KPMG

Safeguarding real estate investment trusts

Six key strategies to help avoid trouble

November 2017

kpmg.com

Table of contents

Introduction

Navigating changing global markets, interest rate fluctuations, and shifts in real estate investment activity by geography and property type. The launch of a new global real estate sector index.[1] More pressure to achieve long-term value appreciation in a market with more competition for investment opportunities. Cyber threats abound, becoming more precipitous with unprecedented technological advances. Managing career paths of talent and retaining top quality employees.

All of these potentially disruptive developments are taking place at increasing speeds. What's more, news — especially bad news — travels around the globe almost instantaneously thanks to the Internet and social media.

The upshot of all this is that the value of a REIT can plunge even before there's a chance to react. That's why it's essential for REITs to keep close watch on the myriad of strategic, operational, and external risks that can potentially impact them. Equally, if not more, important is for these firms to have an effective risk management framework in place.

Funding risk management measures a challenge

While these are challenging tasks for virtually all companies, regardless of industry, they are particularly tricky for REITs, which often view risk management as a lower priority of their strategic mission, and may lack the budget required to manage these escalating risks.

What's more, getting buy-in from deal-focused REIT management to expend resources on risk prevention measures can be difficult. After all, every dollar spent on risk prevention means fewer funds available to invest in real estate properties or in staff retention and development, and there's no guarantee that the potential risk — whether its fraud, misconduct, or cyber — will actually occur.

The flip side of the coin, however, is that by not taking proper risk prevention measures, you expose your firm to far greater losses in terms of value, reputation, resources and penalties, which impacts the ability to fund raise and secure new investors.

[1] Source: S&P Dow Jones Indices LLC, "S&P Dow Jones Indices and MSCI Announce August 2016 Creation of a Real Estate Sector in the Global Industry Classification Standard (GICS®) Structure" (March 13, 2015)

KPMG

Top risk management issues

We've listened to industry experts, spoken with compliance professionals, and gained insight from KPMG LLP (KPMG) colleagues who work with REITs. The result is our list of top risk management issues facing REITs — along with practical actions we recommend they take to eliminate, or at least mitigate, these risks.

The top risk management issues are:

— Third-party risk

— Fraud and misconduct risks

— Cyber risk

— Expanding internationally

— Compliance and regulatory risk

— Succession planning

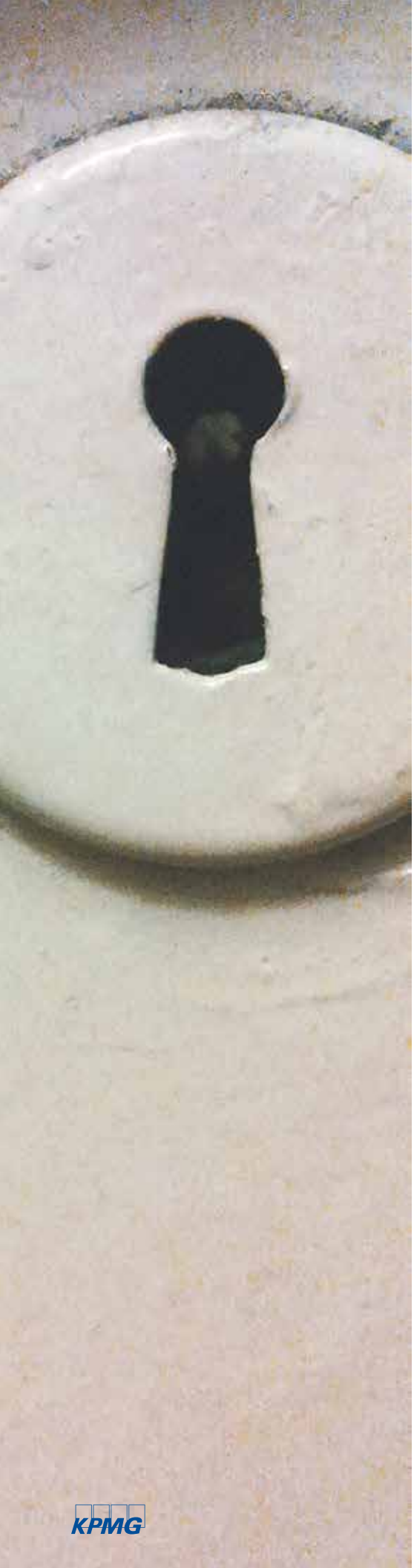
U.S. Securities and Exchange Commission (SEC) and other domestic and global regulatory bodies — as well as new, more sophisticated investors — expect REITs, especially public REITs, to have a well-developed and thought-out risk management framework to address these issues. This framework begins with REIT managers maintaining a proper internal control environment which allows the firm to better manage these risks.

Investors of REITs care about long-term capital appreciation of their investment and a consistent, periodic cash dividend. Investors want to know that as markets change, REITs are ready to expand into new emerging markets and can manage talent internally, as well as oversee third-party external talent, to execute and drive results. Additionally, the involvement of activist investors in the REIT industry is evolving day to day and can immediately influence the way you operate and manage your business and risk.

To ensure the stability of their investment, investors are also demanding more transparency from REITs and want to know they have the proper internal control environment in place to manage risk.

"Real estate investment trusts are all about providing investors with stability and a consistent dividend payment. But if you choose not to make the necessary investments needed to manage the risks inherent in your firm, you may find that the trust and stability you've built with investors is washed away in the blink of an eye."

