Cloud Compliance Center - United States

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

UNITED STATES

*This content was last reviewed around March 2025.*

**Cloud neutral**

**1. Are financial institutions legally permitted to use cloud services?**

With respect to banks, there are no specific laws or regulations that expressly allow or govern the use of cloud services. Banks would be expected to manage a relationship with a cloud service provider in accordance with the general safety and soundness standards applicable to all banks, as well as guidance and guidelines issued by the Federal Reserve Board ("**Fed**"), the Federal Deposit Insurance Corporationd(collectively, "**Banking Agencies**"), as well as the Federal Financial Institutions Examination Council ("**FFIEC**") (an interagency council that prescribes uniform principles and standards for the examination of financial institutions). The Banking Agencies have issued consolidated joint supervisory guidance on sound risk management of all third-party relationships, namely the Interagency Guidance on Third-Party Relationships: Risk Management (Fed Letter SR 23-4; OCC Bulletin 2023-17; FDIC Financial Institution Letter FIL 29-2023). The FFIEC issued the Outsourcing Technology Services Booklet to provide guidance to banks on establishing, managing and monitoring third-party relationships. More recently, it issued the Joint Statement on Security in a Cloud Computing Environment, which highlights examples of bank risk management practices for safe and sound use of cloud computing services.

None of these statements or guidelines are laws or regulations. These documents are intended to provide guidance to banks and bank examiners to assist in evaluating a bank's risk management processes for establishing, managing and monitoring third-party and outsourcing relationships, including third-party cloud computing services. They are a reflection of both regulatory expectations and industry best practices, both of which are continually evolving.

Broker-dealers and investment advisers are permitted to use cloud services, although no statute or rule affirmatively confers this permission, and no relevant regulator has defined the term "cloud services" or "cloud service providers" through rulemaking. Rather, the recordkeeping rules envisage the use of electronic storage providers. Regulatory guidance issued by the Securities and Exchange Commission and the Financial Industry Regulatory Authority has accepted that electronic storage providers may include cloud services.

Entities regulated by the Commodity Futures Trading Commission ("**CFTC**") may also use cloud services. Both the CFTC and National Futures Association considered cloud services while recently revising their recordkeeping rules; therefore, both accept that CFTC entities will use cloud services.

**2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

The US financial regulatory landscape comprises multiple regulators covering banking, securities, commodities and derivatives, with varying levels of guidance to the institutions they oversee.

**Banks**

There are no laws or regulations that expressly allow or govern banks' use of cloud services. Banks would be expected to manage a relationship with a cloud service provider in accordance with general safety and soundness standards.

As mentioned above, there are several guidance documents from the Banking Agencies and the Federal Financial Institutions Examination Council ("**FFIEC**"). The Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency (collectively, "**Banking Agencies**") jointly issued the Interagency Guidance on Third-Party Relationships: Risk Management. In accordance with this guidance, banks are required to take a life cycle view of third-party relationships using a risk-based approach appropriate to the size and complexity of the banking organization and the criticality and complexity of the third-party service. Engaging a third party to perform services, such as cloud services, does not remove the bank's obligation to operate in a safe and sound manner, as well as ensure compliance with applicable laws and regulations to the same extent as if the services or activities were performed by the bank itself.

The bank's board of directors is ultimately responsible for overseeing third-party risk management and holding management accountable, as well as establishing risk appetite, approving policies and ensuring that appropriate procedures and practices are established. Bank management implements policies, procedures and practices commensurate with the bank's risk appetite and the level of risk and complexity of its third-party relationships. The Banking Agencies emphasize the importance of periodic independent reviews of third-party relationships by management to assess whether any adjustments to the bank's risk management processes are needed. In addition, the bank should properly document important aspects of the third-party relationship, such as risk assessments, due diligence results and recommendations, results of independent reviews, and periodic reporting to the board of directors.

The Banking Agencies describe effective third-party risk management as following a continuous life cycle. The stages of this life cycle are as follows:

Planning

Due diligence and third-party selection

Contract negotiations

Ongoing monitoring

Termination

For each step of this life cycle, the Banking Agencies identify several factors that a bank may consider or requirements that a bank may include in its due diligence or in the contract itself. Each step and factor is focused on ensuring sound risk management and planning by the bank in a manner that is appropriate to the size of the bank and the risk and complexity of the third-party relationship. No one factor is required, and there are no required contractual terms.

The FFIEC's Outsourcing Technology Services Booklet and Joint Statement on Security in a Cloud Computing Environment take a similar approach regarding risk management of third-party relationships, highlighting board oversight, appropriate due diligence and monitoring, and the importance of clearly defining contractual responsibilities. More broadly, the FFIEC IT Examination Handbook provides across-the-board guidance to banks and examiners on several IT issues, including outsourcing of technology systems, supervision of technology service providers, information security, audit and business continuity management.

**Broker-dealers**("**BDs**")

The rules applicable to BDs, investment advisers ("**IAs**") and entities regulated by the Commodity Futures Trading Commission ("**CFTC**") are recordkeeping rules and related interpretations and guidance on third-party providers of electronic storage, rather than rules specifically designed around the concept of cloud storage.

For BDs, the core recordkeeping rule for cloud governance purposes is Securities and Exchange Commission ("**SEC**") Rule 17a-4(f)(3) under the Securities Exchange Act of 1934, with a focus on Rule 17a-4(f)(3)(vii) and related SEC interpretations and staff guidance on electronic data storage providers. This includes a Division of Examinations ("Safeguarding Customer Records and Information in Network Storage — Use of Third-Party Security Features") OCIE alert.

