build a positive, supportive, and trusting environment that allows employees to thrive will attract and retain the most desirable workers. Ultimately a positive workplace culture enables achievement of organizational aims. Conversely, organizations that fail to cultivate such a culture may incur significant reputational, regulatory, legal, and financial repercussions.



News item

In 2021, New York Governor Andrew Cuomo resigned from office amid a sexual harassment probe following accusations brought by nearly a dozen women. An investigation described the work environment in the governor's office as "[extremely toxic, extremely abusive](#)."



Data points

86%

of executives surveyed around the world rate culture as "very important" or "important."

12%

of companies believe their organizations are driving the "right culture."



따돌림 및 괴롭힘에 대한 내부감사의 역할

유해한 문화는 기업이 실패하는 근본적인 원인으로 부상했습니다. 내부감사가 상황을 개선하는 데 도움이 될 수 있습니다.



우리의 견해

언론에서 보도하는 압도적인 직장 내 따돌림 및 괴롭힘에 대한 이야기를 보면서 우리는 왜 더 많은 기업이 이러한 문제에서 빠져나오지 못하는지 의문스러웠습니다. 우리가 무지했던 만큼 다양한 핑계가 존재했습니다.

- 1 "대단한 일로 만들어 버리면, 수많은 항의와 보고를 받게 될 것입니다."
- 2 "우리가 겪은 일부의 사례가 우리의 전반적인 조직문화를 나타내지 않습니다."
- 3 "우리에게는 오랜 기간동안 우리를 보호해 준 행동지침이 있습니다."

내부감사는 기업이 문화적 리스크를 신중하게 받아들이고 이러한 오해들에 대한 의존을 최소화하도록 지원하는데 중요한 역할을 합니다.

내부감사의 목적은 윤리학자나 심판 또는 보안관이 아닌 협력자, 관찰자 또는 조언자의 역할을 수행하는 것입니다. 설문조사, 인터뷰, 포커스 그룹, 리스크 감지 도구, 분석 및 컴플라이언스와 행동 강령 프로그램 등 다양한 데이터를 삼각측량하여 문화 리스크를 평가할 수 있습니다. 질적 및 양적 데이터의 조합을 분석하면 잠재적인 문제가 발생할 영역을 예측하고 완화하는 전반적인 모습을 구축할 수 있습니다.

문화 문제를 적극적으로 해결함으로써 얻는 혜택은 다양할 수 있습니다. 예를 들어 최고의 인재를 위한 경쟁이 치열한 환경에서, 직원이 성장할 수 있도록 긍정적이고, 지원을 아끼지 않고, 신뢰할 수 있는 환경을 구축하는 기업은 가장 가치있는 인적자원을 유치하고 유지할 것입니다. 궁극적으로 긍정적인 조직문화는 기업이 목표를 달성할 수 있도록 합니다. 반면 이러한 문화를 조성하지 못하는 기업은 후에 평판, 규제, 법률 및 재정적인 측면에서 상당한 영향을 받을 수 있습니다.



뉴스거리

2021년에, 뉴욕 주지사 Andrew Cuomo는 대략 열 두 명의 여성의 고발에 따른 성희롱 수사가 진행되는 동안 사임했습니다. 수사는 주지사실에서의 업무 환경을 "[극도로 유해하고, 극도로 모욕적](#)"이라고 묘사했습니다.



데이터 포인트

86%

전 세계 경영진을 대상으로 진행한 설문조사에 의하면 86%가 문화는 "매우 중요"하거나 "중요"하다고 평가했습니다.

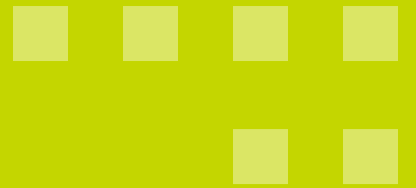
12%

기업 중 12%가 본인의 기업이 "올바른 문화"를 추진한다고 믿고 있습니다.