— Shruti Shah, KPMG Partner, Risk Consulting



Managing third-party risk

With a continually expanding portfolio of investments that span multiple segments, locations and property types, REITs routinely engage third parties to perform specialized services, including property management, asset management, investment valuation, payroll, and/or corporate expense management.

The National Real Estate Investor and CBRE[2,3] observed that there are multiple reasons REITs consider outsourcing to third parties, including:

- Gaining knowledge and expertise in a rapidly evolving public REIT sector
- Achieving cost savings by outsourcing property management services
- Increasing flexibility to move capital between property types and locations by externally managing assets
- Spreading — and reducing — costs for training and development through large, specialized management companies
- Enhancing the focus on investment and portfolio management business by outsourcing information technology using external management at the property level
- Improving efficiency — and margin — particularly for smaller REITs.

These third-party arrangements are often critical for REITs, whose primary focus is on property acquisitions and property value health. However, it may expose them to information security and cyber risk, as well as operational, compliance, reputational, concentration, country, legal, performance, and financial risk. Many REITs outsource the financial reporting process, including lease management and reporting of rental income, which presents additional risk factors.

Government regulators recognize the increased use of third parties by REITs and other financial services organizations to support critical operations. But they have routinely and repeatedly stated that "using [third-party] providers does not relieve the financial institution of its responsibility to ensure that outsourced activities are conducted in a safe and sound manner."[4]

---

[2] Source: National Real Estate Investor. "Six Ways REITs Benefit from Third-Party Property Management," (August 9, 2015)

[3] Source: CBRE, Challenging REIT Property Management Orthodoxy (August 2015)

[4] Source: Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook, Appendix J, "Business Continuity Planning" booklet: "Strengthening the Resilience of Outsourced Technology Services," (February 2015)

KPMG

Six-part risk management framework

The following six-part framework can help guide REIT risk management professionals in the development of their own third-party risk management (TPRM) program.

1. **Define a TPRM strategy:** Establish a strategy that defines when it's appropriate, or not appropriate, to engage a third party. Factors included in this decision are: (1) the cost of doing the work on your own, (2) the direct costs of the third party, (3) the added costs of the risk-based program needed to oversee the third party, and (4) the potential savings realized through outsourcing.

2. **Establish a strong governance structure:** A strong governance structure sets the tone from the top, and enables you to establish a framework for overseeing third parties and resolving issues throughout the life cycle of your relationship. This structure should include a dedicated committee or subcommittee, and involvement of senior management and the board.

   An effective TPRM must have organizational buy-in and ownership, as it needs the cooperation and coordination of the REITs various risk oversight functions and/or business units, including the operational (procurement) function. What's more, initial and ongoing due diligence work needs to be conducted to determine whether to commence and/or continue the third-party relationship.

3. **Adopt enterprise-wide policies and procedures:** A formal enterprise-wide policy and procedures document reinforces strategy and governance components of a TPRM program. This document should establish a common vocabulary and minimum standards that apply to the firm.

   For example it should include a definition of third parties, risk-rating methodology, and required pre- and post-contract activities. In addition, the document should define activities, roles, and responsibilities of the business unit engaging the third party, as well as risk management and internal audit functions.

   Many REITs do not have a separate internal audit function. In such cases, it is important for them to develop internal control policies and procedures to monitor TPRM within the firm and ensure that their personnel — as well as the third-party providers — understand these policies and procedures. It is management's ultimate responsibility to take ownership of their books and records regardless of third-party assistance. This includes fully understanding user controls, monitoring third parties, and ensuring complete and accurate reporting.

4. **Implement consistent life cycle processes:** Develop and implement a standardized set of life cycle processes related to engaging a third party. To ensure consistent implementation and execution across business lines and functions, these processes should cover everything from planning (e.g., inherent risk identification), due diligence and risk assessment, contracting, ongoing monitoring, and termination.

5. **Clearly define roles and responsibilities:** Knowledgeable personnel who understand their roles are critical to the successful implementation and execution of a TPRM program. Therefore, REITs should provide training that is specific to individuals' roles so they have a clear understanding of expectations and the necessary skills to do what's required. REITs should also provide appropriate training to third-party services providers.

   The training should be ongoing to serve as both a refresher and account for changing circumstances and responsibilities. Ongoing annual evaluations that assess individuals' performance relative to assigned TPRM roles and responsibilities should also be included as part of the TPRM program.

"As more work is outsourced to third parties, the more likely it is that one of them won't manage risk as diligently as you would. And unless you take steps to address this situation, it can have serious consequences for your firm."

— Greg Matthews, KPMG Partner, Risk Consulting

6. **Strengthen information reporting:** A well-designed TPRM program:

   (1) Establishes relevant and actionable key risk indicators (KRIs) based on the firm's risk tolerance and limits

   (2) Analyzes data collected either regularly or continuously

   (3) Provides senior management and the board with relevant information regarding the effectiveness of the program.

Example of KRIs may include the number of:

— Third parties with overdue risk assessments of more than 90 days

— Losses over $250K related to services provided by third parties

— Breaches of regulatory requirements by third parties.

The use of state-of-the art technology is critical to the success of a REIT's information reporting process. Innovative technology can help you (1) facilitate internal and third-party work flows, (2) provide audit trails, and (3) conduct near real-time analysis of inherent and residual risks in portfolios.

Continuous performance review

While the focus on risk management of a third party is critical, it's also important to maintain a continuous focus on the third party's performance and the value it's delivering to your firm. Even after your firm contracts with the third party, you should continually assess whether it is receiving the expected services and benefits, and to determine if other suppliers might offer a better arrangement.

