NEBRASKA
Good Life. Great Opportunity.
DEPARTMENT OF BANKING AND FINANCE

Proposed Digital Asset Depository Nebraska Supervision Process Handbook

Nebraska Department of Banking and Finance

Version 1.0 – October 2022

Table of Contents

1. Introduction

The Nebraska Department of Banking and Finance (or "the Department") is responsible for the supervision of Digital Asset Depository ("DDs") chartered under the Nebraska Financial Innovation Act ("NFIA"). The Department's vision is to make Nebraska the most trusted financial home for both people and businesses. In accordance with this vision, its mission includes the protection and maintenance of public confidence through fair, efficient, and experienced supervision of state-regulated financial services industries, which entails regulating such industries in a manner that allows them to remain competitive while maintaining safety, soundness, and compliance with the law. Moreover, the NFIA seeks to attract digital asset operations to the state of Nebraska and recognizes that authorizing digital asset depositories in Nebraska will provide a necessary and valuable service to blockchain innovators and prospective customers.

To support its mission and the aims of the NFIA, the Department has prepared this "DD Supervision Process Handbook" (or "DD Handbook") for use by Department examiners in connection with their supervision of DDs.[1]

The purpose of this DD Handbook is to provide an overview of the Department's DD charter-specific supervision process, including specific areas tailored to considerations around digital assets. As part of the overall supervisory process, the Department will determine whether the risks a DD undertakes or plans to undertake are warranted; whether they can be identified, measured, monitored, and controlled by the DD; and whether they are within the DD's capacity to readily withstand in the event of adverse performance.

Philosophical Approach to Supervision

The state of Nebraska and the Department recognize the opportunities associated with the provision of digital asset services, and in particular, the high-skill, high-wage job opportunities associated with this innovative new industry.[2] The state of Nebraska strives to be a leader in financial innovation and acknowledges that digital asset and "fintech" services will bring Nebraska into the future, helping the state attract entrepreneurs and investment. However, the state and the Department, in enacting the NFIA, recognize that innovative new forms of financial services raise unique safety and soundness considerations, and therefore remain committed to responsible regulation and supervision, including enforcement of Know Your Customer ("KYC") requirements, prohibitions on certain lending activities, and increased capital requirements to

[1] The DD Supervision Process Handbook leverages the Office of the Comptroller of the Currency (or "OCC")'s Comptroller's Handbook – Bank Supervision Process (Version 1.1, September 2019), the Federal Deposit Insurance Corporation's (or "FDIC") Risk Management Manual of Examination Policies, and relevant Nebraska regulation, including the Nebraska Financial Innovation Act, §§ 8-3001 – 8-3031 and the Nebraska Revised Statutes, Chapter 8, governing Banks and Banking. In certain instances, where the DD Supervision Process Handbook references "banks" in the context of OCC and FDIC guidance, examiners can treat this guidance as referring to DDs.

[2] Nebraska Legislature, "Transcript Prepared by Clerk of the Legislature Transcribers Office Banking, Commerce and Insurance Committee" (February 2021).

protect consumers. Accordingly, the NFIA, and the supervision thereof, revolves around three core guiding principles:

1. Enabling innovation and economic development in the state;
2. Providing legal certainty; and
3. Enhancing consumer protections and compliance with federal and state law.

The Department's philosophical approach is consistent with federal guidance, including guidance adopted by the Office of the Comptroller of the Currency ("OCC"), which notes:

> First, any regulation adopted should be technology-neutral, so that products, services, and processes can evolve regardless of the changes in technology that enables them. Second, any regulation should facilitate appropriate levels of consumer protection and privacy, including features that ensure transparency and informed consent. Finally, regulations on digital activities should be principle-based, rather than prescriptive, to enable effective management of evolving risks and to reduce the potential that the regulations quickly become outdated.[3]

This approach is consistent with Nebraska's vision of becoming the most trusted financial home for both people and businesses.

Structure of Manual

To support Department examiners and to ensure compliance with state and federal banking standards, the Department supervisory process builds on the core structure of the OCC's Supervision Process, and overlays this with Nebraska-specific laws, rules, and guidance, where applicable, tailoring requirements to address the unique nature and inherent risks of digital assets. The DD Handbook consists of the following sections:

- Introduction
- Risks Associated with Digital Assets / the Risk Assessment System ("RAS")
- Risk-based Supervision
- Supervisory Actions
- Regulatory Ratings
- Recovery and Resolution Planning
- Disaster Recover and Business Continuity Planning

1.1. Nebraska Department of Banking and Finance

The Nebraska Department of Banking and Finance regulates and supervises the state-chartered financial institutions of Nebraska, including DDs. The Director of the Department of Banking and

[3] Department of Treasury, Office of the Comptroller of the Currency. "Advanced Notice of Proposed Rule-Making: National Bank and Federal Savings Association Digital Activities." (2020).

Finance (the "Director") has the power to issue DD charters under the NFIA and has general supervision and control over these DDs.[4] Furthermore, the NFIA imbues the Director with the authority to "issue any order and adopt and promulgate any rules and regulations necessary to implement the [NFIA]."[5] Per Nebraska law, the Director has "charge of and full supervision over the examination of and the enforcement of compliance with" relevant state regulation and statutes by banks, trust companies, and other financial institutions, including DDs,[6] however, any bank or trust company, including DD, "may become a member of the federal reserve system…and may assume such liabilities and exercise such powers as a member of such system..." Where the DD "remain[s] a member of such system, it shall be subject to examination by the legally constituted authorities, and to all provisions of such Federal Reserve Act and regulations made pursuant thereto by the Federal Reserve Board…and…[t]he Director may, in his or her discretion, accept examinations and audits made under the provisions of the Federal Reserve Act in lieu of examinations required of banks or trust companies organized under the laws of [the State of Nebraska].[7] Accordingly, DDs will generally be subject to state and federal laws governing banks and trust companies and will therefore be supervised in a manner similar to other state and national banks or trust companies engaged in deposit-taking, custodial, and fiduciary activities.

On-Site Supervision

The NFIA states that "[e]very digital asset depository is subject to examination by the department to determine the condition and resources of a digital asset depository, the mode of managing digital asset depository affairs and conducting business, the actions of officers and directors in the investment and disposition of funds, the safety and prudence of digital asset depository management, compliance with the requirements of the Nebraska Financial Innovation Act, and such other matters as the Director may require."[8] In accordance with this provision, each DD will be subject to a full-scope examination conducted by the Department, and if a member of the federal reserve system, by the Department and the Federal Reserve System, at least every twelve (12) months during its first three (3) years of operations, i.e., the *de novo* period. Additionally, the Department may choose more frequent targeted examinations at the discretion of the Director where the DD exhibits practices that raise concerns of unsafe or unsound conditions, warranting a more frequent or targeted examination. After the *de novo* period has concluded, the Director will determine whether an eighteen-month cycle may be appropriate in certain circumstances, based on the size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology relating to a particular institution.

For *de novo* DDs, some combination of supervisory conditions and enhanced supervision is usually warranted until the DD has achieved financial and operational stability. *De novo* status is not removed until the DD achieves stability with regard to earnings, core business operations, and management. The Department generally follows existing federal standards for its assessment of

[4] Neb. Stat. §8-3004 (LB 646, 2021)
[5] Neb. Stat. §8-3031 (LB 646, 2021)
[6] Neb. Rev. Stat. § 8-103
[7] Neb. Rev. Stat. § 8-130
[8] Neb. Stat. §8-3023(3) (LB 646, 2021)

DDs *de novo* status,[9] including activity restrictions and heightened supervision during this period, with the typical *de novo* period projected to occur over a three-year period absent changes to the DD's business plan or the identification of material weaknesses.

Each full-scope examination will include summary reviews of the DD's status against federal standards for the OCC's categories of risk (or Risk Assessment System ("RAS"): credit, interest rate, liquidity, price, operational, compliance (including legal), strategic, and reputational risk. Given the reliance on emergent technologies for a DD's operations and activities, the Department also embeds considerations around technology risk under the operational, compliance, reputation, and strategy risk assessments.

The Department will also conduct a CAMELS-ITCC review, assessing the DD for: (1) Capital, (2) Asset Quality, (3) Management, (4) Earnings, (5) Liquidity, and (6) Sensitivity to Market Risk, as well as Information Technology ("IT") and Compliance with the NFIA. Depending on the operations of the DD, the Department may also conduct a Uniform Interagency Trust Rating System ("UITRS") trust examination.

Given the recognition of unique risks associated with digital assets and the novelty of permissible DD activities, the Department also provides more detailed assessments of certain additional topic areas:

- Custody and Fiduciary Services
- Information Security
- Payment Systems Risk
- AML/CFT and OFAC Compliance

[1]It is noted that in January 2021, Congress passed the AML Act of 2020, which required U.S. Department of the Treasury's Financial Crimes Enforcement Network or FinCEN (in consultation with Federal functional regulators) to promulgate AML/CFT regulations. Due to the addition of the CFT, FinCEN is generally now using the term AML/CFT instead of AML/CFT. For consistency with FinCEN and the other Federal banking agencies, the Department will use the term AML/CFT (which includes AML/CFT) instead of AML/CFT when referring to, issuing, or amending regulations to address the requirements of the AML Act of 2020.

Department examiners should refer to the examination manuals and procedures for each of the above listed topic areas.

Ongoing Department Supervision

The NFIA grants the Director the right to "call for reports verified under oath from a digital asset depository at any time as necessary to inform the Director of the condition of the digital asset depository" and further stipulates that "such reports shall be available to the public."[10] Accordingly, the Department requires each DD to submit call reports on a quarterly basis that generally follow the standard call report structure but include specific additional line items relevant to DDs, such as stablecoin reserve ratios.

Consistent with the Director's authority under the NFIA, the Director and Department may require additional reporting from DDs beyond quarterly call reports. Where required, the Department

intends to focus these reporting requirements on assessing the safety and soundness of DD operations while aiming to streamline reporting requirements and reduce the DDs' compliance burdens.

Additional supervisory measures include, but are not limited to:

- Ad hoc meetings or calls between the DD and the Department;
- Follow-up on results from examination reports, independent testing results, or other sources, as well as appropriate remedial action; and
- Regular update calls with other relevant regulators (U.S. market regulators and other state, federal, and foreign bank regulators, as appropriate).

[9] FDIC. *Enhanced Supervisory Procedures for Newly Insured FDIC-Supervised Depository Institutions* (August 28, 009).
[10] Neb. Stat. §8-3023(1) (LB 646, 2021)

1.2. DD Background

In January 2021, Senator Michael Flood introduced Bill 649 to the Nebraska Legislature proposing the adoption of the Nebraska Financial Innovation Act that would authorize the creation of digital asset depositories and provide for the chartering, operation, supervision, and regulation of such institutions by the Nebraska Department of Banking and Finance.[11] The intent of the bill, as described by Senator Michael Flood to the Committee on Banking, Commerce and Insurance was to enable the state of Nebraska "to leap to the forefront of financial innovation" by "passing legislation to recruit digital asset companies to invest and grow" in the state.[12] On May 26, 2021, Nebraska became the second state to pass legislation authorizing digital asset depositories (LB649). The NFIA is the state of Nebraska's chosen statutory framework designed to encourage the creation of Nebraska DDs, protect digital asset consumers, preserve confidence in Nebraska Financial Institutions, and promote financial technology ("FinTech") innovation.[13]

The NFIA allows two ways to create a digital asset depository or DD:

1) A business may be organized and apply for a Nebraska Digital Asset Depository Institution Charter, or
2) An existing Nebraska Chartered Financial Institution may apply for authority from the Director to operate a Digital Asset Depository "Department".

Authorization of DDs became operative October 1, 2021, while sections amending the Nebraska Uniform Commercial Code to include "controllable electronic records", otherwise known as digital assets, including definitions, perfection, control and discharge of security rights in digital assets, became effective on July 1, 2022.[14]

Permissible Activities

The NFIA specifies that a DD is authorized to provide digital asset and cryptocurrency custody services. Additionally, DDs may issue stablecoins, carry on a nonlending digital asset banking

[11] Nebraska Legislature, Legislative Journal, One Hundred Seventh Legislature, First Session, (January 2021).
[12] Nebraska Legislature, One Hundred Seventh Legislature, First Session, Introducer's Statement of Intent LB648, (February 2021).
[13] Nebraska Department of Banking and Finance, Notice Regarding Availability of NDBF Draft of Digital Asset Depository Application: Business Plan, (April 2022).
[14] Nebraska Legislature, Legislative Journal, One Hundred Seventh Legislature, First Session, Committee Statement LB649 (February 2021).

business for customers, and provide payment services upon request of a customer. Finally, though prohibited from fiat currency lending, a DD may facilitate the provision of digital asset business services resulting from the interaction of customers with centralized finance or decentralized finance platforms including, but not limited to, controllable electronic record exchange, staking, controllable electronic record lending, and controllable electronic record borrowing.[15] Examples of other facilitation activities may include trading or exchanging of digital assets as well as providing sub-custodian services. Refer to *Section 10. Asset Lending* of the *DD Custody and Fiduciary Examination Manual* for more information on the facilitation of asset lending transactions on behalf of custody customers.

A DD shall consult with the Director and seek any necessary approval, before engaging in a substantially new activity or line of business. The activities of a particular DD will be evaluated for their consistency with law and supervisory guidance and safety and soundness, including institution management, earnings, information technology, operational controls, and AML/CFT and OFAC compliance.

1.3. Digital Assets/Controllable Electronic Records Under the NFIA

The NFIA defines controllable electronic records as "an electronic record that can be subjected to control," noting that "the term has the same meaning as digital asset and does not include electronic chattel paper, electronic documents, investment property, and transferable records under the Uniform Electronic Transactions Act."[16] Further, the NFIA recognizes that digital assets/controllable electronic records are recorded on the blockchain, which it defines as a "distributed digital record of controllable electronic record transactions."[17]

Examples of technological and design features of digital assets in contrast to other traditional asset classes include:[18]

- **Digital / virtual nature**: Digital assets are digital in their nature, and do not possess physical characteristics (in contrast, to say, banknotes or coins). As such, they are typically transferred, stored, and traded electronically.

- **Reliance on cryptography**: Digital assets rely primarily on cryptography and advanced mathematical techniques to restrict the transmission of data to the relevant intended parties. As explained by the Bank of International Settlements ("BIS"), "Examples of cryptographic tools include symmetric encryption cryptography (which relies on the same digital key to create and verify cryptographic signatures data), asymmetric encryption cryptography (which relies on different keys), and hashing (to verify the integrity of data);"[19]

[15] LB 649, Nebraska Legislature. "Legislative Bill 649: Nebraska Financial Innovation Act" (2021).
[16] Neb. Stat. §8-3003 (LB 646, 2021)
[17] *Ibid.*
[18] Bank for International Settlements – Basel Committee on Banking Supervision. *Discussion Paper: Designing a Prudential Treatment for Crypto-Assets* (December 2019). Refer to this discussion paper for additional considerations around economic functions and potential sources of value of crypto-assets.
[19] Ibid.

- **Use of distributed ledger technology**: Digital assets typically rely on distributed ledger technologies or similar technologies to administer and record information and data.

- **Consensus mechanism**: All digital assets which rely on distributed ledger technology (or "DLT") systems have a mechanism that allows a number of participants – who trust each other only to a limited extent – to agree on the current state of the system.

The digital asset ecosystem can enable users to create, store, and transfer digital assets without the need for any third-party intermediary such as a financial institution. Further, the nature of many digital assets allows for pseudonymous and irreversible transactions, where transactions can take place absent customer information and are generally immutable and irreversible (meaning that such transactions are typically push-based and can only be returned by the receiver of the transaction rather than a third party or intermediary). Absent tailored mitigating controls, institutions engaging with digital assets, can be exposed to significant risks in light of these unique inherent characteristics.

2. Risks Associated with Digital Asset Depository Institutions

Given the novelty of permissible activity associated with the DD charter, the Department expands upon certain federal and state standards with respect to its examination approach. At a high level, the Department aligns its supervisory approach to existing federal, inter-agency guidance[20] where available, and supplements this approach through state rules, industry guidance, and other jurisdictional approaches, where appropriate, to account for nuances and unique inherent risks associated with DDs.

