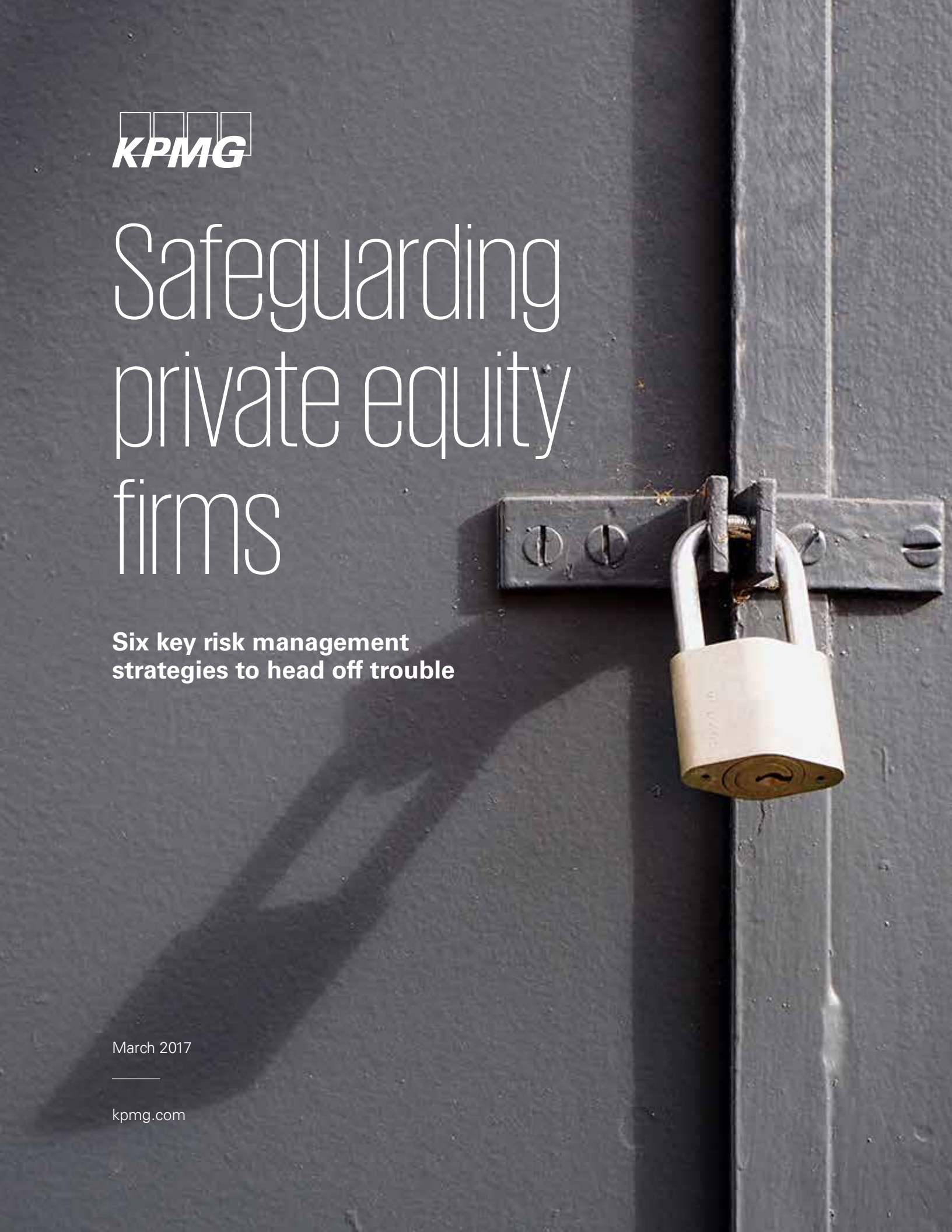


KPMG

Safeguarding private equity firms

Six key risk management strategies to head off trouble

March 2017

kpmg.com

Authors

Shruti Shah

Shruti is a principal in KPMG's Advisory Services practice. With more than 20 years' experience in the financial services sector, Shruti specifically focuses on alternative investments such as private equity, asset management, and real estate.

Christine Buchanan

Christine is a partner in KPMG's Advisory Services practice. She has more than 20 years of experience serving clients in the financial services industry. Her primary focus is large investment management organizations, alternative investment vehicles, and mutual funds. Before moving to the advisory side, Christine spent many years auditing asset management clients.

We would also like to acknowledge the following members of our KPMG asset management advisory team for their invaluable contributions to this white paper: David Calef, Andres Cools, Ray Dookhie, Sean Gleason, Laurence Godin, Jeff Lee, Greg Matthews, Mark McKeever, and Vivek Mehta.

Contents

Introduction

Increasing competition for portfolio company investments. More pressure to deliver returns to investors. Mounting regulatory requirements domestically and globally. Cyber threats abound, becoming more precipitous with unprecedented technological advances.

And all of these potentially disruptive developments are taking place at ever-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 private equity firm and/or its portfolio companies can plunge even before there's a chance to react. That's why it's essential for private equity firms to keep close watch on myriad 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 private equity firms, which may lack the focus and budgets required to manage these escalating risks.

What's more, getting buy-in from deal-focused private equity firm 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 a portfolio company or to award as a bonus. And there's no guarantee that the potential risk—whether it's fraud, misconduct, or cyber—will actually occur.

The flip side of the coin, of course, is that by not taking proper risk prevention measures, you expose your firm to far greater losses in terms of resources, value, penalties, and reputation.

Top risk management issues

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

The top risk management issues are:

— Technology risk

— Third-party risk

— Fraud and misconduct risks

— Cyber risk

— Compliance risk

— Crisis management

The U.S. Securities and Exchange Commission (SEC) and other domestic and global regulatory bodies expect private equity firms to have a well-developed and thought-out risk management framework to address these issues. What's more, this expectation applies to the firm itself as well as its portfolio companies.