For more information on TPRM, please visit our Web site at: https://advisory.kpmg.us/risk-consulting/third-party-risk.html.

KPMG

The illustration below sets out the six elements of a third-party oversight framework, including the three lines of defense (LOD): lines of business, compliance function, and internal audit.

Policies and procedures
- Standards Setting
- Policy Management
- Code of Conduct

Compliance management
- Regulatory Change Management
- Compliance Risk Assessments
- Complaints Management
- Exam Management
- Issues Management

People & skills
- Skills & Training
- Roles & Responsibilities
- Performance Management & Compensation

Monitoring & testing
- Transactional, Process & Control Testing
- Compliance-Focused Third-Party Risk Management
- Surveillance (Market, Employee, etc.)

Information reporting & technology
- Governance Risk Compliance (GRC) Platform
- Dashboards/Reports
- Predictive Measures: KRIs/Key Performance Indicators (KPI's)
- Process Automation

Governance & culture
- Board & Committee Interaction
- Ethics and Compliance
- Structure and Organization
- Tone & Culture
- Risk Appetite
- Communication

Managing fraud and misconduct risk

Prevalence of corporate misconduct and fraud

73 percent of respondents reported that they have observed misconduct in the prior 12-month period.

More than 55 percent reported that what they had observed could cause "a significant loss of public trust if discovered.

Source: KPMG LLP Integrity Survey

75 percent of bribery cases involved payments through third-party intermediaries.

Source: OECD Bribery Report, 2015

REITs are particularly susceptible to risks of corporate misconduct and fraud because of their inherent nature and characteristics, which include:

— Involvement in complex transactions

— Lean operating structures

— Nonliquid assets

— Eagerness to expand into new or emerging markets.

Types of misconduct and fraud

Financial reporting fraud and misconduct: Managers that are overly motivated to meet investor expectations may have an incentive to commit fraud. For example, the former Chief Financial Officer (CFO) of a REIT was convicted in 2017 of misleading investors by falsely inflating a key financial metric used to evaluate the performance of the REIT. **(See sidebar at right.)**[5]

And the Chief Executive Officer (CEO) and two other top officers of another REIT resigned in 2016 after an internal review found that its financial statements were tampered with, sending its shares down as much as 25 percent.[6]

[5] Source: *The Wall Street Journal*, "Former (Company) CFO Convicted of Securities Fraud," Justina Vasquez (June 30, 2017)

[6] Source: Reuters, "(Company)'s top executives exit after accounting review, shares plunge," Arunima Banerjee (February 8, 2016)

[7] Source: MarketWatch, "Which non-GAAP metrics will likely catch the SECs eye?," Francine McKenna (April 4, 2016)

KPMG

The REIT admitted that it smoothed income items to achieve consistent growth in a metric called "same property net operating income," a financial performance measure of interest in the REIT business.[7]

A manager's ability to manipulate financial statements and financial metrics can have a significant impact on the overall value of the firm and also raise potential liability issues. For instance, REITs commonly supplement their financial communications under U.S. generally accepted accounting principles (GAAP), with non-GAAP metrics, and both the REIT examples above are based on manipulation of non-GAAP figures.

Risk management is a top concern for audit committees. More than 40 percent of audit committee members think their risk management program and processes "require substantial work," and a similar percentage say that it's increasingly difficult to oversee those major risks, according to KPMG's 2017 Global Audit Committee Pulse Survey.[8] With the SEC's new guidance on non-GAAP metrics issued in May 2016, REITs may need to take further action to ensure their non-GAAP financial metrics meet the SEC's requirements and have a prominent place on the audit committee agenda.[9]

[8] Source: KPMG LLP, KPMG's 2017 Global Audit Committee Pulse Survey, (January 2017)

[9] Source: KPMG LLP, Audit Committee Institute, "On the 2017 audit committee agenda", (2016)

Managing fraud and misconduct risk:

Case in Point

The Securities and Exchange Commission (SEC), in the fall of 2016, charged two former accounting executives of a large publicly-traded REIT with purposely inflating a key metric used by analysts and investors to assess the company.

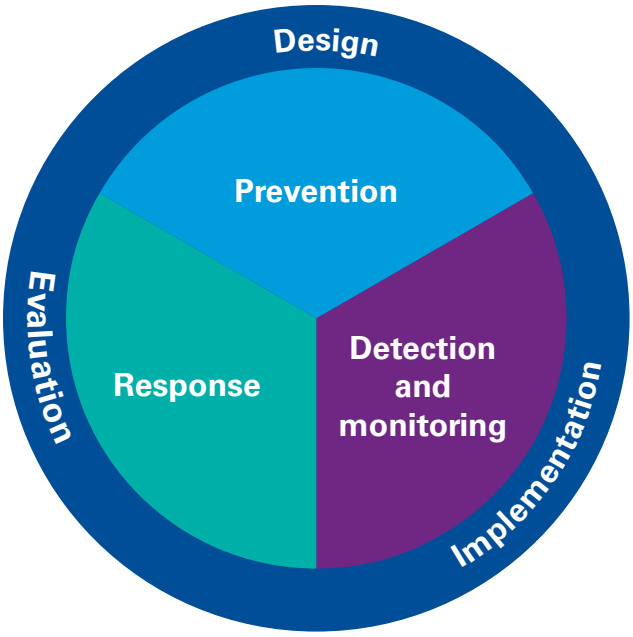
According to the SEC's complaint, the former Chief Financial Officer and former Chief Accounting Officer manipulated the calculation of the company's adjusted funds from operations (AFFO). AFFO was a key non-GAAP financial metric used by analysts and investors to assess the company's performance, and AFFO per share was the primary measure in the company's earnings guidance.