This section follows with an overview of the OCC's eight key categories of risk for bank supervision,[21] flagging additional digital asset-specific criteria as identified by the Department:

1. Credit Risk.
2. Interest Rate Risk.
3. Liquidity Risk.
4. Price Risk.
5. Operational Risk.
6. Compliance/Legal Risk.
7. Reputation Risk.
8. Strategic Risk.

As noted by the OCC, these categories are not meant to be mutually exclusive, and an institution's activity, whether through its products and services, customers, geographies, or distribution channels, may expose the institution to multiple risks. While such risks may be identified and assessed separately, Department examiners should not consider these risks in silos. Instead, these categories serve as a method through which Department examiners identify, evaluate, document, and communicate judgements to DDs related to the quantity of risk and quality of risk management processes.[22] While Department examiners will be required to form their own conclusions with respect to these eight risk categories, Department examiners may use the results of a DD's internal audit and third party assessment reports as well as any risk and compliance self-assessments performed by the DD, to inform their conclusions.

2.1. Credit Risk

Credit risk arises from the potential that a borrower or counterparty will fail to perform on an obligation in accordance with agreed terms. Credit risk is found in all activities in which settlement or repayment depends on counterparty, issuer, or borrower performance. Credit risk exists any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether reflected on or off the balance sheet. Credit risk is the most recognizable risk associated with traditional banking. This definition encompasses more than the traditional definition associated with lending activities. Credit risk also arises in conjunction with a broad range of bank activities, including selecting investment portfolio products, derivatives

[20] This includes the OCC's Asset Management (AM) Unique and Hard-to-Value Assets (August 2012).
[21] Office of the Comptroller of the Currency, "Categories of Risk", NR 96-2, (January 1996).
[22] See the OCC's *OCC Bulletin. OCC 98-3, Technology Risk Management, Guidance for Bankers and Examiner* (February 4, 1998).

trading partners, or foreign exchange counterparties. Credit risk also arises due to country or sovereign exposure, as well as indirectly through guarantor performance[23].

The Department expects DDs to develop and maintain robust processes to ensure that their capitalization remains consistent with Nebraska statute and the requirements set by the Director, and that any activities that DD customers take part in do not create credit risk via counterparty exposure to the DD or through other means.

A DD cannot make any consumer loans for personal, property, or household purposes, mortgage loans, or commercial loans of any fiat currency and the provision of temporary credit relating to overdrafts. A DD, however, may facilitate the provision of digital asset business services resulting from the interaction of customers with centralized finance or decentralized finance platforms including, but not limited to, controllable electronic record exchange, staking, controllable electronic record lending, and controllable electronic record borrowing.[24]

If the DD facilitates digital asset lending, the Department examiners should address the following credit-related considerations:

- Does the DD face meaningful counterparty credit risk?
  - Is the DD providing indemnification guarantees?
  - Does the DD's fiduciary liability for digital asset lending transactions include certain elements of credit risk as a result of a fiduciary duty breach?
  - How does the DD select counterparties when facilitating lending activities? See the *DD Custody and Fiduciary Examination Manual* for further information.
- What types of affiliates or third-party exposure does the DD face that may present credit quality issues through its affiliate network?
- If the DD interacts with decentralized protocols, including borrowing from decentralized protocols, or participating in liquidity pools, has the DD addressed risk exposure associated with price volatility in collateral provided to lending protocols?
- Did the DD establish separate reserve or liability accounts to protect against potential losses?

Based on the above considerations and any another applicable factors, Department examiners should develop the following conclusions:

- Quantity of credit risk (low, moderate, or high).
- Quality of credit risk management (strong, satisfactory, insufficient, or weak).
- Aggregate credit risk taking into consideration credit risk exposures and quality of credit risk management controls (low, moderate, high).
- Direction of credit risk over the next 12 months (decreasing, stable, or increasing).

2.2. Interest Rate Risk

[23] Refer to OCC Comptroller's Handbook "Large Bank Supervision", (January 2010)
[24] Neb. Stat. §8-3005(2)(b) (LB 646, 2021)

Interest rate risk is the risk to current or projected financial condition and resilience arising from movements in interest rates. Interest rate risk results from differences between the timing of rate changes and the timing of cash flows (repricing risk); from changing rate relationships among different yield curves affecting bank activities (basis risk); from changing rate relationships across the spectrum of maturities (yield curve risk); and from interest-related options embedded in bank products (options risk).

The assessment of interest rate risk should consider risk from both an accounting perspective (i.e., the effect on the bank's accrual earnings) and an economic perspective (i.e., the effect on the market value of the bank's portfolio equity). In some banks, interest rate risk is included in the broader category of market risk. In contrast with price risk, which focuses on portfolios accounted for primarily on a mark-to-market basis (e.g., trading accounts), interest rate risk focuses on the value implications for accrual portfolios (e.g., held-to-maturity and available-for-sale accounts).

NFIA allows DDs to hold highly liquid securities (e.g., Treasuries and Agencies) as reserve for issued stablecoins, which could potentially create a duration mismatch. The Department will review the reserve composition to ensure that investments are managed prudently, consistent with safe and sound banking practices, in a manner that addresses interest rate risk, including gap, basis and options risk, and accounts for potential stress scenarios. Although on its face, DDs may not face high levels of interest rate risk based on the nature of the DD's business activities, Department examiners should assess the DD's holdings and proposed or current activity to make this determination with each on-site examination. Although DDs are required to hold liquid assets[25] in order to match depository liabilities, the composition of these holdings may present different risks to the DD.

Additional considerations pertaining to interest rate risk include:

- Does the DD adequately manage repricing, basis, yield curve and options risk?
- What types of fiat-based exposure does the DD have based on the composition of its different reserves? What risks do these currently pose given different adverse conditions?
- Does the DD have any hedging activity or foresee any impacts to existing or proposed activities in the event of an interest rate event?
- Does the DD have adequate planning for interest rate events or stress scenarios that can minimize potential safety and soundness concerns?

Based on the above considerations and any another applicable factors, Department examiners should develop the following conclusions:

- Quantity of interest rate risk (low, moderate, or high)
- Quality of interest rate risk management (strong, satisfactory, insufficient, or weak).
- Aggregate interest rate risk taking into consideration interest rate risk exposures and quality of interest rate risk management controls (low, moderate, high).
- Direction of interest rate risk over the next 12 months (decreasing, stable, or increasing).

[25] Refer to the Liquidity Risk section of this Handbook.

2.3. Liquidity Risk[26]

Liquidity is a DD's capacity to readily meet its cash and collateral obligations at a reasonable cost. Liquidity risk reflects the possibility an institution will be unable to obtain funds, such as customer deposits or borrowed funds, at a reasonable price or within a necessary period to meet its financial obligations. Failure to adequately manage liquidity risk can quickly result in negative consequences for an institution despite strong capital and profitability levels.[27] Liquidity risk also includes the inability to access funding sources or manage fluctuations in funding levels. Liquidity risk also results from an institution's failure to recognize or address changes in market conditions that affect its ability to liquidate assets quickly and with minimal loss in value.

The nature of liquidity risk has changed in recent years. Increased investment alternatives for retail depositors and sophisticated off-balance-sheet products with complicated cash-flow implications are examples of factors that complicate liquidity risk. To efficiently support daily operations and provide for contingent liquidity demands, DDs must[28]:

- Establish an appropriate liquidity risk management program,
- Ensure adequate resources are available to fund ongoing liquidity needs,
- Establish a funding structure commensurate with risks,
- Evaluate exposures to contingent liquidity events, and
- Ensure sufficient resources are available to meet contingent liquidity needs.

The Nebraska Financial Innovation Act requires the DD to maintain unencumbered liquid assets denominated in United States dollars valued at no less than one hundred percent of the value of any outstanding stablecoins issued by the digital asset depository[29]. The definitions of liquid assets are the following:

1) United States currency held on the premises of the digital asset depository that is not a digital asset depository institution;

2) United States currency held for the digital asset depository by a federal reserve bank or a Federal Deposit Insurance Corporation-insured financial institution which has a main-chartered office in [the state of Nebraska], any branch thereof in [the state of Nebraska], or any branch of the financial institution which maintained a main-chartered office in [the state of Nebraska] prior to becoming a branch of such financial institution; or

3) Investments which are highly liquid and obligations of the United States Treasury or other federal agency obligations, consistent with rules and regulations or order adopted by the Director.

[26] Refer to OCC Comptroller's Handbook "Liquidity" (August 16, 2021)
[27] Refer to FDIC, Risk Management Manual of Examination Policies: Section 6.1 Liquidity and Funds Management (October 2019).
[28] Refer to FDIC, Risk Management Manual of Examination Policies: Section 6.1 Liquidity and Funds Management (October 2019).
[29] Nebraska Legislature, Amendments to LB707 (Amendments to Standing Committee amendments, AML1859), AM2205 LB649 (March 2022).

The Department draws upon existing federal guidance around risks associated with new activities (with reference to digital assets), which include:

- "new activities include the use of investment alternatives for retail depositors or sophisticated off-balance-sheet products with complicated cash-flow implications.
- an offered product or service affects current or future funding costs, introduces or increases the volatility of asset/liability mismatches that are inappropriately hedged or managed, increases the rate of credit-sensitive liabilities, or affects a bank's ability to meet collateral obligations."[30]

Given the nature of DD activity and the off-balance sheet nature of activity, additional considerations pertaining to liquidity risk include:

- How are liquidity reserves tracked?
  - Based on the DD's activity, are there assets that have less liquidity under certain scenarios?
  - Does the DD perform independent audits for proof of reserves?
- How does the DD assess risks based on price volatility for its different digital assets offerings?
- Has the DD appropriately selected investment assets that appropriately reflect existing or expected transaction volumes and values and velocity of deposits and custodial or fiduciary assets?
- Based on its product offerings, does the DD have any agreements in place that allow for early termination/return or other terms and conditions where it faces liquidity events? If so, how does the DD account for such instances (e.g., where the DD may face contractual mismatches and be required to assume contracts and refund customers)?
- Does the DD have appropriate planning for liquidity events, including as it relates to customers with large balances or periods of high digital asset volatility or trading activity?

Based on the above considerations and any another applicable factors, Department examiners should develop the following conclusions:

- Quantity of liquidity risk (low, moderate, or high).
- Quality of liquidity risk management (strong, satisfactory, insufficient, or weak).
- Aggregate liquidity risk taking into consideration liquidity risk exposures and quality of liquidity risk management controls (low, moderate, high).
- Direction of liquidity risk over the next 12 months (decreasing, stable, or increasing).

2.4. Price Risk

Price risk is the risk to current or projected financial condition and resilience arising from changes in the value of either trading portfolios or other obligations that are entered into as part of

[30] Refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

distributing risk. These portfolios typically are subject to daily price movements and are accounted for primarily on a mark-to-market basis. This risk occurs most significantly from market-making, dealing, and position-taking in interest rate, foreign exchange, equity, commodities, and credit markets.

Price risk also arises from DD activities whose value changes are reflected in the income statement, such as in lending pipelines, other real estate owned, and mortgage servicing rights. The risk to earnings or capital resulting from the conversion of a DD's financial statements from foreign currency translation also should be assessed under price risk. As with interest rate risk, many DDs include price risk in the broader category of market risk.

Particularly given historical price volatility associated with digital assets, quickly changing prices of virtual currencies or other digital assets could present material risks to a DD's overall earnings. As such, considerations based on the DD's proposed or existing activities include:

- What measures are in place to address significant fluctuations in price (on a short-term or long-term basis)?
- What kinds of concentration risks does the DD face to specific digital asset types?
    - What kind of impact could such concentrations have on earnings in the event that there is a large increase or decrease in price for digital assets where the DD has exposure (e.g., via custody fees)?
    - Similarly, what is the impact of price volatility on fiat-based assets held, such as Treasuries?

Based on the above considerations and any another applicable factors, Department examiners should develop the following conclusions:

- Quantity of price risk (low, moderate, or high).
- Quality of price risk management (strong, satisfactory, insufficient, or weak).
- Aggregate price risk taking into consideration price risk exposures and quality of price risk management controls (low, moderate, high).
- Direction of price risk over the next 12 months (decreasing, stable, or increasing).

2.5. Operational Risk

Operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events. Operational loss events may result from internal fraud; external fraud; inadequate or inappropriate employment practices and workplace safety; failure to meet professional obligations involving clients, products, and business practices; damage to physical assets; business disruption and systems failures; and failures in execution, delivery, and process management (which can result from failed transaction processing or process management or losses arising from relations with trade counterparties and vendors.[31] Operational losses do not include opportunity costs,

[31] 12 CFR § 1240.101

forgone revenue, or costs related to risk management and control enhancements implemented to prevent future operational losses.

Firms can strengthen their operational resilience by identifying, measuring, monitoring, and controlling operational risk exposures related to internal processes, people, systems, external threats, and third parties. Effective operational risk management involves close engagement by the firm's senior management, business line operations, independent operational risk management function, and independent internal (or external) audit function to assess, identify, mitigate, and resolve operational disruptions, consistent with the firm's risk tolerance standards.[32]

Given the unique inherent risks associated with digital assets, the Department places a heightened emphasis on operational risk management, with special consideration around transaction risk, Information Technology (or "IT") and information security (or "InfoSec"), custody (such as key management), third-party risk management, and other digital assets-specific considerations. Further, the Department recognizes that specialized industry expertise is required for the DD's management and oversight of its unique operational risks, including through audit and model risk management. Accordingly, the Department expects DDs to have a clearly documented and audited operational risk management program, inclusive of methods for identifying, measuring, monitoring, and controlling operational risk, as well as procedures pertaining to operational risk management, development of an operational risk assessment, and management information systems reporting and escalations related to operational risk. Moreover, the Department expects DDs to establish clear risk tolerance standards around operational risks to inform management reporting and escalations.

As noted above operational risk includes transaction risk, which is the risk to earnings or capital arising from problems with service or product delivery. Technology can give rise to transaction risk in many ways, particularly in the digital asset space. Transaction risk often results from deficiencies in system design, implementation, or ongoing maintenance of systems or equipment, but in the case of digital assets, transaction risk can also occur, or be exacerbated by, underlying features of a given blockchain. Given that DDs will be processing both fiat and digital asset transactions, their transaction risk will be two-fold. In both instances, incompatible internal and external systems and, in the case of digital assets, tokens and custodial infrastructure, all serve to increase transaction risk. This transaction risk may increase if the DD relies on vendor solutions or hires outside contractors to design products, services, delivery channels, and processes that do not fit within its existing system architecture. The failure to establish adequate security measures, contingency plans, testing, and auditing standards also increases transaction risk. [33]

Due to the unique nature of digital assets and the variability in blockchain protocols associated with different assets, a number of unique transaction risk considerations may apply:

- Transaction authorization/signing and immutability of transactions (e.g., fraudulent, or inadvertent authorization for fund movement and associated transaction irreversibility);

[32] OCC. OCC Bulletin 2020-94, Sound Practices to Strengthen Operational Resilience (October 2020).
[33] See the OCC's, OCC Bulletin. OCC 98-3, Technology Risk Management, Guidance for Bankers and Examiner (February 1998).

- Storage of digital assets based on hardware security module capabilities (e.g., incompatibility in custody system architecture and supportable digital assets);
- Infrastructural and/or network limitations/failures (e.g., cloud computing/storage limitations and/or failures, transaction finality and network congestion, single points of failure through interoperable blockchain services such as bridges[34], oracles[35], and scaling solutions[36]); and
- Blockchain protocol technical limitations/failures (e.g., source code errors/bugs, smart contract throughput limitations), as well as protocol updates (e.g., hard forks).

