www.pwc.com/sg

Transforming Internal Audit to drive digital value

Meeting technology disruption with strategically aligned solutions

Internal Audit. Expect More.

Technology disruption is raising expectations that Internal Audit will deliver quality and will support strategic business objectives

Technology is the most pervasive of today's core business drivers because it is woven integrally into an evolving business environment defined by rapid globalisation, industry convergence, and changing consumer behaviors and demands. Companies are spending big to acquire the data, software, and hardware that can best connect them to customers worldwide and give them the insights and efficiencies to outpace their competitors. But just suiting up with good technology isn't enough. In the face of accelerating Information Technology (IT) infrastructure demands, market pressure for constant technology evolution, and persistent IT security threats, businesses need to know that their IT investments are delivering on their promise and bringing real value to the business.

In that environment, Internal Audit finds itself in the spotlight. Boards of Directors, Executives, and Audit Committees are looking for the function to step up by moving beyond its spreadsheet columns of financial and IT general controls and jumping onto the three-dimensional chessboard of today's IT systems, networks, threats, and opportunities. Those Boards, Executives, and Audit Committees want Internal Audit to become proactive by throwing out its checklists of IT audits and what it thinks it *should do* and, instead, look further and see deeper, by engaging with stakeholders across the organisation in order to discover exactly what it *must do* to support the company and the company's business objectives.

Through that type of engagement, Internal Audit can develop a big-picture understanding of the strategic, operational, reporting, and compliance objectives behind the company's IT investments and can apply that understanding to drive its IT risk assessments, audit plans, and resource allocations.

By aligning its own mission, vision, and functional strategies with its key stakeholders' expectations, by linking its activities to the most significant risks to the overall business agenda, and by enhancing existing Internal Audit processes through the use of data analytics and other advanced solutions, Internal Audit can move beyond its traditional, reactive assurance stance and take on a more proactive, business-enabling role, positioning itself as a trusted advisor on technology issues and driving return on today's unprecedented levels of IT investments.

Tech today: An environment of disruption and transformation

The capabilities, promises, and dangers resulting from new digital technologies are driven by five main trends:

1. **Digital disruption.** Technologies such as mobile platforms, data analytics, social media, the cloud, and the Internet of Things have been disrupting business models across sectors.
2. **Business and technology transformation.** Evolving business models, the consumerisation of IT, and the massive transformation of applications and infrastructure have put some businesses on unfamiliar footings.
3. **Big data.** Huge increases in transaction volume, data volume, and data quality have increased the need for better data governance and management.
4. **Cyber security and privacy risks.** Cyber risks—including the theft of customer data and intellectual property, denial-of-service attacks, and cyberespionage—have become clear and present dangers to the global business ecosystem.
5. **Regulatory pressure.** An emerging web of global regulation focused on privacy, cyber security, resilience, and critical technology platforms has been adding complexity for companies across industries.

Those trends, coupled with the unprecedented levels of IT investments companies are making to keep up, are top of mind among business leaders.

In PwC's *18th Annual Global CEO Survey*, an overwhelming majority of CEOs reported that mobile technologies (81%), data mining and analysis (80%), and cyber security (78%) are strategically important to their businesses. After meeting those strategic issues with significant IT funding, CEOs want to ensure a strong connection between their digital investments and their business objectives: respondents stressed the importance of (1) a clear vision of the ways digital technologies will help achieve competitive advantage and (2) a well-thought-out plan that includes concrete measures of success.

