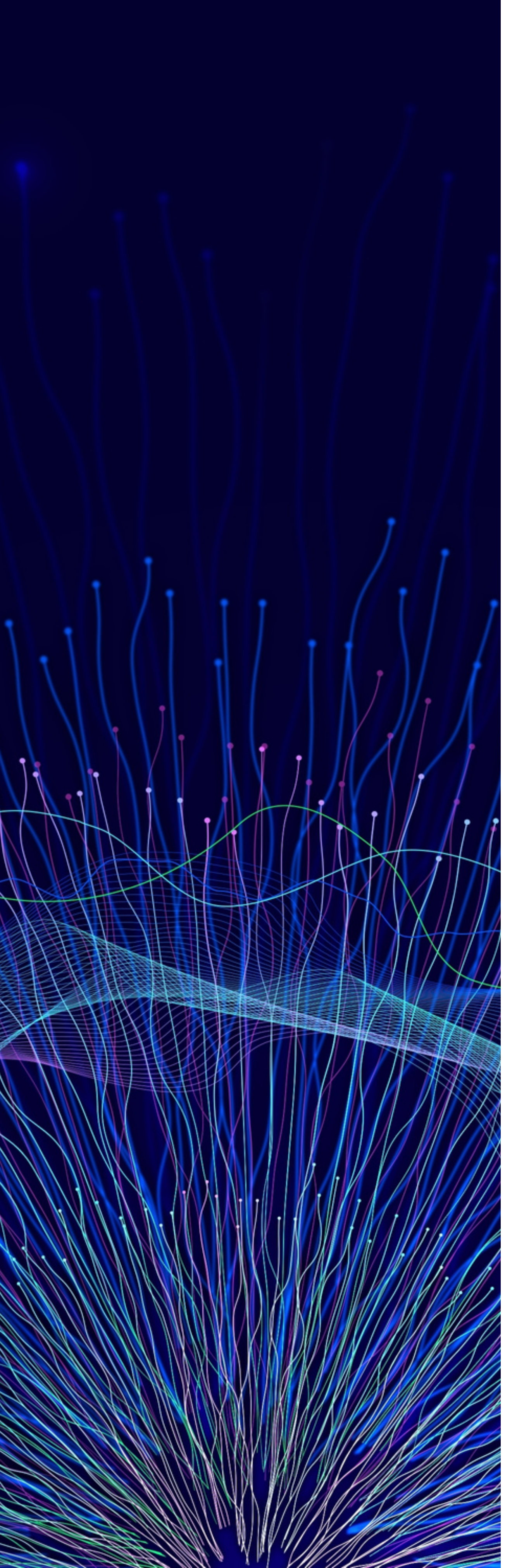
WHITEPAPER

Cybersecurity Compliance Guidance

Navigating Cybersecurity Compliance for Private Equity Firms

RKON™



Without Clear Guidance, PE is Responsible

To make matters worse, it is clear that the SEC, based on varying alerts and statements, has yet to introduce actionable cybersecurity compliance guidance beyond the broad areas defined below:

- The accurate creation of required records and their maintenance in a manner that secures them from unauthorized alteration or use and protects them from untimely destruction;
- Safeguards for the privacy protection of client records and information; and business continuity plans

To fulfill these broad requirements, CCO's are left with broad unanswered questions:

- What processes need to be put in place?
- What tools do I need to buy?
- Do I hire or outsource?
- How much should I budget?

Private Equity Cybersecurity Survey

78%

believe cybersecurity is not analyzed or specifically quantified as part of the M&A process.

83%

of businesses say a deal could be abandoned if previous cybersecurity breaches were identified.

90%

say a cybersecurity breach could reduce the value of a deal.

A New World for PE

The passing of the Dodd-Frank Act on March 30, 2012, exposed all private fund advisors and Private Equity Funds to the Advisor Act of 1940 and the subsequent Compliance Program Rule 206(4)-7.