In addition to BDs, Financial Industry Regulatory Authority ("**FINRA**") members continue to be governed by guidance previously issued by the National Association of Securities Dealers in conjunction with the New York Stock Exchange. This guidance presents best practices for supervision and reminds FINRA members of functions that may not be outsourced to third parties, such as those that must be performed by registered persons. Even for functions that may be outsourced, FINRA members are not absolved of responsibility for these functions, and they must implement supervisory procedures to ensure they are carried out compliantly. There are also regulatory requirements concerning supervision (FINRA Rule 3110) and business continuity planning (SEC guidance and FINRA Rule 4370), as well as Regulation SP on privacy. The 2005 FINRA Outsourcing Guidance and the FINRA 2015 and 2018 Cybersecurity Reports provide requirements for BDs, particularly around controls and authentication.

For IAs, they are subject to SEC Rule 204-2, which is the books and records rule for IAs. IA compliance with SEC Rule 17a-4, which is the BD rule, assures compliance with SEC Rule 204-2.

For entities regulated by the CFTC/National Futures Association ("**NFA**"), there are four categories of applicable rules. They are as follows:

Recordkeeping rules: CFTC Rule 1.31 and NFA Rule 2-10

Rules relating to supervising the activities of regulated entities (The futures regulators do not have explicit outsourcing rules, but instead generally mandate that the CFTC entities supervise both employees and agents (i.e., third-party service providers). These rules are contained in CFTC Rule 166.3, NFA Rules 2-9 (CPOs, CTAs and FCMs) and Rule 2-49 (SDs).)

Privacy/data protection rules contained in CFTC Rule 160.1-5

Business continuity rules contained in NFA Compliance Rule 2-38 (CPOs, CTAs and FCMs), Rule 2-49 (SDs), CFTC Regulation 23.603 and NFA Interpretive Notice 9052

For BDs, a checklist of key matters is as follows:

Audit rights

The use of subcontractors

Technical and organizational measures or IT guidelines, including security requirements (e.g., encryption and key management)

Business continuity/disaster recovery (including whether any specific BCP measures are required)

BDs are currently required to (i) preserve the records exclusively in a non-rewritable, non-erasable format, (ii) automatically verify the quality and accuracy of the storage media recording process, (iii) serialize the original and, if applicable, duplicate units of storage media, and then time and date for the required period of retention the information placed on the electronic storage media, and (iv) have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under the relevant rule and as required by the SEC or self-regulatory organizations. An undertaking from the third party is required under the rule. In 2022, the SEC made amendments to this rule that permit an "audit trail" exception to the current requirement that BDs' electronic records be stored solely in a non-rewritable, non-erasable format, also known as "write once, read many" (or WORM) format.

IAs are generally subject to a more principles-based approach as opposed to the prescriptive approach of BDs.

**CFTC/NFA**

The core recordkeeping rules are CFTC Rule 1.31 (in particular, Rule 1.31(c)-(d)) and NFA Rule 2-10. Generally, regulatory records must be retained in a form and manner that ensure their authenticity and reliability in accordance with applicable law. Electronic records systems must include (i) systems that maintain the security, signature and data necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with applicable law, (ii) systems that ensure the CFTC entity is able to produce electronic regulatory records in accordance with Rule 1.31, and ensure the availability of these regulatory records in the event of an emergency or other disruption of the CFTC entity's electronic record retention systems, and (iii) the creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains the information necessary for accessing or producing electronic regulatory records.

These regulatory records must be available to the regulator promptly upon request, in the form and medium in which the CFTC entity must produce them.

NFA Rule 2-10 requires members to maintain adequate books and records necessary and appropriate to conduct its business. The rule's broader requirements are harmonized with CFTC Rule 1.31.

As a general matter, the CFTC and NFA take a principles-based approach to compliance with these (and other requirements). As a result, different CFTC entities may tailor their compliance programs to their specific circumstances.

Neither the CFTC nor the NFA explicitly addresses data localization, termination rights, service levels, dispute resolution or governing law in the context of cloud storage.

**3. Are there any specific contractual requirements for cloud outsourcing?**

Agreements with a cloud service provider should sufficiently manage the risk associated with sharing clients' "nonpublic personal information" ("**NPPI**") across country borders and prevent sharing clients' NPPI with third parties in accordance with applicable laws.

With respect to banks, there are no mandated specific contractual provisions. The Interagency Guidance on Third-Party Relationships: Risk Management identifies several subject areas that third-party contracts may want to address, consistent with the institution's risk profile and the functions being performed. These subject areas include performance measures or benchmarks; audit rights and remediation; compliance obligations; operational resilience and business continuity; indemnification; insurance; customer complaints; subcontracting; and regulatory supervision of the activities performed, including the possibility of a direct examination of the third-party service provider by one or more of the Federal Reserve Board ("**Fed**"), the Federal Deposit Insurance Corporation ("**FDIC**") and the Office of the Comptroller of the Currency ("**OCC**"), or a state banking agency. Institutions regulated by the Securities and Exchange Commission, the Financial Industry Regulatory Authority and the Commodity Futures Trading Commission are subject to high-level requirements, including audit requirements, supervision requirements (which would extend to subcontractors), technical and organizational measures, and business continuity and disaster recovery. These requirements would be expected to be covered in an agreement with third-party providers.

**4. When does cloud outsourcing fall within the scope of the rules?**

A bank's engagement of any third party to perform services, including cloud services, does not remove the bank's obligation to operate in a safe and sound manner, as well as ensure compliance with applicable laws and regulations to the same extent as if the services or activities were performed by the bank itself.

With respect to broker-dealers ("**BDs**") and investment advisers, the Securities and Exchange Commission ("**SEC**") has not defined "third-party cloud service providers" with any specificity in its rules. Rather, third-party providers have been part of the electronic storage media paradigm since the 1997 amendments to SEC Rule 17a-4.

