The Flip Sides of Data – A Strategic Asset and a Potential Risk

Data. In everyday life we are constantly consuming it. On a conscious level, we are trying to make use of that information for the task at hand, discounting the inessential and focusing on the essential. In business, the collection, storage, and use of data follows the same principles. An approach which aims to harness data and technology in perfect harmony.

Large volumes of data are valuable. But as data volumes, processing and consumption demands continue to rise exponentially, businesses that manage data are exposed to a host of challenges such as rising operating costs, the potential of temporary (downtime) and permanent data loss, data theft, increasing regulation, and sustainability concerns.

Firms such as asset managers, insurers, and banks, along with regulators, must therefore consider these 'flip sides' and continuously determine how to overcome these challenges, whilst making the best use of their data.

Data storage, governance, and resilience

What is commonly referred to as 'Big Data' involves a massive volume of information that exceeds the capacity of traditional data management tools. It makes it hard, or even impossible, to process and analyse effectively using conventional means.

It also demonstrates significant variety, as the data comes in different formats, via different means and from various sources. It encompasses a wide variety of data types, including structured data, such as dates, phone numbers, and sensor readings which are defined and searchable, and unstructured data, such as images, videos, broadcast media, social media interactions, and more. All such data used by firms must be consumed and categorised and is frequently stored in a data lake.[1]

Once stored, data must also be readily available, of high quality and relevant. Given that data acts as a foundation for application programming interfaces (APIs), robotic process automation, machine learning, and artificial intelligence (AI), it is essential that thorough governance processes are in place to check that data is accurate, comprehensive, has been sourced legitimately, and is protected.

It should therefore come as no surprise that with the increase in data being stored, the potential misuse or abuse of that data has also increased, resulting in legislators around the world regulating the storage, protection, and use of data.

Potential risks inherent in data storage and risk mitigants

According to a recent report from Verizon[2], large-scale data losses (100 million-plus records) are estimated to cost an organization anything between USD5 million and USD15.6 million, highlighting that data protection is key.

There are various forms of storage for data 'assets', with the one most frequently referenced being cloud storage. This combines the benefits of flexibility, reliability, increased performance, and efficiency, and helps to lower information and communications technology (ICT) costs compared to in-house solutions.

Cloud storage is suitable for storing all forms of electronic data and offers features like data scalability and data accessibility and allows users to rent out space on a virtual server that is dedicated solely to their use.

Whilst the benefits of cloud storage may include affordable pricing, access to massive storage, and remote accessibility, cloud data is also subject to potential risks that need to be controlled for a firm to maintain robust governance arrangements. Risk outcomes relating to poor data management can include, but are not limited to:

- **Cybercrime:** In the UK, for example, the National Cyber Security Centre provides some high-level principles for firms, the most relevant in this scenario being 'Principle 2: Asset protection and resilience'. This states that your data (and the assets storing or processing it) should be adequately protected by considering physical location and legal jurisdiction, data centre security, data encryption, data sanitisation and equipment disposal and physical resilience and availability.
- **System failure:** A situation where a computer system or network is unable to perform its intended functions or experiences a significant disruption in its operation.
- **Data corruption:** Errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data. Unlike simple data loss, corrupted data maintains its presence within the system but in a degraded, incorrect, or unusable form.
- **Insufficient backup and recovery:** The process of backing up your data in the event of a loss and setting up secure systems that allow you to recover your data as a result. Data backup requires the copying and archiving of computer data to make it accessible in case of data corruption or deletion. You can only recover data from an earlier time if you have backed it up with a reliable backup device.

