
Will the Cloud Change Your Risk Forecast?
Understanding Regulator Expectations for Outsourcing to the Cloud
LexisNexis®

"IT IS IMPORTANT TO NOTE THAT WHERE A THIRD PARTY DELIVERS SERVICES ON BEHALF OF A REGULATED FIRM— INCLUDING A CLOUD PROVIDER— **THIS IS CONSIDERED OUTSOURCING** AND FIRMS NEED TO CONSIDER THE RELEVANT REGULATORY OBLIGATIONS AND HOW THEY COMPLY WITH THEM."

Financial Conduct Authority
FG 16/5 - Guidance for firms outsourcing to the 'cloud' and other third-party IT services
July 2016[1]

OUTSOURCING IN A VIRTUAL WORLD

The cloud has transformed how many companies conduct business—and for good reasons. Moving applications, processes and data to the cloud lowers IT management and maintenance costs, improves work efficiency, supports more resilient operations and fuels company growth. The potential benefits have accelerated cloud adoption in recent years. London-based IT consultancy Ovum reported in its global cloud adoption forecast that more than 80 percent of large enterprises currently use or plan to use public, private or managed hybrid (public/private) cloud services.[2]

But companies in highly regulated industries—Banking, Financial Services and Healthcare, for example—have lagged in cloud adoption. The reason? These types of companies need to consider data security—not just to protect the privacy of their customers or avoid the negative media attention that accompanies a data breach, but to mitigate the risk of regulator investigations, fines and penalties related to non-compliance.

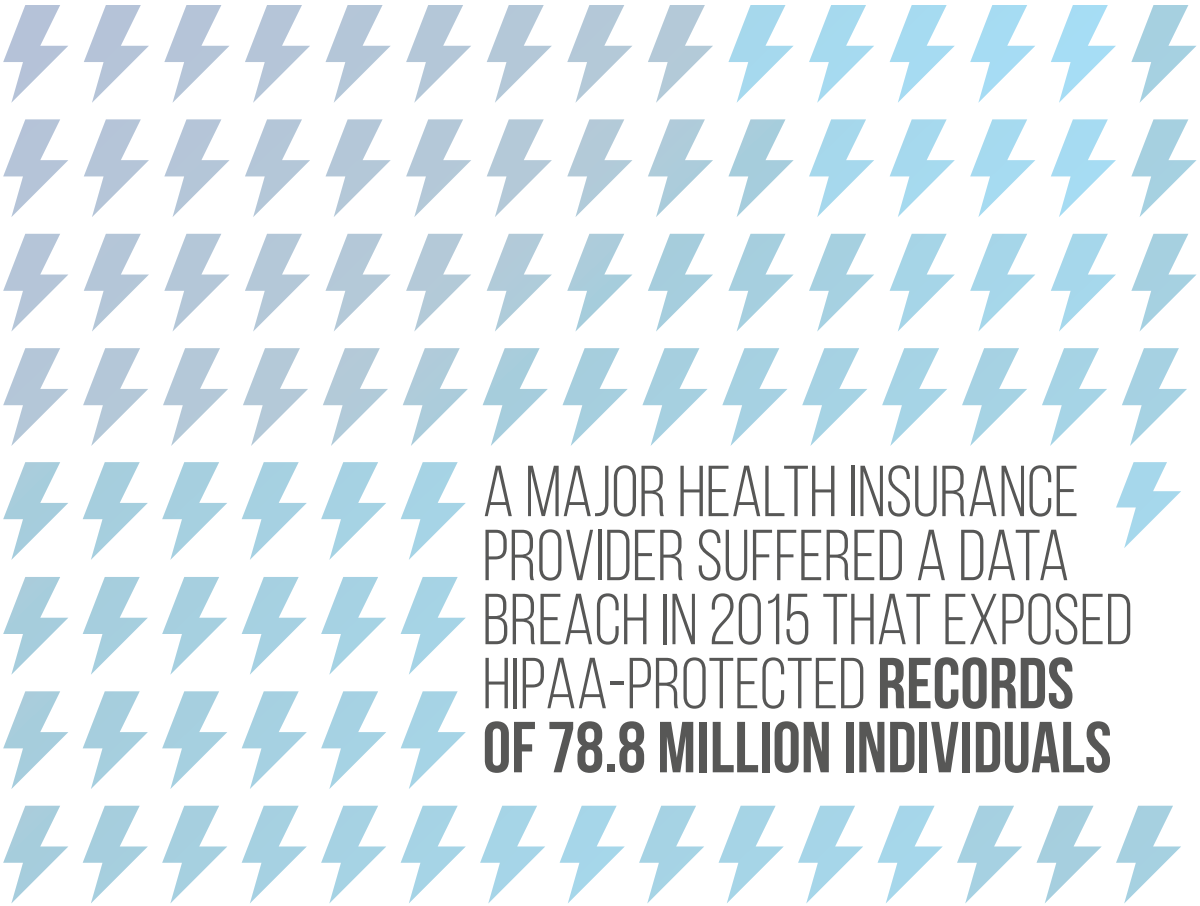
> "BY 2020, A CORPORATE "NO-CLOUD" POLICY WILL BE AS RARE AS A "NO-INTERNET" POLICY IS TODAY. CLOUD-FIRST, AND EVEN CLOUD-ONLY, IS REPLACING THE DEFENSIVE NO-CLOUD STANCE THAT DOMINATED MANY LARGE PROVIDERS IN RECENT YEARS."
>
> Gartner, Inc.
> June 22, 2016 Press Release