Similarly, investors are demanding more transparency from private equity firms (often with the SEC's backing). They want to know that the private equity firm with whom they've placed their assets has anticipated these risks, is prepared to take action if or when they occur, and that their assets are secure.

Private equity is all about increasing value and achieving a return on investment for you and your investors. But if you choose not to make the necessary investments needed to manage the risks inherent in your firm and your portfolio companies, you may find that all you built up is washed away in the blink of an eye."

–Shruti Shah, KPMG Partner, Risk Consulting

Managing technology risk

Private equity firms have traditionally focused their technology risk management (TRM) on identifying and addressing risks related to information security. But in recent years, as private equity firms continue to increase their technology footprint, TRM has undergone an evolution.

More and more, it's being viewed as an opportunity to provide business value, anticipate issues before they happen, and support business growth objectives.

"A robust technology risk management function not only measures a private equity firm's risk exposure, it also defines the organization's overall IT risk appetite and enhances the control environment by working directly with the business lines," stated Vivek Mehta, KPMG Technology Risk Advisory partner.

"A robust TRM function measures a private equity firm's risk exposure, defines its overall IT risk appetite, and enhances its control environment by working directly with the business lines."

–Vivek Mehta, KPMG Partner, Emerging Technology Risk

"As TRM becomes more mature within a firm, it transitions from providing ad hoc control reviews to enabling proactive risk management," he added. "It does so by using a combination of techniques, such as controls testing, key risk indicators (KRIs), and data analytics to address threats before they occur."

Following are three best practices that can maximize technology risk preparedness at both the firm and portfolio company levels:

Holistic approach to TRM

The traditional approach to TRM included three lines of defense: (1) those aligned with the business or operational function, (2) those tasked with oversight of compliance and risk management, and (3) auditors, audit committee, and/or compliance.

Now, increasing numbers of financial services firms are placing a dedicated risk management professional in the first line of defense (at the business or operational level), and charging him or her with effectively engaging and integrating with the second and/or third lines of defense.

This is a more holistic approach to TRM, and also allows for real-time identification, escalation, and resolution of risks. However, based on our observations, it seems that private equity firms as a whole are lagging behind in this evolving practice. We would recommend that it is something they should consider adopting.

Maintaining an evolving risk inventory

As private equity investment strategies continue to evolve, your risk inventory—the risks against which you are guarding—should adapt accordingly. For example, PE firms and their portfolio companies now need to identify risks related to cyber threats, cloud-based software, identity and access management, e-mail, protection of intellectual property, and protection of investor information, to name a few.

Performing an annual risk assessment and adopting integrated tools to help maintain and update your inventory are essential. This might include an enterprise risk management (ERM) tool to house your risk library. This will allow for real-time monitoring of risks.

What's more, periodic monitoring and updating of your risk inventory help ensure that you're accurately addressing those risks that can impact the firm's strategic goals. Even better would be a continuous risk monitoring program that could help ensure that risks potentially impacting the firm's strategic goals are dealt with on a real-time basis.

In addition, an ERM solution may provide the chief information officer (CIO), or those charged with overseeing technology, with the information and other resources needed to influence the management of critical IT risks on an enterprise-wide basis.

Align technology risk with other risk functions

IT risk should not be viewed in a silo, but rather in the context of other risk functions within the enterprise, including the others risks identified in this white paper. A common language must be established within the firm—and throughout its portfolio companies, if appropriate—to provide a platform for identifying interrelationships between risks.

Integrating the firm's technology risk with other enterprise risk functions will provide a holistic approach to analyzing the impact of potential future obstacles in achieving the organization's goals and objectives.

