Cloud Compliance Center - United States

Rules for cloud outsourcing

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

# 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.

©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.