SEC rules generally permit companies to present non-GAAP financial measures to convey supplemental information about how company management views the results of operations in ways that GAAP results alone may not convey. But companies cannot present non-GAAP measures in a way that is misleading.

Source: SEC.gov, "Executives Charged With Inflating Performance of Real Estate Investment Trust," September 8, 2016

Misappropriation of assets: REITs that enter into financing or "build-to-suit" transactions (where a third-party developer is responsible for the construction of the real estate asset) are at an increased risk of asset misappropriation. Companies need a robust set of guidelines to ensure that developers are identified and selected based on an appropriate bidding selection process and that the proper due diligence of the third party had been performed.

While there is no sure-fire way to eliminate the risk of fraud, corporate misconduct, or misappropriation of assets, there are best practices that REITs can employ to mitigate their exposure to corporate liability, sanctions, and litigation. REITS should adopt a fraud risk management strategy grounded in the three lines of defense: **prevention, detection and monitoring, and response.**



Prevention

REITs should take steps to identify areas of potential exposure to fraud and misconduct, and put in place strategies to mitigate this exposure. At a minimum, this includes the following:

1. **Do your "homework"** before entering into a financing or build-to-suit transaction: Perform enhanced fraud-related diligence, including a forensic analysis of financial results, and determine if the firm, or any related third parties, are violating any Anti-Money Laundering (AML), Office of Foreign Assets Control (OFAC) or other anti-bribery and corruption rules and regulations.
2. **Seek legal counsel** to help craft representation, warranty, and indemnification clauses that will be included in contracts and agreements.
3. **Perform an annual compliance review** of high-risk areas (e.g., directors and officers (D&O) insurance).

REITs should also:

— Conduct thorough, periodic fraud risk assessments that take into account industry, location, compliance requirements, operations and mitigation controls.

— Take appropriate remedial actions to bridge significant control gaps, such as adding another level of review for third-party reports.

— Implement "whistleblower" mechanisms designed to encourage employees, vendors, and contractors to report instances of fraud, misconduct, or suspicious behavior.

— Design and implement compliance policies and procedures, establish a compliance infrastructure, and provide adequate training in support of these compliance efforts.

KPMG

Detection and monitoring

A well-designed detection and monitoring program is essential to demonstrate your established policies, procedures, and internal controls have remained effective and are functioning as designed. The program should include the monitoring or auditing of activities to identify fraud and misconduct risks and potential internal control vulnerabilities.

Response

Any comprehensive program must contain a framework that includes procedures on how to respond to fraud and misconduct. This will increase the odds of getting ahead of potential issues. Hearing about an issue for the first time from the SEC is a place you and your investors do not want to be in!

To that end, REITs should require that they, as well as their third-party property managers:

1. **Periodically assess** the effectiveness of their whistleblower hotlines (e.g., survey employees on their willingness to use it; compare year-over-year use).
2. **Reinforce "open door" policies** for reporting issues during employee meetings as well as by sending out written communications.
3. **Take prompt action** with respect to potential issues by establishing an effective investigative triage process. This process must ensure that all investigations, regulatory inquiries, subpoenas, or inspections are promptly reported to appropriate stakeholders and designated firm personnel.

SEC Whistleblower program

The SEC Whistleblower Program has awarded more than $111 million to 34 whistleblowers, and the program appears to be gaining popularity.

Source: 2016 Annual Report to Congress on the Dodd-Frank Whistleblower Program

Cyber risk vulnerabilities
Why are real estate companies attractive to hackers? Consider some of the specific vulnerabilities:

— Real estate company technology systems contain leases, rental applications, credit reports, and deal financing terms – all filled with payment card industry data and personally identifiable information on tenants and clients.

— Real estate professionals regularly pass confidential data back and forth through email, mobile devices, and cloud-based business applications.

— Apartment, retail and office assets are wired and computerized, creating potential intrusion vulnerabilities through connected technologies like smart alarms, locks and lights, environmental controls, and voice-assisted devices.

— REITs manage huge sums of money online and could even be targeted for the cash from transactions handled by their internal systems.

— Real estate owners and operators with high-profile tenants may be targets of cyberattacks intended to ultimately steal secrets or financial information from those tenants.

— All service providers to the organization, or those operating in and around a real estate company's properties, may end up posing a cyber risk, as a vulnerability in a service provider's cybersecurity could expose the extended network.

Source: KPMG LLP, "Securing real estate assets in a digital world – How internal audit can focus your organizations' cybersecurity" (May 2017)

Managing cyber risk

Cyber-attacks continue to escalate, and it is truer than ever that every company, in every industry, is at risk.

In 2016 alone, hackers compromised 500 million accounts from a major email provider, leaked 19,000 emails from U.S. political party officials, stole $81 million from a foreign bank, and even brought down major parts of the Internet.[10]

Infosec Institute predicts that, in 2017, "the number of cyber-attacks will continue to grow in almost every industry."[11] And BI Intelligence estimates "$655 billion will be spent on cybersecurity initiatives to protect PCs, mobile devices and Internet of Things (IoT) devices between 2015 and 2020."[12]

Cyber risk and REITs

But is cyber risk a real problem for real estate firms and REITs? What specific threats are likely to impact them? What makes real estate companies attractive targets to hackers? **(See sidebar at left.)** And what steps can REIT leaders take to proactively prepare their organizations to protect valuable data and assets from cyber attackers?

