KPMG
cutting through complexity

Internal Audit Insights for REITs:

Data & analytics, cybersecurity and third-party risks

kpmg.com

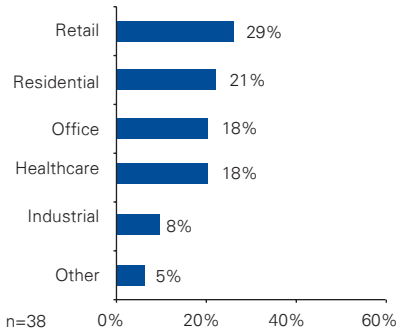
Insights around data & analytics, cybersecurity, and third-party risks

Real estate investment trusts (REITs) face an increasingly complex business environment while trying to maintain performance in a sector strongly influenced by economic trends and fiscal policy. In addressing these issues, internal audit (IA) is playing an increasingly active role, evolving from merely ensuring compliance to assisting management evaluate the strategies needed to overcome these challenges.

To get a better understanding of some of the key issues that REIT IA professionals are focusing on, KPMG LLP conducted a survey of attendees in advance of the recent Real Estate Internal Audit Roundtable in Las Vegas on a number of topics related to third-party risks, data & analytics, (D&A) and cybersecurity, among others.

To those who participated in the survey, we offer our sincere thanks, and we are pleased to present this report on the results.

Q. Which of the following best describes your organization's sector?



We received responses from 38 REIT IA professionals. Most, 87 percent, were from publicly traded companies, representing the retail, residential, office, healthcare, and industrial sectors. Most worked for organizations that have revenue of $500 million or above, and nearly half have revenue greater than $1 billion. Almost 70 percent represented REITs that own more than 300 properties, while 24 percent represented organizations that owned between 151 and 300.

Challenges and focus

Q. What is the most significant challenge currently facing your IA department? (select one)

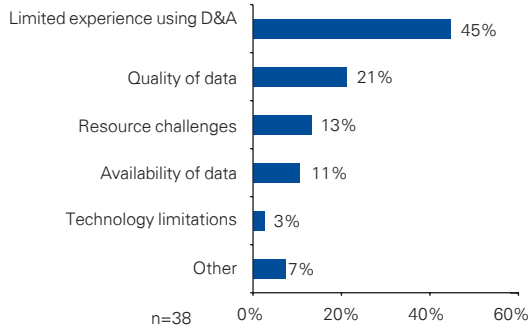
Today, the IA department is being called upon to address ever-more complex issues. Our survey confirmed that sentiment, with respondents citing "increasing corporate complexity" and "resource capability/technical ability" as the most significant challenges facing their IA departments.

Looking out to the horizon, our survey also asked IA professionals to tell us the primary areas for the allocation of their time over the next 18 months. Topping the list was "technology, IT, and security," followed closely by "finance and accounting" and "construction and developmental activities." This focus is fairly consistent to the areas IA professionals have allocated their time over the past 18 months.

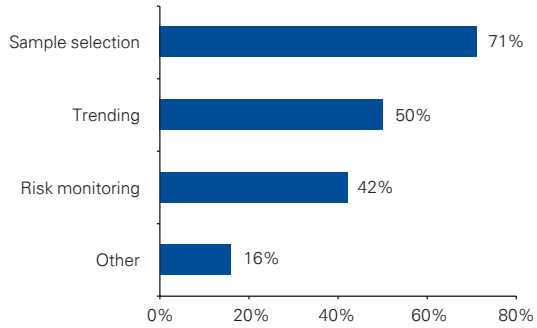
With regard to the other topics covered in the overall survey and the roundtable, we found three of interest that particularly stood out: D&A, cybersecurity, and third-party risks. What follows is our initial analysis of these three themes.

Data & analytics

Q: What is the most significant challenge to leveraging D&A in your IA department activities? (select one)



Q: In what ways does your IA department leverage D&A capabilities? (multiple responses permitted)



When it comes to D&A, REIT IA departments are just beginning their journey to more fully benefit from the latest tools and techniques. Among survey respondents, 66 percent said they use D&A on only between 1 percent and 25 percent of their projects, while a mere 3 percent said they use D&A for 100 percent of their projects. Similarly, a large majority—71 percent—said they use D&A for sample selection, a fundamentally lower-value use of analytics, while only 42 percent said they used D&A for risk monitoring.