  Data backup is one form of disaster recovery, making it an essential part of any sensible disaster data recovery plan.
- **Misconfigured permissions and access controls:** These can occur when security settings are not adequately defined in the configuration process or maintained and deployed with default settings. They could impact any layer of the application stack, cloud, or network.
- **Data expiration and retention policy violations:** The data set expiration date or retention period is determined when a new tape data set is created. The expiration date or retention period can be specified at multiple levels and will then usually be included in a firm's retention policy.
- **Natural disasters:** Such as fires, floods, earthquakes, and resulting power outages.
- **Human error:** Can stem from negligent actions or lapses in judgment by employees. Examples include the mishandling of sensitive information, such as inadvertently sharing confidential data with unauthorized parties, or falling victim to phishing scams.
- **API Vulnerabilities:** These refer to the potential weaknesses or gaps in an API's security that could be exploited by a malicious actor. These vulnerabilities can be present in any part of the API, from the design phase to the deployment stage. They can result in severe consequences, such as data breaches, unauthorized access, and even system crashes.
- **Data litigation:** This is on the rise and the exposures can potentially be significant.
- **Coding errors:** ICT needs code (software) to operate, which can sometimes include mistakes. Undetected coding errors can result in system crashes, in turn resulting in loss of access to data, loss of operability, and ultimately loss of reputation and business.

Risk mitigants for cloud and on-premises storage
When a cloud storage solution is provided by a vendor, some of the above risks shift to the cloud provider. So, a vital risk mitigant is ensuring that you backup your data, even when storage is outsourced.

Consider asking yourself and your data storage providers the following questions: How is my data backed-up? Will your liability insurance cover you in the event of data loss? And will it still be covered if that data was not securely backed up?

How far is the data backed-up, is there a time limit on retrieval, and if my data does get encrypted by a virus, can I get the data back?

Other questions you might want to ask... what if my cloud services company decides to discontinue its offering? What happens if my cloud service, or other type of provider experiences a crash, or even creates a crash in my own system?

You may have thought the above issues unlikely but there have been some examples over the last couple of years.

Errors like this expose how fragile advanced security systems (designed to protect against cyber-attacks) and IT interdependencies, such as a widespread reliance upon a limited number of providers, can be in practice given the wrong combination of events.

Of course, the same risks listed above also apply to traditional on-premises storage methods, but there is a significant difference between how these risks need to be managed.

When an on-premises data storage solution is built, the same risk mitigating actions and capabilities also need to be maintained and developed in-house.

For cloud storage provided by a third-party vendor, some of the risks shift to the provider. Since an external provider offers those functions at a larger scale, they may be expected to do it better than someone utilizing in-house capabilities. But where that is the case, it requires an even more robust vendor oversight capability to ensure that a firm can oversee the cloud providers' capabilities at the required levels.

Other risks remain the same, regardless of whether data is stored on premises, or on the cloud. For example, risks such as user error and data retention policy violations remain for a firm sourcing the data. When an outsourced model is utilized, a piece of the risk mitigation solution is knowing who in the relationship is taking primary responsibility for the potential risks, requiring the right balance of internal ownership and robust oversight.

A particularly relevant consideration for global firms sourcing data from all over the world is the fact that some jurisdictions require data to be stored in country. Firms sourcing such data, are not allowed to move it, so a hybrid model solution, mostly based on public cloud, but also allowing local on-premises storage, could be a solution. One where data can seamlessly and automatically end up in the 'right' storage container and then be delivered to the end owner of the data in a way which is invisible and seamless.

Regulation

Data Protection
Fundamentally, data must not have been obtained in contravention of local data laws, for example the European General Data Protection Regulation (EU GDPR) and a whole tranche of similar data handling and storage laws across the globe.

Many firms are looking at how they can use the data they hold to debut or build on their AI programs. For example, looking to use that data to train AI models, or fine-tune third-party models. That data will almost certainly include personal data, meaning that the processing must comply with the General Data Protection Regulations in the EU, UK or elsewhere, depending on the specific nature of the data being stored.

The EU GDPR provides mandatory rules on how organizations and companies must use personal data in an integrity friendly way, further providing for provisions on data protection principles, accountability, data security, when you are allowed to process data, and obtaining consent etc.