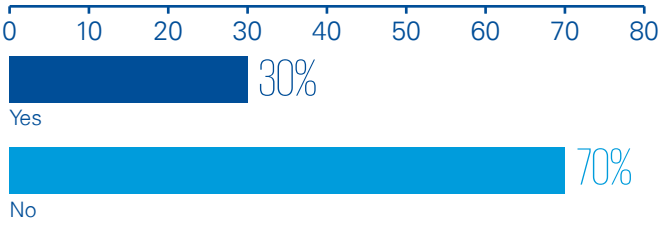
[10] Source: Venture Beat, "Here's how cyber-attacks get worse in 2017," Justin Fier, (December 11, 2016)

[11] Source: Infosec Institute, "2017 Cyber Security Predictions," (December 19, 2016)

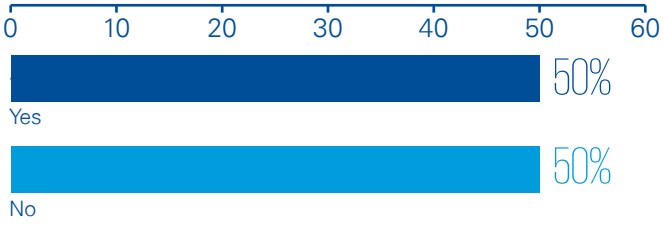
[12] Source: BI Intelligence, "This one chart explains why cybersecurity is so important," (April 5, 2016)

Data breaches are now a clear and present danger — 30 percent of senior U.S, commercial real estate executives in the KPMG 2017 Real Estate Industry Outlook Survey said their firm (or one of their properties) experienced a cybersecurity event in the last 24 months. Yet half of respondents (50 percent) say their organizations are not adequately prepared to prevent or mitigate a cyber attack **(see charts below).**

Has your firm (or one or more of your properties) experienced a cybersecurity event within the last 24 months?



Do you feel you are adequately prepared to prevent of mitigate a cyber attack?



Source: KPMG LLP "KPMG 2017 Real Estate Outlook Survey" (May 29, 2017)

REITs face cyber risks from both internal and external sources, including employees, third parties you work with, and other players who are completely outside of your organization but intent on stealing information or otherwise doing you harm.

Indeed, the headlines are filled with examples of companies that have been the victims of cyber attacks. For example, a management company operating hotels for some of the industry's most recognized brands discovered malware in payment systems at 20 properties, likely affecting tens of thousands of customers.[13]

These attacks have become so routine that some company boards are reluctant to fund their CIOs' request for additional resources based on the belief that it won't deter these attacks. In our opinion, this is a short-sighted view.

Not only does it make it easier for a company to become a victim of a cyber breach, it also exposes them to penalties for regulatory failures. For example, in late 2015, the SEC fined an investment advisor for failing to adopt appropriate cyber security policies and procedures, failing to conduct periodic risk assessments, as well as failure to implement a firewall or maintain a response plan for cyber incidents.[14]

[13] Source: KPMG LLP "Securing real estate assets in a digital world", page 6, (May 2017)

[14] Source: SEC release 2015-202, "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach," (September 22, 2015)

Where to focus your cybersecurity efforts

Real estate leaders must heed the call to ramp up capabilities to secure real estate assets from cybercriminals. But many don't know where to start. Internal audit plays a critical role in the battle against cybercrime – providing executives with an initial roadmap, ongoing assessments of emerging cyber risks, and current strengths and weaknesses that inform decisions to strengthen defenses. There are a number of key areas where internal audit should focus their cyber reviews **(see sidebar below).**

Perimeter protection: As real estate companies become more high-tech, mobile and connected, the universe of people with access to their systems and data expands. In this new landscape, internal audit can ramp up assessments of cyber awareness training, identity and authentication, security intelligence methods, and protocols for accessing, storing, sharing and securing information.

Critical data protection: In the real estate industry, critical data includes corporate intellectual property and investor listings and holdings containing personally identifiable information and sensitive financial information. Internal audit reviews can provide careful oversight of privacy policies and other safeguards related to classifying, storing and accessing the most valuable data an organization currently manages.

Incident response: All real estate companies should have a formal cybersecurity incident response plan in place so, when an incident does occur, they can minimize the damage. The plan lays out action steps from both a business and a technical perspective, defining what individual people and teams do to:

— Stop the intrusion from spreading

— Re-secure the network

— Investigate the incident

— Communicate with customers.

Internal audit reviews can ensure the plan works and is regularly tested and updated as threats evolve, including addressing relevant incidents that occur outside of their organization.

Reporting to top leadership: Cybersecurity should be viewed as a technology risk and a business risk, too. Internal audit can assess whether senior executives outside of IT, even all the way up to the audit committee, CEO and the board, have clearly defined roles and responsibilities for designing, implementing and overseeing policies and processes for mitigating cyber risk — and that each person meets his or her critical responsibilities.

Reporting to stakeholders: External communication is often where organizations fall short in managing cybersecurity incidents. Internal audit can validate the ability of the organization to communicate relevant, appropriate and timely information about a cybersecurity event to all effected outsiders, such as shareholders, investors, customers, the board, the press, or members of a family office.

For example, developing a standardized template for public relations and marketing communications to inform stakeholders:

— That an event occurred

— What the organization knows and doesn't know

— How the organization is investigating

— Where people can go to get more information.

