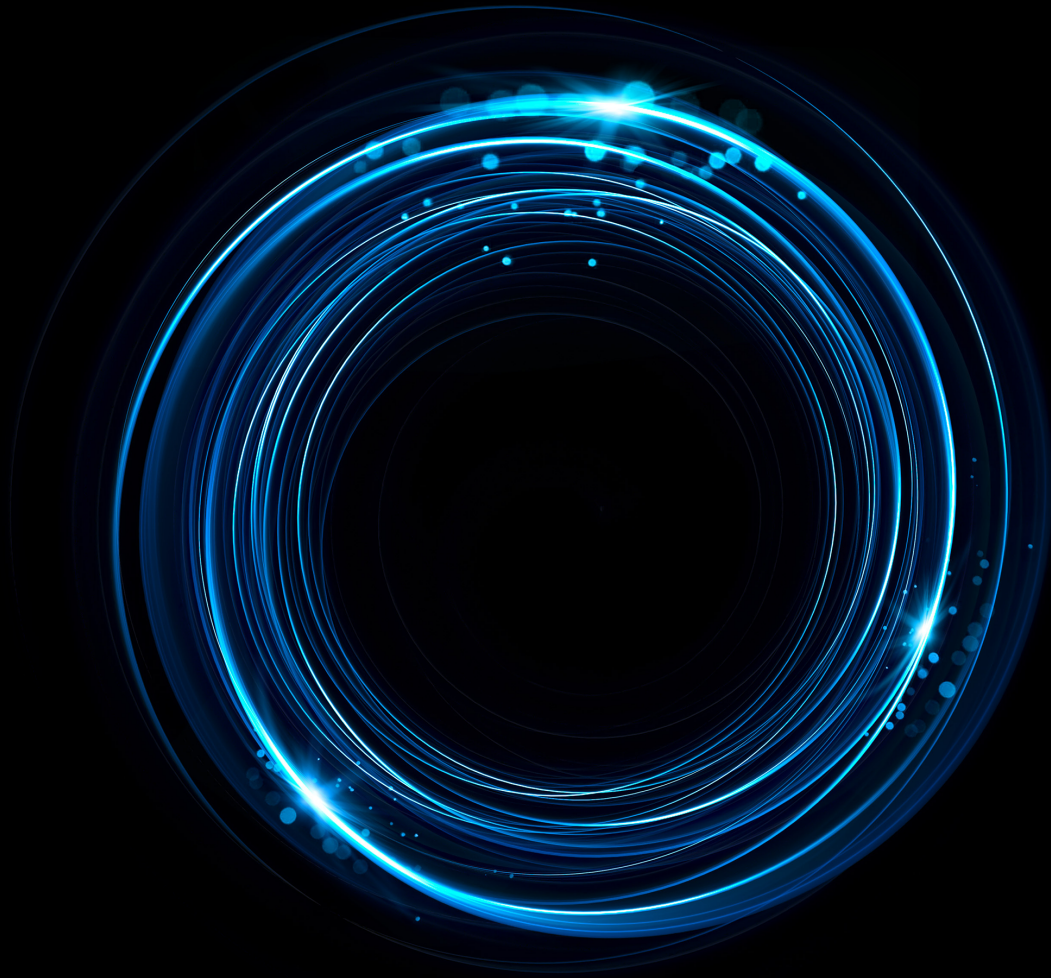


**Deloitte.**



## Rethinking IT internal audit

A new mindset for today's IT-driven enterprise

Business strategy and technology strategy are rapidly converging. In many instances, IT is no longer just an enabler of the business; it is the business. This coalescence is readily apparent in the technology sector among companies that have either grown up in the cloud or transitioned to cloud-centric business models. Instances where technology is driving the business model are less obvious, but no less important in other sectors. In a world where everything from automotive manufacturing to electricity to banking relies upon technology to exist—as well as to thrive—the traditional way of auditing IT needs to change. Internal Audit (IA) is being challenged to realign itself with IT's new strategic role and to act as an adviser, not solely as an auditor.