As part of the DD transaction risk evaluation, Department examiners should review the documentation established by a DD's operational risk function, including its assessment of critical operations and core business lines, as well as the extent of exposure to various operational risks faced by the firm, including both on-chain and off-chain operational risks, as well as the controls that the DD's various risk functions have implemented to readily identify and mitigate such risk exposures (e.g., policies around transaction pausing and disclosures, hardware security module controls, code reviews for smart contract interoperability and scaling solutions, etc.). Examiners may also consider transaction-related risks with respect to IT and InfoSec as well as custody implications, and consult the relevant examination manuals accordingly:

- **Information Technology and Information Security**. Depending on their activities, DDs may also have exposure to various blockchain and protocol limitations that may heighten transaction risk exposures. Refer to the *DD Information Security Examination Manual* for additional considerations around InfoSec and, in particular, private key management and transaction authorization. The Department should assess the degree to which the DD's IT and InfoSec processes mitigate the relevant transaction risk.

- **Custody.** Depending on the nature of the DD's transactions, the DD may face certain digital-asset specific transaction considerations, including around smart contracts and source codes for underlying blockchain protocols. Refer to the *DD Custody and Fiduciary Examination Manual* for more information.

As part of the Department's review of a DD's operational risk controls, Department examiners will leverage existing operational risk considerations as appropriate from the *DD Payment System*

[34] Cross-chain bridges, blockchain bridges, token bridges, or simply bridges, are interoperability solutions designed to enable the transfer of digital assets from one blockchain to another by creating a representation of the digital asset that needs to be transferred into a token on the target blockchain while freezing/limiting the capability of said token on the original blockchain to prevent double-spend.

[35] Oracles are look-up mechanism solutions that enable token developers to query off-chain data/information and incorporate this information into a smart contract to trigger a certain command (e.g., disbursement of funds, setting a collateralization ratio, etc.). Common oracles include pricing oracles that query the listing price of a particular digital asset from multiple large public exchanges to power decentralized finance automated market makers.

[36] Scaling solutions, also referred to as "Layer 2" solutions, are built on top of an existing "Layer 1" blockchain (settlement layer) to improve transaction speed and load on a single blockchain.

Risk Examination Manual, DD *Information Security Examination Manual,* and the *DD Custody and Fiduciary Examination Manual.*

In addition to specific operational risk considerations denoted above, the Department is especially cognizant of unique third-party risks associated with DDs. These additional risk considerations are outlined in greater detail below.

2.5.1. Third Party Risk[37]

A third-party relationship is any business arrangement between a financial institution and another entity, by contract or otherwise.[38] Recognition of third-party risk is vital to operational resilience.[39] Financial institutions are expected to practice effective risk management regardless of whether they perform an activity internally or through a third party. Moreover, the use of third parties does not diminish a financial institution's responsibility to perform the activity in a safe and sound manner and in compliance with applicable laws and regulations.[40] However, third-party relationships create unique risk management challenges by increasing a financial institution's exposure to operational risk given that the financial institution may not have direct control of the activity or activities performed by a third party. Further, operational risk can increase significantly when third-party relationships result in concentrations, i.e., when an institution relies on a single third party for multiple activities, particularly when several of the activities are critical to the institution's operations,[41] as in the case where a financial institution relies on its affiliate for the execution of centralized controls. In addition to operational risk exposure, third-party relationships may also pose legal/compliance, reputational, strategic, and credit risks. Such extant risks may manifest where a financial institution fails to conduct effective due diligence and ongoing oversight of third parties that act on behalf of the financial institution.

A financial institution's third-party risk management should be commensurate with the level of risk and complexity of its third-party relationships; the higher the risk of the individual relationship (e.g., if the relationship entails the performance of critical activities), the more robust the third-party risk management should be for that relationship. Activities are typically considered critical and therefore requiring of more comprehensive and rigorous oversight include: i) significant banking functions, such as payments, clearing, settlement; ii) outsourcing of entire lines of business or products; iii) outsourcing of activities with significant legal or compliance impact; and iv) other activities that could have a significant impact on customers and/or the financial

[37] See the OCC's *OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance,* (October 2013).

[38] Per OCC Bulletin 2013-29: "Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records. Affiliate relationships are also subject to sections 23A and 23B of the Federal Reserve Act (12 USC 371c and 12 USC 371c-1) as implemented in Regulation W (12 CFR 223). Third-party relationships generally do not include customer relationships."

[39] OCC. OCC Bulletin 2020-94, Sound Practices to Strengthen Operational Resilience (October 2020).
[40] See the OCC's *OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance,* (October 2013).
[41] OCC's *OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance,* (October 2013).

institution's operations, such as in the event that the third party fails to meet expectations, or if the financial institution needs to find an alternate third party or would otherwise require significant investment to implement the third-party relationship and manage associated risks.[42] It is up to the financial institution's management to determine the risks associated with each of the financial institution's third-party relationships,[43] including affiliates, and to mitigate such risks accordingly by adopting a third-party risk management process that follows a continuous life cycle for all third-party relationships, covering:

- Planning,
- Due diligence and third-party selection,
- Contract negotiation,
- Ongoing monitoring, and
- Relationship termination, where and if required.[44]

Through each of these five stages, the financial institution is responsible for:

- Assessing the inherent risk associated with the planned outsourced activities;
- Conducting in-depth due diligence of potential third parties across all relevant risk considerations (e.g., compliance with all applicable laws and regulations, reputation and negative news, use of subcontractors, quality of information security controls and resilience, scale of operations, financial position, etc.)[45] before selecting and entering into the third-party relationship;
- Negotiating contractual terms where the financial institution will specify, *inter alia*, performance measures defining the expectations and responsibilities for both parties (including conformance with regulatory standards or rules), provision and retention of information, and rights to audit (and remediation, where applicable);
- Performing ongoing and risk-based monitoring over the lifetime of the third-party relationship, including monitoring for adherence to contractual terms as well as any changes in the third-party's business, operations, financials, compliance with laws and regulations, and information security controls; and
- Terminating or amending the third-party relationship, as required, in the event of contractual breach, or changes in the institution's business strategy requiring a change or termination of the third-party relationship.

[42] See the OCC's *OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29,* (March 2020).
[43] *Ibid.*
[44] See the OCC Comptroller's Handbook - Safety and Soundness, "Corporate and Risk Governance" (Version 2.0, July 2019), "Third Party Risk Management".
[45] Per the OCC's *OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29, "In conducting due diligence and ongoing monitoring, bank management may obtain and review various reports (e.g., reports of compliance with service-level agreements, reports of independent reviewers, certificates of compliance with International Organization for Standardization (ISO) standards,12 or SOC reports). The person reviewing the report, certificate, or audit should have enough experience and expertise to determine whether it sufficiently addresses the risks associated with the third-party relationship…[B]ank management should consider whether reports contain sufficient information to assess the third party's controls or whether additional scrutiny is necessary through an audit by the bank or other third party at the bank's request."*

The Department will therefore need to assess whether the DD has established an appropriate risk-based third-party risk management process, tailored to its unique profile and its third-party relationships, including relationships with affiliates. Moreover, the Department will take into account the unique third-party risk considerations associated with digital asset services.

The provision of digital asset services can involve significant third-party risk, including in instances where a third-party relationship is critical to an institution's operations. Several key areas of third-party risk unique to DDs include, but are not limited to, the following[46]:

- **Digital asset custody**. The DD may rely on third parties to execute critical activities related to digital asset custody, including storage of customer digital assets and protection of customer private keys, as well as digital asset transfer and settlement. Additional third-party risk considerations may apply depending on whether the DD enters into a sub-custodial arrangement with a third-party, licenses a custody and settlement technology solution from a third-party, or enters into an arrangement with an affiliate for digital asset custody, including licensing of custody architecture and technology from an affiliate. Refer to the *DD Custody and Fiduciary Examination Manual* for additional details on digital asset custody-specific considerations.

- **Blockchain analytics and transaction screening.** DDs are likely to rely on third parties for the execution of certain preventative and detective AML/CFT and OFAC compliance controls, including blockchain analytics for AML/CFT and OFAC investigations and execution of regulatory reporting requirements as well as digital asset custody and settlement architecture for real-time transaction screening. Given the importance of these third parties in supporting a DD's compliance with its AML/CFT and OFAC obligations, the Department will need to consider, among other things, whether the DD has identified specific performance measures and rights to audit (including rights to perform model validation/review) in relevant contractual provisions, whether the DD performed appropriate due diligence prior to third-party selection, and the ongoing monitoring performed by the DD to maintain a level of confidence in the strength of the third-party's controls. Refer to the *DD AML/CFT and OFAC Examination Manual* for additional details on AML/CFT and OFAC-specific considerations.

- **Exchange partnership risk.** Where the DD engages in digital asset exchange services and relies on partnerships with either centralized or decentralized exchanges to execute such services, the Department will need to consider, among other things, the level of due diligence and ongoing monitoring performed on the exchange, including, due diligence around the exchange's compliance with all applicable laws and regulations, the quality of the exchange's information security controls, and any negative news associated with the exchange. Where the DD partners with decentralized exchanges, additional unique risk considerations apply, including coding, centralization, and financial risks that may impact the overall stability of the decentralized exchange. The Department should look for

[46] These key third-party relationship risk areas are illustrative and will differ depending on the DD's structure, product and service offering, and business strategy.

evidence that the DD has considered such risks, such as through the review of smart contract code audits to identify code errors or vulnerabilities that can serve as attack vectors and whether the DD has given due consideration to centralized and systemic risk exposures such as pricing oracles, and the stability of the underlying public blockchain based on the price of its native asset.[47]

- **Staking-as-a-Service partnership risk.** Where the DD engages in digital asset staking, either for its own purposes or as an auxiliary service for its custodial customers, and partners with a third-party staking service provider to perform such staking, the DD will be responsible for performing third-party risk controls for the staking-as-a-service provider. The Department should look for evidence that the DD has considered the unique risks associated with the provision of staking and performed a thorough review of the staking contract, including the terms and conditions specified in the contract and the rights of parties whose funds are being staked (contracts should clearly articulate lock up periods, staking rewards, and treatment of stakers, including whether staked funds are treated according to the principle of *pari-passu*).

Furthermore, in all instances where a DD relies on an affiliate to conduct centralized controls, such as information security, custody, or compliance controls on its behalf, it must provide appropriate oversight of the affiliate and document requisite service levels between itself and its affiliate, as it would with an unaffiliated third-party.

Based on the above considerations and any another applicable factors, Department examiners should develop the following conclusions:

- Level of operational risk exposure (low, moderate, or high).
- Quality of operational risk management (strong, satisfactory, insufficient, or weak).
- Aggregate operational risk exposure taking into consideration operational risk exposures and quality of operational risk management controls (low, moderate, high).
- Direction of operational risk over the next 12 months (decreasing, stable, or increasing).

2.6. Compliance Risk

Compliance risk is the risk to earnings or capital arising from violations of laws or regulations, or from nonconformance with prescribed practices, internal bank policies and procedures, or ethical standards. This risk exposes an institution to potential fines, civil money penalties, payment of damages, and the voiding of contracts.

Compliance risk can result in reputational damage, harm to customers, limited business opportunities, and decreased expansion potential. Compliance risk also includes exposure to litigation, otherwise known as legal risk. Compliance risk is not limited to risk from a failure to comply with consumer protection-related laws and regulations; it encompasses the risk of noncompliance with all laws and regulations, as well as prudent ethical standards and contractual

[47] Such considerations are illustrative and may differ based on the nature and purpose of the DD's interactions with the decentralized exchange.

obligations. [48] For example, in the context of digital assets, compliance with AML/CFT and OFAC requirements is an area of focus given the unique inherent risks posed by digital assets. FinCEN has made clear that digital asset intermediaries are subject to the funds transfer/Travel Rule and recordkeeping requirements, despite industry-wide challenges in implementing a holistic Travel Rule solution. Similarly, for certain new digital asset activities, such as initial coin offerings ("ICOs") and digital asset lending/borrowing, noncompliance with securities and commodities regulations have led to penalties and enforcement actions. In light of these specific considerations, the Department places particular emphasis on issues of noncompliance uniquely associated with digital assets, including:

- **AML/CFT and OFAC Compliance.** As identified by FinCEN, "[virtual currencies] may create illicit finance vulnerabilities due to the global nature, distributed structure, limited transparency, and speed of the most widely utilized virtual currency systems."[49] The Department recognizes these considerations, and therefore applies AML/CFT and OFAC criteria as part of its evaluation. Refer to the *DD AML/CFT and OFAC Examination Manual* for detailed compliance risk considerations associated with AML/CFT and sanctions.

- **Market Integrity and Market Manipulation.** The Congressional Research Service highlights that the digital assets industry raises significant market manipulation concerns.[50] Market manipulation in the context of digital assets may include any number of typologies traditionally associated with fiat-based activity such as wash trading, spoofing, layering, pump and dump schemes, spot hunting, rug pulls, and front-running orders, as well as crypto-specific market manipulation schemes such as cross-market abuse and cross-asset wash trading.[51] Moreover, the speculative nature of digital asset investing coupled with regulatory uncertainty around the treatment of digital assets, raises questions with respect to the treatment of material non-public information and the potential to commit insider trading offenses.[52] Accordingly, Department examiners should assess to what extent DDs

[48] Per OCC's 98-3, "Compliance risk also may arise when a bank does not have systems in place to ensure compliance with mandatory reporting statutes, such as the Bank Secrecy Act. The use of technology to automate lending decisions also could expose a bank to compliance risk if the programs are not properly tested or if the quality of the data is not verified. For example, the use of credit scoring models to automate lending decisions could expose a bank to compliance risk if the data upon which the programs rely are flawed or if the program design itself is flawed. In some cases, such flawed credit scoring models could result in lending patterns that violate fair lending laws and regulations. As banks move increasingly from paper to electronic-based transactions and information exchanges, they need to consider how laws designed for paper-based transactions apply to electronic-based transaction and information exchanges. Some new technologies raise unexpected compliance issues. Legislatures and agencies are frequently modifying their laws and regulations to accommodate new technologies. Transactions conducted through the Internet also can raise novel questions regarding jurisdictional authority over those transactions. Therefore, banks should be careful to monitor and respond to changes to relevant laws and regulations arising from these developments."

[49] Financial Crimes Enforcement Network (FinCEN). "FIN-2019-A0003: Advisory on Illicit Activity Involving Convertible Virtual Currency." (May 9, 2019).

[50] Congressional Research Service Report, "Digital Assets and SEC Regulation," R46208, (June 2021).
[51] Global Digital Finance. Part X – Code of Conduct – Principles for Market Integrity.
[52] Department of Justice, Press Release: "Former Employee Of NFT Marketplace Charged In First Ever Digital Asset Insider Trading Scheme," (June 2022).

have established appropriate trade surveillance controls, including policies, procedures, and associated systems to address the risks associated with market manipulation and insider trading.[53]

2.6.1. Legal Risk

The Board of the Governors of the Federal Reserve System notes that "legal risk arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a banking organization."[54]

The State of Nebraska's regulatory regime outlines the permissible activities of DDs, while at the federal level, the OCC's July 2020 Interpretive Letter provides certain legal clarity around digital assets.[55] However, institutions may face heightened legal risks depending on the types of activities they pursue, their customer base, the relevant jurisdictions in which they operate, their distribution channels, and other factors. Department examiners should assess the DD's legal standing across its activity both within Nebraska, and as applicable, in other U.S. states and foreign jurisdictions, including pending litigation and past judgments, to assess the DD's compliance with applicable laws and regulation and its general level of legal risk exposure.

2.6.2. Consumer Compliance and Consumer Protection

The U.S. federal government recognizes that the dramatic growth in digital assets markets has profound implications for the protection of consumers.[56] As noted by the Congressional Research Service, "digital asset investors—which may include less-sophisticated retail investors, who may not be positioned to comprehend or tolerate high risks—may be especially vulnerable to new types of fraud and manipulation, leading to questions about investor protection."[57] The Congressional Research Service notes four areas of concern with respect to digital assets and consumer harm:

1) The high levels of fraud, scams, and business failures associated with the digital asset industry;
2) The lack of compliance with Securities and Exchange Commission ("SEC") registration requirements and disclosure obligations, impacting investors' ability to understand and appreciate their risk exposures;

---

[53] Examiners should refer to the FDIC's RMS Manual of Examination Policies on Bank Fraud and Insider Abuse (Section 9.1-2). (April 1998) for additional insight on insider abuse, including warning signs and suggested actions for in-depth reviews.