While there are no SEC regulations specific to services provided by cloud vendors, the scope of the SEC's approach to using third parties for recordkeeping and storage has remained broad over the years. SEC guidance in the form of risk alerts and Financial Industry Regulatory Authority ("**FINRA**") reports for BDs will likely be the way that these regulators continue to set expectations regarding cloud outsourcing.

In addition, the use of a cloud service vendor for data storage by any BD entities would be considered outsourcing under FINRA guidance. Accordingly, a BD must conduct appropriate due diligence prior to the implementation of such a vendor's services, and procedures for ongoing supervision. These may involve (i) using programmatic checks through business operations, (ii) including the procedures in the contracts with the vendors, (iii) requiring status reports and periodic meetings and (iv) testing and reviewing the vendor's procedures.

Moreover, in 2015, the FINRA undertook a comprehensive review of member firms and published a study that set forth a set of principles and best practices regarding BD approaches to cybersecurity. Notably, the FINRA specifically addressed firms' use of cloud service providers and, in particular, stressed the importance of identity and access management to establish appropriate controls to limit users' access to a firm's systems and data. While the report does not impose new rules on FINRA firms, it makes clear the expectations that regulators have regarding supervision and controls with respect to vendor management.

For Commodity Futures Trading Commission ("**CFTC**") entities, similarly, the CFTC and the National Futures Association ("**NFA**") do not define "third-party cloud service providers" within their rules. They have not adopted specific outsourcing rules similar to those found in other jurisdictions. However, both the CFTC and NFA considered cloud computing while revising their recordkeeping and supervision rules in recent years. Both the CFTC and NFA rules are expressly intended to be technology-neutral and therefore do not address specific types of cloud storage medium vendors.

**5. Does the outsourcing need to be notified to the regulator?**

Possibly, depending on what services the cloud services company provides.

Section 7(c)(2) of the Bank Service Company Act (12 U.S.C. 1867) requires banks to notify their supervisory banking agency within 30 days of any contracts with a technology service provider that provides certain services, including the following:

… check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution.

Broker-dealers need Financial Industry Regulatory Authority approval for first-time usage and subsequent notifications of changes or additions, but there are also additional process-based steps.

Investment advisers do not need to notify the regulator about outsourcing.

With respect to entities regulated by the Commodity Futures Trading Commission ("**CFTC**")/National Futures Association, there is no explicit notification requirement regarding cloud service providers. However, the rules mandate a process through which each CFTC entity must adopt an information systems security program, and each information systems security program would necessarily address the use of cloud service providers.

**6. What are the potential consequences for breaching financial services rules on cloud outsourcing?**

The bank may be subject to various regulatory actions if it fails to perform proper risk management of its relationship with a third-party cloud service provider. These include, but are not limited to, formal orders that limit bank activities, require specific remedial actions (audits, written plans, increased board oversight, etc.) and possibly impose civil money penalties. The Office of the Comptroller of Currency has imposed civil money penalties in excess of USD 50 million on banks for failure to properly manage the decommissioning of a third-party cloud service provider and for failure to establish appropriate risk management for migrating its technology operations to the cloud.

Numerous cases cite violations of Securities and Exchange Commission ("**SEC**") Rule 17a-4. These involve both SEC and Financial Industry Regulatory Authority ("**FINRA**") enforcement matters, as well as the results of routine examinations of broker-dealers. Typically, the findings stem from failures to maintain data in the appropriate format or for the requisite period, and do not implicate cloud service providers per se. The FINRA also routinely checks for deficiencies in connection with firms' failure to file the required undertakings.

Outside the realm of enforcement, the SEC's Division of Examinations has focused on vendor relationships (including cloud-based vendors). Examination questions have focused on due diligence prior to outsourcing data to a cloud service provider and processes for the ongoing monitoring of vendors, understanding vendor controls and settings, and the nature of the agreements between the broker-dealer/investment adviser and cloud service provider.

The Division of Examinations has also noted its focus on information security issues generally, in both its 2020 Examination Priorities and, shortly after that, its Cybersecurity and Resiliency Observations Reports.

On 3 January 2020, the Commodity Futures Trading Commission ("**CFTC**") issued two cyber threat alerts regarding the hacking of approximately 12 cloud service providers. While no specific sanctions were levied against CFTC entities, the CFTC required regulated entities to disclose whether they were affected by the hacking.

**7. Are there any data privacy and/or data security laws that would apply?**

Yes, US federal law imposes privacy obligations on financial institutions, including foreign financial institutions with offices in the US, as outlined below.

Financial services firms must be aware of additional state requirements prior to conducting business out of a particular jurisdiction.

The Gramm-Leach-Bliley Act restricts financial institutions from disclosing certain "nonpublic personal information" ("**NPPI**") collected from or about individual "consumers" in connection with the provision of financial products and services to nonaffiliated third parties. NPPI includes information that a consumer or customer puts on an application; information about the individual from another source, such as a credit bureau; or information about transactions between the individual and the financial institution, such as an account balance. Indeed, even the fact that an individual is a consumer or customer of a particular financial institution is NPPI. A "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons. Certain exceptions apply, including when disclosure is as follows:

With the customer's or consumer's consent

To process the customer's transactions

To maintain the customer account(s)

To comply with civil, criminal or regulatory investigations, or subpoenas or summons by federal, state or local authorities

To respond to judicial processes or government regulatory authorities with jurisdiction over the financial institution for examination, compliance or other purposes as authorized by law

For required institutional risk controls or for resolving disputes or inquiries

In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of NPPI concerns solely consumers of that business or unit

For specified other disclosures that a financial institution normally makes, such as to protect against or prevent actual or potential fraud; to the financial institution's attorneys, accountants and auditors; or to comply with applicable legal requirements, such as know-your-customer requirements and the disclosure of information to regulators

The Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency have each adopted the Interagency Guidelines Establishing Information Security Standards as an appendix to their privacy regulations. These guidelines require a bank's information security program to be designed to ensure the security and confidentiality of customer information in accordance with the Gramm-Leach Biley Act and other applicable privacy laws, protect against any anticipated threats or hazards to the security or integrity of this information, protect against unauthorized access to or use of this information that could result in substantial harm or inconvenience to any customer, and ensure the proper disposal of customer and consumer information. A bank using a cloud service provider is required to conduct appropriate due diligence regarding the provider's privacy practices and capabilities, include in the contract terms a requirement that the provider implement appropriate measures designed to meet the security standards, and monitor its provider in accordance with the bank's risk management program.

