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 January 2022.*

**Cloud neutral**

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

Yes, in general terms, provided that the institution meets all applicable legal requirements for the use of cloud services.

The Federal Reserve ("**Fed**"), the Federal Deposit Insurance Corporation ("**FDIC**"), the Office of the Comptroller of the Currency ("**OCC**") and the Federal Financial Institutions Examination Council have each issued guidance on risk management in third-party relationships. There are no express provisions prohibiting or governing the specific use of cloud service providers, as long as a financial institution takes appropriate steps to manage its data and its cloud service provider relationship. This guidance, although not formal "rules," is the source of regulatory expectations on the use of cloud service providers and outsourcing, as well as regulatory expectations of general applicability regarding all third-party contracts, including cloud computing contracts.

In July 2021, the Fed, the FDIC and the OCC issued proposed joint guidance on banking organizations' risk management of third-party relationships. The proposed interagency guidance would replace existing third-party risk management guidance that was issued separately by each agency. The purpose of this guidance would be to harmonize the risk-based approach to third-party relationships (including cloud service providers) previously issued by each regulator independently. The proposed guidance does not announce new risk management principles or mandate new procedures for financial institutions going to the cloud.

Broker-dealers and investment advisers are permitted to use cloud services, although no statute or rule affirmatively confers such permission and no relevant regulator has defined the term "cloud services" or cloud service providers through rulemaking. Rather, the record-keeping rules envisage the use of electronic storage providers. Regulatory guidance issued by the Securities and Exchange Commission ("**SEC**") and the Financial Industry Regulatory Authority has accepted that electronic storage providers may include cloud services. The SEC proposed 2021 amendments regarding record-keeping rules do not address the cloud directly, although the amendments could update existing rules to be more closely aligned to cloud requirements.

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

**2. Are there any rules which 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**

Yes, banking regulators' guidance on third-party risk management applies to the use of cloud services. In addition, the Federal Financial Institutions Examination Council recently issued a statement on security risk management principles for financial institutions using cloud services.

Financial institutions are required to take a life cycle view of third-party relationships using a risk-based approach appropriate to the criticality and complexity of the function. This risk management process is the purview of senior management and the board of directors. The initial steps are to consider whether the function can be safely outsourced to a third party and conducting appropriate due diligence, while maintaining robust contingency plans. Written contracts with third parties are required, and they should address the following:

Performance obligations (including quality metrics) and the consequences of the failure to perform

Notification of financial difficulty, catastrophic events and significant incidents (including security incidents)

Notification of significant changes, including acquisitions, subcontracting, offshoring, key personnel changes and material policy changes

Audit rights and requirements, including independent review

Legal and regulatory compliance, including data privacy, anti-money laundering and sanctions compliance

Fee calculations and ensuring no unduly burdensome up-front or exit fees

Exit rights

Data and IP ownership

Confidentiality and integrity of data and systems

Business continuity

Limits on liability and indemnification

Insurance

Dispute resolution

Regulatory supervision

The regulatory guidance does not mandate the substance of the terms of the parties' contract; rather, the terms are required to reflect the risk profile of the financial institution for the services contracted.

Finally, the guidance requires financial institutions to conduct ongoing monitoring of the third-party relationship. This includes a periodic assessment of the third-party relationship to determine if the services now include critical activities, and assigning staff with the requisite skills to oversee the third-party provider commensurate with the level of risk and complexity of the relationship. An ongoing risk-based monitoring program should have oversight with respect to the following:

Business strategy and reputation

Legal and regulatory compliance

Financial condition

Insurance coverage

Key personnel and institutional knowledge

Identifying and managing risk prior to audit reporting

Process for policy changes to address new threats

Response to service interruption and service quality degradation

Reliance on subcontractors

Conflicts of interest and operational and reputational risks

Confidentiality and integrity of data and systems

Trending in customer complaints and ability to remediate

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

The rules applicable for broker-dealers, investment advisers ("**IAs**") and Commodity Futures Trading Commission ("**CFTC**") regulated entities are record-keeping rules and related interpretation and guidance over third-party providers of electronic storage, rather than rules specifically designed around the concept of cloud storage.

For BDs, the core record-keeping 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 interpretation and staff guidance on electronic data storage providers, including a Division of Examinations ("Safeguarding Customer Records and Information in Network Storage — Use of Third-Party Security Features") OCIE alert. In November 2021, the SEC proposed amendments to this rule, although it does not reference cloud-related requirements specifically.

In addition for 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, which presents best practices for supervision and reminds them of functions that may not be outsourced to third parties, such as those functions that must be performed by registered persons. Even for functions that may be outsourced, FINRA member firms 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,theyare 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:

Record-keeping 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 — addressed in FINRA guidance, but only at a high level in an OCIE alert or SEC guidance

Technical and organizational measures or IT guidelines, including security requirements (e.g., encryption and key management) — only addressed in a general way through SEC and FINRA guidance

Business continuity/disaster recovery (including whether any specific BCP measures are required) — the SEC has addressed BCP largely through guidance, while FINRA has provided more specific guidance

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 time-date for the required period of retention the information placed on such 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 rule and as required by the SEC or self-regulatory organizations. An undertakingfrom the third party is a requirement of the rule.  November 2021 SEC proposed amendments to this rule could eliminate the current requirement that electronic records of BDs be stored solely in a non-rewritable, non-erasable format, also known as "write once, read many" (or WORM) format. The undertaking may also be removed from the rule should amendments be finalized as proposed.

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

**CFTC/NFA**

The core record-keeping rules are CFTC Rule 1.31 (in particular, Rule 1.31(c)-(d)) and NFA Rule 2-10. Generally, records must be retained in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with applicable law. Electronic records systems must include: (i) systems that maintain the security, signature and data as 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 such 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 information necessary for accessing or producing electronic regulatory records.

Such records must be available to the regulator promptly upon request in a reasonable form and medium in which the CFTC entity must produce such regulatory records.

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?**

For banking institutions, please see the response to question 2 on whether any rules apply to cloud use by financial institutions. Banking regulators have not mandated specific provisions but, consistent with a risk-based approach, they have identified subject areas that third-party contracts should address to be consistent with the risk profile of the institution and the functions involved.

Generally, an outsourcing entity should enter into an appropriate agreement with its cloud service provider that sufficiently manages the risk associated with sharing clients' "nonpublic personal information" ("**NPPI**") across country borders and prevents sharing clients' NPPI with third parties.

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?**

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 rulemaking. 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 the use of third parties for record-keeping 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, which 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 rulemaking. 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 record-keeping 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?**

Banks are not required to notify regulators prior to engaging third parties to perform services, including cloud computing.

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 in respect of outsourcing.

With respect to entities regulated by the Commodity Futures Trading Commission ("**CFTC**")/National Futures Association, there is no explicit notification requirement with respect to 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 Office of the Comptroller of Currency ("**OCC**") has fined banks for failing to maintain and exercise adequate risk management programs, including loss mitigation policies. It has also issued fines for the failure to exercise adequate oversight of disengagement from third-party providers. The OCC has levied substantial fines against banks in connection with the lax information security practices of bank subsidiaries in connection with customer data breaches. Fines for egregious conduct have exceeded USD 80 million.

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 the 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 the failure of firms 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 thereafter, 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 such 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 Office of the Comptroller of the Currency ("**OCC**") has adopted the Interagency Guidelines Establishing Information Security Standards at 12 C.F.R., Part 30, Appendix B. The Interagency Security Standards require a bank using a cloud service provider to address service provider information security before signing a contract, as part of the terms of the contract, and on an ongoing basis after establishing a service provider relationship.

The Federal Financial Institutions Examination Council ("**FFIEC**") has published a guidance booklet on outsourcing practices, and it states that financial institutions may outsource many areas of operations, including all or part of any service, process or system operation. However, the use of a subcontractor or, in this case, a cloud service provider does not diminish the responsibility of the financial institution's senior management to ensure that the subcontractor's activity is conducted in a safe manner and in compliance with applicable laws and regulations.

That same FFIEC guidance warns, however, that financial institutions must not share US regulatory examination reports or information contained therein with either foreign regulators or foreign-based service providers without the express written approval of the appropriate US regulatory authority. The FFIEC recently issued the "Security in a Cloud Computing Environment" bulletin, which addresses key risks in cloud computing. Although this bulletin does not contain new regulatory expectations, it highlights examples of risk management practices related to the safe use of cloud computing services, and directs financial institutions to also review the FFIEC's IT Handbook and other documents providing general information on best industry practices.

Regarding broker-dealers ("**BDs**") and investment advisers ("**IAs**"), Securities and Exchange Commission ("**SEC**") Regulation SP and Regulation S-ID apply to both BDs and 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 which 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. Foreign-based cloud service providers, however, 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.

In addition, sharing US regulatory examination reports with foreign regulators or foreign-based cloud service providers without the express written approval of the appropriate US regulatory authority is prohibited.

**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. Are express consents from customers or other data subjects required before moving data to the cloud?**

Generally, no consents are 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 which 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 the privacy laws of other countries cannot serve asa 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 longstanding 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 those materials to 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. The legal assessment courts perform in these types of cases, however, 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. Even when such a showing is made, however, 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 which 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 utilize 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 governing 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 such 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 later be adopted.

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 the data of foreign entities under the CLOUD Act, 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 jurisdiction of the US.