THE DARK SIDE OF THE CLOUD

Companies in highly-regulated industries have good reasons for a cautious approach. In addition to typical regulatory considerations, a spate of high-profile hacks and data breaches caused many organizations to re-think their go-to-cloud strategy. In the U.S., for example, a major health insurance provider suffered a data breach in 2015 that exposed Health Insurance Portability and Accountability Act (HIPAA) protected records of 78.8 million individuals, and in 2016 organizations within the U.S. healthcare sector experienced 377 data breaches.[3] The financial service industry in the UK has also been susceptible, experiencing a 183 percent increase in data breaches since 2013.[4] Moreover, a lack of transparency into where cloud data resides—especially in Europe which has strict geographic data privacy requirements—made maintaining data centers in a single location more appealing.

Fortunately, cloud providers are stepping up to address these issues. Enhanced data security is a new selling point because, as former CIO of the U.S. federal government Vivek Kundra notes, "Cloud computing is often far more secure than traditional computing, because companies like Google and Amazon can attract and retain cyber-security personnel of a higher quality than many governmental agencies."[5] Meanwhile, international cloud service providers recognize the geographic restrictions and have used data routing control as a valuable differentiator in recruiting regulated companies as customers.

More confidence in the technology, along with the lure of efficiencies and cost-savings, have resulted in cloud use within regulated industries growing by 71 percent or more. And based on recent guidance from the UK's Financial Conduct Authority (FCA), the pace of adoption will likely quicken. What do compliance professionals need to know to mitigate risk as they make the shift to the cloud?



A MAJOR HEALTH INSURANCE PROVIDER SUFFERED A DATA BREACH IN 2015 THAT EXPOSED HIPAA-PROTECTED **RECORDS OF 78.8 MILLION INDIVIDUALS**

IN 2016 ORGANIZATIONS WITHIN THE U.S. HEALTHCARE SECTOR EXPERIENCED **377 DATA BREACHES**

THE UK FINANCIAL SERVICE INDUSTRY HAS ALSO BEEN SUSCEPTIBLE, EXPERIENCING A **183 PERCENT INCREASE IN DATA BREACHES** SINCE 2013

OFFICIAL GUIDANCE SEES THE CLOUD'S SILVER LINING

When the Financial Conduct Authority (FCA) published its guidance, it acknowledged, "Using the cloud can provide more flexibility to the service that firms receive, enabling innovation and bringing benefits to firms, their consumers, and the wider market." It then added a caveat: "However it can also introduce risks that need to be identified, monitored and mitigated." This perspective on cloud benefits and risks is not unique to the FCA. Regulatory agencies in countries across the globe are developing new standards for outsourcing of IT services.

Current guidance identifies a range of considerations in leveraging cloud-based solutions.

LEGAL AND REGULATORY

As with any third-party provider, companies have a responsibility to:

- Clearly document the business case for moving to the cloud
- Consider relevant legal or regulatory obligations
- Conduct adequate due diligence to ensure an outsourcing agreement does not elevate risk
- Evaluate how the geographic location of the cloud service provider may expose the company to additional regulatory requirements
- Identify all service providers in the supply chain when services are related to a regulated activity

SERVICE PROVIDER OVERSIGHT

Like requirements for other third-party relationships, companies must adhere to accountability standards under the regulatory system as well.

- Assign responsibility for day-to-day and strategic management of the cloud service provider
- Clarify "where responsibility and accountability between the firm and its service provider begins and ends"
- Empower internal staff to oversee and test outsourced activities to proactively manage risk

> "WE CONSIDER IT AN IMPORTANT PART OF A FIRMS' OVERSIGHT OF THEIR PROVIDER TO HAVE SUFFICIENT IN-HOUSE ABILITY TO SUPERVISE THEIR OUTSOURCING ARRANGEMENTS, AND TO TAKE CONTROL OF THE RELEVANT FUNCTIONS IF THINGS GO WRONG."

Financial Conduct Authority
FG 16/5 - Guidance for firms outsourcing to the 'cloud' and other third-party IT services
July 2016[8]

DATA SECURITY AND MAINTENANCE

In highly-regulated industries, meeting data protection and privacy standards represents a major compliance requirement. As such, guidance recommends that companies:

- Ensure data loss and breach notification processes align with regulatory obligations
- Set a data residency policy with the provider outlining jurisdictions where data can be stored, processed or managed
- Avoid potential data residency jurisdictions that inhibit access for UK regulators or jeopardize data security due to political instability
- Implement secure data encryption for sensitive data
- Specify auditors or regulatory bodies have encryption keys and access to data as required
- Follow DPA and ICO guidance as it relates to data

RISK MANAGEMENT

The FCA guidance also specifies that risk management is "a fundamental principle of the rules and guidance on outsourcing," and suggests companies:

- Undertake a risk assessment and create a risk mitigation plan
- Maintain an audit trail of due diligence and risk assessments
- Identify and implement industry best practices
- Require prompt, detailed notification of breaches or other relevant compliance risk events
- Ensure contracts address remediation of such risk events

REGULATORY AGENCIES WORLDWIDE RECOGNISE THE VALUE OF THE CLOUD

The FCA guidance acknowledges that companies face an array of international standards related to outsourcing of IT services. In Asia, for example, the rise in outsourcing has led to "rapid expansion in recent years of comprehensive 'European style" data privacy regulations.[9] In the U.S. the Federal Financial Institutions Examination Council indicated that it views use of public cloud services the same as other IT outsourcing, urging caution while acknowledging that moving to the cloud is inevitable. Meanwhile, the EU's cybersecurity agency has specifically identified the public cloud as distinctly higher risk.

In view of these evolving views, companies in highly-regulated industries can begin to realize the advantages of the cloud—if they have appropriate risk mitigation strategies in place. In addition to third-party screenings, risk assessments and due diligence, companies need to maintain a thorough audit trail of these efforts and conduct ongoing monitoring to address regulator expectations.

1. https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
2. http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/#60dd4c91740c
3. http://www.modernhealthcare.com/article/20170121/MAGAZINE/301219987/data-points-healthcare-data-breaches
4. http://www.computerweekly.com/news/4500247427/Financial-sector-data-protection-breaches-up-183-in-past-two-years
5. http://www.cloudcredential.org/
6. http://www.cio.com/article/3015377/cloud-computing/cloud-adoption-soars-in-regulated-industries.html
7. https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
8. https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
9. http://www.hoganlovells.com/files/Uploads/Documents/Outsourcing__Technology_Procurement_and_Cloud_in_Asia__the_Legal_and_Regulatory_Essentials.pdf

"IN THE U.S. THE FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL INDICATED THAT IT VIEWS USE OF PUBLIC CLOUD SERVICES **THE SAME AS OTHER IT OUTSOURCING**."

Federal Financial Institutions Examination Council

ABOUT LEXISNEXIS®

We help our customers mitigate business risks, meet their strategic goals and accomplish greater return on investment. Using our efficient, agile and cost-effective due diligence and monitoring solutions empowers our customers to find the information they need on people, companies and countries. Our experienced industry specialists and thought leaders are well-versed in the evolving requirements our customers need to address.

LexisNexis Business Insight Solutions delivers interconnected and flexible product modules aligned to the customer workflow including:

- PEP, watch list and negative news screening
- Enhanced due diligence and reporting
- Proactive supply-chain and third-party risk media monitoring that leverages PESTLE-based risk scoring
- Outsourced due diligence, compliance and risk advisory
- Content integration and data feeds into proprietary systems

Ask how we can support an efficient due diligence and monitoring strategy that mitigates the third-party risks you face—on the ground or in the cloud.

For more information

lexisnexis.de/compliance

kontakt@lexisnexis.de

+49(0)211 417435-40

LexisNexis®