## The board imperative

Boards are recognizing this paradigm shift, and they expect IT not just to keep pace, but also to think critically about how IT-centric business models affect risk. As outlined in [The tech savvy board: Engaging with CIOs and management on strategy, risk and performance](#), technology governance and oversight in the boardroom has traditionally reinforced the necessity to defensively protect and preserve an organization and its assets.<sup>1</sup> Increasingly, boards are shifting their focus to understand how technology can also be leveraged offensively to create and

enable new opportunities, business models, and revenue sources.<sup>2</sup> Furthermore, they are trying to understand the new kinds of technology risks. These risks are pervasive, touching nearly every aspect of the business, such as the risk of not executing a new strategy because of IT issues; failing to have the technology infrastructure needed to deliver a world-class customer experience or to support an M&A growth strategy; or the inability to enter a new market due to technological deficiencies.



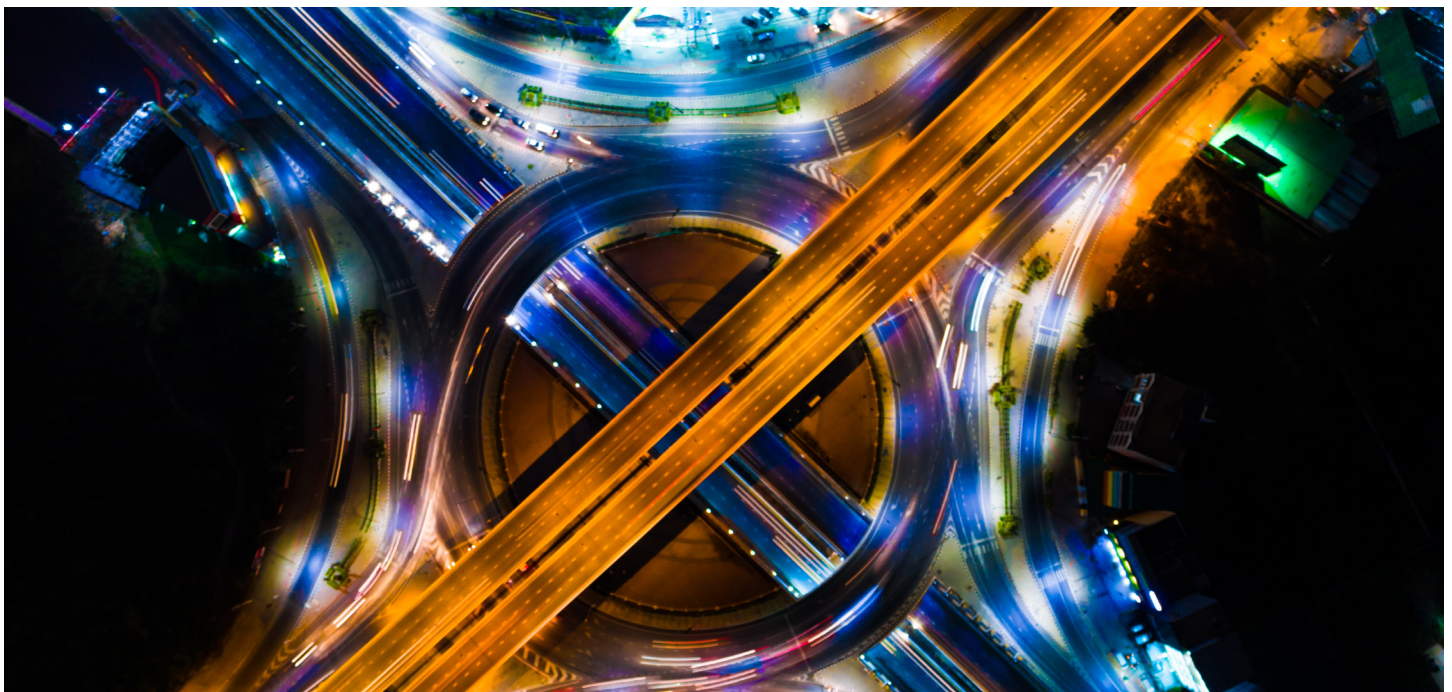
<sup>1</sup> Tonie Leatherberry et al., "The tech savvy board: Engaging with CIOs and management on strategy, risk, and performance", Deloitte Insights, May 15, 2019.