[54] Board of the Governors of the Federal Reserve System. SR 95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies" (November 14, 1995).
[55] OCC. *Interpretive Letter #1170, Vol. 33, No. 7 ("Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers")* (July 22, 2020).
[56] The White House, Presidential Actions: Executive Order on Ensuring Responsible Development of Digital Assets, (March 2022).
[57] Congressional Research Service Report, "Digital Assets and SEC Regulation," R46208, (June 2021).

3) The high volatility of digital assets, which may result in outsized losses for investors and may be poorly understood by less sophisticated investors; and
4) The lack of transaction protections typically seen in traditional finance (e.g., chargebacks, reversals) due to the irreversibility of digital asset transactions.[58]

In accordance with the above observations, and consistent with the Department's mission to, *inter alia,* protect and maintain public confidence, the Department places significant emphasis on a DD's consumer compliance and expects heightened consumer protection measures, commensurate with the unique risks posed by digital assets.

Per the NFIA, a DD is expected to "help meet the digital financial needs of the communities in which it operates, consistent with safe and sound operations," requiring the DD to maintain publicly visible information with respect to its:

a. collection and reporting of data;
b. policies and procedures for accepting and responding to consumer complaints; and
c. efforts to assist with financial literacy or personal finance programs to increase knowledge and skills of Nebraska students in areas such as budgeting, credit, checking and savings accounts, loans, stocks, and insurance.[59]

In assessing the DD's compliance with these NFIA requirements, the Department will consider the customer base served by the DD and may look to industry best practices around*, inter alia*, disclosures with respect to information collection, publication of consumer complaint policies and response times, and establishment of digital asset training/interactive "learn" to "earn" modules.

Furthermore, in alignment with its mission, the Department expects DDs to adhere to the Consumer Financial Protection Bureau's ("CFPB") Unfair, Deceptive, or Abusive Acts and Practices ("UDAAP") regulations, remaining vigilant for any UDAAPs that may cause significant financial injury to consumers, erode consumer confidence, and undermine the financial marketplace.[60] Accordingly, the NFIA requires DDs to provide full and complete disclosures that are readily understandable, containing no material misrepresentations, which shall include:

(1) A schedule of fees and charges the DD may assess, the manner by which fees and charges will be calculated if they are not set in advance and disclosed, and the timing of the fees and charges;
(2) A statement that the customer's DD account is not protected by Federal Deposit Insurance Corporation insurance;
(3) A statement whether there is support for forked networks of each digital asset;
(4) A statement that investment in digital assets is volatile and subject to market loss;
(5) A statement that investment in digital assets may result in total loss of value;
(6) A statement that legal, legislative, and regulatory changes may impair the value of digital assets;
(7) A statement that customers should perform research before investing in digital assets;

[58] *Ibid.*
[59] Neb. Stat. §8-3005 (LB 646, 2021)
[60] CFPB. Consumer Laws and Regulations: Unfair, Deceptive, or Abusive Acts or Practices, Manual v.3 (March 2022).

(8) A statement that transfers of digital assets are irrevocable, if applicable;
(9) A statement how liability for an unauthorized, mistaken, or accidental transfer shall be apportioned;
(10) A statement that digital assets are not legal tender in any jurisdiction;
(11) A statement that digital assets may be subject to cyber theft or theft and become unrecoverable;
(12) A statement about who maintains control, ownership, and access to any private key related to a digital assets customer's digital asset account; and
(13) A statement that losing private key information may result in permanent total loss of access to digital assets.[61]

Moreover, given the extant volatility and security risks associated with digital assets, as noted above, the NFIA requires DDs to both provide notices with respect to the risks associated with digital assets as well as obtain acknowledgement from customers to ensure that customers understand that digital asset deposits held with DDs are not insured by the Federal Deposit Insurance Corporation ("FDIC"): "With respect to all digital asset business activities, a digital asset depository shall display and include in all advertising, in all marketing materials, on any Internet website it maintains, and at each window or place where it accepts digital asset deposits:

a) a notice conspicuously stating that digital asset deposits and digital asset accounts are not insured by the Federal Deposit Insurance Corporation, if applicable, and

b) the following conspicuous statement:

Holdings of digital assets are speculative and involve a substantial degree of risk, including the risk of complete loss. There is no assurance that any digital asset will be viable, liquid, or solvent. Nothing in this communication is intended to imply that any digital asset held in custody by a digital asset depository is low-risk or risk-free. Digital assets held in custody are not guaranteed by a digital asset depository and are not FDIC insured.

Upon opening a digital asset depository account, and if applicable, a digital asset depository shall require each customer to execute a statement acknowledging that all digital asset deposits at the digital asset depository are not insured by the Federal Deposit Insurance Corporation. The digital asset depository shall permanently retain this acknowledgment, whether in electronic form or as a signature card."[62]

The Department will assess the DD's compliance with the above NFIA requirements, including public disclosure notices, notices and receipts provided to consumers as part of the transaction process, and internal consumer protection and anti-fraud policies and controls. Where the DD serves retail/consumer customers, Department examiners will review the DD's policies and controls around protection of vulnerable customer segments, including the DD's policies on the prevention of social engineering and elder abuse.

[61] Neb. Stat. §8-3008 (LB 646, 2021)
[62] Neb. Stat. §8-3011 (LB 646, 2021)

The Department recognizes the DD's approach for consumer protection and related consumer compliance will be assessed as an element for the DD's overall compliance risk. However, the Department also assesses consumer compliance as a specialty rating against a number of discrete criteria based on the OCC's approach, tailored as appropriate to DD-specific factors.

Based on the above considerations and any another applicable factors, Department examiners should develop the following conclusions:

- Level of compliance risk exposure (low, moderate, or high).
- Quality of compliance risk management (strong, satisfactory, insufficient, or weak).
- Aggregate compliance risk exposure taking into consideration compliance risk exposures and quality of compliance risk management controls (low, moderate, high).
- Direction of compliance risk over the next 12 months (decreasing, stable, or increasing).

2.7. Strategic Risk

Strategic risk is the risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the banking industry and operating environment. This risk is a function of an institution's strategic goals, business strategies, resources, and quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities.

The assessment of strategic risk includes more than an analysis of a firm's written strategic plan. It focuses on opportunity costs and how plans, systems, and implementation affect the firm's financial condition and resilience. It also incorporates how management analyzes external factors, such as economic, technological, competitive, regulatory, and other environmental changes, that affect the firm's strategic direction.[63,64]

[63] Per OCC's 98-3, "Use of technology can create strategic risk when management does not adequately plan for, manage, and monitor the performance of technology-related products, services, processes, and delivery channels. Strategic risk may arise if management fails to understand, support, or use a technology that is essential for the bank to compete or if it depends on a technology that is not reliable. In seeking ways to control strategic risk, a bank should consider its overall business environment, including: the knowledge and skills of senior management and technical staff; its existing and planned resources; its ability to understand and support its technologies; the activities and plans of suppliers of technology and their ability to support the technology; and the anticipated life cycle of technology-related products and services."

[64] Per OCC's Unique and Hard-to-Value Assets booklet, "A bank fiduciary assumes strategic risk when taking on new product lines without having the expertise and systems to properly manage and control risks associated with the line of business. […] Because the management of unique assets falls outside the more traditional equity and fixed-income strategies, management must ensure that personnel are qualified to manage these assets. With more traditional financial investments, administrators have numerous financial tools to monitor performance and do not need to focus on physical safekeeping of the assets. Because unique asset market values are associated with a specific asset, financial reviews have to be tailored to the particular asset and its real or potential profitability."

In doing so, the Department draws upon existing federal guidance around risks associated with new activities (with reference to digital assets), which include:

- "new activities are not compatible with the firm's risk appetite or strategic plan or do not provide an adequate return on investment.
- the firm engages in new activities without performing adequate due diligence, including upfront expense analysis.
- management does not have adequate resources, expertise, and experience to properly implement and oversee the new activities."[65]

In reviewing a DD's strategic risk, examiners should take note of the entity's business plan, quality and speed of plan execution, and speed of adoption when it comes to industry best practices. Moreover, given the rapid scaling frequently associated with the digital assets industry, examiners should review whether the DD's senior management has implemented reasonable planning and risk mitigants to account for rapid scaling, including appropriate investments in the people (staffing), processes, and technologies (including automation) necessary to support growth plans.

Based on the above considerations and any another applicable factors, Department examiners should develop the following conclusions:

- Level of strategic risk exposure (low, moderate, or high).
- Quality of strategic risk management (strong, satisfactory, insufficient, or weak).
- Aggregate strategic risk exposure taking into consideration strategic risk exposures and quality of strategic risk management controls (low, moderate, high).
- Direction of strategic risk over the next 12 months (decreasing, stable, or increasing).

2.8. Reputation Risk

Reputation risk is the risk to current or projected financial condition and resilience arising from negative public opinion. This risk may impair a bank's competitiveness by affecting its ability to establish new relationships or services or continue servicing existing relationships. Reputation risk is inherent in all bank activities, and management should deal prudently with stakeholders, such as customers, counterparties, correspondents, investors, regulators, employees, and the community.

A bank that actively associates its name with products and services offered through outsourced arrangements or asset management affiliates, or fiduciary services, is more likely to have higher reputation risk exposure. Significant threats to a bank's reputation also may result from negative publicity regarding matters such as unethical or deceptive business practices, violations of laws or regulations, high-profile litigation, or poor financial performance. The assessment of reputation

[65] Refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

risk should take into account the bank's culture, the effectiveness of its problem-escalation processes and rapid-response plans, and its engagement with news media.[66,67]

The Department recognizes that the success of the emergent activities associated with the DD charter may present significant reputation risks to the Department and bank community in the event that issues arise. Even in highly-regulated environments with regular examinations of digital assets activities, there have been significant reputational risk events, including: [68]

- Facilitation of proceeds of illicit activity, including funding of terrorist financing and violations of AML/CFT and sanctions regulation or other deficiencies that enable criminal activity to flow through the firm;
- Information technology risks, including issues around systems and operational breakdowns or cyber attacks that led to significant loss of customer assets;
- Events associated with third-party relationships and vendor reliance (such as unique negative news introduced through blockchain analytics vendors and associated acquisitions thereof); and
- Market integrity and market manipulation incidents such as fraud, insider transactions, conflicts of interest, parent/affiliate relationship or misuse of customer funds.

Accordingly, the Department puts a particular emphasis on incident and issues management for DDs. In the event issues or incidents do arise, DDs should: inform the DD's board of directors and the Department (depending on the severity of the incident); provide timely notice to customers; and implement corrective actions as soon as possible.

The Department draws upon existing federal guidance around risks associated with new activities (with reference to digital assets), which include:

- "new activities offered without management and the board's full understanding of the customers' needs or goals, the appropriateness of the activities for customers, or the intended effect of the new activity on customers.

---

[66] *Per OCC's 98-3, "Reputation risk arises whenever technology-based banking products, services, delivery channels, or processes may generate adverse public opinion such that it seriously affects a bank's earnings or impairs capital. Examples may include: flawed security systems that significantly compromise customer privacy; inadequate contingency and business resumption plans that affect a bank's ability to maintain or resume operations and to provide customer services following system failures; fraud that fundamentally undermines public trust; and largescale litigation that exposes a bank to significant liability and results in severe damage to a bank's reputation. Adverse public opinion may create a lasting, negative public image of overall bank operations and thus impair a bank's ability to establish and maintain customer and business relationships."*

[67] *Per OCC's Unique and Hard-to-Value Assets booklet, "Bank fiduciaries must ensure that they have sufficient processes and resources in place to manage, secure, and protect unique assets under their care. […] Reputation risk may arise if a bank does not have the expertise to administer an asset type, monitor the condition of the asset, or assess a value for those assets, and the bank is ultimately required to outsource those processes. Because third-party providers act as agent for the bank, any weakness in third-party supervision has the potential to affect the bank directly through negative publicity or litigation. Because many fiduciary relationships result from client referrals, maintaining a good reputation is critical to building future business."*

[68] *Refer to the U.K. Financial Conduct Authority's Policy Statement 19/22: Guidance on Cryptoassets – Feedback and Final Guidance to CP 19/3 (July 2019).*

- management, in an effort to achieve higher returns or income, offers complex products or services that incorporate practices or operations that differ from the bank's strategies, expertise, culture, or ethical standards.
- management permits—or fails to notice—poor service, inappropriate sales practices, or employee misconduct.
- inadequate protection of customer data, or violations of consumer protection, Bank Secrecy Act or anti-money laundering laws or regulations occur, which may result in litigation, adverse publicity, or loss of business."[69]

In reviewing a DD's management of reputational risk, examiners should take note of any existing material negative news/adverse media associated with the DD and its senior management team, as well as its policies and procedures for incident handling and escalations, and timely remediation of issues, particularly as these relate to higher-risk exposures such as AML/CFT, Information Security, Data Privacy, and Consumer Protection. Moreover, examiners should consider whether more general adverse media pertaining to digital assets (e.g., high profile hacks, digital asset volatility, prominent blockchain project collapse) may impact the DD's reputational risk exposures even where such adverse media is not unique to the specific DD being examined.

Based on the above considerations and any another applicable factors, Department examiners should develop the following conclusions:

- Level of reputational risk exposure (low, moderate, or high).
- Quality of reputational risk management (strong, satisfactory, insufficient, or weak).
- Aggregate reputational risk exposure taking into consideration reputational risk exposures and quality of reputational risk management controls (low, moderate, high).
- Direction of reputational risk over the next 12 months (decreasing, stable, or increasing).

2.9. Relationship Between the Risk Assessment Systems (RAS) and Regulatory Ratings

The RAS is used in conjunction with CAMELS, ROCA, and other regulatory ratings during the supervisory process to evaluate a bank's financial condition and resilience. The RAS **provides both a current (aggregate risk) and a prospective (direction of risk) view of the bank's risk profile** that examiners incorporate when assigning regulatory ratings. For example, under the RAS, examiners may assess credit risk in a bank with insufficient risk management practices and increasing adverse trends as "moderate and increasing" or "high and increasing." If the component rating for asset quality does not reflect the quality of risk management identified in the credit RAS, examiners should consider whether changing the component rating is warranted. Similarly, given the higher operational risks associated with custody and safekeeping of digital assets, a DD with insufficient operational controls (e.g., around key management or information security) and increasing adverse trends could be "high and increasing." In this case, if the component rating for management does not reflect quality of risk management in the operational RAS, examiners should consider that component rating. Additionally, examiners consider their assessments of risk

[69] Refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

management practices for each of the risk categories when assigning management component ratings.

Given the novelty and heightened risks associated with digital assets, Department examiners may consider multiple risk ratings as "high and increasing," particularly where DDs are putting into place or considering additional product and service offerings during the *de novo* period (with attendant impact on appropriate CAMELS-ITCC rating.) In practice, this approach puts further emphasis on clear lines of communication between the Department and the DD's Board of Directors and senior management around heightened regulatory expectations related to product launches and uses of different types of digital assets and transaction types across existing or new products and services.

3. Risk-based Supervision

In carrying out its mission, the Department employs an ongoing risk-based supervision approach focused on evaluating risk, identifying material and emerging concerns, and requiring institutions to take timely corrective action before deficiencies compromise their safety and soundness.

The Department's risk-based supervision approach requires examiners to determine how existing or emerging issues for an institution, its related organizations, or the financial services industry as a whole affect the nature and extent of risks in the DD in question. Department examiners evaluate risk using the OCC's RAS and tailor supervisory activities to the risks identified for DDs. This assessment should include DD-specific risk considerations where appropriate, including clear internal guidelines around focus areas for closer oversight, particularly with respect to proposed business activities during the *de novo* period. Examiners must include periodic testing in supervisory activities to validate their risk assessments.