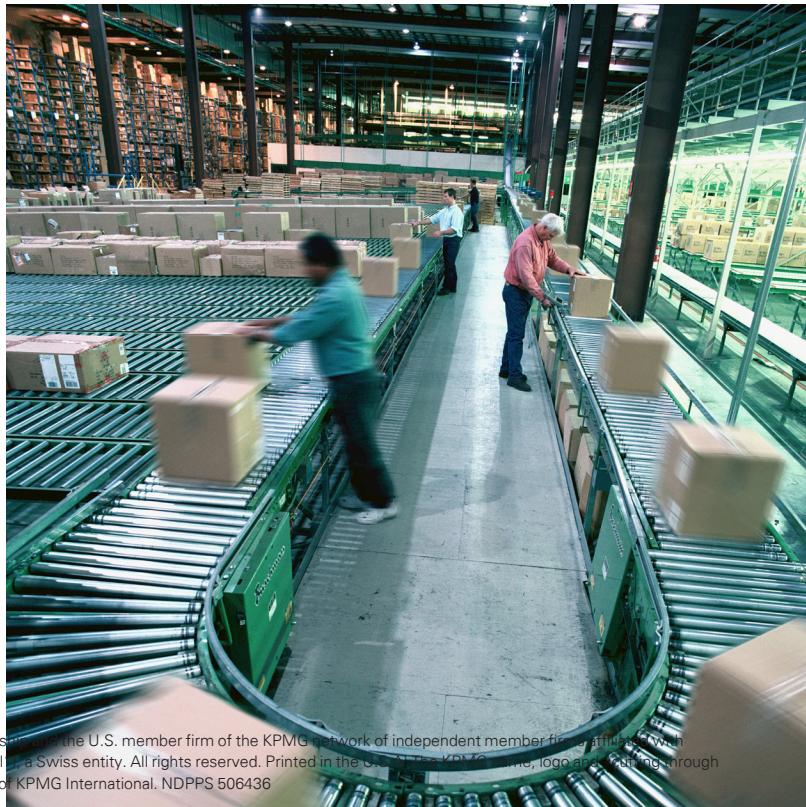
Given these responses, it is not surprising that 45 percent said their limited experience in using D&A was the most significant challenge to leveraging D&A in their IA department activities.

D&A can add value to IA in many ways by providing increased insight into the business and risk management, and creating greater efficiencies. For instance, IA departments can audit smarter by using D&A for trending, risk monitoring, and identifying anomalies and outliers.

Key to the success of D&A within the IA function is aligning the objectives of a D&A plan with the objectives of the internal audit. IA professionals can then more precisely determine the analytics that need to be performed to meet those objectives. Performing D&A for the sake of D&A will not be successful; D&A must be aligned with specific audit objectives and validated with the business.

Another factor critical to a successful D&A program is inviting both the business parties and the IT department to the table at the beginning of the initiative, as each will contribute significantly. The business leaders will know how to use the data but may not know how to acquire it. Likewise, the IT department will have access to the data, but may not be aware of all the implications for the business.

Although not every IA professional can or should be executing D&A techniques, all should be able to interpret and apply the results. To help achieve that end, IA departments need to take advantage of data visualization techniques—that is, charts and other graphics that cannot only aid in the interpretation of data but also facilitate decision making. According to the survey, only 3 percent of survey respondents said they use data visualization, suggesting that IA departments fall short in this area. Not only can data visualization help audit professionals interpret D&A results, but it can also help provide leadership with an enhanced dynamic reporting mechanism, enabling audit professionals to easily understand findings and drill into details to help determine root cause.