<sup>2</sup> Ibid.

Additionally, an important, overriding risk is often overlooked. When a business strategy is technology-led, it then becomes dependent upon rapid changes in technology innovation. For example, the swift movement to hybrid and multicloud infrastructures, if not kept up with, can provide an advantage to a competitor who is more tech-savvy or forward-looking. In other words, Company A may have a superior business strategy but a less sophisticated technology platform, and thus it may lose share to Company B, which has the inverse.

As boards shift their attention to a broader set of technology risks and opportunities, IA is being challenged to do the same. The traditional bifurcated approach, where IT-related concerns are handled by a separate IT internal audit group, should be updated to address today's heavily IT-centric business models. As technology transforms, disrupts, and enables entire businesses, the notion of identifying and assessing IT risks as a separate discipline has become a thing of the past.

IA, in many instances, is still functioning with the legacy concept that IT supports, rather than leads, business strategy. Business units and IA commonly view IT as a supporting enabler; thus the IT internal audit group typically focuses on auditing areas such as IT general controls, cybersecurity strategy, cloud migrations, and ERP implementations. The output is typically gap analyses, which outline omissions and vulnerabilities in various controls. Though valuable for understanding the security and controls ramifications of different IT initiatives and for shoring up a company's cyber defenses, this approach creates its own gap because it doesn't articulate how the findings affect business strategy. Today, the business implications are largely being left on the table—and with them, a chance for IA to add more value and for audit committees and senior executives in finance, IT, operations, and the business units to gain indispensable business insight from the IA organization.





## Action items

Since IT is increasingly driving the business strategy, it is quickly becoming untenable for IA to maintain a purely supportive IT unit. As IA decides how best to transform its approach to align with IT's new strategic role, it is important to take the following actions, depending upon your role:

### If you're an IA leader:

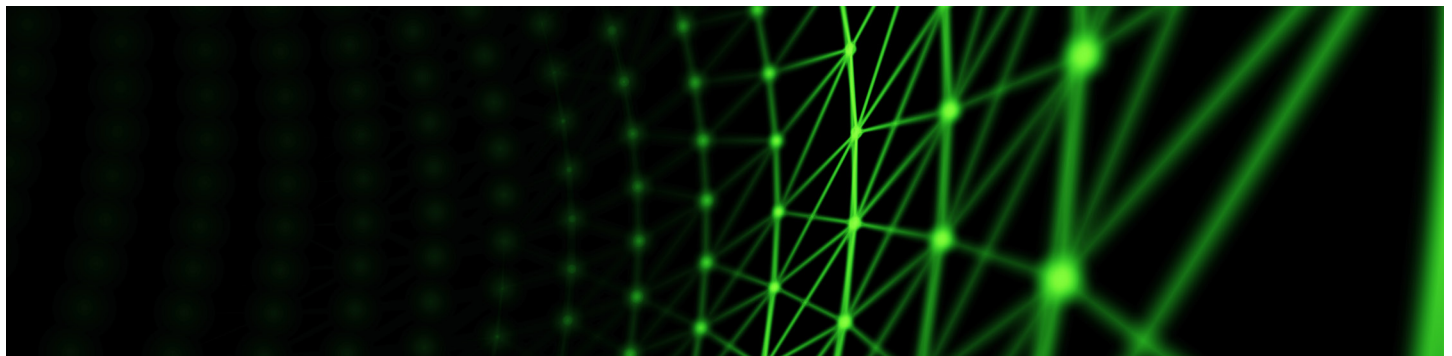
- Directly engage with IT leadership in evaluating the risks, skills, and capabilities required to assist the organization in mitigating IT execution risk, which today can represent an existential threat to the business. This includes fully understanding the business strategy and its dependencies upon technology delivery.
- More specifically, IA leaders should become highly conversant on the strategic plan and consider IA's role in evaluating management's monitoring of IT-execution risk. For example, you may wish to assess the following: How is management evaluating the security, privacy, and resiliency of the technology that is being relied upon to execute the strategy? Is the technology state-of-the-art, leading, or trailing? What are the technology risks associated with delivering the strategy?