The risk-based supervision approach concentrates on systemic risks and banks that pose the greatest risk to the federal and state banking system. Under this approach, the Department allocates greater resources to areas of higher risk by:

- identifying risk using common definitions. The categories of risk, as they are defined, are the foundation for supervisory activities, for which the Department leverages existing federal agency expectations where available.
- measuring risk using common methods of evaluation. Risk cannot always be quantified in dollars. For example, numerous or significant internal control deficiencies may indicate excessive operational risk.
- evaluating risk management to determine whether bank systems adequately identify, measure, monitor, and control risk.
- providing flexibility to modify planned supervisory activities based on changes to a bank's risk profile.
- performing examinations based on the core assessment, expanded procedures, or verification procedures, reaching conclusions on the bank's risk profile and condition, and following up on areas of concern.[70]

3.1. Coordination with Other Regulators

The Department coordinates with federal agencies, state-based regulators, and foreign jurisdictions as applicable based on existing supervisory agreements. In the case of certain federal agencies, if a DD becomes a member of the Federal Reserve System, this may include shared resources with federal examiners for on-site examinations where possible, as well as coordination via information-sharing and inter-agency meetings including with the Federal Deposit Insurance Corporation ("FDIC"), Federal Reserve, FinCEN, OFAC, and OCC, as appropriate.

In the case of DDs with foreign operations or supporting affiliates, the Department will generally enter into an information-sharing agreement or memorandum of understanding with the foreign

[70] Refer to the OCC's Comptroller's Handbook – Bank Supervision Process (Version 1.1, September 2019) for additional background around conducting the OCC's risk-based supervisory approach as well as the FDIC's Risk Management Manual of Examination Policies.

financial regulator to facilitate complete, coordinated supervision, allowing for the assessment of risks on a consolidated basis.

3.2. Supervisory Process

3.2.1. Planning

Planning[71] is essential to effective supervision and occurs throughout a DD's supervisory cycle. Planning requires careful and thoughtful assessment of a DD's current and anticipated risks (e.g., examiners should assess the risks of both existing and new banking activities). The purpose of the examination planning process is to ensure that the institution's operations and activities are understood prior to the start of an examination, so that examination procedures can be appropriately tailored to the institution. By understanding the unique nature of each institution, examiners can evaluate fundamental risks of the institution's activities and the strength of management practices in mitigating those risks, and focus examination activities and procedures on risks that are not as well mitigated or that have not been previously assessed because they are new.[72] New banking activities may be either traditional activities that are new to the DD or activities new to the financial services industry,[73] such as novel activities involving digital assets.

The examination planning process can be divided into three phases: 1) initial contact, 2) initial examination planning, and 3) final examination planning and conducting off-site work:

- **Phase 1: Initial Contact.** During this phase, the Department examiners will develop a timeline of examination activities for the upcoming examination at least 90 days ahead of the projected examination start date. At this time, the Department examiners will contact the DD's management to inform them of the upcoming examination date and collect additional information from the DD as necessary to help the examiner understand material changes to the business model, risk profile, and complexity of the institution, thereby enabling examiners to develop a more tailored information request list for the start of the examination.

- **Phase 2: Initial Examination Planning.** Initial planning typically occurs six to eight weeks ahead of the examination start date in order to allow the Department Examiner sufficient time to learn about the DD and prepare an examination plan tailored to the institution's areas of greatest risk. During this phase, examiners will spend time understanding the institution, including reviewing prior Reports of Examination and prior external audits, where available. The Department Examiner will contact the institution's management to better understand the institution's business model, risk profile, and complexity and tailor the examination information request letter to the institution accordingly. The Department Examiner will also develop off-site and on-site examination

[71] Refer to OCC's Supervisory Process for a discussion on overall approach to Planning (e.g., supervisory strategy, examination planning) as well as the FDIC's RMS Manual of Examination Policies on Examination Planning.
[72] Federal Deposit Insurance Corporation. RMS Manual of Examination Policies: Examination Planning (Section 21.1). (February 2021).
[73] Refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

procedures, including identifying which examination activities are more appropriate for off-site vs. onsite review, incorporating these procedures into the overall examination plan. Finally, the Department Examiner will develop the examination planning memo that outlines the examination activities and procedures necessary to fulfill the full-scope examination statutory requirement.

- **Phase 3: Final Examination Planning and Conducting Off-Site Work.** During the final planning phase, examiners review all materials provided by the institution, at least one to two weeks prior to the on-site examination start date. The Department Examiner finalizes the Examination Plan and examination planning memo and determines the examination staff assignments. [74]

  As part of both Phases 2 and into Phase 3 of the examination planning process, the Department Examiner will identify benchmark training needs for the pre-commissioned examination team members. The Department Examiner may recommend specialized digital asset training for examination staff (e.g., introduction to blockchain analytics for AML/CFT examiners) where it is determined that such training would be required to perform an effective full-scope examination of the DD and its controls.

3.2.2. Supervisory Activity Components

Supervisory activities, regardless of type, include discovery, correction (when applicable), monitoring, and examination management. The extent of these components during a given activity depends on the type of activity, nature and extent of the bank's risks, and existence of deficiencies. The nature and extent of examination management also depends on other factors, such as the number and experience of examiners assigned.

3.2.3. Communication

The Department is committed to ongoing, effective communication with the DDs that it supervises and with other regulators as appropriate. For DD *de novo* entities, the Department may engage in more frequent communication. Communication includes formal and informal conversations and meetings, ROEs, supervisory letters, and other written materials. Regardless of form, communications should convey a consistent conclusion regarding the DD's condition. Department communications must be professional, objective, clear, and informative. Examiners must not have communications with DDs that could be perceived as suggesting that the examination process is in any way influenced by political issues or considerations.

Communication should be ongoing throughout the supervisory process and tailored to a DD's structure and dynamics. The timing and form of communication depend on the situation being addressed. Examiners should communicate with the DD's management and board as often as the DD's condition and supervisory findings require. The Department Examiner or portfolio manager should include plans for communication in the supervisory strategy.

[74] Federal Deposit Insurance Corporation. RMS Manual of Examination Policies: Examination Planning (Section 21.1). (February 2021).

Examiners should meet with DD management frequently and directors as needed to collect information and discuss supervisory issues. These discussions, which establish and maintain open lines of communication, are an important source of information. For example, examiners meet with management throughout the supervisory cycle and before, during, and after supervisory activities. When a DD's supervisory cycle is complete, examiners meet with the board to discuss the Department's supervision of the DD, results of the examination(s), and other topics. Examiners should document these meetings as appropriate in relevant supervisory information systems.

When the Department is considering an enforcement action, examiners should use care in communications with the DD related to the potential enforcement action. Department examiners should consult internally with the Director before meeting with the DD regarding a potential enforcement action.

3.2.4. Documentation

Documentation is an ongoing process throughout the supervisory cycle. Examiners must document their decisions and conclusions. Supervisory offices must also document actions the Department takes with respect to individual DDs, including decisions regarding enforcement actions, corporate applications, and other formal communications.

Documentation includes correspondence, ROEs, work papers, and records of key meetings and significant events. In most cases, work papers need not include all of the information reviewed during a supervisory activity. Generally, only those documents necessary to support the scope and conclusions of the supervisory activity should be retained as work papers. Examiners must abide by the Department's information security policies when handling, storing, and disposing of sensitive DD information.

4. Supervisory Actions

Regulatory agencies may use formal or informal procedures to address weak operating practices, deteriorating financial conditions, or apparent violations of laws or regulations.[75] Examiners must initiate corrective measures promptly if they identify excessive risks at financial institutions.
Generally, examiners can use examination comments and supervisory recommendations or informal agreements to correct problems. However, examiners are also authorized to use formal enforcement actions, when necessary, to reduce risks and address deficiencies.[76] The Department generally aligns to the existing standards for supervisory actions, including Matters Requiring Board Attention (or "MRBAs"), Memoranda of Understanding (or "MOUs"), violations of law and regulations, and enforcement actions (including civil monetary penalties and supervisory letters).

4.1. Examination Comments and Supervisory Recommendations

4.1.1. Matters Requiring Board Attention

The Department uses MRBAs to communicate concerns about a firm's deficient practices. Examiners must communicate such concerns to management and the board when the concerns are discovered and must not defer issuing MRBAs pending management's efforts to address the concerns. Examiners must not use a graduated process by first communicating the Department's concern with a deficient practice as a recommendation,[77] then, if the deficient practice is not addressed, using an MRBA. For consistent reporting, the Department focuses on the concerns within the MRBA, tracking them through their duration. The Department requires interim reporting and communication on the status of MRBAs until issues are remediated.

4.1.2. Citations for Violations of Laws and Regulation

A violation of **law or regulation** is an act (or failure to act) that deviates from, or fails to comply with, a statutory or regulatory requirement. Violations are often the result of deficient practices. Frequently, correcting violations alone does not address the deficient practices that may have led to the violations. When examiners identify a violation, they should also identify any deficient practices that contributed to violations. If DD management has not corrected deficient practices that caused or contributed to the

[75] Federal Deposit Insurance Corporation. RMS Manual of Examination Policies: Informal Actions (Section 13.1). (April 2016).
[76] Federal Deposit Insurance Corporation. RMS Manual of Examination Policies: Formal Administrative Actions (Section 15.1). (July 2016).
[77] Consistent with the OCC's approach, recommendations must not be included in the ROE or other formal written communication to the bank (e.g., supervisory letter). Recommendations can be provided informally to bank management or the board as suggestions to enhance policies or as best practices. Recommendations do not require specific action by bank management or follow-up by examiners; however, the Department will generally include any recommendations as part of the ROE listed as an observation.

violation, examiners must communicate the Department's concern with these practices in an MRBA.

4.2. Informal Enforcement Actions

4.2.1. Reprimands, Supervisory Letters, Imposition of Conditions

In certain cases, the issuance of a reprimand or a supervisory letter may be more appropriate than the assessment of a civil monetary penalty ("CMP"). A reprimand is a strongly worded document used in lieu of a CMP when, for example, the CMP would be too small to justify spending resources required or when the individual or DD has recognized the supervisory problem and taken steps to correct it. A supervisory letter is generally used to call attention to a supervisory problem that is not severe enough to warrant a CMP.

The Department may impose conditions in connection with the approval of an application, a notice, or another request by a DD if it determines that one or more conditions are necessary or appropriate for the approval to be consistent with applicable laws, regulations, or Department policies. Conditions may be imposed, for example, to protect the safety and soundness of the institution, prevent conflicts of interest, or require the institution to provide for customer protections. Conditions imposed in writing are often used by the Department in approvals of corporate applications and interpretive letter opinions on requests to engage in permissible activities.

4.2.2. Memorandum of Understanding

An MOU provides a structured way to correct problems at institutions that have moderate weaknesses, but have not deteriorated to a point requiring formal corrective actions. An MOU may be appropriate if examiners determine that the board of directors and management are committed to, and capable of, implementing effective corrective measures and may be used to address specific problems and control weaknesses at institutions that are determined to be fundamentally sound. MOUs should be considered for all institutions that are deemed to exhibit some degree of supervisory concern. Examiners may determine that an MOU may not be required if the Director or designee determines that the institution's condition and operations have improved significantly or if there are other strong mitigating circumstances, such as a strong management team. However, the mere belief that management recognized its errors and will improve the DD's condition is generally not a sufficient reason to make an exception from applying an MOU. Examiners should consider recommending formal enforcement action for DDs where management appears unwilling to take appropriate corrective measures, and for all institutions with serious deficiencies exhibiting unsafe and unsound practices and/or conditions. [78]

[78] Federal Deposit Insurance Corporation. RMS Manual of Examination Policies: Informal Actions (Section 13.1). (April 2016).

Upon issuance of an MOU, examiners will need to ensure that they are monitoring the DD's progress in achieving the goals of the outstanding MOU. Such monitoring can be performed through a combination of offsite monitoring, visitations, and examinations.[79]

4.3. Formal Enforcement Actions

4.3.1. Civil Money Penalties

CMPs are a type of enforcement action that requires monetary payments to penalize a bank or DD, its directors, or other persons participating in the affairs of the institution for violations,[80] unsafe or unsound practices, or breaches of fiduciary duty. CMPs may be used alone or in combination with other enforcement actions. Examiners should propose CMPs for serious misconduct, including misconduct that is reckless, flagrant, willful, or knowing and that, because of its frequency or recurring nature, shows a general disregard for law or regulation. Added consideration should be given to violations that occurred or continued in direct contravention of the institution's policy guidelines, correspondence from the regulator, or audit reports. CMPs are assessed not only to punish the violator according to the degree of culpability and severity of the violation, but also to deter future violations; the primary purpose for utilizing CMPs is not to effect remedial action. Such action, in the form of restitution or other corrective measures, should be separately pursued.[81]

4.3.2. Consent Orders and Cease and Desist Orders

The purpose of a cease-and-desist order is to remedy unsafe or unsound practices or violations and to correct conditions resulting from such practices or violations. Formal actions may be pursued before a violation, or unsafe or unsound practice occurs in order to prevent a developing situation from reaching more serious proportions. Cease and desist orders generally contain provisions that require a firm to take, or prohibit a firm from taking, specific actions relating to inappropriate practices, violations, or conditions. Cease and desist orders apply when an institution does not agree to a proposed enforcement action.[82]

Alternatively, if the institution agrees to a proposed enforcement action, the Department can issue a consent order. By agreeing to a consent order, the institution waives its right to an administrative hearing and consents to the enforcement action without admitting or denying engagement in unsafe or unsound practices or violations.[83]

---

[79] *Ibid.*
[80] Per the OCC, the term "violation," for the purpose of CMPs under 12 USC 1818(i), is defined by 12 USC 1813(v) to include "any action (alone or with another or others) for or toward causing, bringing about, participating in, counseling, or aiding or abetting a violation."
[81] Federal Deposit Insurance Corporation. RMS Manual of Examination Policies: Civil Money Penalties (Section 14.1). (February 2000).
[82] Federal Deposit Insurance Corporation. RMS Manual of Examination Policies: Formal Administrative Actions (Section 15.1). (July 2016).
[83] *Ibid.*

4.3.3. Charter Revocation

In addition to standard supervisory actions, the NFIA grants the Director the right to: "suspend or revoke the charter or authority of a digital asset depository if, after notice and opportunity for a hearing, the Director determines that:" [84]

1) The digital asset depository has failed or refused to comply with an order issued under certain key Nebraska banking regulation pertaining to consumer lending and the Nebraska Money Transmitters Act;

2) The application for a charter or authority contained a materially false statement, misrepresentation, or omission; or

3) An officer, a director, or an agent of the digital asset depository, in connection with an application for a charter or authority, an examination, a report, or other document filed with the Director, knowingly made a materially false statement, misrepresentation, or omission to the Department, the Director, or the duly authorized agent of the Department or Director."[85]

Further, the NFIA notes that where the Director finds that a DD "has failed, is operating in an unsafe or unsound condition, or is endangering the interests of customers, and the failure, unsafe or unsound condition, or endangerment has not been remedied" within a prescribed timeframe or as directed by the Department, the Director will be empowered to conduct a liquidation or appoint a receiver.[86]

[84] Neb. Stat. §8-3025 (LB 646, 2021)
[85] *Ibid.*
[86] Neb. Stat. §8-3027(1) (LB 646, 2021)

5. Regulatory Ratings

5.1. CAMELS

The FFIEC adopted the UFIRS in 1979 and revised it in 1996.[87] Under the UFIRS, the supervisory agencies endeavor to ensure that all financial institutions are evaluated in a comprehensive and uniform manner and that supervisory attention is appropriately focused on the financial institutions exhibiting financial and operational weaknesses or adverse trends. The UFIRS serves as a useful vehicle for identifying problem or deteriorating financial institutions, as well as for categorizing institutions with deficiencies in particular component areas. Further, the rating system assists Congress in following safety and soundness trends and in assessing the aggregate strength and soundness of the financial industry. The UFIRS assists the agencies in fulfilling their collective mission of maintaining stability and public confidence in the nation's financial system.
The rating system is commonly referred to as the CAMELS rating system because it assesses six components of a bank's performance: capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk. Under the UFIRS, each bank is assigned a composite rating based on an evaluation and rating of six essential components of the institution's financial condition and operations. The rating is based on a scale of 1 through 5 in ascending order of supervisory concern, with 1 representing the strongest performance and management practices and least degree of supervisory concern, and 5 representing the weakest performance and management practices and highest degree of supervisory concern.