Amongst other data protection obligations, firms are also expected to understand exactly where its data is stored – that is where data applications are physically located – 'data sovereignty'.[3] Data sovereignty means that regulators in specific countries have placed restrictions on where your data can be stored.

It's important to be aware of this as data can be moved around by your cloud provider in search of their own efficiencies and cost optimisation. So, a firm must factor in data sovereignty, localisation, and residency requirements in each country where its data resides. Currently, there are 7,716 data centres from 147 countries worldwide.[4]

Given the rapid advancement of AI technologies, this raises questions regarding data privacy, transparency, and accountability. The Belgian Data Protection Authority has just published a brochure entitled "Artificial Intelligence Systems and the GDPR - A Data Protection Perspective" to explain the GDPR requirements specifically applicable to the development and deployment of AI systems.

Whilst the EU GDPR provides a robust framework for protecting personal data within the EU. Concurrently, the EU AI Act, which came into effect on 1 August 2024 introduces additional provisions specifically addressing the complexities associated with high-risk AI systems. (To learn more about the EU AI Act see our article 'Doing the Right Thing for Business and Society – Gen AI').

There are several GDPR principles that are critical to the processing of personal data within AI systems:

- Lawfulness;
- Fairness;
- Transparency;
- Purpose limitation and data minimisation;
- Data accuracy and being up-to-date;
- Storage limitation;
- Automated decision-making;
- Security of processing;
- Data subject rights; and
- Accountability.

Other recent developments regarding data governance regulation include:

- 9 August 2024, when the European Commission announced the launch of a public consultation to gather feedback for its upcoming report on the first review of the EU-US Data Privacy Framework (DPF). The DPF allows free flows of personal data from the EU to participating companies in the US. This review, mandated by the adequacy decision adopted in July 2023, is intended to assess the effectiveness and proper implementation of the DPF.
- 27 August 2024, the European Union and China officially launched discussions under the new Cross-Border Data Flow Communication Mechanism. This mechanism aims to address the challenges European companies face with cross-border transfers of non-personal data in China. Further expert-level engagements are planned to assess progress and enhance cooperation.

Operational resilience for on premise and cloud-hosted IT infrastructures

The Digital Operational Resilience Act (DORA) is a European Union regulation that comes into effect on 17 January 2025. It is intended to provide guidance to the financial sector to help address concerns around cyber resilience, both for on premise and cloud-hosted IT infrastructure. DORA applies to financial entities operating in the EU, including banks, investment firms, credit institutions and more. It also applies to third-party ICT providers such as cloud service providers.

As it regards data, in-scope entities must establish systems for monitoring, managing, logging, classifying, and reporting ICT-related incidents. Depending on the severity of the incident, entities may need to make reports to both regulators and affected clients and partners. Entities will be required to file three different kinds of reports for critical incidents: an initial report notifying authorities, an intermediate report on progress toward resolving the incident, and a final report analysing the root causes of the incident.

There must also be policies and procedures explaining which data will be backed up, how often, and the restoration methods for the backups. Further, backup data must use ICT systems that are physically and logistically segregated from the source ICT system, which may require firms to put in place new contracts with their ICT service providers.

In its recent Supervisory Newsletter, the European Central Bank highlighted the jump in the number of outsourcing contracts as banks have increased their reliance on non-EU providers for IT-related services. Banks' management of outsourcing risks and compliance with regulatory requirements will remain a key area of focus, particularly as it regards the approaching application date for DORA.

Regulators also have expectations regarding the use of critical third parties – which can include outsourced data providers.

Whilst in the UK, the Bank of England, and the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) also hold firms and Financial Market Infrastructure (FMIs) firms accountable for their operational resilience, regardless of whether, or not, they rely on third parties to support the delivery of their important business services. This is particularly the case when those third parties designated as 'critical third parties' (CTPs) by HM Treasury, could create systemic harm.