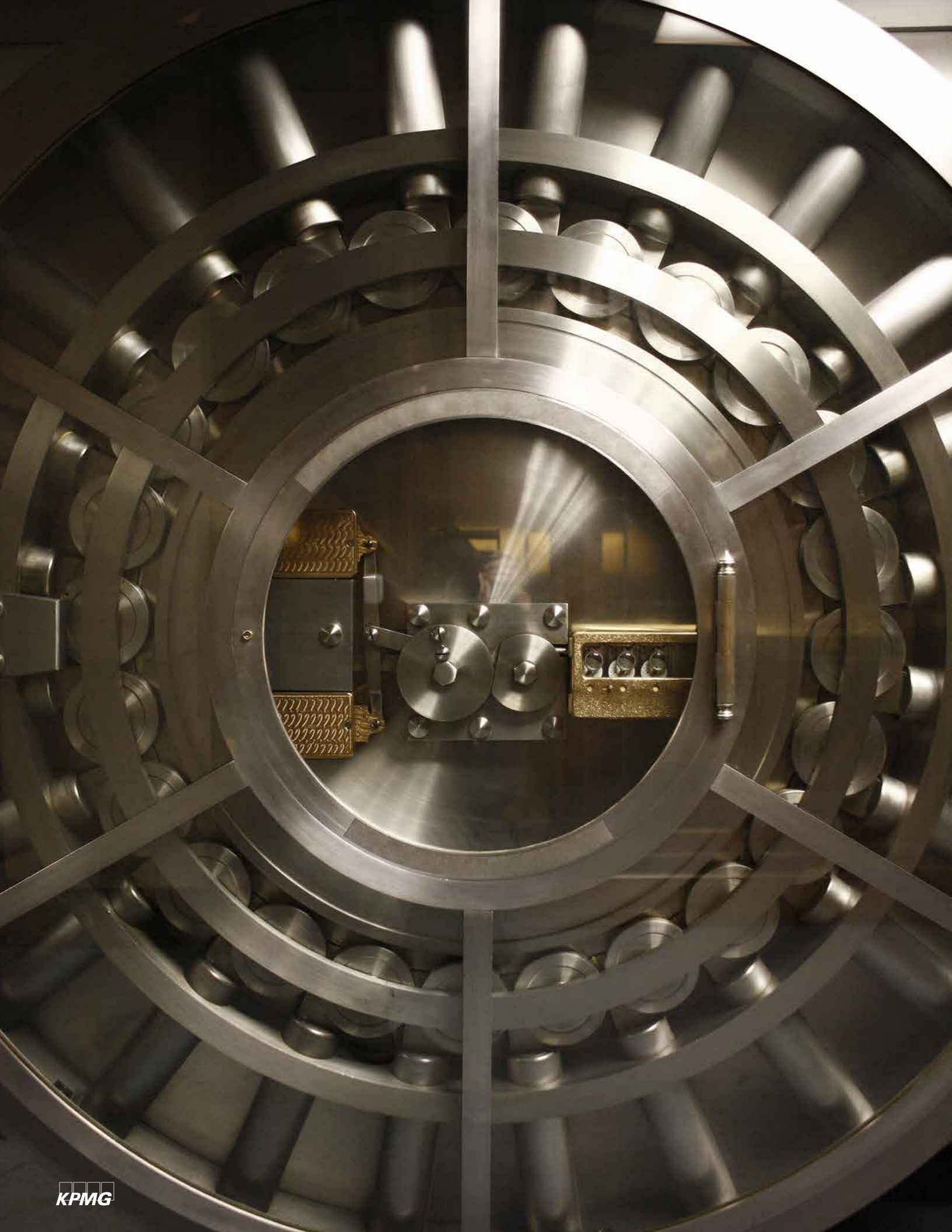
Private equity firms should also give TRM a "seat at the table." This will provide for a more comprehensive approach to firmwide risk management, early identification and remediation of potential pitfalls, and create awareness at the most senior levels of the firm.

Be strategic

"To be truly strategic, CIOs need to think about how value is created. Many are good at cost cutting, but this is almost by definition a backward-looking exercise—optimizing something that is already in place.

This is not strategic. CIOs need to think about what future possibilities there are to leverage technology for new value and top-line growth. This is what differentiates the strategic CIO."

–Peter A. High,
Implementing World Class IT Strategy: How IT Can Drive Organizational Innovation



KPMG

Managing third-party risk

With a continually expanding portfolio of investments that span multiple industries, private equity firms routinely engage third parties to perform services that they're unwilling or unable to do, or where a third party can do it smarter, faster, and better.

Private Equity International observed that there, are generally four key reasons private equity firms consider outsourcing to third parties:[1]

— As a response to increased demand and volume

— To reduce costs

— To help the firm grow by leveraging the third party's global footprint

— To manage increased regulatory burden

These third-party arrangements are often critical for private equity firms whose focus is on corporate acquisitions and portfolio health. However, it may expose them to information security and cyber risk (see ADP sidebar on right), as well as operational, compliance, reputational, concentration, country, legal, performance, and financial risk.

Financial services regulators recognize the increased use of third parties to support critical operations. But these regulators have routinely and repeatedly reminded financial services organizations that "using such providers does not relieve the financial institution of its responsibility to ensure that outsourced activities are conducted in a safe and sound manner."[2]

"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

Third-party risk: Case in point

ADP is a well-known third-party provider of payroll, tax, and benefits administration for more than 640,000 companies.

In April 2016, due to a weakness in ADP's customer portal, one the nation's largest financial services firms had some of its employees' W-2 data stolen.

Regardless of who was at fault, the financial services firm had to deal with a public relations nightmare as well as potential legal liability.

Source: Fraudsters Steal Tax, Salary Data from ADP, krebsonsecurity.com, 5/3/2016

[1] The Fund Administration & Technology Special 2015, Private Equity International, June 2015

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

Six-part risk management framework

The following six-part framework can help guide private equity 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 will set the tone from the top, and enable 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 private equity firm's 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 and to its portfolio companies.

   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 defines activities, roles, and responsibilities of the business unit engaging the third party, as well as risk management and internal audit (IA) functions.

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 (e.g., 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, private equity firms 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.

   What's more, this training should be ongoing to serve as both a refresher and to account for changing circumstances and responsibilities.

   Ongoing annual evaluations that assess individuals' performances relative to assigned TPRM roles and responsibilities should also be included as part of the TPRM program.

6. **Strengthen information reporting:** A well-designed TPRM program (1) establishes informational and actionable key risk indicators (KRIs) based on the firm's risk tolerance and limits, (2) regularly analyzes data collected, and (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.

   Critical to the success of a private equity firm's information reporting process is the use of state-of-the art technology. Innovative new technology can help you (1) facilitate internal and third-party work flows, (2) provide audit trails of oversight, 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 continue to review the third-party universe to determine if other suppliers might offer a better arrangement.

For more information on TPRM, please visit our Web site at KPMG/Insights/Third Party Risk Management.

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

Prevalence of corporate misconduct and fraud

Seventy-three 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 Integrity Survey

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

Source: OECD Bribery Report, 2015

Managing fraud and misconduct risk

Private equity firms—both large and small—are particularly susceptible to risks of corporate misconduct and fraud because of their inherent nature and characteristics, including:

— Involvement in complex transactions

— Lean operating structure

— Nonliquid assets

— Intense competition for portfolio company investments

— Extensive involvement with third-party intermediaries (TPIs)

— Lack of transparency

— Rising trend of investor activism.