Securities and Exchange Commission ("**SEC**") Regulation SP and Regulation S-ID apply to both broker-dealers ("**BDs**") and investment advisers ("**IAs**"). However, Regulation SP and Regulation S-ID are not the sole privacy and data security requirements that BDs and IAs must comply with, as there are additional requirements beyond the scope of the securities laws (generally, state law requirements). With regard to information security, cybersecurity and data privacy, BDs are subject to a wide-ranging regulatory framework, which includes SEC rules, Financial Industry Regulatory Authority guidance, and federal and state law requirements. IAs are subject to SEC rules, as well as federal and state law requirements.

Commodity Futures Trading Commission entities (other than swap dealers) are subject to similar consumer data privacy rules under the commission's Rule 160.1-3.

**8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?**

No, there are generally no laws that would prohibit a cloud service provider from hosting data outside of the US. However, foreign-based cloud service providers must acknowledge the authority of US regulatory agencies to examine the services performed. As a result, a cloud service provider should agree that US regulatory and enforcement agencies might audit the cloud service provider abroad, to the extent necessary to assess its compliance with the relevant US legal framework. The cloud service provider must also be willing to cooperate with any audit of its practices and information security program.

The Office of the Comptroller of the Currency ("**OCC**") has issued a bulletin regarding the use of foreign service providers: Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance (OCC Bulletin 2002-16). This bulletin highlights that, although the use of foreign third-party service providers is permissible, these providers may raise unique compliance issues and risks for the bank that may require enhanced monitoring of the third party, management of country risk through protective contract provisions, and other risk management tools. In addition, the guidance notes that the bank should consider how foreign data privacy laws or regulatory requirements may interact, or even conflict, with US privacy laws and regulations, including with respect to the bank's access to information and the bank's obligations regarding safeguarding customer information.

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

No. This concept is not currently applicable in the US banking, securities and commodities/derivatives regulatory regimes. Vendors generally remain unregistered entities.

**10. Is express consent from customers or other data subjects required before moving data to the cloud?**

Generally, no consent is required, assuming that no client contract terms expressly prohibit the transfer of data to externally hosted cloud service provider systems in the US or elsewhere.

**11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?**

Yes, based on case law. Courts in the US usually take the view that other countries' privacy laws cannot serve as a defense to the legal obligation to comply with subpoenas, warrants or orders lawfully issued and served when they seek the disclosure of records or other data stored in the US. Though this authority continues to evolve, it is rooted in the long-standing principle that US courts are empowered to exert authority on people and entities over whom they have jurisdiction, even if that authority has consequences overseas. US federal courts have repeatedly and consistently expressed "great reluctance" to excuse the compelled disclosure of records simply because of competing directives from foreign sovereigns. Where a person or entity within the jurisdiction of a court has control over documents or materials, government officials may order that those materials be produced.

Under federal discovery rules, the issue is centered on whether a party or subpoena recipient has "possession, custody, or control over the requested documents" within the meaning of the Federal Rules of Civil Procedure. However, the legal assessment that courts perform in these types of cases is not without due consideration to foreign law.

A party claiming the shelter of foreign law to avoid discovery must first show that foreign law in fact bars production. However, even when this has been shown, there remains a presumption in favor of American courts. Furthermore, states have discovery rules that may affect the analysis.

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Yes. The Clarifying Lawful Overseas Use of Data Act ("**CLOUD Act**") amended the Stored Communications Act ("**SCA**") and established a procedure for a provider of electronic communication services to seek protection from the mandatory disclosure of non-US data to the US government where disclosure would violate the non-US law of the jurisdiction where the data is stored. The CLOUD Act also established a framework for qualifying foreign governments to procure non-US data stored in the US without creating legal liability under the SCA for the provider of electronic communications services. The CLOUD Act clarified the requirements to preserve data stored abroad even if the company plans to use the procedures available to contest disclosure.

A threshold requirement for invoking the protective procedures under the CLOUD Act is that the data at issue must be stored in a "qualifying foreign country." A qualifying foreign country is one that has entered into an executive agreement with the US government regulating access to data in this context. The CLOUD Act prescribes certain prerequisites for a foreign government to be eligible to enter into such an executive agreement, including that the foreign country must have robust substantive and procedural civil liberties protections that are comparable to those in the US. To date, the US government has only entered into an executive agreement with the UK and Australia, but subsequent agreements with other countries may be adopted later.

The CLOUD Act amended the SCA to allow US federal law enforcement authorities to use a warrant or subpoena to compel entities subject to US jurisdiction to provide certain types of data stored in foreign countries. However, several requirements must be met before US law enforcement authorities can properly request foreign entities' data under the CLOUD Act. These are as follows:

**First**, the entity to which a CLOUD Act request is issued must be an applicable network provider, i.e., a provider of an electronic communication service ("**ECS**") or a provider of a remote computing service ("**RCS**").