As such there are proposals for CTPs to have their own building blocks such as: minimum resilience standards to develop and test 'financial sector continuity playbooks' to improve their own ability to respond and recover from disruption affecting multiple firms and FMIs simultaneously. Plus, a range of tools for testing the resilience of material services that CTPs provide to firms and FMIs – tools such as scenario testing, participation in sector-wide exercises, cyber resilience testing and skilled person's reviews of CTPs.

On 12 November 2024, the PRA, FCA and Bank of England published a joint package establishing the UK's CTP oversight regime. The package includes: a joint policy statement (PRA PS16/24 – FCA PS 24/16[5]) detailing the final rules for CTPs; a document detailing the PRA and FCA approach to the oversight of CTPs[6]; supervisory statement SS6/24 setting out the regulator's expectations of how a CTP should comply with the duties and obligations placed on it by the regulations[7]; and supervisory statement SS7/24 detailing the PRA and Bank of England's policy on the use of skilled persons as part of their supervisory responsibilities.[8]

In terms of next steps, HM Treasury is currently in the process of compiling the schedule of CTPs.

US regulators are also considering their own IT resilience legislation as, in Europe, the EU gears up for DORA implementation in January 2025, and Network Information Security (NIS 2) Directive, which is already in force.

> "Fund accounting data deliveries have been based on pushing pre-defined data sets to end recipients. With the advent of data sharing capabilities, we see a wholesale shift in this model with more agile delivery changing our clients' relationship with our data. While firms like Citi sees this as an opportunity to build our relationship with our clients, it is different for specialists supporting historical data delivery. For them, this change will have implications on the relevance of their business models."
>
> Tim Roderick, Global Head of Fund Accounting, Citi Securities Services.

Approach to data and governance

Data governance is the foundation for all products and services and is a true driver for business improvement, growth, and the development of new offerings. Having a high standard for data is also a differentiator for current and potential clients who have increasing optionality with respect to data providers. Regulatory scrutiny on the quality of data that supports key business processes, risk management and regulatory/financial disclosures has also increased exponentially in recent years.

The key drivers for data governance include:

- **Client Enablement** - Equipping clients with the knowledge, tools and resources required to get the most out of their providers.
- **Business Enablement** - Effectively utilising people, processes, and technology to aid business success.
- **Regulatory Compliance** - Anticipating and meeting any regulatory requirements such as the Basel Committee on Banking Supervision's standard 239. (BCBS 239). The subject title of this standard being 'principles for effective risk data aggregation and risk reporting'.
- **Operational Resilience/Risk Management** - The ability to avoid or adapt to adverse scenarios and to mitigate risk.
- **Technology Enablement** - Strategic use of technology (e.g., AI) and tooling to increase operational efficiency and meet business outcomes.

Data Governance can be a central utility, supported by the following pillars:

1. Data as an Asset.
2. Data Ownership.
3. Data Cataloguing.
4. Data Quality Monitoring and Remediation.
5. Data Right-Sourcing.

Data as an Asset, one that has intrinsic value from both a risk standpoint and the client-side. Clients are increasingly expecting data to be centralized as part of a standard offering and expect the data they use (e.g., master and reference data types such as securities (ISINs, CUSIPs, SEDOLs), pricing, events, etc.) to be normalized yet provided at desired levels of granularity. They also want data that can be seamlessly integrated into their operational procedures.

Data Ownership ensures accountability for data is embedded within an organization's culture – meaning that everyone is a data manager. Here roles can be codified to ensure data is sponsored within each business line/sub-business line; owned across operations teams; and stewarded across the technology organization. Combined, data is overseen by subject matter experts who know their clients' needs; practitioners with a ground-level understanding of product processes and technologists with a constant view of architectural best-practices and a firm's target state.

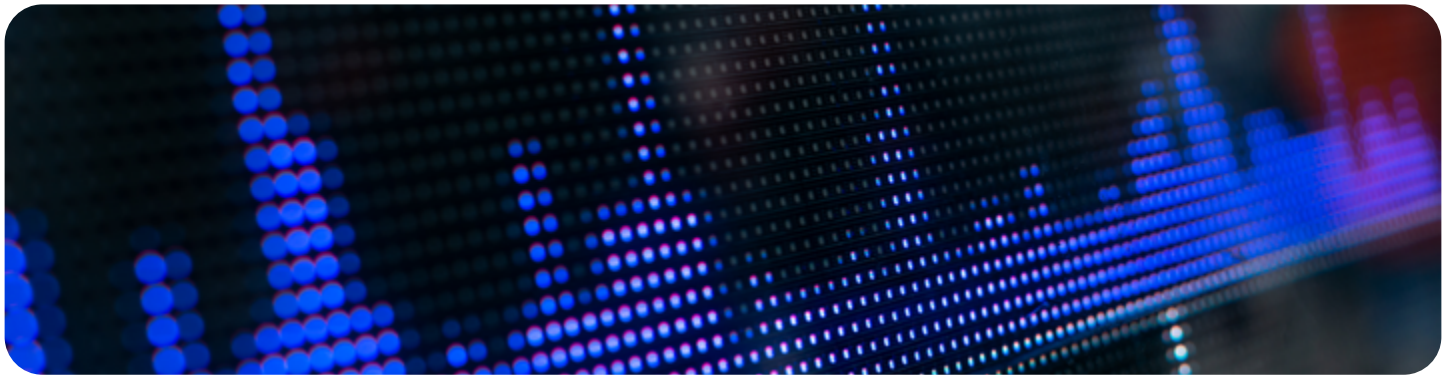
Data Cataloguing provides a consistent way of defining data in a language that both business and clients understand. Data rests and travels, and on this journey can be produced, consumed, transformed, and demised. Throughout, it's important that data doesn't lose meaning so that it can be defined correctly wherever it resides.

Data Quality Monitoring and Remediation defines rules at both a business and technical level e.g., for Timeliness, Accuracy and Completeness. These rules are executed in a way that enables breaches in standards to be quickly identified, routed to the correct owners, and managed through to remediation. This underpins the concept of producer-consumer agreements allowing data quality handshakes to occur at every "hop" enroute to its ultimate destination.

Data Right-Sourcing provides accuracy of data by certifying systems of record and redistributors of data concepts. Today firms can operate in a complex, multi-data-vendor environment, also curating internal master and reference datasets. Therefore, it is vital for firms to adopt a principle of "source once, publish many". Whether it's securities, pricing, corporate events, legal entities, client identifiers, or even geography and holiday data, all consumers of data must adopt the designated standard for that dataset.

There are also other ancillary data services which could fall into a firm's overall data governance framework such as data lineage, data architecture design, cross-border compliance, and data privacy. These pillars should not exist in silos but instead be brought together to drive a holistic data governance operation that permeates the data lifecycle. It's also vital that data governance processes have a "feedback loop" connecting data with business as usual and change management processes e.g., implementing data controls during agile/waterfall[9] development ensures "good data by design" when it finally emerges into a production environment.

If the above represents the pillars of the data governance house, data management tooling represents the foundation. Firms could utilize a toolkit driving data responsibilities directly to Data Owners via workflow in a way that democratizes data fix. Firms' may also consider leveraging AI for preventative data quality monitoring e.g., pattern-matching and stochastic analysis. Ultimately, all of this can come together via a suite of executive dashboards that enables clients, management, and practitioners to keep their fingers on the pulse of the data that they're interested in.



"Whether developing new business products, enhancing operational efficiency, or making the most out of AI-driven solutions, no longer is data governance a secondary consideration. Data hygiene is a primary management metric within Citi Securities Services and is a differentiator to winning business."

Randeep Buttar, Global Head of Data Governance for Citi Securities Services

Data for supervisory use

For many years, regulators have been improving regulatory activities by using advanced data analysis techniques, helping them to identify where intervention is needed. They have been able to do this, given the increased availability of data informing their analysis. For years, firms have been required to provide increasing regulatory reports.

Of note, the European Securities and Markets Authority (ESMA) Data Strategy 2023-2028 provides comprehensive details on how ESMA intends to further scale up its own data capabilities. For example, in relation to:

- Recently established supervisory mandates on critical benchmark administrator's, EU Data Reporting Service Providers and Tier 2 Central Counterparties.
- New regulatory work on Digital Finance e.g., DORA, the Markets in Crypto-Assets Regulation (MiCA), the DLT Pilot Regime and sustainable finance in relation to the Corporate Sustainability Reporting Directive (CSRD) and the Sustainable Finance Disclosure Regulation (SFDR).
- And further progress on the Capital Markets Union Agenda, including the establishment of a European Single Access Point (ESAP).

The ESMA Data Strategy includes details around the possibilities created and challenges posed by the rapid growth of new technologies suited for supervision, reporting, data collection or data use, and fast evolving digital developments in areas such as Cybersecurity, Big Data, DLT, AI, Regulatory Technology and Supervisory Technology.

ESMA's objectives can be summarised as:

ESMA has already started to scale up on its data capabilities and the implementation of some of its first planned deliverables. This plan will however be revisited over time as new legislative, technological developments emerge.

Also in Europe, the EIOPA Strategy 2023-2026 has a strategic priority stating that data is at the heart of the insurance and pension sectors, and the backbone of the digital transition. EIOPA therefore is also aiming to enhance data availability and data standardization, contributing to the development of a sound European Data Eco-System.

How do asset managers and insurers utilise data?

Role of data science in asset management

One aspect of data science is an ability to uncover hidden patterns in data. It can be used by asset managers in optimising investment strategies or allocations and portfolio management, enabling investment professionals to gain a better understanding of market trends, identification of patterns and making more accurate predictions. It can also be used for risk management.

The increasing use of alternative data sources (e.g., social media sentiment analysis, satellite imagery, sensor data, etc.) can also be used to gain unique insights and generate alpha.

Of course, using data in these ways also comes with its own challenges, such as the availability (or lack thereof) and quality of the data, and a need for skilled data science professionals.

> Linked to the trend analysis point, asset managers are thirsty for relevant, complete, timely and accurate data. Moving away from any constraints and the guardrails present with traditional file or message-based reporting, asset managers want direct access to the underlying data.
>
> Chris Nunn, Global Head of Middle Office, Citi Securities Services.

The role data plays for insurers

As more insurance customers have moved online to interact with firms and compare products and process, the volume of data has increased.

With all the new technology available today, this data can be used in different ways which benefits customers. For example, your insurance company may ask to install sensors in your house which can detect gas or water leaks to minimize any damage caused to your home, or a young driver could install a Blackbox in their car or install an app to reduce their car insurance premium. Even wearable technology – creating a more accurate picture of health risks.

The Internet of Things has also helped create products which focus on prevention or situational insurance, for example, a sensor will be able to monitor a household's water consumption patterns, detecting potential leaks and interrupting the flow before the basement is flooded. This can prevent major damage and a potentially costly claim.

For insurers, the use of data analytics can be seen in areas such as marketing and distribution, underwriting and claims and the identification of new opportunities such as enhancing or completely changing business models, strengthening customer engagement and relationships, redesigning products, customer acquisition and personalisation as well as improving regulatory compliance.

Data can also be used to work out how much a customer's premium should be and the probability of an event happening.

Sustainability considerations relating to data and AI's carbon footprint and greenhouse gas emissions

The datasets used to train AI are becoming increasingly large and take an enormous amount of energy to run. So, the technologies impact on the planet is something that big tech companies are increasingly taking into consideration. They are investing heavily in AI-driven services that rely on continuous data analysis, which translates to an exponential increase in power requirements. As a result, such companies are exploring innovative energy solutions because rising demand for electricity from data centers to power AI technology has created a need for clean and sustainable sources of energy such as solar, wind, and nuclear power.