Source: KPMG LLP "Securing real estate assets in a digital world," (May 2017)

KPMG

Expanding into international markets

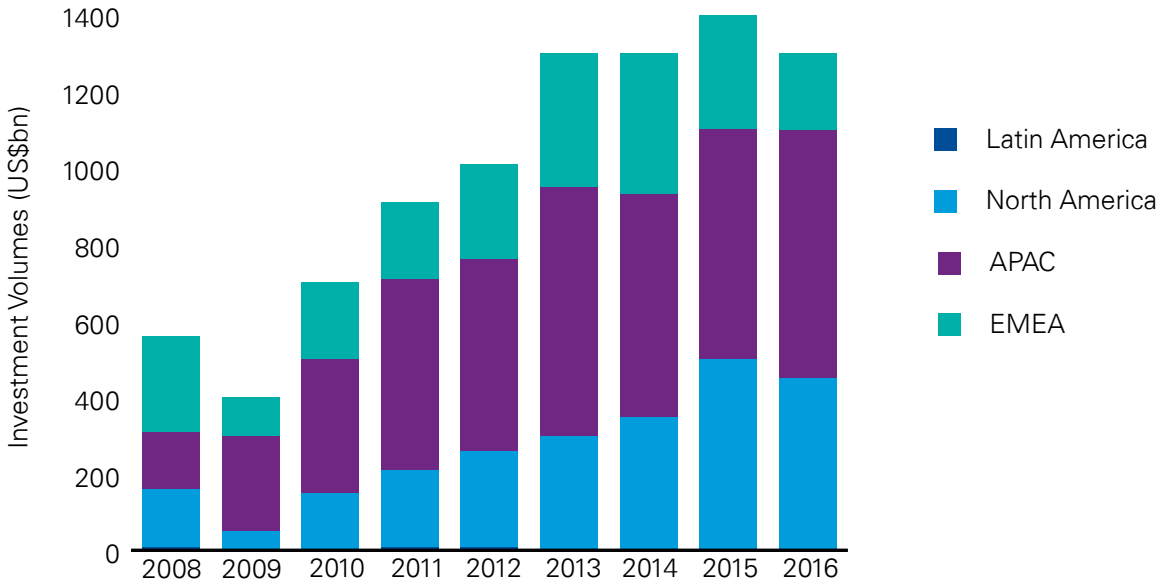
Despite recent global political turmoil and economic uncertainty, interest and engagement in global real estate investment remains strong, with continued global capital flow coming into the space. But the impact of these social and economic disruptions on the global market have caused a shift in activity with respect to the types of investors participating, as well as their priorities.

Based on these overarching global trends, it's safe to assume that sources of capital will continue to shift rapidly to mitigate global political and economic risks. Of course, many investors will remain focused on core cities in North America, EMEA (Europe, the Middle East and Africa) and Asia Pacific in 2017 as they seek to weather risk while building portfolio liquidity and longevity.[15]

At the same time, new areas will be in demand as investors seek to balance their need for security with a requirement for growth. For example, as global population grows and the trend toward urban migration continues, there will be increasing development opportunities in the global real estate market, especially in emerging economies.

But with these opportunities – and greater growth potential in new geographies and sectors – comes new risks.

Global property investment by region



Source: Cushman & Wakefield and RCA. Deals over US$5 mn including land

[15] Source: Cushman & Wakefield, *The Atlas Summary 2017 (April 2017)*

Considering global investment risks

In order to develop a sound investment strategy, investors, developers, and those involved in the formulation of a business strategy must consider numerous factors that help shape and characterize a particular region, and the accompanying risks.

Below is a listing of key considerations – and risks – to think about before investing in the global real estate market, and particularly in emerging markets:

Regional and local laws, legal processes and governments: Especially when dealing with emerging economies, regional and local governments typically have significant influence in the development of urban real estate and infrastructure. For those looking to invest in these markets, REITs must be able to communicate with the governments to understand the lay of the land and if there are certain strategies that need to be avoided or modified. Also, they may need to collaborate with the governments and develop a cohesive plan that fits with the region's development ambitions.

- **Reporting requirements:** REITs also need to comply with local reporting requirements when investing globally. This may require retaining individuals with local expertise as there may be financial and non-financial information that needs to be reported to government agencies.
- **Criminal laws for cybercrimes:** Many countries have established local criminal laws with respect to cybercrimes. And while many developing and emerging countries are behind the curve in terms of cyber legislation, others are not. So REITs must take steps to protect themselves against cyber breaches as well as comply with whatever cyber laws are being enforced.[16]
- **Transparency:** As emerging economies and sovereign wealth funds (SWF) continue to develop, there will be greater competition for assets in the global marketplace in which to invest. In addition, these investors are demanding more transparency from REITs with respect to fees and expense, and also to the underlying real estate investments. With capital allocations to real estate growing, pressure is growing, from both investors as well as local and regional governments, for real estate to have similar transparency as other international asset classes.[17]

Federal anti-corruption laws: Many companies engage local partners and suppliers in order to address the cultural differences of conducting business. But unless care is taken, this may result in violations of the Foreign Corrupt Practices Act (FCPA), which prohibits payments of bribes to foreign officials to assist in obtaining or retaining business. And the U.S. Securities and Exchange Commission (SEC) has said that enforcing the FCPA is a high priority.[18]

The FCPA also requires companies to maintain accurate books and records, and have a system of internal controls ensuring that transactions are authorized by management. Therefore, it's critical to perform extensive due diligence with foreign business partners and suppliers to ensure there are no FCPA violations, which includes establishing clearly articulated anti-corruption policies up front.

[16] Source: Cyber Law and Cyber Security in Developing and Emerging Economies by Zeinab Karake Shalhoub, Sheikha Lubna Al Qasimi.