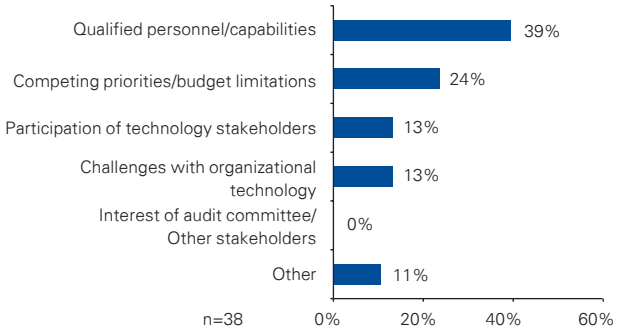


Cybersecurity

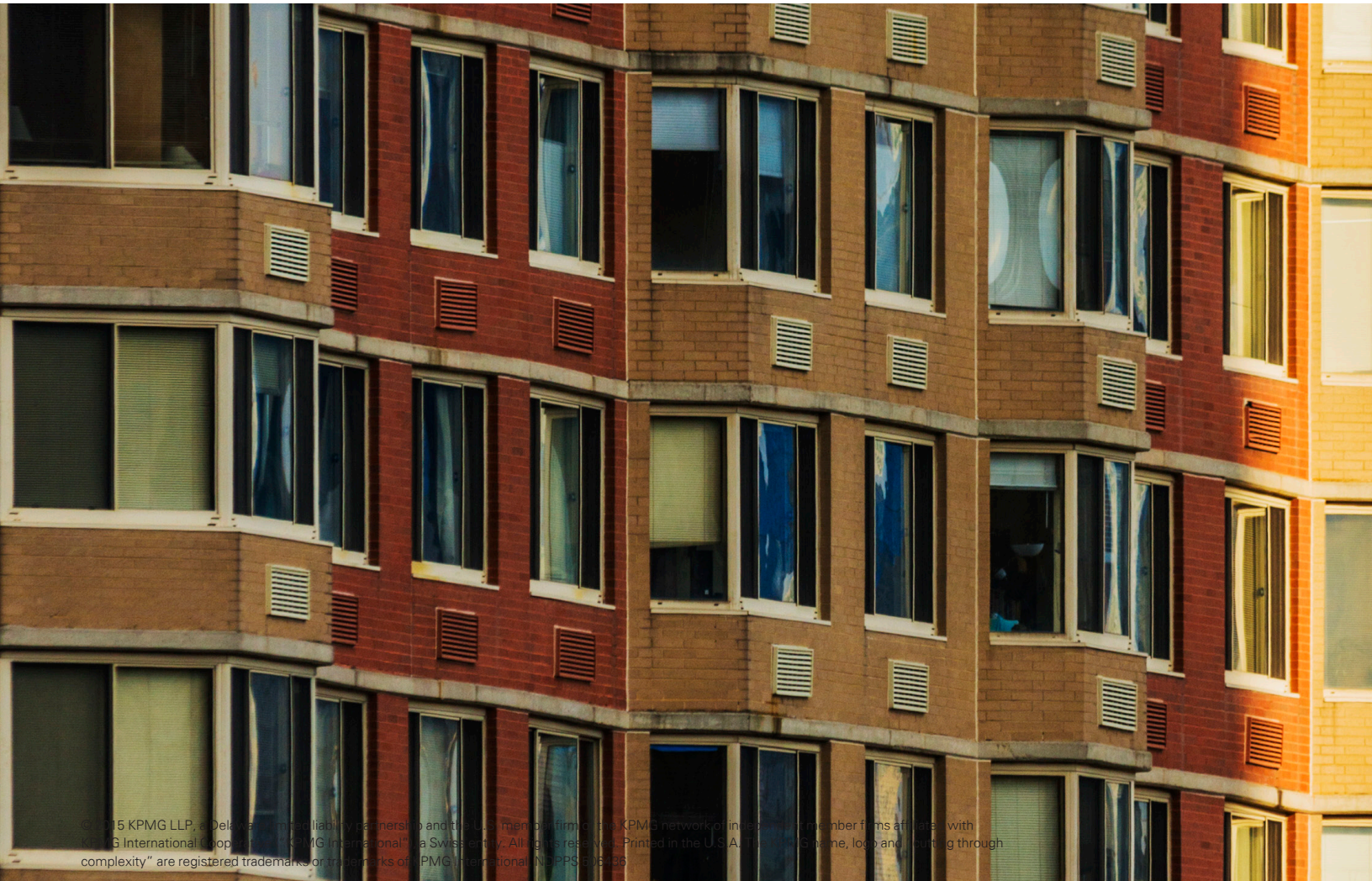
Cybersecurity is another area of high concern among respondents. A full 92 percent of survey respondents said the level of interest in cybersecurity risks from management, board members, and other stakeholders was increasing or significantly increasing. Respondents listed "level of dependence on IT at your organization" as the number one driver, though in our experience, this view is heavily influenced as well by substantial media attention to the topic.