For more info on bullying & harassment

- Deloitte: [Workplace culture and conduct: Challenges & opportunities](#)
- Deloitte: [Designing work for well-being](#)
- Wall Street Journal: [Well-being can offer healthy returns](#)



Warning signs

- **Sounds of silence:** One warning sign might be no warning signs. Employees may have gone silent because prior complaints have fallen on deaf ears. Other communication squelchers: fear of retribution; convoluted reporting processes; onerous burdens of proof.
- **Talent drought:** If you've noted accelerating attrition or slowed hiring, cultural issues may be a factor.
- **Background noise:** Negative feedback on social media and job search sites can be precursors to full-blown crises that play out in newsrooms and courtrooms.
- **Pressure cooker:** Organizations that exert unrelenting pressure around quarterly earnings and sales targets may be creating an environment where harassment and bullying arise. Abusive behavior is often correlated with unrealistic or unattainable performance demands.

Getting the fundamentals right

- **Take stock:** Take an Inventory of and review codes of ethics, anti-fraud programs, misconduct policies and procedures, and hotlines or alternative reporting mechanisms with an eye toward timeliness, clarity, relevance, and enforceability.
- **Talk shop:** Encourage board and audit committee to add work culture as a recurring topic to their agendas.
- **Bust siloes:** Consider who is in charge of culture issues. Oftentimes responsibility is fragmented among HR, legal, compliance, and business units. Sometimes one team raises concerns, another investigates, and the rest of the organization is left in the dark. Become the matchmaker who brings the parties together.

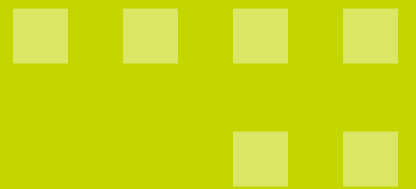
Taking the next steps

- **Consult:** Advise management on establishing a culture risk assessment framework that provides insight into organizational culture, employee engagement and behaviors, and market signals.
- **Measure:** Add cultural assurance to your audit plan. Establish, monitor, and report on metrics related to employee conduct and ethical violations and ensure the board reviews these data points.
- **Incentivize:** Recommend realignment of pay for performance and reconsideration of how pay incentives drive behavior.
- **Evangelize:** Urge frequent messaging and comprehensive training on culture issues.
- **Report:** Your audit reports on culture need not "name and shame," but can frame the discussion around data and trends: "In the last six-month period, we had X number of claims, X of which were substantiated, representing a decrease of X percent over the prior period. The following proactive steps by management contributed to the improvement ..."



따돌림 및 괴롭힘에 대한 더욱 자세한 정보는

- 델로이트: [Workplace culture and conduct: Challenges & opportunities](#)
- 델로이트: [Designing work for well-being](#)
- 월 스트리트 저널: [Well-being can offer healthy returns](#)



위험신호

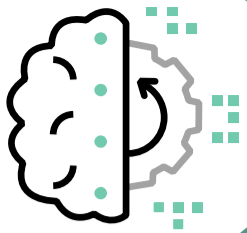
- **침묵의 소리:** 위험신호 중 하나는 위험신호가 존재하지 않는다는 것입니다. 이전에 항의한 사항을 무시했기 때문에 직원들이 침묵하는 것일 수도 있습니다. 이 밖에도 커뮤니케이션을 제한하는 요인에는 보복에 대한 두려움, 복잡한 보고 절차, 입증에 대한 부담이 있습니다.
- **인력 가뭄:** 직원이 이탈하는 속도가 가속되거나 채용되는 속도가 둔화되었다면 문화적인 문제가 원인일 수 있습니다.
- **배후 소리:** 소셜 미디어와 채용 게시판에 적힌 부정적인 의견은 뉴스 및 법정에서 일어날 법한 위기가 만발했다는 징후일 수 있습니다.
- **압박감이 커져가는 상황:** 분기별 수익 및 매출 목표를 달성하는 것에 대해 끊임없이 압박을 가하는 기업은 따돌림 및 괴롭힘이 발생하는 환경을 형성하고 있을 수 있습니다. 폭력적인 행위는 종종 비현실적이거나 달성 불가능한 성과를 요구하는 것과 관련이 있습니다.

기초 다지기

- **목록 작성:** 적시성, 명확성, 관련성 및 집행가능성을 감안하여 행동지침, 부정행위 방지 프로그램, 잘못된 정책 및 절차, 핫라인 혹은 그 밖의 보고 체계에 대한 목록을 작성하고 검토하십시오.
- **전문적인 이야기:** 이사회와 감사위원회에게 조직문화를 정기적인 안건으로 추가하도록 장려하십시오.
- **부서간 장벽 허물기:** 문화에 대한 문제를 누가 담당하고 있는지 생각해 보십시오. 책임은 종종 인사부, 법무부서, 컴플라이언스 부서 등 각 사업부별로 세분화됩니다. 때때로 어느 팀에서 문제를 제기하고, 다른 하나의 팀이 문제를 조사하면, 나머지 직원들은 기업에서 무슨 일이 일어난지 모른 채 남게 됩니다. 여러 부서를 한데 모으는 중매인 역할을 하십시오.