The same is true for regulators. For example, the recast Energy Efficiency Directive has recently implemented reporting obligations for EU data centre operators to report certain information and KPIs regarding their data centres with the intention of providing this to the public and European Commission.

The European Commission states that with data centres estimated to account for close to 3% of EU electricity demand and likely to significantly increase in the coming years, the associated reporting scheme is intended to increase transparency and potentially to promote new designs and efficiency developments in data centres that can not only reduce energy and water consumption, but also promote the use of renewable energy, increased grid efficiency, or the reuse of waste heat in nearby facilities and heat networks.

Also, given the longer-term climate ambitions and goals of the EU, in the next few years it will also be on the European Commission's agenda to review whether a legislative proposal is ultimately warranted to improve the footprint of data centres.

The future?

Whilst technology solutions such as data governance platforms can help, they are not a panacea. Firms that underestimate or underinvest in data governance can expose their organizations to real regulatory risk, as well as reputational, customer and financial risks.

Also, as data availability continues to expand – so will advanced storage solutions like public cloud. Their benefit being that they can centralize and consolidate, the substantial amounts of unstructured and structured data held in a data lake, or a data warehouse, with its analytical capabilities allowing firms to derive valuable business insights from their data to improve decision-making.

Some trends driving today's accelerating market include advances in data analytics, big data and data science, innovations related to the cloud, AI, automation, and new data architectures. So, for firms such as asset managers, insurers, and banks, embracing these data trends will be crucial for staying competitive as they move forwards.

Ultimately, competitive advantage may come down to who can turn raw data into actionable data most quickly and with the most accuracy, whilst also embedding or following an existing robust data governance framework. Effectively managing the flip sides of data – as a strategic asset and a potential risk.

Citi contributors
Karolina Belwal
Randeep Buttar
Matthew Cherrill
Amanda Hale
Robert Harvey

[1] A data lake is a repository of structured and unstructured data in its original format, from which required data can be extracted for future use.

[2] 2024 Data Breach Investigations Report | Verizon

[3] The localization of regulated data such as personal information within a particular region or country. That could include only storing the data, but it could also include processing it. Heavily regulated countries include China, Germany, India, Indonesia, Japan, Kuwait, Russia, Saudi Arabia, Switzerland for example: Data Residency Laws by Country: an Overview - InCountry

[4] Data Centers - Database (datacentermap.com)

[5] See PS16/24 – Operational resilience: Critical third parties to the UK financial sector at www.bankofengland.co.uk

[6] See Approach to the oversight of critical third parties at www.bankofengland.co.uk

[7] See SS6/24 – Critical third parties to the UK financial sector at www.bankofengland.co.uk

[8] See SS7/24 – Reports by skilled persons: Critical third parties at www.bankofengland.co.uk

[9] A 'waterfall' model can be described as a linear model of software design employing a sequential design process. The 'agile' method proposes an incremental and iterative approach to software design. Here the design process is broken down into individual models that designers work on.

[10] See ESMA Data Strategy 2023-2028, page 13.

Please contact for further details:

David Morrison
Global Head of Trustee and Fiduciary Services
david.m.morrison@citi.com
+44 (0) 20 7500 8021

Amanda Hale
Head of Regulatory Services
amanda.jayne.hale@citi.com
+44 (0)20 7508 0178

Kelli O'Brien
United States
Head of Fund Administration
Product
kelli.a.obrien@citi.com
+1 617 859 3468

Ramesh Selva
North & South Asia (ex-Korea)
Head of Trustee & Fiduciary Services
ramesh.selva@citi.com
+65 6657 4142

Sung-Wook Han
Korea
Head of Trustee & Fiduciary Services
sungwook.han@citi.com
+82 22004 2162

Shane Baily
EMEA Head of Fiduciary Services
UK and Europe
shane.baily@citi.com
+353 1 622 6297

Jan-Olov Nord
EMEA Head of Fiduciary Services
Netherlands and New Markets
janolov.nord@citi.com
+31 20 651 4313

www.citibank.com/mss

CBS38765 12/24