[17] Source: World Economic Forum website, How disruptive technology could improve real estate transparency, (August 16, 2016)

[18] Source: U.S. Securites and Exchange Commission website, SEC Spotlight section Foreign Corrupt Practices Act

Managing compliance risk

While REIT managers focus on the deployment of capital to best achieve long-term value appreciation, they must also constantly monitor the firm's compliance with Internal Revenue Service rules and regulations, to ensure the REIT maintains its REIT status. The Internal Revenue Code (IRC) includes many detailed rules that put in place operational and organizational requirements. If these rules are not met, there could be resulting penalties and interest to the company, or REIT disqualification.

A REIT must pass a quarterly asset test and an annual income and distribution test, as well as meet structural organizational requirements, to maintain its REIT status. For example, a REIT must:

- Meet an "asset test" whereby 75 percent of the value of the REIT's total assets are invested in real estate (including real property, mortgages, and shares in other U.S. REITs).
  - Monitor investment holdings in other companies and ensure the company's investment does not exceed ownership interest restrictions.
- Monitor its operations and ensure that the company is earning income from the right sources and distributing an adequate share of its earned income.
  - Derive 75 percent of its gross income from rents from real property, interest on mortgages financing real property, or from sales of real estate.
  - Distribute 90 percent of the sum of its taxable income to investors as a shareholder dividend each year.

Organizationally, a REIT must:

- Be managed by one or more trustees or directors for the entire taxable year
- Be held by 100 or more persons for at least 335 days of the 12 month taxable year
- Not be closely held (i.e., not more that 50 percent owned, directly or indirectly, by five or fewer individuals, domestic pension plans, private foundations, and certain other organizations).

What's more, a REIT is required to maintain adequate documentation to cover all of the requirements listed above. In addition, a REIT must file and maintain records of myriad tax forms with federal, state and local governments.

Facing all of these challenges requires an effective compliance risk management program to achieve the appropriate monitoring, communication and documentation.

Management-led compliance efforts

To effectively monitor and ensure compliance with the REIT requirements, firms must take a top-down approach involving corporate leaders in the organization.

- Appoint and support a Director of Taxation who has unfettered access to senior management, and can anticipate and respond to any changing regulatory obligations of the REIT
  - Ideally, the Director of Taxation has stature and influence in the firm, and is also well versed in IRC and compliance obligations. This will better enable the Director to leverage the resources of outside legal counsel, compliance consultants, and internal staff to round out an effective compliance function.
- Empower the Director of Taxation to communicate to all levels of the firm the strategic importance of the compliance program.

Among its many benefits, a comprehensive and rigorously enforced compliance program will give regulators greater comfort when examining a firm. If regulators determine compliance is taken seriously, they may mitigate fines and other penalties even if lapses are found to exist.

KPMG

Establishing a framework

In order to have a strong compliance risk management program, and an underlying compliance framework which will reinforce effective corporate strategy, certain fundamental components are required, as set out below:

Governance and culture: A robust governance structure should provide for fluid downstream and upstream reporting, and clear and open lines of communication between senior management, compliance, and operations.

Policies and procedures: Establish policies and procedures tailored to the unique risks, business activities, and regulatory obligations of the firm.

The policies and procedures should (1) include a disciplined process of managing ongoing reviews, and (2) require periodic review and assessment to ensure that they continue to be effective in addressing regulatory obligations and mitigating risks.

Compliance risk assessment: Effective management of a robust compliance program should contain regulatory change management that monitors whether the firm needs to modify its compliance program and business practices in light of changing regulatory rules.

Issues tracking and management: It is critical to stay ahead of potential regulatory and other risk issues, and ensure that any observations or issues that are uncovered are appropriately tracked and resolved in a timely manner.

From a governance perspective, managing incidents from start to finish across the organization allows management to gain real-time visibility and insights. This helps firms prevent reoccurrence, and better positions them to proactively address any regulatory scrutiny.

Communication and training: It is essential to provide comprehensive communications to, and compliance training for, key business stakeholders and other personnel, as needed. For example, develop a compliance training program for all advisory personnel so they understand their roles and responsibilities as employees.

Additionally, training should be ongoing, and be refreshed as needed to account for changing circumstances and responsibilities, such as new and emerging regulations that impact the firm, and/or new compliance risks resulting from changes to the business.

Documentation: The compliance program should require robust documentation. This helps ensure that the firm can prove it has properly followed its policies, procedures, and processes.

Regulators look for this type of documentation as proof that the firm's compliance program is working effectively. In addition, it's often the basis for compliance monitoring and testing. Keep in mind that documentation should be done contemporaneously in most cases; it may not be as impactful or credible if it's done after the fact.

"The SEC's current mantra is that if you didn't write it down, it didn't happen. Therefore, well-managed firms should ensure they get credit for the good compliance work they're doing by thoroughly documenting their efforts."

— Laurence Godin, KPMG Principal, National Leader of the Investment Management Segment, Risk Consulting

Succession planning

Any company, including a REIT, is at risk if a member of the current executive team unexpectedly leaves. If there's a delay in finding a suitable replacement it's possible that the REIT may suffer adverse consequences such as lost investor confidence, rising investor activism, difficulty raising capital, and of course, value reduction due to decreased share price.

Investors in the real estate industry - and specifically in REITs - are demanding more clarity about firms' executive succession plans.[19] What's more, according to a KPMG survey, audit committees insist that succession planning is a critical item to consider on an on-going basis.[20] But succession planning can fall by the wayside due to short-term regulatory and disclosure pressures, which are intensifying as a result of the continued growth of REITs.[21] The results of the KPMG survey bear this out:

- Forty-four percent of audit committees were not satisfied that their agenda and strategy was properly focused on CFO succession planning.
- Another 46 percent were only somewhat satisfied.
- Few were satisfied with the level of focus on talent and skills in the finance organization.