**Second**, that entity must have "possession, custody, or control" of the stored data sought in the request.

**Third**, the request must pass US constitutional muster, i.e., US law enforcement must meet certain standards of proof before obtaining data from an ECS or RCS.

**Fourth** and finally, the ECS or RCS to which a CLOUD Act request is issued must be subject to the US' jurisdiction.

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

With respect to banks, there are no specific laws or regulations that expressly allow or govern the use of cloud services. Banks would be expected to manage a relationship with a cloud service provider in accordance with the general safety and soundness standards applicable to all banks, as well as guidance and guidelines issued by the Federal Reserve Board ("**Fed**"), the Federal Deposit Insurance Corporationd(collectively, "**Banking Agencies**"), as well as the Federal Financial Institutions Examination Council ("**FFIEC**") (an interagency council that prescribes uniform principles and standards for the examination of financial institutions). The Banking Agencies have issued consolidated joint supervisory guidance on sound risk management of all third-party relationships, namely the Interagency Guidance on Third-Party Relationships: Risk Management (Fed Letter SR 23-4; OCC Bulletin 2023-17; FDIC Financial Institution Letter FIL 29-2023). The FFIEC issued the Outsourcing Technology Services Booklet to provide guidance to banks on establishing, managing and monitoring third-party relationships. More recently, it issued the Joint Statement on Security in a Cloud Computing Environment, which highlights examples of bank risk management practices for safe and sound use of cloud computing services.

None of these statements or guidelines are laws or regulations. These documents are intended to provide guidance to banks and bank examiners to assist in evaluating a bank's risk management processes for establishing, managing and monitoring third-party and outsourcing relationships, including third-party cloud computing services. They are a reflection of both regulatory expectations and industry best practices, both of which are continually evolving.

Broker-dealers and investment advisers are permitted to use cloud services, although no statute or rule affirmatively confers this permission, and no relevant regulator has defined the term "cloud services" or "cloud service providers" through rulemaking. Rather, the recordkeeping rules envisage the use of electronic storage providers. Regulatory guidance issued by the Securities and Exchange Commission and the Financial Industry Regulatory Authority has accepted that electronic storage providers may include cloud services.

Entities regulated by the Commodity Futures Trading Commission ("**CFTC**") may also use cloud services. Both the CFTC and National Futures Association considered cloud services while recently revising their recordkeeping rules; therefore, both accept that CFTC entities will use cloud services.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

The US financial regulatory landscape comprises multiple regulators covering banking, securities, commodities and derivatives, with varying levels of guidance to the institutions they oversee.

**Banks**

There are no laws or regulations that expressly allow or govern banks' use of cloud services. Banks would be expected to manage a relationship with a cloud service provider in accordance with general safety and soundness standards.

As mentioned above, there are several guidance documents from the Banking Agencies and the Federal Financial Institutions Examination Council ("**FFIEC**"). The Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency (collectively, "**Banking Agencies**") jointly issued the Interagency Guidance on Third-Party Relationships: Risk Management. In accordance with this guidance, banks are required to take a life cycle view of third-party relationships using a risk-based approach appropriate to the size and complexity of the banking organization and the criticality and complexity of the third-party service. Engaging a third party to perform services, such as cloud services, does not remove the bank's obligation to operate in a safe and sound manner, as well as ensure compliance with applicable laws and regulations to the same extent as if the services or activities were performed by the bank itself.

The bank's board of directors is ultimately responsible for overseeing third-party risk management and holding management accountable, as well as establishing risk appetite, approving policies and ensuring that appropriate procedures and practices are established. Bank management implements policies, procedures and practices commensurate with the bank's risk appetite and the level of risk and complexity of its third-party relationships. The Banking Agencies emphasize the importance of periodic independent reviews of third-party relationships by management to assess whether any adjustments to the bank's risk management processes are needed. In addition, the bank should properly document important aspects of the third-party relationship, such as risk assessments, due diligence results and recommendations, results of independent reviews, and periodic reporting to the board of directors.

The Banking Agencies describe effective third-party risk management as following a continuous life cycle. The stages of this life cycle are as follows:

Planning

Due diligence and third-party selection

Contract negotiations

Ongoing monitoring

Termination

For each step of this life cycle, the Banking Agencies identify several factors that a bank may consider or requirements that a bank may include in its due diligence or in the contract itself. Each step and factor is focused on ensuring sound risk management and planning by the bank in a manner that is appropriate to the size of the bank and the risk and complexity of the third-party relationship. No one factor is required, and there are no required contractual terms.

The FFIEC's Outsourcing Technology Services Booklet and Joint Statement on Security in a Cloud Computing Environment take a similar approach regarding risk management of third-party relationships, highlighting board oversight, appropriate due diligence and monitoring, and the importance of clearly defining contractual responsibilities. More broadly, the FFIEC IT Examination Handbook provides across-the-board guidance to banks and examiners on several IT issues, including outsourcing of technology systems, supervision of technology service providers, information security, audit and business continuity management.

**Broker-dealers**("**BDs**")

The rules applicable to BDs, investment advisers ("**IAs**") and entities regulated by the Commodity Futures Trading Commission ("**CFTC**") are recordkeeping rules and related interpretations and guidance on third-party providers of electronic storage, rather than rules specifically designed around the concept of cloud storage.

For BDs, the core recordkeeping rule for cloud governance purposes is Securities and Exchange Commission ("**SEC**") Rule 17a-4(f)(3) under the Securities Exchange Act of 1934, with a focus on Rule 17a-4(f)(3)(vii) and related SEC interpretations and staff guidance on electronic data storage providers. This includes a Division of Examinations ("Safeguarding Customer Records and Information in Network Storage — Use of Third-Party Security Features") OCIE alert.

