SS&C | ADVENT

# A Clearer View

## Security, Compliance, and the Cloud

WHITEPAPER

advent.com

For investment management firms considering a cloud-based technology option, security and compliance are important concerns.

## Facing the Fears—Reducing the Risk to Reap the Benefits

By now any investment firm that depends heavily on systems and data has heard the case for the cloud. And it is compelling. No big investment in onsite infrastructure. No physical servers taking up space. Lower your total cost of ownership. Better scalability and workplace flexibility. Reduced risk in the event of a workplace disaster. A cloud-based technology platform can make your firm more agile and responsive, which translates to better client service. It's a clear value-added differentiator in an increasingly competitive business.

Then comes the "Yes, but" part of the conversation: are my systems and data secure? What about regulatory requirements for protection of client data? Am I exposed to operational risk if the system goes down?

These are no small questions in a highly regulated industry that deals with other people's money. Investment managers have a fiduciary duty to protect their clients' assets and confidential information, enshrined in statutes and regulations around the globe.

Further obscuring the picture, regulation and security standards that directly govern the cloud are still evolving. As some observers have pointed out, technology advances at a much faster pace than the legislative bodies seeking to regulate it.

Cloud solution providers need to show they understand their clients' compliance requirements and are addressing them. This document provides an overview of the current state of data protection regulation and the compliance implications for cloud-based solutions. It also explains the security measures that cloud solution providers are adopting—or should be—to help ensure your data is as safe (or even safer) in the cloud as it would be onsite. It aims to provide guidance on what to look for and ask about when talking to cloud providers.

## The Regulatory Climate: Mixed

Concerns about compliance with regulations requiring the protection of confidential client data help explain the investment industry's comparatively slow adoption of cloud services.

In the US, the Federal Gramm-Leach-Bliley Act of 1999 requires firms to notify clients each year about personal information that has been collected—how it is used, with whom it is shared and, most significantly, where it is kept and how it is protected. The rule further requires firms to maintain a written information security plan describing how they intend to protect private client information.

In Europe, the landscape is more complex. The European Union enacted the Data Protection Directive 95/46/EC in 1995, which applies data protection regulation broadly to all types of commerce, not just financial services. In addition, the individual member states of the European Union also have various data protection laws and regulations covering their own citizens' personal data.

Global cloud service providers need to be able to adapt to the regulatory requirements of any jurisdiction in which they offer service.

In 2012, the EU initiated a reform process aimed at updating the Directive and eliminating inconsistencies in its application among various member states. A new pan-European regulatory regime specific to the cloud is expected by 2016. Among the provisions under consideration are standardized cloud computing contracts clearly spelling out service providers' legal obligations and EU-wide certification of approved providers. The onus will be on cloud services users to determine whether their providers have implemented sufficient security measures to ensure the protection of personal data.

Part of what makes the cloud work is the flexibility of providers to move data and processing from one data center to another, sometimes across national borders, in order to help manage traffic and processing capacity, and improve scalability. It also provides data replication and resilience to support business continuity and disaster recovery. This complex infrastructure is often invisible to the end user. In a world where business and financial markets transcend jurisdictional boundaries, a trend accelerated by the Internet, global cloud service providers need to be able to adapt to the regulatory requirements of any jurisdiction in which they offer service.

## Generally Accepted Industry Practices and Certifications

Generally accepted practices in cloud security and reliability have begun to coalesce, along with well-defined certification frameworks addressing both vulnerability and operational risks. Top-tier cloud data center providers are taking a variety of measures to assure users that their information is safe and their businesses are protected, including:

- Physical security and tightly restricted access
- Surveillance cameras
- Limited onsite personnel
- Background checks on staff
- Strict authentication measures for entry
- Backup power generators
- Data replication and redundancy

Within the cloud infrastructure, the web hosting providers and network carriers provide robust security functionality that includes firewalls and intrusion detection, as well as techniques such as limiting open ports and requiring secure transport protocols where feasible.

On top of the measures taken by the cloud infrastructure provider, your solution provider should be adding its own layers of security, including hard isolation, strong encryption of data, and secure sockets layer (SSL) communication to ensure your data is protected in transit. Your provider should also take technical and procedural steps to secure your data against anticipated threats and hazards, including obtaining a security and controls assessment such as the SOC-1/SSAE 16 (The Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization developed by the American Institute of Certified Public Accountants).

## "Give Me a Private Cloud"

Early in the cloud conversation, the question usually arises about public versus private cloud computing. Upon hearing the distinction, many firms' initial inclination is that private may be preferable. In a private cloud arrangement, you do not share computing resources or infrastructure with other users. You're the only one using it and it runs on your own private network. Your data may be off premise but it's within your business firewall. This, some may argue, means optimal security and control over access. On the other hand, you purchase the infrastructure and software and pay for the maintenance. Those costs will likely reduce the ROI that makes the cloud proposition so compelling.

On top of the measures taken by the cloud infrastructure provider, your solution provider should be adding its own layers of security.

In the public cloud, multiple users access computing services and data via the Internet. The sharing of resources and infrastructure among several users enables efficiencies and economies of scale not possible in a private cloud setup. Meanwhile, your data and activity can remain separate from the public.

No system, whether in the public cloud, private cloud, or locally installed, can guarantee 100% invulnerability. Onsite system installations with connections to the outside world and exchanging data over a network are no less vulnerable to hacking. That is why large institutions employ comprehensive security countermeasures to detect and block intrusions. It's why software developers build safeguards into their systems and test them rigorously. There is no reason such measures can't be replicated in a cloud computing environment—which is precisely what the more advanced providers are doing.

A firm may have compelling business, legal, or regulatory reasons for insisting on the private cloud. In that case, be mindful of the future costs. Understand that your service provider will likely need privileged access to your data and systems in order to perform the services you have contracted. Before you commit, it's helpful to talk to a provider who supports both the public and private options, as well as a hybrid option, which employs a private platform for certain functions and public for others.

## A Safer Place for Your Data

While the cloud may still have an aura of novelty, it is simply another form of technology and operational outsourcing, which has been with us in various forms for some time. As such, the rules governing technology outsourcing for financial firms apply to the cloud too. Users are required to do their due diligence and make sure the provider has adequate security and service reliability measures in place. Outsourcing contracts and service level agreements spell out the provider's obligations.

To read some forecasts, it won't be long before cloud computing becomes the mainstream and locally installed systems the exception. For technology providers and users alike, the economic benefits, ease of deployment, and operational efficiencies are too compelling to ignore. However, security and compliance issues are by no means trivial. Cloud service providers must be able to demonstrate that they have taken the necessary measures to help protect you and your clients from a data breach or system failure. You should feel confident that you are in compliance with your fiduciary and regulatory responsibilities. More to the point, you should have peace of mind in taking advantage of the cost savings and efficiencies the cloud promises. A provider who understands your compliance requirements and has taken the measures to meet them makes that possible.