Let's take a look at the primary types of corporate misconduct and fraud that occur in private equity firms and their portfolio companies. Then, we will address some strategies for reducing the chances of these actions occurring, and limiting the damage if and when they do occur.

Types of misconduct and fraud

Financial reporting and asset misappropriation: A private equity firm that is highly motivated to sell a portfolio company may have an incentive to commit fraud. In one recent court case, a private equity firm allegedly manipulated financial statements and inflated the value of one if its portfolio companies to persuade another private equity firm to buy the portfolio company.[3]

[3] *Prairie Capital III v Double E Holding Corp*, 10127-VCL, Delaware Chancery Court

Anecdotally, KPMG has seen an uptick in inquiries from private equity clients for forensic analysis of financial results, specifically with respect to asset tracing, asset valuation, and reliability of financial results.

Additionally, we have experienced an increase in inquiries from private equity clients for auditing and monitoring portfolio company investment activities.

For example, one private equity client expressed concern about sharp increases in the operating expenses of one of its portfolio companies. In another case, a private equity client was concerned about inflated costs and fraudulent payments by a portfolio company.

Bribery and corruption: Increased investor demands and activism, among other factors, have led to increased investment activity in emerging markets. One of the hazards inherent in these markets, however, is that they're located in foreign countries where fraud, bribery, and corruption are often part of the business culture.

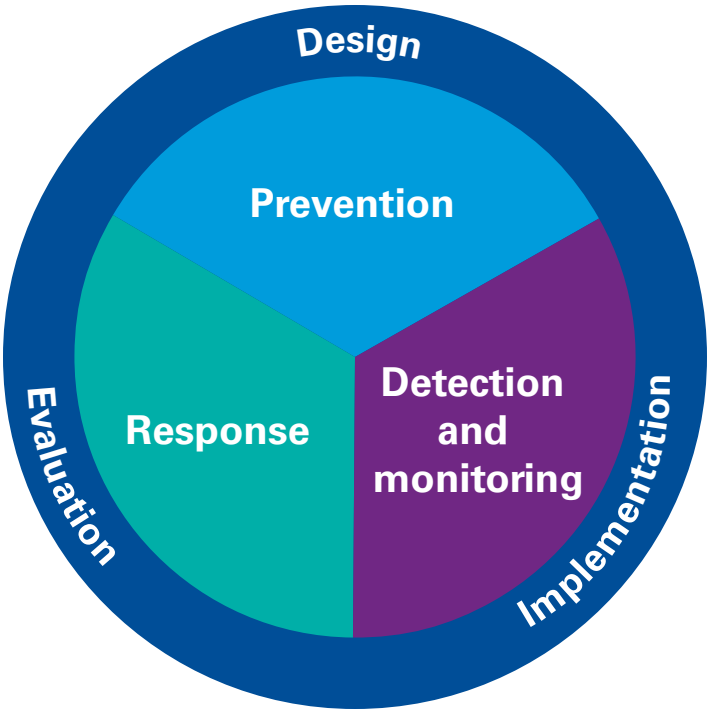
Complicating this situation even further is that private equity firms have to engage TPIs to perform critical functions (e.g., serve as "introducers," brokers, advisers, and consultants). In fact, according to the latest OECD Bribery Report, 75 percent of bribery cases involved payments through intermediaries.

The recent Och-Ziff bribery case[4] highlights several examples where TPIs were used to facilitate bribery, and resulted in Och-Ziff paying over $400 million in fines and penalties.

Market misconduct: With over $4.2 trillion in private equity and venture capital assets under management (AUM), private capital investment have soared to all-time highs; AUM was just over $700 billion in 2000.[5] And this huge growth has, in large part, spawned increased regulatory focus by the U.S. Securities and Exchange Commission (SEC).[6]

The SEC, as well as European regulatory authorities, are particularly concerned about transparency to investors. Specifically, they want to ensure that investors are given appropriate information that shows how fees and expenses are charged to portfolio companies or the firms. They are also focused on disclosures regarding the amount of these fees. Other areas of concern are failure to disclose conflicts of interest and misallocation of fund expenses.

There is no sure-fire way to eliminate the risk of fraud or corporate misconduct. But there are some best practices that private equity firms have found to be effective in mitigating their exposure to corporate liability, sanctions, and litigation. Private equity firms should adopt a fraud risk management strategy grounded in the three lines of defense: **prevention, detection and monitoring,** and **response.**



Prevention

Steps should be taken to identify areas of potential exposure to fraud and misconduct, and put in place strategies to mitigate this exposure. At a minimum, this includes private equity firms doing the following:

1. **Do your "homework"** before investing in a portfolio company: Perform enhanced fraud-related diligence, including a forensic analysis of financial results, and determine if the firm, the portfolio company, or any related third parties are violating any Anti-Money Laundering (AML), Office of Foreign Assets Control (OFAC) or other antibribery 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).

[4] Och-Ziff Capital Management Admits to Role in Africa Bribery Conspiracies and Agrees to Pay $213 Million Criminal Fine, U.S. Department of Justice, 9/29/2016

[5] https://www.preqin.com/docs/samples/2016-Preqin-Global-Private-Equity-and-Venture-Capital-Report-Sample_Pages.pdf

[6] https://www.sec.gov/news/speech/private-equity-enforcement.html

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: 2106 Annual Report to Congress on the Dodd-Frank Whistleblower Program

4. **Require that your portfolio companies:**
    a. Perform periodic fraud risk assessments that take into account their industry, location, compliance requirements, operations, and mitigation controls
    b. Take appropriate remedial actions to bridge significant control gaps
    c. Implement "whistle-blower" mechanisms designed to encourage employees, vendors, and contractors to report instances of fraud, misconduct, or suspicious behavior
    d. Design and implement compliance policies and procedures, establish a compliance infrastructure, and provide adequate training in support of these compliance efforts.