### If you're currently in an IT-focused audit group:

- Learn the business strategy and understand IT's critical role in executing it. This includes retooling

yourself, if needed. It used to be enough simply to become knowledgeable in the latest and greatest technologies, such as cloud, cyber, and the Internet of Things (IoT). Today, it isn't. Internal audit professionals need to be able to put that technical knowledge in the context of the IT-driven enterprise and the IT-driven business strategy.

- Draw upon external resources to bolster your understanding of IT-execution risks. This may include attending IT-focused webinars, in addition to IT IA-focused webinars and industry association conferences. Becoming knowledgeable about common IT governance frameworks can also be helpful, such as International Organization for Standardization (ISO) 27001; Control Objectives for Information and Related Technology (COBIT), created by the Information Systems Audit and Control Association (ISACA); and the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). Additionally, obtaining a certification in an IT discipline or engaging outside advisers to help you understand IT in the context of the enterprise are other avenues for building your knowledge. Whatever route you choose, it isn't necessary to earn a PhD in computer science; there are numerous resources at your disposal to supplement your understanding in order to be highly functional and effective in performing your IA role.



### If you're an audit committee member, chief compliance officer, chief risk officer, or chief audit executive:

- Examine your viewpoints in terms of IT-driven business strategy, IA's role in providing business insight, and the evolving skills needed to assess and mitigate the new breed of existential IT risks.
- Self-education is essential, and there are many resources that provide a strategic view of IT risk, including risk and compliance journals, the [National Association of Corporate Directors \(NACD\)](#), and [Deloitte's Center for Board Effectiveness](#).
- In addition to self-education, IA management should also dialogue with the chief executive officer (CEO), chief strategy officer (CSO), chief technology officer (CTO), chief information officer (CIO), and chief information security officer (CISO) to obtain their perspectives firsthand.

### If you're any of the above:

- Consider how this new view may change IA's approach and the process of assessing risks. Enterprise risk management (ERM) begins with the question: "What risks could result in failure to execute the business strategy?" IA has an opportunity to adopt a similar mindset, leveraging the ERM conceptual framework to evaluate the risks of implementing and managing IT technologies that are critical to executing the business strategy.



## Conclusion

IA organizations have traditionally maintained a separate IT focus in the context of IT as a supporting enabler. This siloed approach can be traced to the historic view that the technical experience required to function in an IT capacity had to be cultivated and managed separately. This separation often created more challenges than it solved, and it is misaligned with many of today's business models. No longer is IT just an enabler of the business; it is central to business success. Accordingly, it is critical to recognize that IT risk is much more significant than previously understood—and it may ultimately threaten the viability of the core business itself.

This new reality calls for a new integrated approach to IA—one that brings IT internal audit into the fold as an essential adviser that helps the organization reduce the risk of not executing its business strategy.

## Contact us

### Pete Low

Managing director  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
+1 312 486 5600  
[plow@deloitte.com](mailto:plow@deloitte.com)

### Greg Boehmer

Senior manager  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
+1 212 492 4269  
[gboehmer@deloitte.com](mailto:gboehmer@deloitte.com)

### Sarah Fedele

US Internal Audit leader, principal  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
+1 713 982 3210  
[sarahfedele@deloitte.com](mailto:sarahfedele@deloitte.com)

# Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

#### About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.