Evaluations of the components consider the institution's size and sophistication, the nature and complexity of its activities, and its risk profile. The UFIRS takes into consideration certain financial, managerial, and compliance factors that are common to all financial institutions. Examiners have the flexibility to consider any other evaluation factors that, in their judgment, relate to the component area under review. The evaluation factors listed under a component area are not intended to be all-inclusive, but rather a list of the more common factors considered under that component.

Each component is interrelated with one or more other components. For example, the level of problem assets in an institution is a primary consideration in assigning an asset quality component rating. But it is also an item that affects the capital adequacy and earnings component ratings. The level of market risk and the quality of risk management practices are elements that also can affect several components. Examiners consider relevant factors and their interrelationship among components when assigning ratings.

The OCC considers AML/CFT examination findings in a safety and soundness context when assigning the management component rating. Serious deficiencies in a bank's AML/CFT compliance create a presumption that the management rating will be adversely affected because risk management practices are less than satisfactory. Examiners should document application of

[87] The OCC Supervision Processes Manual's appendix contains excerpts from 61 Fed. Reg. 67021–67029, "Uniform Financial Institutions Rating System" and "Joint Interagency Common Questions and Answers on the Revised Uniform Financial Institutions Rating System" (refer to OCC Bulletin 1997-14, "Uniform Financial Institutions Rating System and Disclosure of Component Ratings: Questions and Answers").

this approach in their written comments in the OCC's supervisory information systems, and in supervisory communications, when appropriate.[88]

Composite CAMELS Ratings

The composite rating generally bears a close relationship to the component ratings assigned, but the composite rating is not derived by computing an arithmetic average of the component ratings. When examiners assign a composite rating, some components may be given more weight than others depending on the situation at the institution. In general, assignment of a composite rating may incorporate any factor that bears significantly on the overall condition and soundness of the financial institution. Assigned composite and component ratings are disclosed to the institution's board and senior management.

Management's ability to respond to changing circumstances and to address the risks that may arise from changing business conditions, or the initiation of new activities or products, is an important factor in evaluating a financial institution's overall risk profile and the level of supervisory attention warranted. For this reason, examiners give the management component special consideration when assigning the bank's composite rating.

Examiners take into account management's ability to identify, measure, monitor, and control the bank's risks when assigning each component rating. Appropriate management practices vary considerably among financial institutions, depending on their size, complexity, and risk profile. For less complex institutions engaged solely in traditional banking activities and whose directors and senior managers, in their respective roles, are actively involved in the oversight and management of day-to-day operations, relatively basic management systems and controls may be adequate. At more complex institutions, detailed and formal management systems and controls are needed to address their broader range of financial activities and to provide senior managers and directors, in their respective roles, with the information they need to monitor and direct day-to-day activities. All institutions are expected to properly manage their risks. For less complex institutions engaging in less sophisticated risk-taking activities, detailed or highly formalized management systems and controls are not required to receive strong or satisfactory component or composite ratings. Table 7 lists the definitions of the CAMELS composite ratings.

Table 7: Composite CAMELS Ratings

1	Financial institutions in this group are sound in every respect and generally have components rated 1 or 2. Any weaknesses are minor and can be handled in a routine manner by the board of directors and management. These financial institutions are the most capable of withstanding the vagaries of business conditions and are resistant to outside influences, such as economic instability in their trade area. These financial institutions are in substantial compliance with laws and regulations. As a result, these financial institutions exhibit the strongest performance and risk management practices relative to the institution's size, complexity, and risk profile, and give no cause for supervisory concern.
2	Financial institutions in this group are fundamentally sound. For a financial institution to receive this rating, generally no component rating should be more severe than 3. Only

[88] Refer to OCC Bulletin 2012-30, "AML/CFT Compliance Examinations: Consideration of Findings in Uniform Rating and Risk Assessment Systems."

	moderate weaknesses are present, and they are well within the board's and management's capabilities and willingness to correct. These financial institutions are stable and are capable of withstanding business fluctuations. These financial institutions are in substantial compliance with laws and regulations. Overall risk management practices are satisfactory relative to the institution's size, complexity, and risk profile. There are no material supervisory concerns, and, as a result, the supervisory response is informal and limited.
3	Financial institutions in this group exhibit some degree of supervisory concern in one or more of the component areas. These financial institutions exhibit a combination of weaknesses that may range from moderate to severe; however, the magnitude of the deficiencies generally will not cause a component to be rated more severely than 4. Management may lack the ability or willingness to effectively address weaknesses within appropriate time frames. Financial institutions in this group generally are less capable of withstanding business fluctuations and are more vulnerable to outside influences than those institutions rated a composite 1 or 2. Additionally, these financial institutions may be in significant noncompliance with laws and regulations. Risk management practices may be less than satisfactory relative to the institution's size, complexity, and risk profile. These financial institutions require more than normal supervision, which may include formal or informal enforcement actions. Failure appears unlikely, however, given the overall strength and financial capacity of these institutions.
4	Financial institutions in this group generally exhibit unsafe and unsound practices or conditions. There are serious financial or managerial deficiencies that result in unsatisfactory performance. The problems range from severe to critically deficient. The weaknesses and problems are not being satisfactorily addressed or resolved by the board and management. Financial institutions in this group generally are not capable of withstanding business fluctuations. There may be significant noncompliance with laws and regulations. Risk management practices are generally unacceptable relative to the institution's size, complexity, and risk profile. Close supervisory attention is required, which means, in most cases, formal enforcement action is necessary to address the problems. Institutions in this group pose a risk to the deposit insurance fund. Failure is a distinct possibility if the problems and weaknesses are not satisfactorily addressed and resolved.
5	Financial institutions in this group exhibit extremely unsafe and unsound practices or conditions; exhibit a critically deficient performance; often demonstrate inadequate risk management practices relative to the institution's size, complexity, and risk profile; and are of the greatest supervisory concern. The volume and severity of problems are beyond management's ability or willingness to control or correct. Immediate outside financial or other assistance is needed in order for the financial institution to be viable. Ongoing supervisory attention is necessary. Institutions in this group pose a significant risk to the deposit insurance fund and failure is highly probable.

5.1.1. Capital Adequacy

A financial institution is expected to maintain capital commensurate with the nature and extent of risks to the institution and the ability of management to identify, measure, monitor, and control

these risks. The effect of credit, market, and other risks on the institution's financial condition should be considered when evaluating the adequacy of capital. The types and quantity of risk inherent in an institution's activities determine the extent to which it may be necessary to maintain capital at levels above required regulatory minimums to properly reflect the potentially adverse consequences that these risks may have on the institution's capital.

As identified throughout Department examination materials, and in particular *2.5. Operational Risk*, *2.3. Liquidity Risk*, and *2.4. Price Risk* of this Supervision Manual, the nature of digital assets-related activity may subject the DDs to higher exposure to novel or exogenous events such as price volatility for virtual currencies, significant operational losses beyond insurance coverage due to key theft or misuse, and changes to market conditions. Notably, determining capital adequacy is a highly judgmental process, in part, because each DD's risk profile is arguably unique, and made all the more so when accounting for this operating environment for DDs.

Accordingly, Department examiners should evaluate a bank's initial capital adequacy based on traditional, fiat-based principles where applicable, but also assess capital adequacy based on the risks unique to digital assets and the DD's business model and risk profile. Specifically, the Department considers, among other factors, the DD's pro forma financial statements, which are accompanied by various stress scenarios (i.e., baseline, adverse, severely adverse, and optimistic) and supporting assumptions and rationale, with the Department taking a conservative approach based on these factors given the lack of a historical track record with respect to these activities.

As part of ongoing supervision, Department examiners should assess whether DDs are able to document a clear understanding of exposure to risk events (whether through operational risk scenario planning or stress testing, matching of quality and duration of reserves to business activities, and other measures), with metrics and risk parameters as appropriate evidencing any mitigating controls in place. Examiners should review the DD's capital plan analyzing capital needs based on initial requirements, projected growth, and the availability of capital from identified sources. The Department may require the institution to modify its capital levels based on the size, risk profile, or activities of the institution. This supervisory review may consider whether:

(1) the DD has a sound and effective process commensurate with its overall risk and complexity to determine whether its overall capital is adequate and
(2) the DD maintains a capital level that is commensurate with its risks and is consistent with the DD's internal assessment and identified capital needs on an ongoing basis and as underlying conditions change (for example, changes in a bank's overall risks or economic conditions).[89]

Notably, DDs should have robust controls surrounding the tracking and offsetting of off-balance sheet items. Off-balance-sheet items are contingent assets or liabilities such as unused commitments, letters of credit, and derivatives. These items may expose institutions to credit risk, liquidity risk, or counterparty risk. Off-balance sheet risks could be the result from digital asset lending and other permissible activities, and the DDs should evaluate their impact on the capital level. Lastly, DDs should perform an audit to verify capital levels and assess the capital adequacy.

[91] OCC Comptroller's Handbook. *Capital and Dividends* (Version 1.0, July 2018).

As part of its overall supervisory review and preparations related to capital adequacy, Department examiners should consider any DD Capital Requirement Guidance that may be established and federal supervisory guidance (e.g., supplementary leverage ratio rule for custodial banks based on Federal Reserve guidance).

In its evaluation of capital adequacy, Department examiners should also consider any additional guidance or standards that may be pertinent to the DD's specific risk profile.

DD Capital Requirement Guidance

All DDs must meet the capital and surplus requirements set forth in Section 8-3013 of the NFIA:

1) The capital stock of each digital asset depository institution chartered under the Nebraska Financial Innovation Act shall be subscribed for as paid-up stock. No digital asset depository institution shall be chartered with capital stock of less than ten million dollars.

2) No digital asset depository institution shall commence business until the full amount of its authorized capital is subscribed and all capital stock is fully paid in. No digital asset depository institution may be chartered without a paid-up surplus fund of at least three years of estimated operating expenses in the amount disclosed pursuant to subsection (2) of section 8-3015[90] or in another amount required by the Director.

3) A digital asset depository institution may acquire additional capital prior to the granting of a charter and shall report this capital in its charter application.

Existing Federal Guidance

Applicable federal guidance includes the OCC's Capital and Dividends booklet, which presents a regulatory capital framework and provides guidance to examiners for assessing banks' capital adequacy and compliance with capital and dividend requirements for national banks and federal savings associations. Refer in particular to "Supervisory Review of Capital Planning and Adequacy" and subsequent examination procedures, which include detailed examination procedures whose objective is to "determine the adequacy of the bank's capital planning process, including the adequacy of the capital plan, for the overall risk profile, complexity, and corporate structure of the bank."[91]

For traditional national banks and federal savings associations, the capital adequacy of an institution is rated based on, but not limited to, an assessment of the following evaluation factors:

- The level and quality of capital and the overall financial condition of the institution.
- The ability of management to address emerging needs for additional capital.

[90] Section (2) of 8-3015: The incorporators under section 8-3012 shall apply to the Director for a charter. The application shall contain the digital asset depository institution's articles of incorporation, a detailed business plan, a comprehensive estimate of operating expenses for the first three years of operation, a complete proposal for compliance with the provisions of the Nebraska Financial Innovation Act, evidence of the capital required under section 8-3013, and any investors or owners holding ten percent or more equity in the digital asset depository institution. The Director may prescribe the form of application.

[91] OCC Comptroller's Handbook. *Capital and Dividends* (Version 1.0, July 2018).

- The nature, trend, and volume of problem assets, and the adequacy of allowances for loan and lease losses and other valuation reserves.
- The balance-sheet composition, including the nature and amount of intangible assets, market risk, concentration risk, and risks associated with nontraditional activities.
- Risk exposure represented by off-balance-sheet activities.
- The quality and strength of earnings, and reasonableness of dividends.
- Prospects and plans for growth, as well as past experience in managing growth.
- The bank's access to capital markets and other sources of capital, including support provided by a parent holding company.

Supplementary Leverage Ratio for Custodial Banking Organizations and Custody Banks[92]

On January 27, 2020, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the agencies) issued a final rule that excludes from the supplementary leverage ratio (SLR) certain central bank deposits of banking organizations predominantly engaged in custody, safekeeping, and asset servicing activities consistent with section 402 of the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA). Advanced approaches and Category III banking organizations are subject to the SLR requirement.

Under the final rule, a depository institution holding company is designated as a "custodial banking organization" and considered predominantly engaged in custody, safekeeping, and asset servicing activities if the U.S. top-tier depository institution holding company in the organization has a ratio of average assets under custody (AUC)-to-average total assets of at least 30:1 over the previous four calendar quarters. Similarly, under the provisions in the final rule applicable to national banks and federal savings associations (FSA), the OCC is designating as a "custody bank" any national bank or FSA that is a subsidiary of a custodial banking organization.

In addition, the amount of the deposits with a qualifying central bank that a custodial banking organization is permitted to exclude from the SLR is limited to the amount of on-balance-sheet deposit liabilities that are linked to fiduciary or custody and safekeeping accounts. Specifically, the final rule provides that a custodial banking organization would be able to exclude from its total leverage exposure the lesser of:

- the amount of central bank deposits placed at qualifying central banks by the custodial banking organization (including deposits placed by consolidated subsidiaries), or
- the amount of on-balance-sheet deposit liabilities of the custodial banking organization (including consolidated subsidiaries) that are linked to fiduciary or custodial and safekeeping accounts.

Capital Adequacy Component Ratings
Based on the above inputs, the Department aligns to existing federal standards with respect to its definitions of capital adequacy component ratings, as follows:

Table 1: Capital Adequacy Component Ratings

[92] OCC Bulletin 2020-53

1	A rating of 1 indicates a strong capital level relative to the institution's risk profile.
2	A rating of 2 indicates a satisfactory capital level relative to the financial institution's risk profile.
3	A rating of 3 indicates a less than satisfactory level of capital that does not fully support the institution's risk profile. The rating indicates a need for improvement, even if the institution's capital level exceeds minimum regulatory and statutory requirements.
4	A rating of 4 indicates a deficient level of capital. In light of the institution's risk profile, viability of the institution may be threatened. Assistance from shareholders or other external sources of financial support may be required.
5	A rating of 5 indicates a critically deficient level of capital such that the institution's viability is threatened. Immediate assistance from shareholders or other external sources of financial support is required.

5.1.2. Asset Quality

The asset quality rating reflects the quantity of existing and potential credit risk associated with the loan and investment portfolios, other real estate owned, and other assets, as well as off-balance-sheet transactions (including as applicable to digital assets). The ability of management to identify, measure, monitor, and control credit risk also is reflected here. The evaluation of asset quality should consider the adequacy of ALLL and weigh the exposure to counterparty, issuer, or borrower default under actual or implied contractual agreements. All other risks that may affect the value or marketability of an institution's assets, including, but not limited to, operating, market, reputation, strategic, or compliance risks, should also be considered.

As noted above, a DD cannot make any consumer loans for personal, property, or household purposes, mortgage loans, or commercial loans of any fiat currency and the provision of temporary credit relating to overdrafts. A DD, however, may facilitate the provision of digital asset business services resulting from the interaction of customers with centralized finance or decentralized finance platforms including, but not limited to, controllable electronic record exchange, staking, controllable electronic record lending, and controllable electronic record borrowing.[93]

The asset quality of a financial institution is rated based on an assessment of the following evaluation factors:

- The adequacy of underwriting standards, soundness of credit administration practices, and appropriateness of risk identification practices.
- The level, distribution, severity, and trend of problem, classified, nonaccrual, restructured, delinquent, and nonperforming assets for both on- and off-balance-sheet transactions.
- The adequacy of ALLL and other asset valuation reserves.
- The bank's credit risk arising from or reduced by off-balance-sheet transactions, such as unfunded commitments, credit derivatives, commercial and standby letters of credit, and lines of credit.
- The diversification and quality of the loan and investment portfolios.