The Presence Exams initiated by the OCIE and ensuing actions taken against firms by the SEC sent a clear message that compliance in Private Equity is a real risk and needs to be taken seriously.

Cybersecurity Compliance & Technology Controls: A New Requirement for PE

While the general compliance guidelines provided by the SEC are well within the experience of most firms to implement and execute, cybersecurity and IT controls is one area firms struggle to execute with confidence. Private Equity is learning what other regulated industries have discovered, which is that there is a lack of clarity on what needs to be done to be compliant. The integrity of and access to data is the cornerstone of most compliance standards. However, the technology, processes, and controls needed to achieve that standard continuously evolve based on the evolution of technology and the threat landscape.

Portfolio Company Compliance: A Trend Towards Centralization

In addition to internal controls, PE firms are finding portfolio company level compliance a major source of risk as standards like PCI, HITRUST, and vendor auditing become critical even in mid-size organizations. The challenge is that portfolio companies in the mid-market often lack the economies of scale and expertise to execute an effective and efficient compliance strategy. This inexperience leads to EBIDTA impacting overspending or suffering from the negative valuation impact of poor audit results that get uncovered during exit due diligence or pre-IPO. In the worst-case scenario, portfolio companies overspend and still fall short of compliance standards.

Effective Cybersecurity = Valuation

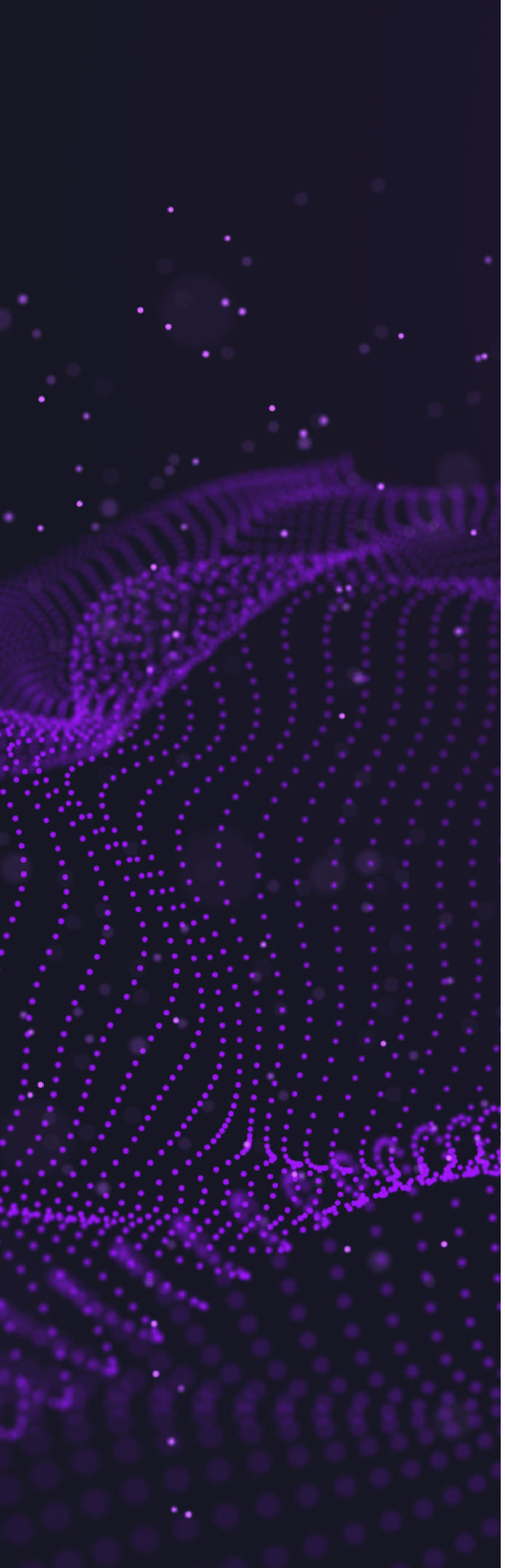
These factors are creating a trend where portfolio compliance is falling under the governance of the PE firm, and in some cases, even establishing a centralized service compliance model. This emerging trend goes against the traditional “hands-off” approach many PE firms have taken in the past, but firms adopting this approach are seeing tangible valuation gains and ROI in what has been seen as a Cost Center in the past.