Detection and monitoring

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

For example, your private equity firm should require:

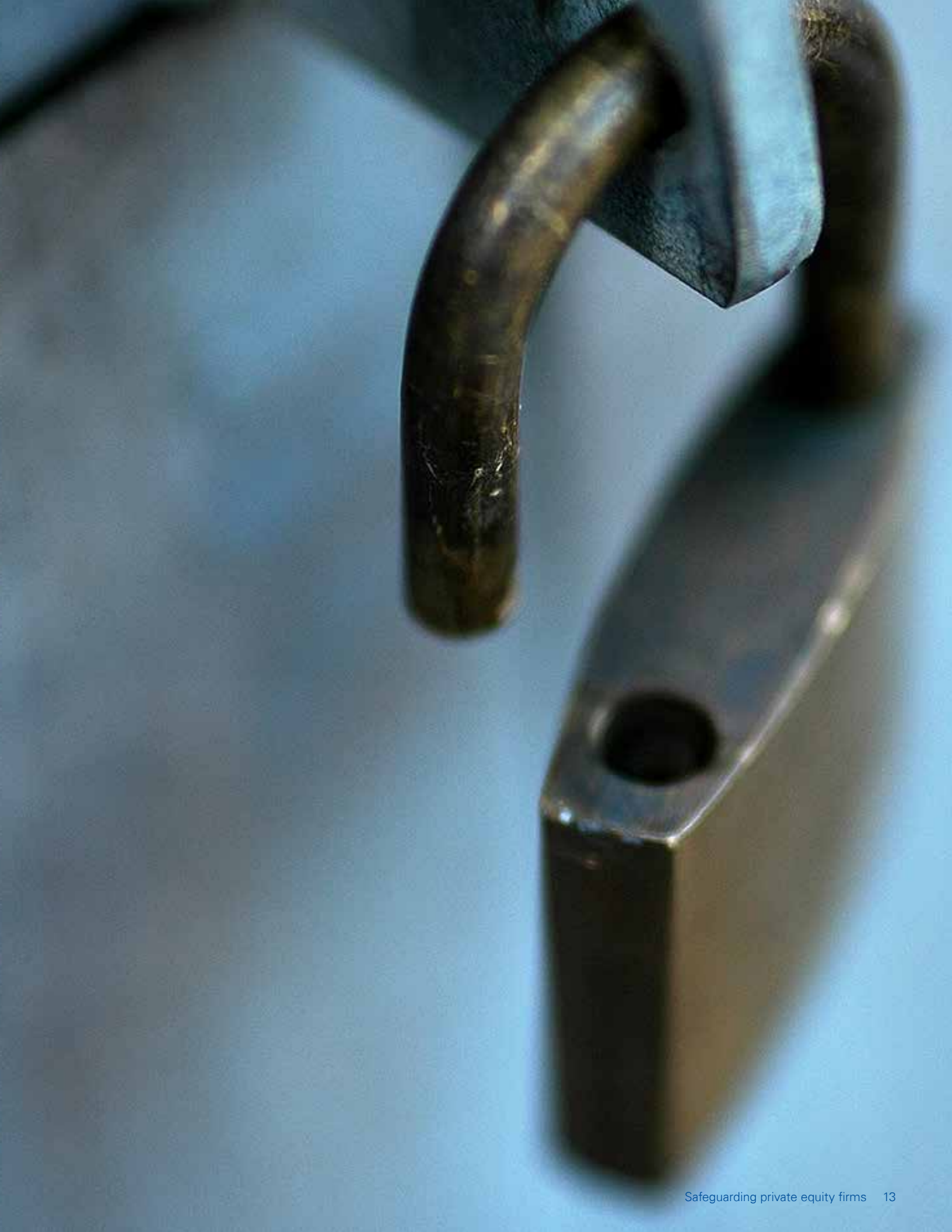
1. **Fund managers to establish KRIs** and perform periodic analytical analysis to identify potential accounts or classes of transactions, which may require follow-up review or analysis
2. **Portfolio companies** to now monitor relevant hot-lines and report any significant fraud or compliance issues; their employees to report fraud and provide periodic certification of their compliance with the code of conduct; and conduct risk-based audits of critical suppliers.

Response

Any well thought out program must set out a framework that includes procedures on how to respond to fraud and misconduct. In this way, you increase the odds of getting out ahead of potential issues. Hearing about an issue for the first time from the SEC is a place you don't want to be in!

To that end, private equity firms should require that they, as well as their portfolio companies:

1. **Periodically assess** the effectiveness of their whistle-blower 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 meetings as well as by sending out written communications
3. **Take prompt action** with respect to potential issues by establishing an appropriate 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.



Managing cyber risk

Private equity firms 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 private equity firms and other companies that have been the victims of cyber attacks.[7] These attacks have become so routine that some private equity firm 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 firm and its portfolio companies to become victims of a cyber breach, it also exposes them to penalties for regulatory failures. For example, in late 2015, the SEC fined an investment adviser with failing to adopt appropriate cybersecurity 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.

[7] SEC Release 2015-202; Also see R.T. Jones investment firm settles SEC violations for $75K after data breach, *The Washington Times*, Sept. 23, 2015.)

Establishing a framework

In order to prevent, or at least mitigate, these types of cyber attacks, private equity firms need to establish a systematic framework for:

— Assessing its potential exposure to cyber risks

— Objectively evaluating the private equity firm's business priorities in a manner that reflects its business strategies and goals, and its risk tolerance

— Allocating resources efficiently and effectively.

