RKON | Solution Paper

Cyber Security Compliance Guidance for Private Equity Post Dodd - Frank

BY CHRIS DEMICHAEL
Chief Security Officer, RKON Inc.

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 PE

While the general compliance guidelines provided by the SEC are well within the experience of most firms to implement and execute, the Cybersecurity and IT controls is one area firms struggled to execute with confidence. Private Equity is learning what other regulated industries have discovered which is a lack of clarity on what you need to do specifically to be compliant. Integrity of data and access to that data are the cornerstones of most compliance standards. However, the technology, processes and controls to achieve that standards continuously evolve in reaction to technology and threat landscape evolution.

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 ike PCI, HITRUST, and vendor auditing becoming table stakes even in midsize organizations. The challenge is portfolio companies in the mid-market often lack the economies of scale and expertise to execute an effective and efficient compliance strategy. The result is EBIDTA impacting overspend or suffering the valuation impact of poor audit results that get uncovered during exit due diligence or pre-IPO. In the worse cases portfolio companies overspend and still fall short of compliance standards.

Without Clear Guidance: PE is Accountable

To make matters worse, it is clear that the SEC, based on the 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
- Business continuity plans

To fulfill these broad requirements, CCO's are left with broad unanswered questions: What processes, what tools, how much should I spent?

- 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?

Consider the following results from a 2015 survey of Private Equity:

78% believe cybersecurity is not analyzed or specifically quantified as part of the M&A process

83% of them saying a deal could be abandoned if previous cybersecurity breaches were identified

90% of them saying a cybersecurity breach could reduce the value of a deal.

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.

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. 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 Cybersecurity Compliance while maintaining a "Hands Off" Approach

The SEC will eventually deliver more specific guidance on Cybersecurity Compliance for PE's 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, while

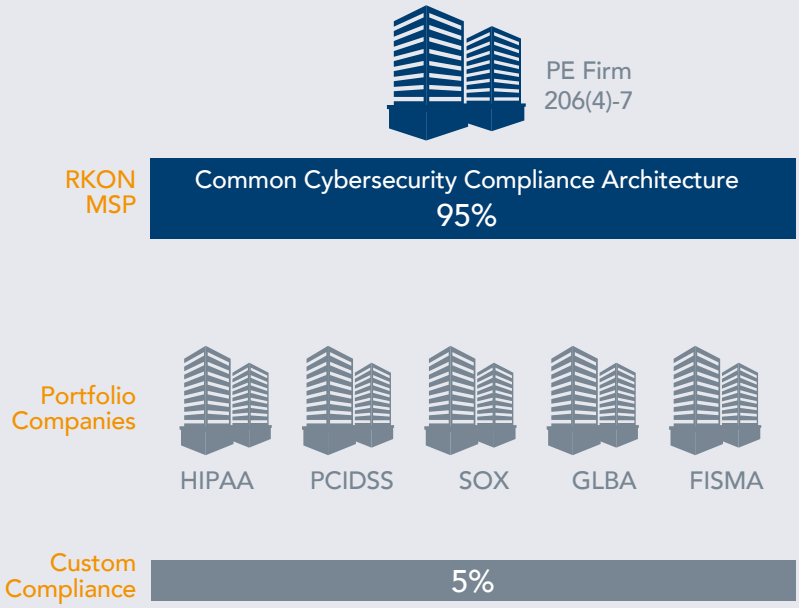
each standard has its own nuances, the majority of compliance can be achieved with the same controls and execution strategy.

Through intelligent mapping of the required cybersecurity controls a common while fulfilling a "hands off" model framework can be applied so that all entities enjoy a cookie cutter, low cost, standardized solution that will reduce the work effort to achieve base complinance down to a bare minimum. The challenge is applying these standards in a way that ensuring portfolio companies have the appropriate separation, independence and portability that enables an efficient exit strategy

Common Cybersecurity Compliance Architecture Approach

The benefits of this approach are obvious. Economies of scale, standardization that can be executed during TSA's as a templated approach, predictability in audit response and ultimately Valuation Building. The complexity of this compliance model is 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
- Requires and independent part to execute



RKON is just that company: We understand Compliance, Private Equity, and Operational Excellence