In addition to BDs, Financial Industry Regulatory Authority ("**FINRA**") members continue to be governed by guidance previously issued by the National Association of Securities Dealers in conjunction with the New York Stock Exchange. This guidance presents best practices for supervision and reminds FINRA members of functions that may not be outsourced to third parties, such as those that must be performed by registered persons. Even for functions that may be outsourced, FINRA members are not absolved of responsibility for these functions, and they must implement supervisory procedures to ensure they are carried out compliantly. There are also regulatory requirements concerning supervision (FINRA Rule 3110) and business continuity planning (SEC guidance and FINRA Rule 4370), as well as Regulation SP on privacy. The 2005 FINRA Outsourcing Guidance and the FINRA 2015 and 2018 Cybersecurity Reports provide requirements for BDs, particularly around controls and authentication.

For IAs, they are subject to SEC Rule 204-2, which is the books and records rule for IAs. IA compliance with SEC Rule 17a-4, which is the BD rule, assures compliance with SEC Rule 204-2.

For entities regulated by the CFTC/National Futures Association ("**NFA**"), there are four categories of applicable rules. They are as follows:

Recordkeeping rules: CFTC Rule 1.31 and NFA Rule 2-10

Rules relating to supervising the activities of regulated entities (The futures regulators do not have explicit outsourcing rules, but instead generally mandate that the CFTC entities supervise both employees and agents (i.e., third-party service providers). These rules are contained in CFTC Rule 166.3, NFA Rules 2-9 (CPOs, CTAs and FCMs) and Rule 2-49 (SDs).)

Privacy/data protection rules contained in CFTC Rule 160.1-5

Business continuity rules contained in NFA Compliance Rule 2-38 (CPOs, CTAs and FCMs), Rule 2-49 (SDs), CFTC Regulation 23.603 and NFA Interpretive Notice 9052

For BDs, a checklist of key matters is as follows:

Audit rights

The use of subcontractors

Technical and organizational measures or IT guidelines, including security requirements (e.g., encryption and key management)

Business continuity/disaster recovery (including whether any specific BCP measures are required)

BDs are currently required to (i) preserve the records exclusively in a non-rewritable, non-erasable format, (ii) automatically verify the quality and accuracy of the storage media recording process, (iii) serialize the original and, if applicable, duplicate units of storage media, and then time and date for the required period of retention the information placed on the electronic storage media, and (iv) have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under the relevant rule and as required by the SEC or self-regulatory organizations. An undertaking from the third party is required under the rule. In 2022, the SEC made amendments to this rule that permit an "audit trail" exception to the current requirement that BDs' electronic records be stored solely in a non-rewritable, non-erasable format, also known as "write once, read many" (or WORM) format.

IAs are generally subject to a more principles-based approach as opposed to the prescriptive approach of BDs.

**CFTC/NFA**

The core recordkeeping rules are CFTC Rule 1.31 (in particular, Rule 1.31(c)-(d)) and NFA Rule 2-10. Generally, regulatory records must be retained in a form and manner that ensure their authenticity and reliability in accordance with applicable law. Electronic records systems must include (i) systems that maintain the security, signature and data necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with applicable law, (ii) systems that ensure the CFTC entity is able to produce electronic regulatory records in accordance with Rule 1.31, and ensure the availability of these regulatory records in the event of an emergency or other disruption of the CFTC entity's electronic record retention systems, and (iii) the creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains the information necessary for accessing or producing electronic regulatory records.

These regulatory records must be available to the regulator promptly upon request, in the form and medium in which the CFTC entity must produce them.

NFA Rule 2-10 requires members to maintain adequate books and records necessary and appropriate to conduct its business. The rule's broader requirements are harmonized with CFTC Rule 1.31.

As a general matter, the CFTC and NFA take a principles-based approach to compliance with these (and other requirements). As a result, different CFTC entities may tailor their compliance programs to their specific circumstances.

Neither the CFTC nor the NFA explicitly addresses data localization, termination rights, service levels, dispute resolution or governing law in the context of cloud storage.

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

Agreements with a cloud service provider should sufficiently manage the risk associated with sharing clients' "nonpublic personal information" ("**NPPI**") across country borders and prevent sharing clients' NPPI with third parties in accordance with applicable laws.

With respect to banks, there are no mandated specific contractual provisions. The Interagency Guidance on Third-Party Relationships: Risk Management identifies several subject areas that third-party contracts may want to address, consistent with the institution's risk profile and the functions being performed. These subject areas include performance measures or benchmarks; audit rights and remediation; compliance obligations; operational resilience and business continuity; indemnification; insurance; customer complaints; subcontracting; and regulatory supervision of the activities performed, including the possibility of a direct examination of the third-party service provider by one or more of the Federal Reserve Board ("**Fed**"), the Federal Deposit Insurance Corporation ("**FDIC**") and the Office of the Comptroller of the Currency ("**OCC**"), or a state banking agency. Institutions regulated by the Securities and Exchange Commission, the Financial Industry Regulatory Authority and the Commodity Futures Trading Commission are subject to high-level requirements, including audit requirements, supervision requirements (which would extend to subcontractors), technical and organizational measures, and business continuity and disaster recovery. These requirements would be expected to be covered in an agreement with third-party providers.

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

A bank's engagement of any third party to perform services, including cloud services, does not remove the bank's obligation to operate in a safe and sound manner, as well as ensure compliance with applicable laws and regulations to the same extent as if the services or activities were performed by the bank itself.

With respect to broker-dealers ("**BDs**") and investment advisers, the Securities and Exchange Commission ("**SEC**") has not defined "third-party cloud service providers" with any specificity in its rules. Rather, third-party providers have been part of the electronic storage media paradigm since the 1997 amendments to SEC Rule 17a-4.