Ideally, a chief information security officer (CISO) should be charged with providing governance, oversight, and a strategic vision for the firm's cyber risk management framework and related activities. As explained below, the framework should incorporate a four-pronged approach aimed at:

Information risk management

The CISO should be responsible for gathering, evaluating and then targeting tangible cyber threats on company operations or property, including:

— Intellectual property

— ERM initiatives/systems

— Business continuity management

— Email and computer systems

— Cybersecurity

— Compliance

Private equity firms typically have an ERM function that incorporates deal risk, compliance risk, and/or credit risk. They need to expand this function to include information risk management that covers the firms as well as their portfolio companies.

Raising the awareness around information risk to the firm and its portfolio companies makes it more likely that these risks can be identified more quickly, and suitable remediation plans can be developed and implemented to mitigate damage.

Business enablement

As the private equity firm's investment portfolio expands, it needs to focus on supporting the portfolio company's rapidly changing needs. This includes understanding how these new businesses expose the firm to risk, and dealing with an ever-changing cyber-threat landscape.

Efforts to develop an adequate risk management approach include focusing on:

— New revenue streams

— Workforce changes

— E-discovery and investigations

— Enhanced business intelligence needs.

Keep in mind that Information security isn't just about a smart technology staff or the latest security technology. Rather it's about recognizing the impact that every employee has on information security.

The business leaders at both the firm and portfolio company level must understand the risks they face, and then develop and implement remediating controls that enable the business to address the risks in a manner aligned to their business imperatives.

Consistent application across organization

To increase the likelihood of success, the CISO's efforts should be deployed consistently across the organization. To do this seamlessly and effectively, you need to get enterprise-wide buy-in from all stakeholders, including:

— Regional and global management

— The board

— Vendors

— Third-party management

— Security services.

Given the entrepreneurial nature of private equity firms, deal teams tend to be organized to focus on accomplishing functional business objectives in the most direct manner possible. The drawback to this approach is that it often leads to inconsistencies in the application of security across the firm, including the firm's infrastructure and/or systems, which can leave the firm exposed to cyber risk.

To address this risk, it's important to develop a consistent set of security controls across the firm and its portfolio companies.

A comprehensive security management approach includes providing training for all appropriate stakeholder groups, explaining both the rationale for it, what the company is doing, and how they can aid in the effort. One key to getting their buy-in is demonstrating the value of this unified control framework in terms of how it will lead to a reduction in the workload, and enhancement of the value of the company and their share of it.

Managing compliance risk

The number of laws, rules, and regulations—as well as the degree of regulatory scrutiny—impacting the private equity sector has grown exponentially over the past several years. As a result, the private equity business model is no longer driven solely by performance. Rather, it's been transformed into one that must balance increased costs and expenses against a duty to ensure that a robust compliance infrastructure is maintained.

The SEC has ramped up its enforcement efforts against private equity firms, creating both the Private Funds Unit and the Division of Economic and Risk Analysis. These new departments have added the power of data mining and analytics, which are designed to drive and support the SEC's examination priorities and enforcement actions.

As a result, the SEC has steadily increased the number of enforcement actions and fines against private equity firms over the past few years. For example, in mid-2016, the SEC fined four private equity fund advisers affiliated with a major private equity adviser approximately $53 million for misleading fund investors about fees and expenses charged to the fund.[8]

Some key risk areas for private equity firms currently receiving close scrutiny from the SEC are:

- Coinvestment policies and procedures
- Improperly disclosed fees and expenses
- Expense shifting and allocation practices
- Disclosure of conflicts of interest
- Allocation of investment opportunities
- Transparency
- Valuation practices
- Cyber security

Management-led compliance efforts

To effectively navigate the uncertainty of impending regulation, and mitigate current compliance risks, firms must take a top-down approach that has corporate leaders:

- Establish a culture of compliance
  - It's important that individuals at the firm understand that it is their responsibility to "raise their hand" when they see something they feel may be wrong or harmful to investors.
- Participate fully and meaningfully in communicating this message to all levels of the firm
- Appoint and support a chief compliance officer (CCO) who has unfettered access to senior management, and can anticipate and respond to changing regulatory obligations
  - Ideally the CCO has stature and influence in the firm, and is also well versed in securities laws and compliance obligations. This will better enable the CCO to leverage the resources of outside legal counsel, compliance consultants, and internal staff to round out an effective compliance function.

Among its many benefits, a comprehensive and rigorously enforced compliance program will give regulators greater comfort when examining a firm. This can result in the mitigation of fines and other penalties if lapses are found to exist.

[8] SEC Press Release 2016-165, 8/23/2016)

Establishing a framework

A strong compliance risk management program, and an underlying compliance framework that reinforces effective corporate strategy, requires certain fundamental components, as set out below:

Governance and culture: As a first step, private equity firms should assess their governance oversight and firm-wide culture. This assessment should identify all risks, including potential conflicts of interest, that are unique to the firm's business activities as well as those of its portfolio companies.

The firm should also assess how quickly it takes action after discovering a potential issue. The length of time that issues remain outstanding often impacts the SEC's approach when it comes to determining fines and penalties.

Finally, 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 and its portfolio companies.

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 the following elements:

- Regulatory change management that monitors whether the firm needs to modify its compliance program and business practices in light of changing regulatory rules
- Regulatory exam management to ensure that the fund and its portfolio companies are prepared for exams by regulators

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.

"The SEC's current mantra is that if you didn't write it down, it didn't happen. Therefore, private equity 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

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 of an SEC registered adviser. Annual training should focus on key areas of compliance risk, including the code of ethics, personal trading, handling of material nonpublic information, conflicts of interest, and transactions with affiliates.

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 model.

Documentation: The compliance program should require robust documentation. This helps ensure that the private equity 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, and internal audit review. 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.