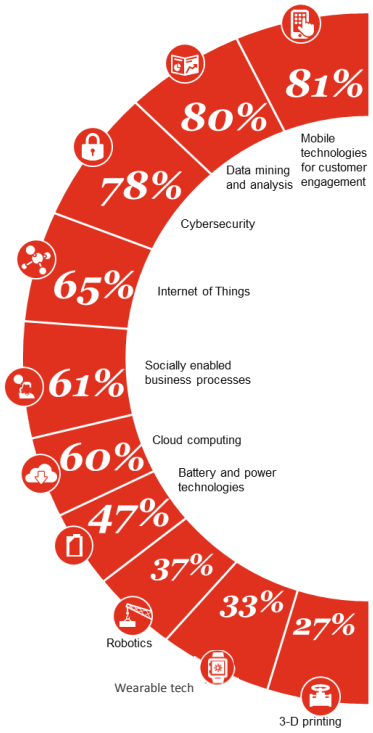
The concern for driving value from IT investments extends to risk management and assurance. According to PwC's *2015 State of the Internal Audit Profession Study*, stakeholders view technology as one of four main areas in which Internal Audit can increase its value to the business, and they say Internal Audit functions can add their most significant value by providing a proactive perspective on transformational initiatives, including by identifying emerging risks and offering internal control recommendations before those risks manifest.

But the fact is that at many organisations, Internal Audit is not meeting stakeholders' technology expectations. According to our *State of the Internal Audit Profession Study,* Internal Audit functions recognise the need to evolve their functions to match the changing business and risk landscape. But even though the majority (60%) of Heads of Internal Audit (HIAs) say they'll need to provide value-added services and proactive advice within the next five years, only 11% say they are indeed doing so now.

To meet those greater organisational needs and those higher expectations, Internal Audit must evolve to become smarter about how it conducts IT audits. By broadening its focus to encompass operations, compliance, and nonfinancial reporting issues and by taking advantage of data analytics, continuous auditing, real-time auditing, and other advanced approaches to enhance its existing processes, Internal Audit will be better positioned to meet stakeholders' expectations of value-added services and proactive strategic advice.

Figure 1: Getting, analysing and using information are key to the current and ermergying techonologies that CEOs see as most important

Q: How strategically important are the following categories of digital technologies for your organisation?



Source: PwC 18th Annual Global CEO Survey

Evolving to engage with IT risks and opportunities

Many Internal Audit functions are following a dated script by conducting the same IT Internal Audits year after year and by ignoring the fact that today's fast-changing technology landscape requires something more—something outside the box. To deliver real value, Internal Audit must focus on technology risks related to achievement of the overall business strategy. Those technology risks include:

- **Data governance and quality risks.** Companies are increasingly citing data as their number one asset—but are usually managing it poorly.
- **IT governance risks.** IT risk and governance issues are increasingly appearing on the agendas of large company boards and audit committees, necessitating the creation of robust IT governance models.
- **Technology megatrends risks.** Technology and technology-related threats and opportunities are evolving. Companies must gain a clear picture of how those threats and opportunities affect their businesses.
- **Cyber security and privacy risks.** With both the frequency and the cost of data breaches and other attacks rising, companies, customers, business partners, and regulators are all laser focused on the ways sensitive data is stored and secured.
- **Regulatory risks.** Companies across sectors are facing amplified regulatory scrutiny and ever-evolving guidances around data protection and cyber security. And companies operating internationally must deal with myriad jurisdictions' divergent standards, such as rules governing the cross-border transfer of personally identifiable information.
- **Business systems risks.** Businesses are becoming more and more dependent on integrated, often global, enterprise resource planning systems and other kinds of business systems. Emerging technologies such as cloud, open-source software, and software as a service are combining to assist businesses, but they can also significantly complicate businesses' IT ecosystems.
- **Global IT risks.** New opportunities—and risks—arise as large companies harmonise their global IT processes, centralise their processing, implement shared-services centers, and conduct offshore activities.
- **IT process and assets risks.** Increasingly, one of the root causes of IT controls breakdown stems from management's unclear views of the systems and software that make up their company's network and the extent to which those systems and software work together.
- **IT compliance risks.** Businesses find themselves confronting a host of new regulatory requirements that require the attention of IT, such as the Sarbanes–Oxley Act, the Health Insurance Portability and Accountability Act, and BASEL II.
- **Sourcing risks.** The growing use of third parties requires an equally growing focus on the control of outsourced processes, the protection of intellectual property, and the pursuit of effective outsourcing contract management.
- **IT resilience and continuity risks.** The survival of today's businesses depends on resilient business infrastructures that are—at the same time—secure, available, recoverable, and sufficiently agile enough to deal with both planned and unplanned events.
- **Project delivery risks.** Combating the belief that technology initiatives go wrong more often than they go right requires forging stronger links between business and IT and encouraging more-professional management of projects, systems, and resources.