While there are no SEC regulations specific to services provided by cloud vendors, the scope of the SEC's approach to using third parties for recordkeeping and storage has remained broad over the years. SEC guidance in the form of risk alerts and Financial Industry Regulatory Authority ("**FINRA**") reports for BDs will likely be the way that these regulators continue to set expectations regarding cloud outsourcing.

In addition, the use of a cloud service vendor for data storage by any BD entities would be considered outsourcing under FINRA guidance. Accordingly, a BD must conduct appropriate due diligence prior to the implementation of such a vendor's services, and procedures for ongoing supervision. These may involve (i) using programmatic checks through business operations, (ii) including the procedures in the contracts with the vendors, (iii) requiring status reports and periodic meetings and (iv) testing and reviewing the vendor's procedures.

Moreover, in 2015, the FINRA undertook a comprehensive review of member firms and published a study that set forth a set of principles and best practices regarding BD approaches to cybersecurity. Notably, the FINRA specifically addressed firms' use of cloud service providers and, in particular, stressed the importance of identity and access management to establish appropriate controls to limit users' access to a firm's systems and data. While the report does not impose new rules on FINRA firms, it makes clear the expectations that regulators have regarding supervision and controls with respect to vendor management.

For Commodity Futures Trading Commission ("**CFTC**") entities, similarly, the CFTC and the National Futures Association ("**NFA**") do not define "third-party cloud service providers" within their rules. They have not adopted specific outsourcing rules similar to those found in other jurisdictions. However, both the CFTC and NFA considered cloud computing while revising their recordkeeping and supervision rules in recent years. Both the CFTC and NFA rules are expressly intended to be technology-neutral and therefore do not address specific types of cloud storage medium vendors.

# Regulatory notifications

## 5. Does the outsourcing need to be notified to the regulator?

Possibly, depending on what services the cloud services company provides.

Section 7(c)(2) of the Bank Service Company Act (12 U.S.C. 1867) requires banks to notify their supervisory banking agency within 30 days of any contracts with a technology service provider that provides certain services, including the following:

… check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution.

Broker-dealers need Financial Industry Regulatory Authority approval for first-time usage and subsequent notifications of changes or additions, but there are also additional process-based steps.

Investment advisers do not need to notify the regulator about outsourcing.

With respect to entities regulated by the Commodity Futures Trading Commission ("**CFTC**")/National Futures Association, there is no explicit notification requirement regarding cloud service providers. However, the rules mandate a process through which each CFTC entity must adopt an information systems security program, and each information systems security program would necessarily address the use of cloud service providers.

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

The bank may be subject to various regulatory actions if it fails to perform proper risk management of its relationship with a third-party cloud service provider. These include, but are not limited to, formal orders that limit bank activities, require specific remedial actions (audits, written plans, increased board oversight, etc.) and possibly impose civil money penalties. The Office of the Comptroller of Currency has imposed civil money penalties in excess of USD 50 million on banks for failure to properly manage the decommissioning of a third-party cloud service provider and for failure to establish appropriate risk management for migrating its technology operations to the cloud.

Numerous cases cite violations of Securities and Exchange Commission ("**SEC**") Rule 17a-4. These involve both SEC and Financial Industry Regulatory Authority ("**FINRA**") enforcement matters, as well as the results of routine examinations of broker-dealers. Typically, the findings stem from failures to maintain data in the appropriate format or for the requisite period, and do not implicate cloud service providers per se. The FINRA also routinely checks for deficiencies in connection with firms' failure to file the required undertakings.

Outside the realm of enforcement, the SEC's Division of Examinations has focused on vendor relationships (including cloud-based vendors). Examination questions have focused on due diligence prior to outsourcing data to a cloud service provider and processes for the ongoing monitoring of vendors, understanding vendor controls and settings, and the nature of the agreements between the broker-dealer/investment adviser and cloud service provider.

The Division of Examinations has also noted its focus on information security issues generally, in both its 2020 Examination Priorities and, shortly after that, its Cybersecurity and Resiliency Observations Reports.

On 3 January 2020, the Commodity Futures Trading Commission ("**CFTC**") issued two cyber threat alerts regarding the hacking of approximately 12 cloud service providers. While no specific sanctions were levied against CFTC entities, the CFTC required regulated entities to disclose whether they were affected by the hacking.

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes, US federal law imposes privacy obligations on financial institutions, including foreign financial institutions with offices in the US, as outlined below.

Financial services firms must be aware of additional state requirements prior to conducting business out of a particular jurisdiction.

The Gramm-Leach-Bliley Act restricts financial institutions from disclosing certain "nonpublic personal information" ("**NPPI**") collected from or about individual "consumers" in connection with the provision of financial products and services to nonaffiliated third parties. NPPI includes information that a consumer or customer puts on an application; information about the individual from another source, such as a credit bureau; or information about transactions between the individual and the financial institution, such as an account balance. Indeed, even the fact that an individual is a consumer or customer of a particular financial institution is NPPI. A "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons. Certain exceptions apply, including when disclosure is as follows:

With the customer's or consumer's consent

To process the customer's transactions

To maintain the customer account(s)

To comply with civil, criminal or regulatory investigations, or subpoenas or summons by federal, state or local authorities

To respond to judicial processes or government regulatory authorities with jurisdiction over the financial institution for examination, compliance or other purposes as authorized by law

For required institutional risk controls or for resolving disputes or inquiries

In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of NPPI concerns solely consumers of that business or unit

For specified other disclosures that a financial institution normally makes, such as to protect against or prevent actual or potential fraud; to the financial institution's attorneys, accountants and auditors; or to comply with applicable legal requirements, such as know-your-customer requirements and the disclosure of information to regulators

The Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency have each adopted the Interagency Guidelines Establishing Information Security Standards as an appendix to their privacy regulations. These guidelines require a bank's information security program to be designed to ensure the security and confidentiality of customer information in accordance with the Gramm-Leach Biley Act and other applicable privacy laws, protect against any anticipated threats or hazards to the security or integrity of this information, protect against unauthorized access to or use of this information that could result in substantial harm or inconvenience to any customer, and ensure the proper disposal of customer and consumer information. A bank using a cloud service provider is required to conduct appropriate due diligence regarding the provider's privacy practices and capabilities, include in the contract terms a requirement that the provider implement appropriate measures designed to meet the security standards, and monitor its provider in accordance with the bank's risk management program.