Monitoring and testing: The compliance program should implement periodic, risk-based, monitoring and testing that includes:

— Periodic expense allocation reviews to ensure that allocations are being made correctly and as per policy

— Process and control reviews to make sure that the program is continuing to function and guard against risks as intended

— Confirmations of books and records requirements to ensure that they haven't been tampered with and are still in compliance

— Reviews of third-party and affiliated-party arrangements to ensure that previously approved third parties and affiliated arrangements continue to be above board.

Technology and data analytics: Once a comprehensive compliance policy is established, private equity firms should leverage advanced technology and data and analytics (D&A) to:

— Perform ongoing monitoring and testing of its policies and procedures

— Modify the risk register as needed by periodically performing a gap analysis that assesses the current set of policies and procedures, and identifies where they need to be enhanced or changed in light of the most critical risks faced by the firm.

Crisis management

When a corporate crisis occurs—and this generally is a matter of *when*, not *if*—the ability to recover quickly, while restoring consumer and investor confidence, is paramount for continued success. No matter the nature of the event sparking the crisis—fraud, bribery, negligence, weather, geopolitical, supply chain, cyber, health, safety or other—the headlines are replete with companies that either successfully addressed the challenge or suffered lingering effects long afterwards.

One only has to read the newspaper headlines or go on social media to see the damage that can be caused. Take a look at Chipotle, a formerly successful company with a pristine reputation. It has yet to recover from its public relations disaster regarding E. coli-infected food, and the manner in which the incident was handled (see sidebar on page 22).

Allegations of fraud, misconduct, or bribery can quickly devalue a private equity firm. Even the smartest, most successful private equity firms may be one or two public relations incidents away from losing their reputation.

"Having a nimble crisis management team spring into action as soon as a crisis emerges is essential," noted David Calef, KPMG Director, Crisis Management. "And it's critical to have that team 'practice' in a simulated table top environment in order to effectively manage the risk and consequences that can occur from an incident."

"In today's highly connected global economy, social media has rewritten the rules in terms of how to approach a crisis," he added. "You may only have a matter of hours, not days, to respond."

Planning and preparation the key

But in order for this to occur, a firm must take steps well before a crisis hits. Although the response, recovery, and remediation components are critical parts of a crisis management program, proactive planning and preparation are the keys to a successful one.

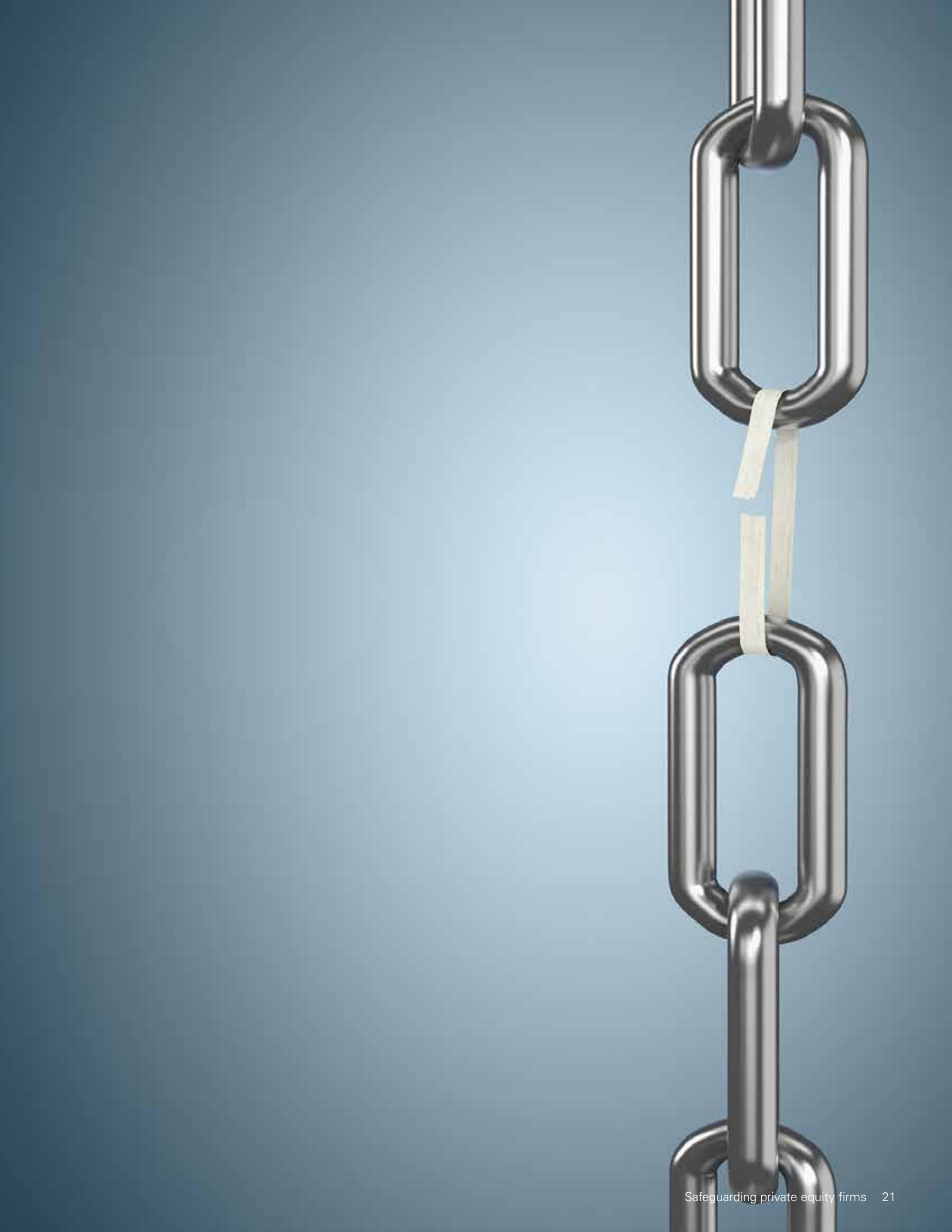
This means taking a cross-functional and cross-organizational approach to crisis management. It also requires the firm to design a crisis management plan, thoroughly vet it with the key stakeholders and decision-makers throughout the organization, and periodically run "fire drills" to test that the plan works as designed prior to a crisis occurring.