The disruptive effects of technological change are broad, with implications for potential system failures, reputational damage, and rapid innovations' tendency to drive customer demand and shorten the shelf lives of new products and services. But potential opportunities are equally vast: By engaging with stakeholders across the organisation—such as the Board, the Audit Committee, the CEO, the Chief Information Officer (CIO), the Chief Financial Officer (CFO), the Chief Operating Officer (COO), the Chief Technology Officer (CTO) - as well as with customers and regulators, Internal Audit

can develop a vital, big-picture understanding of the strategic, operational, reporting, and compliance objectives behind the company's IT investments. And the function can use that understanding to prioritise and promote activities aligned with areas of both greatest potential benefit and greatest potential impediment to the achievement of those objectives and to then identify emerging technology-related risks.

A transformational solution for a disruptive environment

In the face of accelerating technology pressures and demands and all their associated risks, businesses' needs for IT and data security assurance are profound. Even with strong policies and vigorous controls in place, a company can't achieve true comfort around the adequacy of its defenses if it doesn't continually verify that those defenses are sound, uncompromised, and applied consistently.

Performing those assessments, providing that assurance, and then taking it all to the next level by proactively identifying emerging threats and determining mitigation strategies represent the new technology frontier for Internal Audit. The following four steps outline a broad-stroke approach to moving the Internal Audit function deep into the landscape of digital disruption and transformation and thereby driving return on IT investment.

Step 1: Lay the foundation

The first step in sharpening Internal Audit's IT focus consists of developing a clear understanding of key stakeholders' expectations and then recognising that those expectations likely evolved and will continue to evolve in today's rapidly changing environment.

To achieve clarity on those expectations, HIAs and IT audit team heads must engage with the Board, the Audit Committee, and the CEO in order to become able to understand the company's strategic business and IT objectives. They should also meet frequently with the CIO, CFO, COO, and CTO, as well as regulators to become able to understand and align with business and technology strategy, emerging sector trends, and compliance obligations.

To stay ahead of the curve on continuously evolving risks, Internal Audit must network both internally and externally regarding emerging risks and mitigation practices. Participating in forums and conducting internal and external discussions should help Internal Audit:

- Align IT risk assessment activities with overall Internal Audit risk assessment.
- Link IT risk assessment to the company's strategic objectives.
- Incorporate feedback from stakeholder interviews to validate the alignment of risks to objectives.

Internal Audit's role in ensuring that technology-related risks get considered properly becomes especially important when a company is getting ready to roll out a new business process, product, or information system. In such initiatives, the project team sometimes believe it hasn't enough time to fully consider evolving risks, especially when an initiative has fallen behind schedule. If Internal Audit stays on the sidelines, the company might rush into the launch of a new process, product, or system without adequate controls.

By leveraging the IT risk assessment, Internal Audit can serve as a trusted advisor to the business by proactively identifying organisation-specific risks and by providing strategic advice and value-added services when it comes to issues that involve cyber security, privacy, the cloud, big data, social media, the Internet of Things, and other technology challenges.

Step 2: Assess risk coverage

In today's rapidly changing business world, it's more critical than ever that Internal Audit develop an enterprise risk profile and to conduct a dynamic and comprehensive risk assessment that incorporates a company's risk universe, major trends and opportunities, and macrorisks. To properly prioritise audit efforts, Internal Audit should also use data analytics and visualisation tools to find out where risks reside in the organisation. According to PwC's *2015 State of the Internal Audit Profession Study*, only 34% of respondents make proficient use of data analytics to extract actionable insights about the business.