Interestingly, a number of REIT executives we have spoken to believe the risk of a cyber attack is relatively low since their organizations typically do not store or process sensitive data like Social Security numbers or medical records. We would challenge REIT IA and operational executives to consider the impact of a security breach more broadly. Although the definition of sensitive information may differ for REITs, nearly all REITs collect and/or retain information that they would not publicly disclose due to financial or reputational impact. In nearly all cases, a security breach can disrupt a REIT's operations and damage its business reputation, particularly if

Q. What is your IA department's most significant challenge when executing cybersecurity internal audits? (select one)



information about partners or confidential agreements, such as leases, are made public. Finally, we are seeing an uptick in cyber criminals using organizations such as REITs as a conduit to infiltrate the systems of those organizations' business partners—exploiting the inherent trust and relatively lower defenses between the two parties.



An even more persuasive argument exists to consider the need for cybersecurity: There is a good chance your organization has been (or is currently being) breached. While only 29 percent of respondents said that their organization has experienced a notable cybersecurity incident, the same percentage indicated that they were "not aware of any." The ability to quickly and effectively identify covert attacks, triage, and consistently respond to cyber incidents is a key differentiator between companies that are more resilient to responding to attacks and those for which a single cyber event can cause a sea change.

In addition to these real risks, IA professionals indicated significant ongoing issues when executing cybersecurity internal audits: 39 percent cited having the challenge of not having qualified personnel/capabilities. The market for leading cyber talent is incredibly competitive right now, and REITs need to continue to explore ways to attract, retain, and continually train leading-class talent to help ensure cyber risks are appropriately identified and addressed. An additional 24 percent of respondents mentioned the challenge of competing priorities/budget limitations. IA should play a key role in positioning cybersecurity within a broader enterprise risk management context. IA should also work in close collaboration with their counterparts in the IT and security organizations to help identify, rationalize, and prioritize cyber risks. IA can and should help guide REITs to achieve a proper balance between cybersecurity policy that is too restrictive or too lax, and that ultimately aligns with the organization's risk tolerance.

Effective cybersecurity is not just about implementing tools nor is it a "once-and-done" initiative. Effective cybersecurity is based on a thorough understanding of the most sensitive data within your organization and where the largest risk exposures are and driving toward a cross-functional, risk-based approach to protecting that data.

Third-party risks

REITs are increasingly outsourcing more noncore work to focus on their core strengths. This work includes finance, HR, procurement, IT, call centers, and facilities management, each with its own kinds of risk. This growing activity is raising concerns among IA departments over how well their organizations are managing their third-party relationships. Our survey suggested that this was particularly the case when it came to executing due diligence on potential third parties and the onboarding of new third parties.

To be sure, you can outsource work, but you cannot outsource responsibility, and IA is looking to monitor third-party performance to ensure the REIT gets what it is paying for, as well as reduce risks, especially in the areas of regulatory compliance. In addressing its concerns, IA has to balance its need for access to third-party compliance and performance data without becoming burdensome and losing the cost-saving benefits of outsourcing. Including IA early in the planning of an outsourcing arrangement can allow audit processes and data transfers to be developed during the outsourcing event, at the most advantageous or efficient time, instead of after the deal is in place. More importantly, having IA involved in outsourcing services can help prevent a failure in the outsourcing company from becoming a failure for the REIT.

Conclusion

The survey results and accompanying KPMG perspectives above point to key issues on REIT management's agendas. The Internal Audit function can play a critical role in developing organization-specific assurance and consulting strategies to address these issues, ultimately providing greater value to the Board and enterprise. In this context, KPMG can leverage our view of industry best practices to develop and implement effective plans and guide internal audit and management to appropriate resolutions.

For more information on REIT internal audit topics, please contact:

Michael Smith
Partner
Internal Audit, Risk & Compliance Services
T: 214-840-6019
E: michaelasmith@kpmg.com

Duleep C. Rodrigo
Principal
Internal Audit & SOX Strategic Sourcing
T: 213-817-3150
E: drodrigo@kpmg.com

Contributors:

Douglas Burr
Director
Shared Services & Outsourcing
T: 925-895-4747
E: dburr@kpmg.com

Brian Greenberg
Director
Data & Analytics – Internal Audit
T: 216-875-8206
E: bgreenberg@kpmg.com

Orson Lucas
Director
Information Protection
T: 813-301-2025
E: olucas@kpmg.com

kpmg.com