However, whether due to lack of resources or attention, few private equity firms and their portfolio companies have taken these proactive steps.

Act quickly

"Having a nimble crisis management team spring into action as soon as a crisis emerges is essential," noted David Calef, KPMG Director, Crisis Management. "And it's critical to have that team 'practice' in a simulated table top environment in order to effectively manage the risk and consequences that can occur from an incident."

"In today's highly connected global economy, social media has rewritten the rules in terms of how to approach a crisis," he added. "You may only have a matter of hours, not days, to respond."



Chipotle: How not to respond to a crisis

Until the fall of 2015, Chipotle was generally viewed as the fast-food model of the future. Its brand promise: food with integrity.

That all changed when the restaurant was linked to a massive E. coli outbreak. And it has yet to recover.

Same store sales have remained negative, and average store sales have shrunk by double digits.[9] It didn't help that the company's co-CEO, Monty Moran, initially seemed to blame the CDC (Centers for Disease Control) and the media for sensationalizing the severity of the crisis rather than apologizing, acknowledging the severity of the problem, and describing what was being done to fix it.[10]

[9] One year after Chipotle's E. coli crisis, chain still struggling, cnbc.com, 10/31/16

[10] Chipotle's E. coli fiasco teaches us how not to respond to a crisis, fortune.com 12/15/15

Five-step crisis planning process

The following five-step process can assist in crisis planning. It should be overseen by a chief administrative officer (CAO) or another C-level executive with authority that spans the entire organization:

1. **Risk assessment:** The firm should perform a comprehensive risk assessment that looks at incident types, geographical risks, capability risks (by geography), and logistical risks.
2. **Playbook:** Next, the CAO should assemble a playbook that addresses the most critical risks. The playbook should include steps for dealing with individual events, and the subsequent claims that might occur. It should also incorporate the company's philosophy, values, and ideals.
3. **Incident response plan:** The CAO should design a comprehensive response plan that includes details for a crisis response team. The team members should have clearly defined roles for dealing with the most likely crisis scenarios. The plan should also include necessary resources, activities, and time frames for responding to disruptions, and cover people, processes, systems, data, and governance.
4. **Plan testing:** Once the plan is finalized, the CAO should conduct simulated table-top exercises and simulated events that test the firm's response. This will help ensure that the plan is practical and actionable.
5. **Plan maintenance:** The testing phase should be repeated at regular intervals (at least annually), ensuring continued readiness and viability. Revise the plan as the assessment warrants.

For portfolio companies, too: This five-step crisis planning process not only applies to the private equity firm, it should also be implemented at the portfolio company level as well. After all, a crisis that hits a portfolio company can have a significant impact on the firm's value and returns.

Risk assessment	— Incident types — Geographical risks — Capability — Risks (by geography) — Logistical risks
Playbook	— Individual events — Subsequent claims — Firm philosophy — Firm values — Firm ideals
Incident response plan	— Create crisis response team — Define team roles — Resources (people, systems, data) — Activities — Response time frame — Process and governance
Plan testing	— Test firm response — Conduct simulated table-top exercise — Conduct simulated events
Plan maintenance	— Repeat testing at regular intervals (at least annually) — Revise plan as assessment warrants

KPMG

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 your firm and its portfolio companies if they do.

By creating a robust risk management plan, executives at private equity firms and their portfolio companies can increase the probability that their organizations 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 firm a far greater loss of resources, value, and reputation.

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

–Christine Buchanan, KPMG Partner, Risk Consulting

How KPMG can help

We provide audit, tax, and advisory services to a broad range of industry players, from start-ups to FORTUNE 50 diversified financial service firms. We offer tax and advisory recommendations designed to enhance financial and operational structures, and help our clients proactively take advantage of change, not merely react to it.

Our Private Equity practice is a fully integrated, cross-functional team of partners and professionals who are focused on serving global private equity firms and their portfolio companies. Our experienced professionals understand the dynamic nature of the private equity marketplace—domestically and in investment centers around the world—and its enormous growth potential. And we understand the issues that private equity firms face on local, national, and global levels.

Our professionals bring passion and a fresh approach to the issues that challenge our private equity clients through their entire life cycle, from structuring funds to realizing value. Our private equity practice supports the links between fund, managers, transactions, investments, and value realization. Our single-point-of-contact business model makes it easy for you to obtain the services you need, when you need it—whether it's raising capital and making investments, fund and portfolio management, or exit and value realization.

Finally, thanks to our extensive geographic footprint—established through our global network of member firms—we have access to firsthand, real-time information on matters that most impact you, no matter where you are located or where you operate. Our private equity services are delivered through a global network of member firms, with more than 35,000 partners and professionals spanning 115 jurisdictions, covering the world's most prominent financial centers. They serve our private equity clients and their portfolio companies, wherever they're located or do business.

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 Private Equity Web page for more information about our services and to read our latest thought leadership publications. Or call one of the private equity specialists below, talk with them about your situation, and learn how we can help:

Christine Buchanan
Partner, Advisory
T: 212-954-3994
E: cmbuchanan@kpmg.com

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

kpmg.com/socialmedia

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