# Permissibility of cloud

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

Yes, in general terms, provided that the institution meets all applicable legal requirements for the use of cloud services.

The Federal Reserve ("**Fed**"), the Federal Deposit Insurance Corporation ("**FDIC**"), the Office of the Comptroller of the Currency ("**OCC**") and the Federal Financial Institutions Examination Council have each issued guidance on risk management in third-party relationships. There are no express provisions prohibiting or governing the specific use of cloud service providers, as long as a financial institution takes appropriate steps to manage its data and its cloud service provider relationship. This guidance, although not formal "rules," is the source of regulatory expectations on the use of cloud service providers and outsourcing, as well as regulatory expectations of general applicability regarding all third-party contracts, including cloud computing contracts.

In July 2021, the Fed, the FDIC and the OCC issued proposed joint guidance on banking organizations' risk management of third-party relationships. The proposed interagency guidance would replace existing third-party risk management guidance that was issued separately by each agency. The purpose of this guidance would be to harmonize the risk-based approach to third-party relationships (including cloud service providers) previously issued by each regulator independently. The proposed guidance does not announce new risk management principles or mandate new procedures for financial institutions going to the cloud.

Broker-dealers and investment advisers are permitted to use cloud services, although no statute or rule affirmatively confers such permission and no relevant regulator has defined the term "cloud services" or cloud service providers through rulemaking. Rather, the record-keeping rules envisage the use of electronic storage providers. Regulatory guidance issued by the Securities and Exchange Commission ("**SEC**") and the Financial Industry Regulatory Authority has accepted that electronic storage providers may include cloud services. The SEC proposed 2021 amendments regarding record-keeping rules do not address the cloud directly, although the amendments could update existing rules to be more closely aligned to cloud requirements.

Entities regulated by the Commodity Futures Trading Commission ("**CFTC**") may also use cloud services. Both the CFTC and National Futures Association contemplated cloud services while recently revising their record-keeping 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**

Yes, banking regulators' guidance on third-party risk management applies to the use of cloud services. In addition, the Federal Financial Institutions Examination Council recently issued a statement on security risk management principles for financial institutions using cloud services.

Financial institutions are required to take a life cycle view of third-party relationships using a risk-based approach appropriate to the criticality and complexity of the function. This risk management process is the purview of senior management and the board of directors. The initial steps are to consider whether the function can be safely outsourced to a third party and conducting appropriate due diligence, while maintaining robust contingency plans. Written contracts with third parties are required, and they should address the following:

Performance obligations (including quality metrics) and the consequences of the failure to perform

Notification of financial difficulty, catastrophic events and significant incidents (including security incidents)

Notification of significant changes, including acquisitions, subcontracting, offshoring, key personnel changes and material policy changes

Audit rights and requirements, including independent review

Legal and regulatory compliance, including data privacy, anti-money laundering and sanctions compliance

Fee calculations and ensuring no unduly burdensome up-front or exit fees

Exit rights

Data and IP ownership

Confidentiality and integrity of data and systems

Business continuity

Limits on liability and indemnification

Insurance

Dispute resolution

Regulatory supervision

The regulatory guidance does not mandate the substance of the terms of the parties' contract; rather, the terms are required to reflect the risk profile of the financial institution for the services contracted.

Finally, the guidance requires financial institutions to conduct ongoing monitoring of the third-party relationship. This includes a periodic assessment of the third-party relationship to determine if the services now include critical activities, and assigning staff with the requisite skills to oversee the third-party provider commensurate with the level of risk and complexity of the relationship. An ongoing risk-based monitoring program should have oversight with respect to the following:

Business strategy and reputation

Legal and regulatory compliance

Financial condition

Insurance coverage

Key personnel and institutional knowledge

Identifying and managing risk prior to audit reporting

Process for policy changes to address new threats

Response to service interruption and service quality degradation

Reliance on subcontractors

Conflicts of interest and operational and reputational risks

Confidentiality and integrity of data and systems

Trending in customer complaints and ability to remediate

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

The rules applicable for broker-dealers, investment advisers ("**IAs**") and Commodity Futures Trading Commission ("**CFTC**") regulated entities are record-keeping rules and related interpretation and guidance over third-party providers of electronic storage, rather than rules specifically designed around the concept of cloud storage.

For BDs, the core record-keeping 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 interpretation and staff guidance on electronic data storage providers, including a Division of Examinations ("Safeguarding Customer Records and Information in Network Storage — Use of Third-Party Security Features") OCIE alert. In November 2021, the SEC proposed amendments to this rule, although it does not reference cloud-related requirements specifically.