Securities and Exchange Commission ("**SEC**") Regulation SP and Regulation S-ID apply to both broker-dealers ("**BDs**") and investment advisers ("**IAs**"). However, Regulation SP and Regulation S-ID are not the sole privacy and data security requirements that BDs and IAs must comply with, as there are additional requirements beyond the scope of the securities laws (generally, state law requirements). With regard to information security, cybersecurity and data privacy, BDs are subject to a wide-ranging regulatory framework, which includes SEC rules, Financial Industry Regulatory Authority guidance, and federal and state law requirements. IAs are subject to SEC rules, as well as federal and state law requirements.

Commodity Futures Trading Commission entities (other than swap dealers) are subject to similar consumer data privacy rules under the commission's Rule 160.1-3.

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

No, there are generally no laws that would prohibit a cloud service provider from hosting data outside of the US. However, foreign-based cloud service providers must acknowledge the authority of US regulatory agencies to examine the services performed. As a result, a cloud service provider should agree that US regulatory and enforcement agencies might audit the cloud service provider abroad, to the extent necessary to assess its compliance with the relevant US legal framework. The cloud service provider must also be willing to cooperate with any audit of its practices and information security program.

The Office of the Comptroller of the Currency ("**OCC**") has issued a bulletin regarding the use of foreign service providers: Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance (OCC Bulletin 2002-16). This bulletin highlights that, although the use of foreign third-party service providers is permissible, these providers may raise unique compliance issues and risks for the bank that may require enhanced monitoring of the third party, management of country risk through protective contract provisions, and other risk management tools. In addition, the guidance notes that the bank should consider how foreign data privacy laws or regulatory requirements may interact, or even conflict, with US privacy laws and regulations, including with respect to the bank's access to information and the bank's obligations regarding safeguarding customer information.

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

No. This concept is not currently applicable in the US banking, securities and commodities/derivatives regulatory regimes. Vendors generally remain unregistered entities.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

Generally, no consent is required, assuming that no client contract terms expressly prohibit the transfer of data to externally hosted cloud service provider systems in the US or elsewhere.

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

Yes, based on case law. Courts in the US usually take the view that other countries' privacy laws cannot serve as a defense to the legal obligation to comply with subpoenas, warrants or orders lawfully issued and served when they seek the disclosure of records or other data stored in the US. Though this authority continues to evolve, it is rooted in the long-standing principle that US courts are empowered to exert authority on people and entities over whom they have jurisdiction, even if that authority has consequences overseas. US federal courts have repeatedly and consistently expressed "great reluctance" to excuse the compelled disclosure of records simply because of competing directives from foreign sovereigns. Where a person or entity within the jurisdiction of a court has control over documents or materials, government officials may order that those materials be produced.

Under federal discovery rules, the issue is centered on whether a party or subpoena recipient has "possession, custody, or control over the requested documents" within the meaning of the Federal Rules of Civil Procedure. However, the legal assessment that courts perform in these types of cases is not without due consideration to foreign law.

A party claiming the shelter of foreign law to avoid discovery must first show that foreign law in fact bars production. However, even when this has been shown, there remains a presumption in favor of American courts. Furthermore, states have discovery rules that may affect the analysis.

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Yes. The Clarifying Lawful Overseas Use of Data Act ("**CLOUD Act**") amended the Stored Communications Act ("**SCA**") and established a procedure for a provider of electronic communication services to seek protection from the mandatory disclosure of non-US data to the US government where disclosure would violate the non-US law of the jurisdiction where the data is stored. The CLOUD Act also established a framework for qualifying foreign governments to procure non-US data stored in the US without creating legal liability under the SCA for the provider of electronic communications services. The CLOUD Act clarified the requirements to preserve data stored abroad even if the company plans to use the procedures available to contest disclosure.

A threshold requirement for invoking the protective procedures under the CLOUD Act is that the data at issue must be stored in a "qualifying foreign country." A qualifying foreign country is one that has entered into an executive agreement with the US government regulating access to data in this context. The CLOUD Act prescribes certain prerequisites for a foreign government to be eligible to enter into such an executive agreement, including that the foreign country must have robust substantive and procedural civil liberties protections that are comparable to those in the US. To date, the US government has only entered into an executive agreement with the UK and Australia, but subsequent agreements with other countries may be adopted later.

The CLOUD Act amended the SCA to allow US federal law enforcement authorities to use a warrant or subpoena to compel entities subject to US jurisdiction to provide certain types of data stored in foreign countries. However, several requirements must be met before US law enforcement authorities can properly request foreign entities' data under the CLOUD Act. These are as follows:

**First**, the entity to which a CLOUD Act request is issued must be an applicable network provider, i.e., a provider of an electronic communication service ("**ECS**") or a provider of a remote computing service ("**RCS**").

**Second**, that entity must have "possession, custody, or control" of the stored data sought in the request.

**Third**, the request must pass US constitutional muster, i.e., US law enforcement must meet certain standards of proof before obtaining data from an ECS or RCS.

**Fourth** and finally, the ECS or RCS to which a CLOUD Act request is issued must be subject to the US' jurisdiction.

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.