Deloitte.

Internal Audit:
Risks and opportunities for 2022

Table of contents

03 | Introduction

04 | Third-party risk management (TPRM)

06 | ESG (environmental, social, and governance)

08 | Counter fraud

10 | Mergers & acquisitions

12 | Psychological safety

14 | Cybersecurity

16 | Diversity, equality, and inclusion

18 | Assurance by design

20 | Bullying & harassment

22 | Financial controls

24 | Automation

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.

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.

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 your 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.

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 CO_2 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.

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 (TFCD).
- **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.

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.

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.

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.

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.

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."

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.

Internal audit's role in

Cybersecurity

Emerging tech equals emerging threats.

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.

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.

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.

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 months, suggesting 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.

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.

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 sportscar 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.

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.

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."

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 …"

Internal audit's role in

Financial controls

UK SOX is on the horizon, with EU, Africa, Australia, and others poised to follow suit.

Our view

Once US businesses got over the initial shock of the Sarbanes-Oxley Act of 2002, many approached the law not just as a compliance requirement, but as a chance to bring about transformational improvements in their internal controls over financial reporting. The imminent arrival, in an as-yet-unknown form, of the British equivalent, dubbed "UK SOX," offers companies doing business in the UK the same opportunity.

Activities required to comply—and beyond—will impact much of the organization, with internal audit being no exception. Fortunately, lessons learned from the US SOX legislation can help inform your response to its UK progeny. Here are some key takeaways for internal audit and the organization at large:

- A form of UK SOX will likely be introduced in 2023/24. No matter how much time you think you have to prepare, it won't be enough. **Start planning now.**
- When enacted, UK SOX is expected to rank among the world's highest standards for internal control over financial reporting (ICFR). Even if your organization doesn't operate in the UK, **adhering to these rigorous requirements** makes good business sense.
- In ramping up for UK SOX, the demand for talent will be intense, with the largest companies quickly sucking up resources. Mid-size and smaller organizations should **lock in support** now so as not to be caught short later.
- New controls may be required to comply with UK SOX, but in the pandemic era, you should also **reexamine controls that lost rigor** as a result of the rapid move to remote-work arrangements.
- Since US SOX was enacted in 2002, significant advances have been made in **digital controls**, which you should consider leveraging for UK SOX.
- The audit committee and the executive team have critical roles to play in UK SOX implementation. Those parties with firsthand experience with US SOX will get it; the others will **need some tutoring.**
- Some organizations will do only the minimum required to comply. Others will **seize the moment** as an opportunity for transformational improvement. We wrote about these vanguard companies in the *Harvard Business Review* in 2006.

News item

In 2019, the US Securities and Exchange Commission (SEC) charged four public companies with failing to maintain internal control over financial reporting (ICFR) for multiple annual reporting periods. Consequences of the failure included financial penalties, remediation requirements, and reputational damage.

Data points

1400

In 2017, nearly 1,400 public companies in the US reported material weakness in ICFR.

80%

According to a 2013 US Government Accountability Office study, 80% of all companies surveyed viewed the auditor attestation requirement of US SOX as beneficial to the quality of the company's controls.

For more info on financial controls

- **Deloitte:** Considerations for internal audit in light of UK SOX
- **Deloitte:** The future of controls
- **GOV.UK:** Restoring trust in audit and corporate governance

Warning signs

- **Inauspicious audits:** If your external auditor has recently uncovered material weaknesses or significant deficiencies, or if your organization has been forced to restate previously issued financial statements, you may have some work to do to be ready for UK SOX.
- **Manual labor:** Financial processes that are heavily dependent on manual entries and controls will typically suffer a greater likelihood of error than automated systems.
- **New (and old) tech:** The rollout of new enterprise resources planning (ERP), customer relationship management (CRM), and other technology systems can create new risks to ICFR. Older IT systems can also lack modern controls.
- **Departures and arrivals:** The departure of senior finance and accounting personnel can often precipitate a weakness in the control environment. And recent or pending mergers or acquisitions will present new challenges to be addressed.

Getting the fundamentals right

- **Assess areas:** Undertake a financial risk assessment and fraud risk assessment to define the perimeter, to show the breadth of areas likely to be in-scope, and to map processes and identify risks and internal controls.
- **Define good:** Pick an area and undertake a pilot to understand both what good looks like and the likely resource requirements for a full-scope ICFR compliance project.
- **Eye IT:** Agree on the in-scope IT systems. Failure to identify in-scope systems early enough is one of the top causes of non-compliance with US SOX as it leaves insufficient time to assess essential IT controls.
- **Maintain independence:** While internal audit will be a key stakeholder for UK SOX, the function should not be tasked with implementation. Instead, IA should assist the organization with readiness for UK SOX through consultation, recommendation, and validation.

Taking the next steps

- **Make it sustainable:** Identify and validate clear and robust entity-level controls.
- **Look outside:** Identify outsource providers/third parties whose activities impact ICFR and thus may be in-scope.
- **Do documentation:** Generate robust process documentation for material business cycles, with clear process owners. Identify the material controls.
- **Create robust processes:** Define and evidence a robust process for on-going monitoring and year-end assessment of the design and operating effectiveness of material controls.
- **Face up to failure:** Define a significant control failure or weakness that would require detailed consideration and disclosure of remediating actions. Define reporting processes including remedial action tracking.

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.

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.

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.