[19] Succession Planning Strategies for Real Estate Investment Managers, FPL Advisory Group and National Association of Real Estate Investment Managers (NAREIM), 2013

[20] KPMG's 2017 Global Audit Committee Pulse Survey, January 2017

[21] Ben Ashwell, "REIT investors reportedly concerned about succession plans," IR Magazine, January 24, 2017

KPMG

Have a plan in place

Given the risk of CFO turnover and the critical role the CFO plays in maintaining financial reporting quality, it's essential that the company have succession planning in place. The plan should not solely cover the REITs CFO, it should also include other key finance executives, such as the Chief Compliance Officer and Chief Risk Officer as well as tax leadership. Beyond finance, tax and risk compliance, a succession plan should also cover those with key relationships with investors and those involved with real estate deals. Given the importance of relationships in real estate, a Board must protect the company with understanding key relationships and planning if key management or those with critical relationships leave the organization.

Succession planning should focus on short-term and long-term planning as REITs consider aging employees, millennial expectations, market disruptors, investor activism and changing business models.

New skill sets are needed and the above challenges create the perfect storm for finding, developing, and keeping people with the skills and ability to drive competitive advantage.

KPMG believes there are five critical talent risk categories that REITs must carefully and comprehensively address in today's increasingly complex business environment.[22]

- **Capability** – Develop and align desired skills and capabilities to meet business needs
- **Cost** – Invest in recruiting, retaining, and ensuring affordability of the workforce
- **Compliance** – Guide and monitor employee behavior and ensure that talent management processes adhere to local law and regulations
- **Capacity** – Create, maintain, and pave the way for employee advancement
- **Connection** – Ensure top talent doesn't become disengaged, divided, and unable to emotionally connect with leaders and the business

Successful management of these risks extends well beyond the Human Resources (HR) function. A holistic approach to talent risk requires cooperation from the entire enterprise.

HR leaders must shift away from traditional, siloed practices and engage in a comprehensive, strategic business-first approach to managing talent. This will increase the likelihood that key personnel will remain with the REIT, and that qualified replacements are readily available if they opt to leave.

"For those with critical skills and relationships including with investors, the Board must critically assess a succession plan."

— Robert Fraher, KPMG Audit Partner, Asset Management

[22] Source: KPMG LLP, "Managing talent risk today for an innovative tomorrow," (September 2016)

"Knowing that your firm has a comprehensive value protection program in place will provide you with a great sense of confidence and security."

— Phil Marra, KPMG National Audit Leader for Building, Construction and Real Estate practice, and U.S. Real Estate Funds Leader

Final thoughts

In our turbulent global economy, where bad news becomes viral in a matter of seconds, designing and implementing strategies for managing risks is essential. Having appropriate plans in place can prevent potential problems from occurring, and can serve to mitigate the harm to REITs if they do.

By creating a robust risk management plan, executives at REITs can increase the probability that their organization will be able to withstand the impact of a potential crisis, regardless of its nature.

There's no question that creating and maintaining a comprehensive risk management program is a time-consuming task that on the surface has little value creation payoff. However, failure to implement an appropriate program can end up costing your organization a far greater loss of resources, value and reputation.

KPMG

How KPMG can help

KPMG LLP (KPMG) provides services specifically designed to help REITs navigate the challenging and ever-changing environment. Our dedicated professionals bring in-depth real estate knowledge and experience to help you identify opportunities, assess value, overcome obstacles, and navigate tax laws and regulations in jurisdictions throughout the United States and abroad. Our industry depth, global reach, and full range of relevant services can facilitate your success in today's marketplace.

As one of the industry's leading service providers, we have extensive resources dedicated to the real estate industry and possess deep experience serving REITs, real estate and private equity fund managers, institutional investors and advisers, real estate operating companies, real estate management companies, and lenders and intermediaries.

KPMG

Authors

Robert Fraher
With over 25 years of accounting and auditing experience, KPMG Audit partner, Robert Fraher specializes in real estate investment funds, private equity, construction, as well as commercial and residential properties. He has a wide-breadth of experience across the alternative investments space, including working for nearly a decade in Russia, Eastern Europe and the Middle East across a variety of industries.

Shruti Shah
Shruti is a principal in KPMG's Advisory Services practice. With more than 20 years' experience in the financial services sector, Shruti focuses on alternative investments such as real estate investment trusts, private equity and asset management. She has led large scale projects to improve financial performance and reduce risk including compliance exposure such as SOX gap assessment / remediation and post-acquisition process improvement.

Steve Dwyer and Drew Hewitt supported the authors. We would also like to acknowledge the following members of our KPMG Real Estate team for their invaluable contributions to this white paper: Laurence Godin, Greg Matthews, Michael Smith, Andres Cools, Sean Gleason.

Contact Us

Contact us and see how you can benefit from our experience, global bench strength, technological innovation, and customized client care. You can go to our Building, Construction and Real Estate Practice Web page for more information about our services and to read our latest thought leadership publications. Or call one of the real estate specialists below, talk with them about your situation, or learn how we can help:

Robert Fraher
Audit Partner – Building, Construction & Real Estate
T: 212-954-6979
E: rfraher@kpmg.com

Shruti Shah
Principal, Advisory
T: 973-912-6316
E: skshah@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia