dohertyassociates

ACHIEVE MORE, DIFFERENTLY

Modern workplace, modern security:

how to use technology to build compliance, resilience and data protection into your business

The financial services sector is evolving rapidly and private equity funds, in particular, are in the middle of substantial regulatory and operational changes.

At the core of these changes are two key drivers: regulators and investors. Since 2007, regulators have been demanding greater transparency and security across operations, and investors are demanding greater transparency. So far, funds have been meeting these evolving demands through a patchwork of systems, spreadsheets and 'sheer manpower'[1].

This raises a question: how can private equity funds build compliance, resilience and data protection into their businesses more efficiently, to meet the needs of regulators and investors?

The answer: technology.

This white paper examines the security risks and critical business problems faced by firms, and explores how rolling out modern technologies and workplace tools can help. We'll look at how using technology to solve key problems - like data management and reporting - can help build compliance, resilience and data protection into your operations across your portfolio.

1. Implement better data management processes

> Financial services firms are awash in data, both from traditional internal structured sources and, increasingly, from external "unstructured" sources ranging from social media to newly-accessible government and third-party databases. Data is no longer measured in terabytes (a thousand gigabytes) but in zettabytes (a billion terabytes).
>
> *- Accenture, Exploring Next Generation Financial Services: The Big Data Revolution*

Of all the firms surveyed as part of EY's 2016 Global Private Equity Fund and Investor Survey, 63 percent of private equity funds[2] said that their most significant operational challenge is **data**.

Technology and 'big data' have been disrupting financial services for some time now. But though data has become a key factor in decision-making[3] and investment strategy[4] firms have yet to find an efficient way to use the large volumes of data - structured and unstructured, internal and external - they find themselves with. The result is **information overload**.

Having lots of data is good. **But 'lots of data' is useless without a good process for managing, accessing and using it**. So, firms need to implement better data management processes to capitalise on the value of data: having a way to separate the 'signal' from the 'noise' in datasets is essential for making better data-driven decisions.

Technology: a foundation for better data management

Fifty-three percent of finance executives around the globe acknowledge that their focus should be on data[5] to meet their firm's **operational and regulatory requirements**.

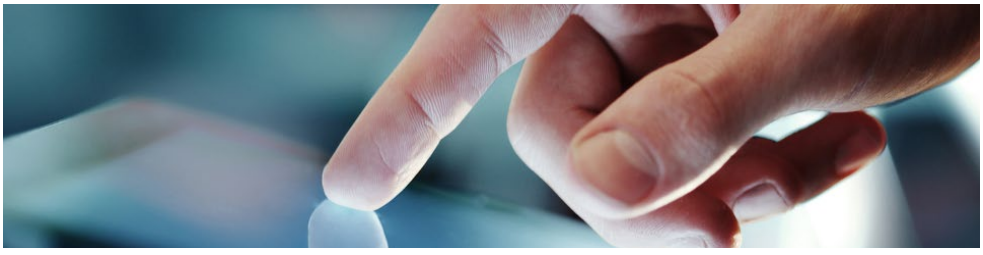
Unfortunately, the reality is that most **firms simply don't have the technology infrastructure** to manage and utilise data effectively. Furthermore, 61 percent of CFOs feel that there aren't many effective data management systems on the market for firms in financial services.[6]

That may have been true 10 years ago, but the **cloud** now makes it easier for firms to manage and access their data. More importantly, it shifts the ownership and management of data from the IT department to the people who use it: the business units.

Three cloud technologies that can improve your data management

Here are some cloud technologies that you can leverage for better sourcing, management and processing of data:

- **Advanced analytics** with Microsoft Azure enables you to securely store infinite amounts of data from diverse datasets and draw upon it in real-time to make actionable insights. It integrates with your existing IT environment and gives you a better way to manage, access and use data.
- **Data warehouses**, like Azure SQL Data Warehouse, allow you to ingest large structured and unstructured dataset and run thousands of analytics queries over all your records. You could use this to monitor price history or explore changing market dynamics, which is how Christoph Leinemann, senior director of data engineering at Jet.com, uses it.
- **Machine learning services**, now part of Microsoft's Cortana Intelligence Suite, are a good option for advanced firms with data science capabilities who want to build and use their own predictive analytics solutions.



Better data management: the key to resilience and competitiveness

Good data management is **essential for building resilience, security and compliance** in your firm - especially in this increasingly competitive and regulated industry. But it can also **differentiate your firm** and become a source of **competitive advantage**, too.

Speaking to the Financial Times in October 2014, Schroders' then-head of investment Peter Harrison - who serves as the firm's CEO - said that asset managers need to 'get to grips with big data in order to remain competitive' and take advantage of data found both internally and externally:

> *"Asset managers have got to get much smarter [and] work out how we can use the vast amount of data out there more effectively. Using data effectively will give you the vital, winning edge."*[7]

2. Develop better cybersecurity policies and protections

According to Accenture, financial services firms across the globe are investing heavily in financial technologies - particularly big data technologies and predictive analytics.[8]

But with more technology comes a higher risk of cyber-attacks. And only seven percent of investors are satisfied with the current cybersecurity policies of their fund managers.[9]

Private equity funds are a target for cybercriminals

Private equity funds are at a significant risk of a data breaches because of the type and volume of customer and market-sensitive data they collect. Examples of this data includes:

- Sensitive information about **investors**;
- Investment **strategies, trade secrets** and other proprietary information;
- Information about **vendors**, portfolio companies and **employees**; and
- Data from limited **partners**, counterparties and other sources.

It's the diversity of this data that makes it so attractive to hackers and cybercriminals. And when (not if) this data falls into the wrong hands; it can severely damage your portfolio and cause extensive business interruption. The financial and legal penalties of a breach are high too: with the EU General Data Protection Regulation (GDPR) reforms, fines for breaches of personal information can be as high as percent of your annual turnover.

How to improve your cybersecurity policies and processes

As private equity funds continue to build their ecosystem of technologies and digital services, they will need to develop better cybersecurity policies and protection mechanisms. Here's how you can start:

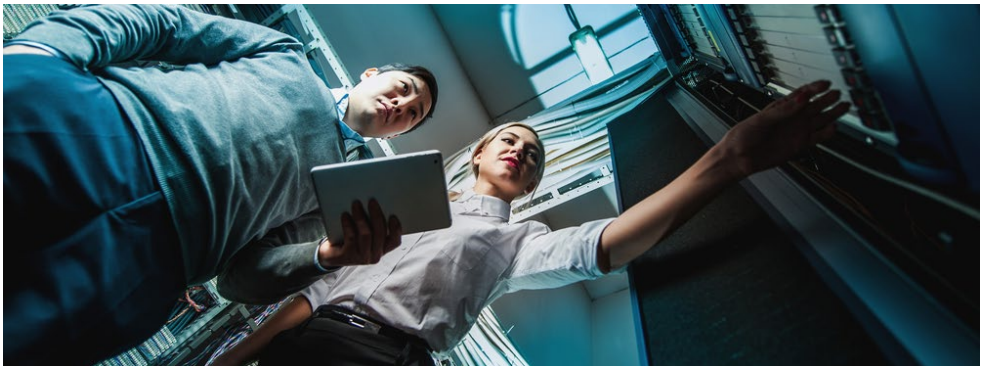
1. **Enforce data protection compliance in your portfolio companies.** Don't let a portfolio company be your fund's weakest link, or that revenue stream will be compromised. Make sure everyone is following your cybersecurity policy and keeps up-to-date with software.

2. **Educate your staff on cybersecurity risks.** Speaking to Financier Worldwide Magazine, Luke Scanlon of Pinsent Masons says that 'mitigating cyber threats is not simply about having the right technology in place.' PE funds need to make sure that everyone in the business - from legal to PR, and finance to front-house - are aware of cyber threats and how to identify, avoid and mitigate them.

3. **Develop a business continuity plan.** Sharon Klein of Pepper Hamilton LLP says that funds 'must maintain plans for resilience and to restore any capabilities or services' affected during a security incident. Having a business continuity and incident response plan is essential for minimising the damage caused by an incident, and will help your fund return to normal operations faster. Our SmartGo programme, part of the EPIC service, includes a 'starter pack' of policies that your team can use and adapt, with a n approval and publishing process attached.

These three things - enforcing compliance across your portfolio, educating your staff, developing continuity and response plans - will help you build compliance, resilience and security into your business.

Engaging the services of an expert IT provider is essential. Some providers, like Doherty Associates, offer packaged IT services that include best-in-class collaboration and productivity tools, a secure IT environment, a subscription to the Microsoft Digital Crimes Unit monitoring system, and 24/7 in-house support. Having access to this kind of support and technology can make a world of difference when managing your security risks.



3. Build scalable, flexible compliance and reporting capabilities

A slew of post-2007 legislative initiatives and regulatory regimes have forced a restructuring of the compliance environment, changing the way PE funds approach transparency and reporting and driving a need for better, more flexible reporting capabilities.

In the US, the Dodd-Frank Wall Street Reform and Consumer Protection Act has come into effect, alongside new Form PF reporting requirements under Title IV. Meanwhile in Europe, governments in France, Sweden and Belgium have pursued legislation to combat 'thin capitalisation' and rewrite tax avoidance rules. In 2010, despite the best efforts of the Brussels Taskforce, the European Commission voted in favour of the Directive on Alternative Investment Funds Managers (AIFM), a new directive designed to prevent hedge funds and private equity from operating 'in a regulatory void outside the scope of supervisors', with increased emphasis on transparency and security.

Private equity funds are facing greater scrutiny at both the national and global level, but not just from legislators and regulators: investors are demanding transparency and information too.

> "As investors across global markets conduct more rigorous due diligence investigations, they are more likely to focus on the same pointed questions as regulators - particularly for issues related to risk management, operations, performance, reporting and valuation.[10]
>
> *-EY 2016 Global Private Equity Fund and Investor Survey*"

Forty-five percent of investors in 2016 are concerned with their fund's reporting capabilities.[11] According to EY, that's a 400 percent increase from the previous year. More and more investors are dissatisfied with the procedures and systems that many PE funds have in place - legacy systems from the pre-GFC era. These systems are incapable of processing and performing the data analysis now required of PE funds.

Invest in analytics and BI tools to improve compliance and reporting

Implementing big data technologies, like Advanced Analytics, can help you meet investor and regulator demands for rich, seamless and transparent data.

With Microsoft Azure in particular, you can store and access your fund's data in the cloud, integrate data from across your portfolio, and leverage modern business intelligence (BI) tools to give your investors and regulators the information they need. These tools make it easier to build **a more resilient and compliant reporting system**, without drowning your analysts and managers in spreadsheets and paperwork.

Technology is the best way to deliver a better experience for your investors, but it will also help you:

- Develop a **cost-effective, enterprise-wide reporting system** that doesn't require excessive manual overhead;
- **Embed compliance** into your reporting processes; and
- Adapt and scale your reporting and compliance systems to **changing regulatory requirements**.

A packaged IT service, like EPIC from Doherty Associates, can further augment your compliance and reporting activities with tools like:

- **Power BI dashboards** that you can use to view your KPIs and data across desktop and mobile devices,
- **Office 365**, which supports advanced security and compliance features to keep your information - and your employees - secure and collaborative
- **Training modules** to help your employees make the most of the technology and tools available to them.

Meeting the ever-evolving requirements of legislators, regulators and investors is a challenge for private equity funds, but technology can help. By investing in cloud technologies, like advanced analytics and BI tools, you'll not only be able to deliver on the demands of today; you'll be able to **build compliance, resilience and security into your reporting processes**, and **scale them to meet the requirements of the future**.

Modern workforce means modern security

Technology has changed the way we work and live, but for PE funds it's more than a tool for improvement: it's a tool for survival.

With the right technology and IT support, you can:

- **Leverage your data** to make better investment decisions, meet reporting requirements and differentiate your firm;
- **Improve your cybersecurity** to protect your investors, safeguard your strategies and avoid hefty fines; and
- **Scale your reporting processes** to meet future regulatory and compliance requirements, while improving your investor's experience.

Implementing digital technologies solves critical business problems that most PE funds face, and it helps to build security into your business. Why does this matter? Because better security means improved compliance and resilience, and it improves your investor's experience as well as your employees'. Technology can drive process improvement across your business but also make lives easier - and more secure.

[1] EY (2016) Global Private Equity Fund and Investor Survey
[2] ibid.
[3] Accenture (2016) Exploring Next Generation Financial Services: The Big Data Revolution
[4] EY (2016) Global Private Equity Fund and Investor Survey
[5] ibid.
[6] ibid.
[7] https://www.ft.com/content/ffed807c-4fa8-11e4-a0a4-00144feab7de
[8] Accenture (2016) Exploring Next Generation Financial Services: The Big Data Revolution
[9] EY (2016) Global Private Equity Fund and Investor Survey
[10] ibid.
[11] ibid.