[93] Neb. Stat. §8-3005(2)(b) (LB 646, 2021)

- The extent of securities underwriting activities and exposure to counterparties in trading activities.
- The existence of asset concentrations.
- The adequacy of loan and investment policies, procedures, and practices.
- The ability of management to properly administer its assets, including the timely identification and collection of problem assets.
- The adequacy of internal controls and management information systems.
- The volume and nature of credit documentation exceptions.

Table 2: Asset Quality Component Ratings

1	A rating of 1 indicates strong asset quality and credit administration practices. Identified weaknesses are minor in nature and risk exposure is modest in relation to capital protection and management's abilities. Asset quality in such institutions is of minimal supervisory concern.
2	A rating of 2 indicates satisfactory asset quality and credit administration practices. The level and severity of classifications and other weaknesses warrant a limited level of supervisory attention. Risk exposure is commensurate with capital protection and management's abilities.
3	A rating of 3 is assigned when asset quality or credit administration practices are less than satisfactory. Trends may be stable or indicate deterioration in asset quality or an increase in risk exposure. The level and severity of classified assets, other weaknesses, and risks require an elevated level of supervisory concern. There is generally a need to improve credit administration and risk management practices.
4	A rating of 4 is assigned to financial institutions with deficient asset quality or credit administration practices. The levels of risk and problem assets are significant and inadequately controlled, and they subject the financial institution to potential losses that, if left unchecked, may threaten its viability.
5	A rating of 5 represents critically deficient asset quality or credit administration practices that present an imminent threat to the institution's viability.

5.1.3. Management

This rating reflects the capability of the board and management, in their respective roles, to identify, measure, monitor, and control the risks of a bank's activities and to ensure a bank's safe, sound, and efficient operation in compliance with applicable laws and regulations. Generally, directors need not be actively involved in day-to-day operations; they should, however, provide clear guidance regarding acceptable risk exposure levels and ensure that appropriate policies, procedures, and practices have been established. Senior management is responsible for developing and implementing policies, procedures, and practices that translate the board's goals, objectives, and risk limits into prudent operating standards.[94]

[94] Refer to the "Corporate and Risk Governance" booklet of the Comptroller's Handbook for more information regarding the role of bank management and the board.

Depending on the nature and scope of an institution's activities, management practices may need to address some or all of the following risks: credit, market, operating or transaction, reputation, strategic, compliance, legal, liquidity, and other risks. Sound management practices are demonstrated by active oversight by the board and management; competent personnel; adequate policies, processes, and controls taking into consideration the size and sophistication of the institution and novelty and risks associated with digital assets; maintenance of an appropriate audit program and internal control environment; and effective risk monitoring and management information systems. This rating should reflect the board's and management's ability as it applies to all aspects of banking operations as well as other financial service activities in which the institution is involved. Consistent with the OCC, the Department considers AML/CFT examination findings when assigning the management rating, since serious AML/CFT deficiencies create a presumption that the rating will be adversely affected.[95]

The capability and performance of management and the board is rated based on an assessment of the following evaluation factors:

- The level and quality of oversight and support of all institution activities by the board and management.
- The ability of the board and management, in their respective roles, to plan for, and respond to, risks that may arise from changing business conditions or the initiation of new activities or products (whether traditional, fiat-based activity or related to digital assets).
- The adequacy of, and conformance with, appropriate internal policies and controls addressing the operations and risks of significant activities.
- The accuracy, timeliness, and effectiveness of management information and risk monitoring systems appropriate for the institution's size, complexity, and risk profile.
- The adequacy of audits and internal controls to promote effective operations and reliable financial and regulatory reporting; safeguard assets; and ensure compliance with laws, regulations, and internal policies.
- Compliance with laws and regulations.
- Responsiveness to recommendations from auditors and supervisory authorities.
- Management depth and succession, including appropriate and evidenced segregation of duties where appropriate.
- The extent that the board and management are affected by, or susceptible to, a dominant influence or concentration of authority.
- The reasonableness of compensation policies and avoidance of self-dealing.
- The demonstrated willingness to serve the legitimate banking needs of the community.
- The overall performance of the bank and its risk profile.

Table 3: Management Component Ratings

1	A rating of 1 indicates strong performance by management and the board and strong risk management practices relative to the institution's size, complexity, and risk profile. All significant risks are consistently and effectively identified, measured, monitored, and controlled. Management and the board have demonstrated the ability to promptly and successfully address existing and potential problems and risks.

[95] Refer to OCC Bulletin 2012-30.

2	A rating of 2 indicates satisfactory management and board performance and risk management practices relative to the institution's size, complexity, and risk profile. Minor weaknesses may exist but are not material to the safety and soundness of the institution and are being addressed. In general, significant risks and problems are effectively identified, measured, monitored, and controlled.
3	A rating of 3 indicates management and board performance that need improvement or risk management practices that are less than satisfactory given the nature of the institution's activities. The capabilities of management or the board may be insufficient for the type, size, or condition of the institution. Problems and significant risks may be inadequately identified, measured, monitored, or controlled.
4	A rating of 4 indicates deficient management and board performance or risk management practices that are inadequate considering the nature of an institution's activities. The level of problems and risk exposure is excessive. Problems and significant risks are inadequately identified, measured, monitored, or controlled and require immediate action by the board and management to preserve the soundness of the institution. Replacing or strengthening management or the board may be necessary.
5	A rating of 5 indicates critically deficient management and board performance or risk management practices. Management and the board have not demonstrated the ability to correct problems and implement appropriate risk management practices. Problems and significant risks are inadequately identified, measured, monitored, or controlled and now threaten the continued viability of the institution. Replacing or strengthening management or the board is necessary.

5.1.4. Earnings

This rating reflects not only the quantity and trend of earnings but also factors that may affect the sustainability or quality of earnings. The quantity as well as the quality of earnings can be affected by excessive or inadequately managed credit risk that may result in loan losses and require additions to ALLL, or by high levels of market risk that may unduly expose an institution's earnings to volatility in interest rates. The quality of earnings may be diminished by undue reliance on extraordinary gains, nonrecurring events, or favorable tax effects. Future earnings may be adversely affected by an inability to forecast or control funding and operating expenses, improperly executed or ill-advised business strategies, or poorly managed or uncontrolled exposure to other risks.

The rating of an institution's earnings is based on an assessment of the following evaluation factors:

- The level of earnings, including trends and stability.
- The ability to provide for adequate capital through retained earnings.
- The quality and sources of earnings.
- The level of expenses in relation to operations.
- The adequacy of the budgeting systems, forecasting processes, and management information systems in general.
- The adequacy of provisions to maintain ALLL and other valuation allowance accounts.
- The exposure of earnings to market risk, such as interest rate, foreign exchange, and price risks.

Table 4: Earnings Component Ratings

1	A rating of 1 indicates earnings that are strong. Earnings are more than sufficient to support operations and maintain adequate capital and allowance levels after consideration is given to asset quality, growth, and other factors affecting the quality, quantity, and trend of earnings.
2	A rating of 2 indicates earnings that are satisfactory. Earnings are sufficient to support operations and maintain adequate capital and allowance levels after consideration is given to asset quality, growth, and other factors affecting the quality, quantity, and trend of earnings. Earnings that are relatively static, or even experiencing a slight decline, may receive a 2 rating provided the institution's level of earnings is adequate in view of the assessment factors listed above.
3	A rating of 3 indicates earnings that need to be improved. Earnings may not fully support operations and provide for the accretion of capital and allowance levels in relation to the institution's overall condition, growth, and other factors affecting the quality, quantity, and trend of earnings.
4	A rating of 4 indicates earnings that are deficient. Earnings are insufficient to support operations and maintain appropriate capital and allowance levels. Institutions so rated may be characterized by erratic fluctuations in net income or net interest margin, the development of significant negative trends, nominal or unsustainable earnings, intermittent losses, or a substantive drop in earnings from the previous years.
5	A rating of 5 indicates earnings that are critically deficient. A financial institution with earnings rated 5 is experiencing losses that represent a distinct threat to its viability through the erosion of capital.

5.1.5. Liquidity

In evaluating the adequacy of a financial institution's liquidity position, consideration should be given to the current level and prospective sources of liquidity compared with funding needs, as well as to the adequacy of funds management practices relative to the institution's size, complexity, and risk profile. In general, funds management practices should ensure that an institution is able to maintain a level of liquidity sufficient to meet its financial obligations in a timely manner and to fulfill the legitimate banking needs of its community. Practices should reflect the ability of the institution to manage unplanned changes in funding sources, as well as react to changes in market conditions that affect the ability to quickly liquidate assets with minimal loss. In addition, funds management practices should ensure that liquidity is not maintained at a high cost, or through undue reliance on funding sources that may not be available in times of financial stress or adverse changes in market conditions.

The Nebraska Financial Innovation Act requires the DD to maintain unencumbered liquid assets denominated in United States dollars valued at no less than one hundred percent of the value of any outstanding stablecoin issued by the digital asset depository[96]. The definitions of liquid assets are the following:

[96] Nebraska Legislature, Amendments to LB707 (Amendments to Standing Committee amendments, AML1859), AM2205 LB649 (March 2022).

1) United States currency held on the premises of the digital asset depository that is not a digital asset depository institution;

2) United States currency held for the digital asset depository by a federal reserve bank or a Federal Deposit Insurance Corporation-insured financial institution which has a main-chartered office in [the state of Nebraska], any branch thereof in [the state of Nebraska], or any branch of the financial institution which maintained a main-chartered office in [the state of Nebraska] prior to becoming a branch of such financial institution; or

3) Investments which are highly liquid and obligations of the United States Treasury or other federal agency obligations, consistent with rules and regulations or order adopted by the Director.

Liquidity is rated based on an assessment of the following evaluation factors:

- The adequacy of liquidity sources to meet present and future needs and the ability of the institution to meet liquidity needs without adversely affecting its operations or condition.
- The availability of assets readily convertible to cash without undue loss.
- The access to money markets and other sources of funding.
- The level of diversification of funding sources, both on and off the balance sheet.
- The degree of reliance on short-term, volatile sources of funds, including borrowings and brokered deposits, to fund longer-term assets.
- The trend and stability of deposits.
- The ability to securitize and sell certain pools of assets.
- Management's capability to properly identify, measure, monitor, and control the institution's liquidity position, including the effectiveness of funds management strategies, liquidity policies, management information systems, and contingency funding plans.

Table 5: Liquidity Component Ratings

1	A rating of 1 indicates strong liquidity levels and well-developed funds management practices. The institution has reliable access to sufficient sources of funds on favorable terms to meet present and anticipated liquidity needs.
2	A rating of 2 indicates satisfactory liquidity levels and funds management practices. The institution has access to sufficient sources of funds on acceptable terms to meet present and anticipated liquidity needs. Modest weaknesses may be evident in funds management practices.
3	A rating of 3 indicates liquidity levels or funds management practices in need of improvement. Institutions rated 3 may lack ready access to funds on reasonable terms or may evidence significant weaknesses in funds management practices.
4	A rating of 4 indicates deficient liquidity levels or inadequate funds management practices. Institutions rated 4 may not have or be able to obtain a sufficient volume of funds on reasonable terms to meet liquidity needs.
5	A rating of 5 indicates liquidity levels or funds management practices so critically deficient that the continued viability of the institution is threatened. Institutions rated 5

	require immediate external financial assistance to meet maturing obligations or other liquidity needs.

5.1.6. Sensitivity to Market Risk

The sensitivity to market risk component reflects the degree to which changes in interest rates, foreign exchange rates, commodity prices, or equity prices can adversely affect a financial institution's earnings or economic capital. When evaluating this component, consideration should be given to management's ability to identify, measure, monitor, and control market risk; the institution's size; the nature and complexity of its activities; and the adequacy of its capital and earnings in relation to its level of market risk exposure.

The Risk Management Association noted that "market risks [for certain digital assets] are idiosyncratic, as the currency trades only on demand. There is a finite amount of the currency, which means that it can suffer from liquidity concerns and limited ownership may make it susceptible to market manipulation. Furthermore, given its limited acceptance and lack of alternatives, the currency can appear more volatile than other physical currencies, fueled by speculative demand and exacerbated by hoarding."[97] Moreover, given that digital assets tend to be treated by institutional investors as "risk-on" investments, market movements have demonstrable effects on digital asset prices. When assessing market risk, DDs should have a robust system to capture all material on- and off-balance-sheet positions and incorporate a stress testing process to identify and quantify the DD's interest rate risk exposure and potential problem areas, especially related to digital assets. When measuring risk, management should give special consideration to concentrations in instruments or markets. Positions may be more difficult to liquidate or offset in stressful situations, and concentrations can amplify this risk.

For many institutions, the primary source of market risk arises from nontrading positions and their sensitivity to changes in interest rates. In some larger institutions, foreign operations can be a significant source of market risk. For some institutions, trading activities are a major source of market risk.
Market risk is rated based on an assessment of the following evaluation factors:

- The sensitivity of the financial institution's earnings or the economic value of its capital to adverse changes in interest rates, foreign exchanges rates, commodity prices, or equity prices.
- The ability of management to identify, measure, monitor, and control exposure to market risk given the institution's size, complexity, and risk profile.
- The nature and complexity of interest rate risk exposure arising from nontrading positions.
- If appropriate, the nature and complexity of market risk exposure arising from trading, asset management activities, and foreign operations.

Table 6: Sensitivity to Market Risk Component Ratings

[97] Risk Management Association. What Are the Inherent Risks Associated with Cryptocurrency?

1	A rating of 1 indicates that market risk sensitivity is well controlled and that there is minimal potential that the earnings performance or capital position will be adversely affected. Risk management practices are strong for the size, sophistication, and market risk accepted by the institution. The level of earnings and capital provide substantial support for the amount of market risk taken by the institution.
2	A rating of 2 indicates that market risk sensitivity is adequately controlled and that there is only moderate potential that the earnings performance or capital position will be adversely affected. Risk management practices are satisfactory for the size, sophistication, and market risk accepted by the institution. The level of earnings and capital provide adequate support for the amount of market risk taken by the institution.
3	A rating of 3 indicates that control of market risk sensitivity needs improvement or that there is significant potential that the earnings performance or capital position will be adversely affected. Risk management practices need to be improved given the size, sophistication, and level of market risk accepted by the institution. The level of earnings and capital may not adequately support the amount of market risk taken by the institution.
4	A rating of 4 indicates that control of market risk sensitivity is unacceptable or that there is high potential that the earnings performance or capital position will be adversely affected. Risk management practices are deficient for the size, sophistication, and level of market risk accepted by the institution. The level of earnings and capital provide inadequate support for the amount of market risk taken by the institution.
5	A rating of 5 indicates that control of market risk sensitivity is unacceptable or that the level of market risk taken by the institution is an imminent threat to its viability. Risk management practices are wholly inadequate for the size, sophistication, and level of market risk accepted by the institution.

5.2. Trust ("UITRS")

The Uniform Interagency Trust Rating System was adopted in 1978 and revised in 1998.[98] The UITRS considers certain managerial, operational, financial, and compliance factors that are common to all institutions with fiduciary activities. Under this system, the supervisory agencies endeavor to ensure that all institutions with fiduciary activities are evaluated in a comprehensive and uniform manner, and that supervisory attention is appropriately focused on those institutions exhibiting weaknesses in their fiduciary operations.
The five key components used to assess an institution's fiduciary activities are the

- capability of management.
- adequacy of operations, controls, and audits.
- quality and level of earnings.
- compliance with governing instruments, applicable laws, and regulations (including self-dealing and conflicts of interest laws and regulations), and sound fiduciary principles.
- management of fiduciary assets.

Under the UITRS,[99] the fiduciary activities of financial institutions are assigned a composite rating based on an evaluation and rating of five essential components of an institution's fiduciary activities. These components are the capability of management; the adequacy of operations, controls, and audits; the quality and level of earnings; compliance with governing instruments, applicable law (including self-dealing and conflicts of interest laws and regulations), and sound fiduciary principles; and the management of fiduciary assets.
Composite and component ratings are based on a scale of 1 to 5. A 1 is the highest rating; it indicates the strongest performance and risk management practices and the lowest degree of supervisory concern. A 5 is the lowest rating; it indicates the weakest performance and risk management practices and the highest degree of supervisory concern. Evaluation of the composite and component ratings considers the size and sophistication, the nature and complexity, and the risk profile of the institution's fiduciary activities.

