Reduce the Risk, Cost, and Chaos of Extending Governance, Risk, and Compliance to Portfolio Companies

INTRODUCTION

Private equity (PE) firms are required to prioritize cybersecurity initiatives, including strong governance, risk management, and compliance (GRC) alongside their deal performances. The continued onslaught of high-profile cyberattacks and investor scrutiny are putting immense pressure on PE firms to ensure their portfolio companies – where a breach could quickly upend a fund and possibly devalue the PE firm – are effectively managing their cybersecurity program.

Private equity firms and portfolio companies amass a large amount of contextual, personal, and financial information on institutions and individuals, making them prime targets for bad actors. In addition, press coverage of a new deal often acts as an attack catalyst – resulting in a substantial increase in cyber incidents.

THE CHALLENGE

The complexity of GRC processes, cost of customizations across multiple portfolio companies, and the time involved in implementing a robust GRC program means the support and control each PE firm has over their portfolio companies varies greatly. Traditionally, PE firms have taken a hands-off approach to managing cybersecurity, IT, and GRC related issues beyond their own walls. Unfortunately, the need to speed up deals to get revenue moving quickly means risk-based due diligence is often fulfilled with shortcuts, skewed workflows, and ineffective risk management.

Often, PE firms rely on their partners and the portfolio companies themselves to manage cybersecurity risk. This has led to several unintended consequences each creating its own unique challenge, including:

- An incomplete view of risk across the portfolio
- An inconsistent assessment of risk within portfolio companies
- Undefined and time-consuming manual processes that lack automation and clear visibility into the cybersecurity maturity posture and financial risk exposure of the portfolio.
- A lack of understanding of the people, processes, and technology necessary to achieve cybersecurity maturity is often met by adding additional staff and ineffective tools which can quickly increase overhead, add layers of complexity, and reduce the portfolio's value.
- Developing an in-house or "homegrown" GRC program can delay implementation. From inception to budget approval to enablement can easily exceed 18-months. In which time, risks, priorities, and technologies change – adding an additional layer of risk to an already vulnerable situation.
- Conventional, consultant-led solutions that are rarely multi-tenant, and often difficult to adapt to unique conditions, creating a rigid solution that's unable to flex to the changes in cybersecurity threats.
- A communication breakdown from a lack of deep expertise in governance and technology and the ability to work with global organizations with a wide variety of skillsets and cultural nuances.

In less tech-savvy environments or those that do not prioritize new technology as a critical component of their overall strategy, these challenges are amplified and not only hinder risk management but can negatively impact trust with investors, market competitiveness, and long-term success.

THE SOLUTION

TruOps is an agile, powerful GRC platform that combines technology, expertise, and processes to deliver robust, cost-effective GRC management consistently across portfolios with a clear, direct line to risk reduction and improved business outcomes for PE firms.

TruOps is the only GRC platform on the market that:

- Is built to scale with the PE firm, growing as the number of portfolio companies increases.
- Provides a single dashboard to view and manage risk across the entire portfolio allowing for proactive risk management, the identification of trends, and effective allocation of resources to mitigate threats.
- Has skilled cybersecurity experts conduct security assessments that follow a consistent methodology defined in alliance with the portfolio company's leadership.
- Delivers risk and maturity reports with detailed insight into each portfolio's current security posture and define improvement opportunities.
- Partners with an experienced managed services team of cybersecurity professionals from their parent company, SDG Corporation. This unique combination delivers the people, processes, and technology at a significantly lower aggregated cost to the PE firm.

SUMMARY

Private equity firms require a strong, scalable, and efficient GRC platform to proactively keep up with the fast pace of cybersecurity threats, regulatory changes, and their competition. The complexity PE firms face when extending homegrown cybersecurity across multiple portfolio companies is often expensive, ineffective, and time consuming. TruOps solves the business challenges firms face by providing robust governance, risk, and compliance across all their portfolio companies to ensure regulatory and investor obligations are met and that their assets remain safe.

REGULATION READINESS
Identify, assess, and mitigate compliance and regulatory risk.

ACCURATE REPORTING
1-click reporting on real-time risk across your internal organization and extended third-party environment.

IMMEDIATE VALUE
Reduce costs and experience ROI from day-1 through automation, collaboration, and simplified processes.

VISIBILITY
Gain a holistic view of cybersecurity, compliance, and risk posture and work collaboratively to respond to threats and mitigate risk.

ADVANCED CONTROL & COLLABORATION
Actionable insight empowers your security and compliance teams to manage and control your organization's risk.

EXTENDED RISK MANAGEMENT
Multi-tenant functionality allows for consolidated risk management oversight for multiple locations, franchises, business units or portfolio companies.

+1 (203) 866 - 8886 sales@truops.com www.truops.com