The risk assessment should factor in relevant sector trends and industry perspectives, stakeholder input via interviews, and results from assessments performed across the three lines of defense: operational management; risk management and compliance functions; and Internal Audit. Most important, the risk universe should be evaluated continually for relevance, completeness, and coverage.

An effective and complete risk assessment promotes increased awareness at the management and Board levels around critical IT risks. It should result in an audit plan of IT audits and advisory engagements that have the potential to deliver results that go beyond value *protection* to drive value *enhancement*.

The risk assessment should also validate the fact that staffing management and talent management are key components in building a successful internal technology audit team. Staffing IT audit engagements with subject matter specialists who can offer deeper insights in cyber security, emerging technology, IT governance and service delivery, business applications, and project assurance promotes depth and quality of delivery, fosters better relationships and strategic partnerships with key stakeholders, and builds credibility for the Internal Audit function.

Step 3: Execute audits

After completing the enterprise risk profile and assessment, Internal Audit can more fully develop the audit plan to drive enterprise value. The plan should be balanced, taking into account identified risk areas, relevant regulatory expectations, stakeholder requests, and emerging trends and opportunities. Leading Internal Audit functions are acting as change agents for their companies by executing audits and advisory engagements that focus on building trust and managing risks in the digital age, identifying performance improvement opportunities, and creating visibility that enables the business to take on additional risk and maintain competitive advantage.

Rather than focusing only on issues that are tactical and already known to the business, advisory engagements should be planned and developed in alignment with emerging technology risks and key organisational needs and objectives. Such alignment helps Internal Audit provide timelier feedback for IT leadership and drive change in critical areas that can help management achieve its strategic goals and objectives.

Step 4: Deliver consequential reporting

A maximised Internal Audit function demonstrates results, improvements, and value. Unfortunately, many Internal Audit functions today are not prepared to deliver a robust set of meaningful recommendations and insights on technology challenges. By expanding from a narrow, fixed approach to an informed, proactive, big-picture stance that evolves with the organisation's needs, Internal Audit can generate more-balanced reporting and IT-value-enhancing deliverables for management consumption. Individual reports, quarterly reports, and annual summaries should focus on providing deeper insights and on connecting IT's delivered business value directly to the company's strategic objectives.

An Internal Audit function has a unique opportunity to become an independent and objective arm for the business—but also to collaborate with and support stakeholder communities by urging improvements in the company's risk posture. For example, Chief Information Security Officers can better coordinate with counterparts on the internal technology audit team to provide updates on preparedness related to cyber security and privacy. Such coordination can better serve in getting technology operations and infrastructure teams to build stronger control environments and operate more effectively.

Further, internal technology audit leaders should leverage their face time with Boards and Audit Committees to create awareness and education around key technology trends. With their ability to view the ecosystem independently and objectively and with their access to standard-setting organisations and peer groups, these leaders can access a wealth of information for facilitating stakeholders' understanding of IT-related risks, as well as for taking opportunities to use technology more effectively to increase shareholder value.

Next-level Internal Technology Audit: The future is now

Digital disruption is here, and it's not going away. To respond effectively, Internal Audit must fight fire with fire by developing truly disruptive, innovative, transformational solutions. By aligning with the expectations of its key stakeholders, identifying and focusing on existing and emerging IT risks with greatest potential impact on the business agenda, and leveraging best-in-class techniques, tools, and skill sets to deliver a more advanced suite of technology audits, Internal Audit will become able to provide timely feedback and reporting for IT leadership and other stakeholders, will facilitate better information in support of decision making, and will drive change to help company leaders achieve strategic objectives.

www.pwc.com/sg

To speak to one of our experts about how this may affect your business, contact:

David Toh

Internal Audit Leader
PwC Singapore
T: +65 6236 3248
E: david.sh.toh@sg.pwc.com

Julia Leong

Partner
PwC Singapore
T: +65 6236 7378
E: julia.sw.leong@sg.pwc.com