다음 단계 수행

- **자문 구하기:** 경영진에게 조직문화, 직원의 참여와 행동 및 시장신호에 대한 통찰력을 제공하는 문화 리스크 평가 체계를 구축하도록 조언하십시오.
- **측정하기:** 감사계획 단계에서 문화적 보장을 추가하십시오. 직원의 행동 및 윤리 위반과 관련한 측정 기준을 수립하고, 모니터링하고, 보고하며 이러한 데이터 포인트를 이사회가 검토하도록 하십시오.
- **인센티브 제공하기:** 성과에 맞추어 급여를 지급하도록 권고하고 인센티브를 제공하는 것이 행동에 어떤 영향을 미치는지 재고하십시오.
- **메시지를 전달하기:** 지속적으로 문화에 대한 메시지를 전달하고 전체적인 교육을 실행하도록 촉구하십시오.
- **보고하기:** 문화에 대한 감사보고서로 "이름을 밝혀 창피를 줄" 필요는 없지만 다음과 같이 데이터 및 동향을 중심으로 논의될 수 있습니다. "지난 6개월 간 X건의 건의사항이 제출되었으며, 그 중 X건은 전기대비 X% 감소했습니다. 경영진의 다음 사전예방적 조치가 개선에 공헌하였습니다..."



Internal audit's role in Automation

Among many tough questions: "How does IA leverage automation to keep up with automation?"

Our view

Gourmets from the Ligurian to the Adriatic have long debated a vexing question: "Which came first, the chicken Parmesan or the eggs Florentine?"

Management faces a similar dilemma when it comes to internal audit: "Which comes first: Get our house in order and then bring in internal audit? Or bring in internal audit to help us get our house in order?"

The problem is particularly acute when it comes to automated solutions such as AI (including automation and cognitive intelligence). Deployment can be messy; governance controls can be sloppy; security can be porous—all of which can significantly impact management's expected ROI for their automation journey, and worse, create internal- and external-facing strategic risks.

If management is hesitant to engage with your internal audit group for fear of negative findings, here's your rejoinder: "Automation is here to stay, but the technology will continually evolve. Software, hardware, opportunities, and vulnerabilities all represent a moving target. As such, the business value from automation may never be realized if you don't involve internal audit."

Once your IA team is engaged, what are the priorities? Start by helping management find a balance between risk taking and risk appetite. Connect early in the process, when strategic decisions about automation are first being made. Ideally, the relationship will include both advisory and assurance elements—helping the organization realize ROI and then providing assurance services for its automation deployment.

Simultaneously, adapt your audit plan to the new environment. Risk assess new capabilities (impacted business processes, ways of working, and new enabling technologies) across key risk domains, such as financial, operational, regulatory, technology, and strategic, and then prioritize based on impact and vulnerability criteria.

Next, inspect your own house. Determine the required skillsets for auditing automated solutions. Can you train to fill the gaps? Or will you have to recruit new staff with the necessary credentials?

Finally, you'll need to grapple with your own vexing conundrum: "How do we leverage automation to keep up with automation?"

News item

The prognosis looked dim for a large technology company with an ambitious plan to revolutionize healthcare through artificial intelligence (AI), after its supercomputer spat out "multiple examples of unsafe and incorrect treatment recommendations" for cancer patients.

Data points

In a recent Deloitte survey:

- 83% of executives said artificial intelligence will be important to their business success in the next two years.
- 23% said their team currently audits advanced digital capabilities.
- 59% said they were not involved in the development of their organization's automation program.



자동화 에 대한 내부감사의 역할

다양한 어려운 문제 중, "자동화를 따라가기 위해 내부감사에서 어떻게 자동화를 활용하고 있습니까?"

우리의 견해

"치킨 파마산과 에그 플로렌틴 중 어느 것이 먼저 존재했는가" 라는 지겨운 문제에 대해 리구리아부터 아드리아 해의 미식가들은 오랫동안 논쟁해 왔습니다.