Common Compliance Controls

SARBANES OXLEY HIPPA **GLBA** 206(4)-7 **PCI-DSS** FISMA

Having and maintaining an effective cybersecurity program is not something to be feared. With a holistic and well-thought-out approach, the program can actually be used to increase value. To achieve this risk assessments will be performed, policies will be written, and controls (both technical and procedural) will be implemented. This is an ideal time to extend those policies and controls to your entire portfolio.

Centralized Security Compliance Using a "Hands-Off" Approach
The SEC will eventually deliver more specific guidance on Cybersecurity Compliance for PE firms, and the controls required are going to be very similar in nature to the standards already in existence. Whether it is Sarbanes–Oxley (SOX), PCI-DSS, GLBA, FISMA, or HIPAA, each standard has its own nuances, and compliance can be achieved with the same controls and execution strategy.



Through the intelligent mapping of the required cybersecurity controls, a common and fulfilling "hands-off" model framework can be applied so that all entities enjoy low-cost, standardized solutions that reduce the work effort to achieve base compliance. The challenge is applying these standards in a way that ensures portfolio companies have the appropriate separation, independence, and portability to enable an efficient exit strategy.

Common Cybersecurity Compliance Architecture Approach

RKON MSP **95%**

Common Cybersecurity
Compliance Architecture

5% **PORTFOLIO COMPANIES**

Custom Compliance: HIPAA,
PCI-DSS, GLBA, SOX,FISMA

The benefits of this approach are obvious: economies of scale, standardization that can be executed during the TSA as a templated approach, predictability in audit response, and ultimately valuation building. The complexity of this compliance model lies in creating an architecture that allows the following:

- **Enabling Separation and operational independence of portfolio companies from PE operations;**
- **Creating Portability so Portfolio companies can be divested and remain whole on compliance;**
- **Repeatability regardless of the compliance standard;**
- **Independence to execute.**

The Value of An IT Partner

As more organizations move to the cloud securing business infrastructure is a critical component to preventing data, financial and operational losses. With technology growing in sophistication, cybersecurity criminals are also growing in sophistication and capability. These cybersecurity criminals know this and that is why private equity and mid-market companies are becoming the prime targets for cyber criminals.

In the past, cyberattacks were relatively resource-intensive, so security breaches were more focused on high value or larger organizations. Now, cybercriminals are infiltrating these private equity and mid-market organizations using automated, scalable, on-demand artificial intelligence to launch sophisticated attacks resulting in large data & financial loses.

Especially given the ever-more sophisticated cyberthreat landscape and competitive business market, it's becoming imperative to optimize IT practices to not only keep pace but also gain the flexibility to more easily manage whatever issues arise.

No matter whether your business is grappling with the ongoing IT skills shortage, struggling to modernize development processes, or needing to better understand your software engineering capabilities, RKON is well-positioned to help.

ABOUT RKON

Founded in 1998 in Chicago, RKON has grown to become one of the nation's leading IT advisory practices. Our comprehensive understanding of execution strategies, technology, business processes, operations analytics, risk and compliance, and planning and integration supports hundreds of organizations.

Recognizing that no two companies have the same IT challenges, RKON takes a truly customized approach. We serve as trusted advisors to our customers, providing strategic guidance, technical resources, and honest assessments to address competitive challenges and meet long-term goals.

CONTACT US

rkon.com (312) 654-0300
328 S Jefferson St #450, Chicago, IL 60661