In addition for 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, which presents best practices for supervision and reminds them of functions that may not be outsourced to third parties, such as those functions that must be performed by registered persons. Even for functions that may be outsourced, FINRA member firms 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,theyare 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:

Record-keeping 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 — addressed in FINRA guidance, but only at a high level in an OCIE alert or SEC guidance

Technical and organizational measures or IT guidelines, including security requirements (e.g., encryption and key management) — only addressed in a general way through SEC and FINRA guidance

Business continuity/disaster recovery (including whether any specific BCP measures are required) — the SEC has addressed BCP largely through guidance, while FINRA has provided more specific guidance

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 time-date for the required period of retention the information placed on such 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 rule and as required by the SEC or self-regulatory organizations. An undertakingfrom the third party is a requirement of the rule.  November 2021 SEC proposed amendments to this rule could eliminate the current requirement that electronic records of BDs be stored solely in a non-rewritable, non-erasable format, also known as "write once, read many" (or WORM) format. The undertaking may also be removed from the rule should amendments be finalized as proposed.

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

**CFTC/NFA**

The core record-keeping rules are CFTC Rule 1.31 (in particular, Rule 1.31(c)-(d)) and NFA Rule 2-10. Generally, records must be retained in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with applicable law. Electronic records systems must include: (i) systems that maintain the security, signature and data as 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 such 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 information necessary for accessing or producing electronic regulatory records.

Such records must be available to the regulator promptly upon request in a reasonable form and medium in which the CFTC entity must produce such regulatory records.

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?

For banking institutions, please see the response to question 2 on whether any rules apply to cloud use by financial institutions. Banking regulators have not mandated specific provisions but, consistent with a risk-based approach, they have identified subject areas that third-party contracts should address to be consistent with the risk profile of the institution and the functions involved.

Generally, an outsourcing entity should enter into an appropriate agreement with its cloud service provider that sufficiently manages the risk associated with sharing clients' "nonpublic personal information" ("**NPPI**") across country borders and prevents sharing clients' NPPI with third parties.

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?

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 rulemaking. 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 the use of third parties for record-keeping 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, which 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 rulemaking. 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 record-keeping 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?

Banks are not required to notify regulators prior to engaging third parties to perform services, including cloud computing.

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 in respect of outsourcing.

With respect to entities regulated by the Commodity Futures Trading Commission ("**CFTC**")/National Futures Association, there is no explicit notification requirement with respect to 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 Office of the Comptroller of Currency ("**OCC**") has fined banks for failing to maintain and exercise adequate risk management programs, including loss mitigation policies. It has also issued fines for the failure to exercise adequate oversight of disengagement from third-party providers. The OCC has levied substantial fines against banks in connection with the lax information security practices of bank subsidiaries in connection with customer data breaches. Fines for egregious conduct have exceeded USD 80 million.

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 the 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 the failure of firms 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 thereafter, 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 such 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 Office of the Comptroller of the Currency ("**OCC**") has adopted the Interagency Guidelines Establishing Information Security Standards at 12 C.F.R., Part 30, Appendix B. The Interagency Security Standards require a bank using a cloud service provider to address service provider information security before signing a contract, as part of the terms of the contract, and on an ongoing basis after establishing a service provider relationship.

The Federal Financial Institutions Examination Council ("**FFIEC**") has published a guidance booklet on outsourcing practices, and it states that financial institutions may outsource many areas of operations, including all or part of any service, process or system operation. However, the use of a subcontractor or, in this case, a cloud service provider does not diminish the responsibility of the financial institution's senior management to ensure that the subcontractor's activity is conducted in a safe manner and in compliance with applicable laws and regulations.

That same FFIEC guidance warns, however, that financial institutions must not share US regulatory examination reports or information contained therein with either foreign regulators or foreign-based service providers without the express written approval of the appropriate US regulatory authority. The FFIEC recently issued the "Security in a Cloud Computing Environment" bulletin, which addresses key risks in cloud computing. Although this bulletin does not contain new regulatory expectations, it highlights examples of risk management practices related to the safe use of cloud computing services, and directs financial institutions to also review the FFIEC's IT Handbook and other documents providing general information on best industry practices.

Regarding broker-dealers ("**BDs**") and investment advisers ("**IAs**"), Securities and Exchange Commission ("**SEC**") Regulation SP and Regulation S-ID apply to both BDs and 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. Foreign-based cloud service providers, however, 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.

In addition, sharing US regulatory examination reports with foreign regulators or foreign-based cloud service providers without the express written approval of the appropriate US regulatory authority is prohibited.

# 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 consents are 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 the privacy laws of other countries cannot serve asa 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 longstanding 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 those materials to 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. The legal assessment courts perform in these types of cases, however, 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. Even when such a showing is made, however, 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 utilize 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 governing 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 such 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 later be adopted.

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 the data of foreign entities under the CLOUD Act, 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 jurisdiction of the US.

©Copyright © 2024 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.