경영진 또한 내부감사와 관련해서 비슷한 딜레마에 마주합니다: "문제를 해결한 후에 내부감사를 들여오는 것이 순서입니까, 내부감사를 통해 문제를 해결하는 것이 순서입니까?"

특히 (자동화 및 인지 기능을 포함한) AI와 같은 자동화된 솔루션에서 문제가 더욱 심각해집니다. 시스템을 구현하는 과정이 복잡하거나, 거버넌스 통제가 미흡하거나, 보안이 허술하거나, 이러한 모든 것은 자동화 여정에 대한 경영진의 기대 ROI에 큰 영향을 미칠 수 있으며, 더 안 좋은 것은 기업 내외부에서 전략적 리스크를 유발할 수 있습니다.

경영진이 부정적인 결과가 두려워 내부감사팀과 소통하는 것을 망설인다면 이렇게 대답하십시오. "자동화는 이제 우리 생활의 일부가 되었지만 기술은 끊임없이 발전할 것입니다. 소프트웨어, 하드웨어, 기회 및 취약성은 모두 움직이는 표적을 의미합니다. 따라서 내부감사를 수반하지 않으면 자동화로 인한 사업가치를 영원히 실현하지 못할 수 있습니다."

내부감사팀이 투입된 이후의 우선순위는 무엇입니까? 위험감수와 위험성향 사이에서 경영진이 균형을 유지할 수 있도록 지원하는 것부터 시작하십시오. 처음 자동화에 대한 전략적 결정을 내리는 과정 초기에 그들과 가까워지십시오. 이상적인 관계는 기업이 목표하는 ROI를 실현하도록 지원한 후, 자동화 도입에 검증을 제공하는 자문 및 검증의 요소를 모두 포함할 것입니다.

아울러 새로운 환경에 맞추어 감사계획을 조정하십시오. 재무, 영업, 법률, 기술 및 전략 등의 전반적인 주요 리스크 영역에서 새로운 능력 (영향을 받는 사업 절차, 업무 방식, 가능하도록 하는 기술)에 대한 리스크를 평가한 후 영향 및 취약성을 기준으로 우선순위를 결정하십시오.

그 다음 귀사의 문제를 분석하십시오. 자동화된 솔루션을 감사하는데 필요한 기술을 파악하십시오. 차이를 줄이도록 직원을 단련시킬 수 있습니까? 혹은 필요한 자격 요건을 갖춘 새로운 직원을 채용해야 합니까?

결국, "자동화를 따라가기 위해 자동화를 어떻게 활용하는지"와 같은 지겨운 문제를 해결해야 합니다.

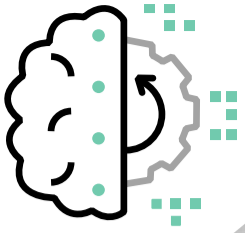
뉴스거리

어느 대형 기술을 가진 기업이 인공지능(AI)을 통한 헬스케어 업계에 대한 야심 찬 변혁을 계획했지만, 슈퍼컴퓨터가 암 환자를 대상으로 "불안전하고 잘못된 치료 권고안"의 다양한 사례"를 내뱉은 후 그러한 예측이 수그러들었습니다.

데이터 포인트

최근 딜로이트의 설문조사에 의하면:

- 83% 경영진의 83%가 인공지능이 향후 2년 간 사업을 성공시키는 데 중요할 것이라고 합니다.
- 23% 경영진의 23%가 본인의 팀이 현재 선진화된 디지털 역량에 대한 감사를 진행하고 있다고 답변했습니다.
- 59% 경영진의 59%가 본인 기업의 자동화 프로그램 개발에 참여하지 않는다고 답변했습니다.



For more info on automation

- Deloitte: [Auditing the risks of disruptive technologies | Keep the tempo](#)
- Deloitte: [Moving internal audit deeper into the digital age: Part I](#)
- Deloitte: [Moving internal audit deeper into the digital age: Part II](#)



Warning signs

- **Ad hoc approaches:** If HR is deploying AI while AP is rolling out RPA and R&D is tinkering with NLP, you've got a piecemeal approach to automation deployment that's likely rife with vulnerabilities.
- **Chair shortage:** If internal audit doesn't have a seat at the table when automated solutions are first being discussed, chances of successful deployment are diminished.
- **Lack of access:** A major hindrance to auditing automated solutions is an inability to review software code and design documentation.



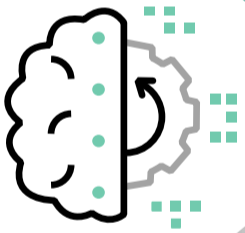
Getting the fundamentals right

- **Take stock:** Understand the business strategy, vision, and journey related to the deployment of automated solutions. How are risk-related matters considered as part of that journey?
- **Ask questions:** What new risks come with these new technologies? How do we ensure our metrics and models are accurate? How do we safeguard against bias in our algorithms?
- **Take controls:** Determine business objectives to advise on the design of control activities and/or perform pre-implementation reviews.



Taking the next steps

- **Build structure:** Create an automation technology risk management strategy and governance structure to manage risks and enable compliance.
- **Cast a wide net:** When auditing automation solutions, include areas such as controls, governance, development lifecycle, strategy, and code reviews.
- **Revamp reports:** Modernize your reporting for the new era. Identify the level and structure of reporting that will be conducted, including technology-level vs. business function-level and assurance-driven vs. consultative. Reconsider the frequency and speed of your audits.



자동화에 대한 더욱 자세한 정보는

- 딜로이트: [Auditing the risks of disruptive technologies | Keep the tempo](#)
- 딜로이트: [Moving internal audit deeper into the digital age: Part I](#)
- 딜로이트: [Moving internal audit deeper into the digital age: Part II](#)



위험신호

- **에드혹(Ad hoc) 접근법:** RPA(Robotic Process Automation, 로봇 프로세스 자동화)를 통해 미지급금이 처리되고, NLP(Natural Language Processing, 자연어 처리)를 통해 연구개발비가 처리되는 동안 인재부에서 시를 도입하고 있다면, 자동화를 도입하는 데 취약점이 가득한 단편적인 접근법을 취하고 있는 것입니다.
- **논의 부족:** 만약 내부감사가 처음 자동화 솔루션에 대해 논의하는 자리에서 언급되지 않으면, 성공적으로 도입할 가능성은 줄어듭니다.
- **접근권한 미달:** 자동화 솔루션을 감사하는 과정에서 중요한 난관은 소프트웨어 코드와 설계 문서에 대한 검토가 불가능하다는 점입니다.



기초 다지기

- **점검하기:** 자동화 솔루션 도입과 관련된 비즈니스 전략, 비전 및 과정을 이해하십시오. 그러한 과정에서 리스크와 관련된 문제를 어떻게 일부분으로 고려합니까?
- **질문하기:** 이러한 신기술이 어떤 새로운 리스크를 수반합니까? 우리의 기준과 모델이 정확하다는 것을 어떻게 확인합니까? 알고리즘 속의 편견으로부터 어떻게 우리를 보호합니까?
- **통제권 쥐기:** 통제활동 설계에 대해 조언하기 위해 사업의 목표를 파악하거나, 혹은 도입 전 검토를 실행하십시오.



다음 단계 수행

- **체계 구축:** 리스크를 관리하고 컴플라이언스를 가능하게 하기 위해 자동화 기술에 대한 리스크 관리 전략 및 거버넌스 체계를 구축하십시오.
- **넓게 다루기:** 자동화 솔루션을 감사할 때 통제, 거버넌스, 개발주기, 전략 및 코드 검토 등의 부문을 포함하십시오.
- **보고서 보완:** 보고 방식을 새로운 시대에 맞추어 현대화하십시오. 기술수준 혹은 비즈니스 기능수준으로 보고할지, 검증중심 혹은 자문중심으로 보고할지를 포함하여 수행될 어질 보고서의 수준과 구조를 파악하십시오. 감사의 빈도와 속도를 재고하십시오.



Peter Astley
Global Internal Audit Leader
+44 20 7303 5264
pastley@deloitte.co.uk



Darryl Butler
Global Internal Audit, Growth
+1 404 220 1357
dbutler@deloitte.com



Sarah Fedele
Global Internal Audit, Transformation
+1 713 982 3210
sarahfedele@deloitte.com



David Tiernan
Global Internal Audit, Innovation
+44 113 292 1520
datiernan@deloitte.com



Neil White
Global Internal Audit, Digital
+1 212 436 5822
nwhite@deloitte.com



Emily Byrne
Global Internal Audit, Program Lead
+1 709 758 5093
embyrne@deloitte.com

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 each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

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 (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2022. For information, contact Deloitte Global.