The composite rating generally bears a close relationship to the component ratings assigned, but the composite rating is not derived by computing an arithmetic average of the component ratings. Each component rating is based on a qualitative analysis of the factors comprising that component and its interrelationship with the other components. When examiners assign a composite rating, some components may be given more weight than others depending on the situation at the institution. In general, assignment of a composite rating may incorporate any factor that bears significantly on the overall administration of the financial institution's fiduciary activities. Assigned composite and component ratings are disclosed to the institution's board and senior management.

Management's ability to respond to changing circumstances and to address the risks that may arise from changing business conditions, or the initiation of new fiduciary activities or products, is an important factor in evaluating an institution's overall fiduciary risk profile and the level of

[98] For additional reference materials, see the OCC Custody Services booklet as part of the *Comptroller's Handbook* as well as the FDIC Trust Examination Manual, which includes additional examination aids.
[99] Excerpt is from 63 Fed. Reg. 54704-54711, "Uniform Interagency Trust Rating System."

supervisory attention warranted. For this reason, the management component is given special consideration when examiners assign a composite rating. Management's ability to identify, measure, monitor, and control the risks of its fiduciary operations is also considered when assigning each component rating. Appropriate management practices may vary considerably among financial institutions, depending on the size, complexity, and risk profiles of their fiduciary activities. For less complex institutions engaged solely in traditional fiduciary activities and whose directors and senior managers are actively involved in the oversight and management of day-to-day operations, relatively basic management systems and controls may be adequate. At more complex institutions, detailed and formal management systems and controls are needed to address a broader range of activities and to provide senior managers and directors with the information they need to supervise day-to-day activities. All institutions are expected to properly manage their risks. For less complex institutions engaging in less risky activities, detailed or highly formalized management systems and controls are not required to receive strong or satisfactory component or composite ratings. The following two sections contain the composite rating definitions and the descriptions and definitions for the five component ratings.

UITRS Composite Ratings

Composite ratings are based on an evaluation of how an institution conducts its fiduciary activities. The review encompasses the capability of management, the soundness of policies and practices, the quality of service rendered to the public, and the effect of fiduciary activities on the institution's soundness. The five key components used to assess an institution's fiduciary activities are the

- capability of management.
- adequacy of operations, controls, and audits.
- quality and level of earnings.
- compliance with governing instruments, applicable laws, and regulations (including self-dealing and conflicts of interest laws and regulations), and sound fiduciary principles.
- management of fiduciary assets.

Table 7: UITRS Composite Ratings

1	Administration of fiduciary activities is sound in every respect. Generally, all components are rated 1 or 2. Any weaknesses are minor and can be handled in a routine manner by management. The institution is in substantial compliance with fiduciary laws and regulations. Risk management practices are strong relative to the size, complexity, and risk profile of the institution's fiduciary activities. Fiduciary activities are conducted in accordance with sound fiduciary principles and give no cause for supervisory concern.
2	Administration of fiduciary activities is fundamentally sound. Generally, no component rating should be more severe than 3. Only moderate weaknesses are present and are well within management's capabilities and willingness to correct. Fiduciary activities are conducted in substantial compliance with laws and regulations. Overall risk management practices are satisfactory relative to the institution's size, complexity, and risk profile. There are no material supervisory concerns and, as a result, the supervisory response is informal and limited.
3	Administration of fiduciary activities exhibits some degree of supervisory concern in one or more of the component areas. A combination of weaknesses exists that may

	range from moderate to severe; however, the magnitude of the deficiencies generally does not cause a component to be rated more severely than 4. Management may lack the ability or willingness to effectively address weaknesses within appropriate time frames. Additionally, fiduciary activities may reveal some significant noncompliance with laws and regulations. Risk management practices may be less than satisfactory relative to the institution's size, complexity, and risk profile. While problems of relative significance may exist, they are not of such importance as to pose a threat to the trust beneficiaries generally, or to the soundness of the institution. The institution's fiduciary activities require more than normal supervision and may include formal or informal enforcement actions.
4	Fiduciary activities generally exhibit unsafe and unsound practices or conditions, resulting in unsatisfactory performance. The problems range from severe to critically deficient and may be centered on inexperienced or inattentive management, weak or dangerous operating practices, or an accumulation of unsatisfactory features of lesser importance. The weaknesses and problems are not being satisfactorily addressed or resolved by the board and management. There may be significant noncompliance with laws and regulations. Risk management practices are generally unacceptable relative to the size, complexity, and risk profile of fiduciary activities. These problems pose a threat to the account beneficiaries generally and, if left unchecked, could evolve into conditions that could cause significant losses to the institution and ultimately undermine the public confidence in the institution. Close supervisory attention is required, which means, in most cases, formal enforcement action is necessary to address the problems.
5	Fiduciary activities are conducted in an extremely unsafe and unsound manner. Administration of fiduciary activities is critically deficient in numerous major respects, with problems resulting from incompetent or neglectful administration, flagrant or repeated disregard for laws and regulations, or a willful departure from sound fiduciary principles and practices. The volume and severity of problems are beyond management's ability or willingness to control or correct. Such conditions evidence a flagrant disregard for the interests of the beneficiaries and may pose a serious threat to the soundness of the institution. Continuous close supervisory attention is warranted and may include termination of the institutions fiduciary activities.

5.3. Information Technology Rating ("URSIT")

On January 13, 1999, the FFIEC issued the Uniform Rating System for Information Technology (URSIT) to uniformly assess financial institution and service provider risks introduced by IT.[100] Examiners assign a composite-only rating to all banks and their operating subsidiaries and assign composite and component ratings to technology service providers.[101]

The URSIT consists of a composite and four component ratings:

- Audit
- Management
- Development and acquisition
- Support and delivery

Examiners focus on the risk issues inherent in automated information systems, rather than the functional activities rated by the URSIT components. These risk issues, common to all automated systems, include:

- management of technology resources, whether in-house or outsourced.
- integrity of automated information (i.e., reliability of data and protection from unauthorized change).
- availability of automated information (i.e., adequacy of business resumption and contingency planning).
- confidentiality of information (i.e., protection from accidental or inadvertent disclosure).

These common technology risk issues are used to assess the overall performance of IT within an organization. Department examiners evaluate each issue to assess the institution's ability to identify, measure, monitor, and control IT risks, leveraging existing federal examinations processes. Each institution is then assigned an URSIT composite rating based on the overall results of the evaluation. The rating is based on a scale of 1 through 5 in ascending order of supervisory concern, with 1 representing the best rating and least degree of concern, and 5 representing the worst rating and highest degree of concern.

URSIT Composite Ratings

Table 8: URSIT Composite Ratings

1	Financial institutions and service providers rated composite 1 exhibit strong performance in every respect and generally have components rated 1 or 2. Weaknesses in IT are minor in nature and are easily corrected during the normal course of business. Risk management processes provide a comprehensive program to identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are well defined and fully integrated throughout the organization. This allows management

[100] 64 Fed. Reg. 3109-3116, "Uniform Rating System for Information Technology," January 20, 1999. The OCC implemented the URSIT rating system for all banks and OCC-supervised service provider examinations that began after April 1, 1999. The URSIT replaced the rating system for information systems adopted in 1978.
[101] The OCC revised the application of the URSIT for examinations that began after April 1, 2001, to assign a composite-only IT rating to banks and their operating subsidiaries.

	to quickly adapt to changing market, business, and technology needs of the entity. Management identifies weaknesses promptly and takes appropriate corrective action to resolve audit and regulatory concerns. The financial condition of the service provider is strong and overall performance shows no cause for supervisory concern.
2	Financial institutions and service providers rated composite 2 exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes, or system development. Generally, senior management corrects weaknesses in the normal course of business. Risk management processes adequately identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are defined but may require clarification, better coordination, or improved communication throughout the organization. As a result, management anticipates, but responds less quickly to, changes in market, business, and technological needs of the entity. Management normally identifies weaknesses and takes appropriate corrective action. Greater reliance is, however, placed on audit and regulatory intervention to identify and resolve concerns. The financial condition of the service provider is acceptable, and while internal control weaknesses may exist, there are no significant supervisory concerns. As a result, supervisory action is informal and limited.
3	Financial institutions and service providers rated composite 3 exhibit some degree of supervisory concern because of a combination of weaknesses that may range from moderate to severe. If weaknesses persist, further deterioration in the condition and performance of the institution or service provider is likely. Risk management processes may not effectively identify risks and may not be appropriate for the size, complexity, or risk profile of the entity. Strategic plans are vaguely defined and may not provide adequate direction for IT initiatives. As a result, management often has difficulty responding to changes in business, market, and technological needs of the entity. Self-assessment practices are weak and are generally reactive to audit and regulatory exceptions. Repeat concerns may exist, indicating that management may lack the ability or willingness to resolve concerns. The financial condition of the service provider may be weak or negative trends may be evident. While financial or operational failure is unlikely, increased supervision is necessary. Formal or informal supervisory action may be necessary to secure corrective action.
4	Financial institutions and service providers rated composite 4 operate in an unsafe and unsound environment that may impair the future viability of the entity. Operating weaknesses are indicative of serious managerial deficiencies. Risk management processes inadequately identify and monitor risk, and practices are not appropriate given the size, complexity, and risk profile of the entity. Strategic plans are poorly defined and not coordinated or communicated throughout the organization. As a result, management and the board are not committed to meeting technological needs and may be incapable of meeting those needs. Management does not perform self-assessments and demonstrates an inability or unwillingness to correct audit and regulatory concerns. The financial condition of the service provider is severely impaired or deteriorating. Failure of the financial institution or service provider may be likely unless IT problems are remedied. Close supervisory attention is necessary and, in most cases, formal enforcement action is warranted.

5	Financial institutions and service providers rated composite 5 exhibit critically deficient operating performance and are in need of immediate remedial action. Operational problems and serious weaknesses may exist throughout the organization. Risk management processes are severely deficient and provide management little or no perception of risk relative to the size, complexity, and risk profile of the entity. Strategic plans do not exist or are ineffective, and management and the board provide little or no direction for IT initiatives. As a result, management is unaware of, or inattentive to, technological needs of the entity. Management is unwilling to correct audit and regulatory concerns or is incapable of doing so. The financial condition of the service provider is poor and failure is highly probable because of poor operating performance or financial instability. Ongoing supervisory attention is necessary.

6. Recovery and Resolution Planning

The Department expects that DDs will submit a draft recovery and resolution plan to the Director for review no later than six (6) months after the DD commences operations.

The draft recovery and resolution plan shall generally encompass the requirements of a national bank recovery plan and the "targeted resolution plan" specified by 12 C.F.R. § 243.6, as of June 1, 2020, and will outline potential recovery actions to address significant financial or operational stress that could threaten the safety and soundness of the DD, as well as strategies for orderly disposition of the institution without the need for the appointment of a receiver.

The plan will also identify at least two (2) business entities that could potentially acquire the special purpose depository institution, or any component of the institution, in the event of financial distress, receivership or another contingency warranting use of the plan. The plan shall include a procedure for quickly and safely transferring all assets of the institution to another entity and a procedure for liquidating the assets of the institution.

Based on the submission, the Director will review the draft recovery and resolution plan and determine that it adequately addresses the risks inherent in a potential recovery or resolution scenario in a way that protects the customers of the institution.

After the submission of the initial recovery and resolution plan, the DD's Board of Directors is responsible for annual review and amendment of the recovery and resolution plan to account for material changes in each of the following areas:

- Critical operations or core business lines, including information technology;
- Corporate structure, including interconnections and interdependences with other business entities, management, and succession planning;
- Deposits and assets under custody, assets under management or similar relationships;
- Funding, liquidity, or capital needs or other sources;
- Changes in law or regulation; and
- Any other area determined to be relevant by the Director.

7. Disaster Recovery and Business Continuity Planning[102]

Business continuity management is the process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services. Disruptions such as cyber events, natural disasters, or man-made events can interrupt a bank's operations and can have a broader impact on the financial sector. The focus of business continuity management should be on more than just the planning process to recover operations after an event. It also should include the continued maintenance of systems and controls for the resilience and continuity of operations. Resilience incorporates proactive measures to mitigate disruptive events and evaluate a bank's recovery capabilities.[103]

The Department expects that DDs, in accordance with their custodial and fiduciary responsibilities, will establish, implement, and maintain written procedures relating to a business continuity and succession plan. The plan shall provide for at least the following:

1. The protection, backup, and recovery of books and records.
2. Alternate means of communication with customers, regulators, key personnel, employees, vendors, and service providers, including third party custodians. Such communications shall include, but not be limited to, providing notice of a significant business interruption or the death or unavailability of key personnel or other disruptions or cessation of business activities.
3. Office relocation in the event of temporary or permanent loss of a principal place of business.
4. Assignment of duties to qualified responsible persons in the event of the death or unavailability of key personnel.
5. Otherwise minimizing service disruptions and client harm that could result from a sudden significant business interruption.

Business Continuity Planning, along with other [procedures], should be revisited on a recurring basis. These procedures should include the scenario planning to be undertaken in connection with development of the DD's contingency planning and business continuity plans.

Examiners should request the Disaster Recovery Plans, Business Continuity Plans, Business Resiliency Plans, and/or Emergency Preparedness Plans. Additional considerations pertaining to associated risk management include[104]:

- Has the DD identified all applicable risks (e.g., service provider interruption, natural disaster, death or disability of key employee, equipment failures, cybersecurity event, terrorist acts, etc.)?
- Once the risks are identified, has the DD prepared a business impact analysis or risk assessment to determine how to manage the impact of such risks on the firm and its customers?

[102] Refer to Nebraska Administrative Code 48 NAC 07.013: Business Continuity and Succession Planning
[103] OCC. OCC Bulletin 2019-57: FFIEC Information Technology Examination Handbook: Revised Business Continuity Management Booklet, (November 2019). Refer to the FFIEC Business Continuity Management Booklet for additional details.
[104] Refer to Nebraska Department of Banking and Finance Business Continuity and Succession Planning training.

- Does the Plan include recovery plans such as the data backup and recovery procedure, record retention, office relocation plan, and customer access to information and accounts?
- Does the Plan address both temporary and permanent disruptions?
- Does the Plan address the implications of corporate structure (e.g., contracts, bank accounts, etc.)?
- Does the Plan address areas such as passwords to key systems, licensing requirements, and responsibility for communication between all stakeholders (e.g., employees, customers, vendors, broker-dealers/custodians, service providers, and regulators)?
- Is there training in place?

Refer to section 3.3.21 "Business Continuity Considerations" of the *DD Information Security Examination Manual* for additional information on InfoSec-specific considerations as they pertain to business continuity.

8. Appendix

Appendix A. Supervisory Guidance and Secondary Sources

U.S. Supervisory Guidance and Secondary Sources:

- CFPB. Consumer Laws and Regulations: Unfair, Deceptive, or Abusive Acts or Practices, Manual v.3 (March 2022).
- Congressional Research Service Report. "Digital Assets and SEC Regulation," R46208, (June 2021).
- FDIC. RMS Manual of Examination Policies.
- Nebraska Legislature. Nebraska Revised Statutes: Chapter 8.
- OCC. Examination Process: Bank Supervision Process (Version 1.1., September 2019).
- OCC. Interpretive Letter #1170, Vol. 33, No. 7 ("Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers") (July 2020).
- OCC. OCC Bulletin 2017-43: New, Modified, or Expanded Bank Products and Services: Risk Management Principles (October 2017).
- OCC. OCC Bulletin 2020-10: Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 (March 2020).
- OCC. OCC Bulletin 2020-94: Sound Practices to Strengthen Operational Resilience (October 2020).
- OCC. *OCC 98-3, Technology Risk Management, Guidance for Bankers and Examiner* (February 1998).
- OCC. *Policies and Procedures Manual – PPM 5000-7 (Subject: Civil Monetary Penalties)* (November 2018).
- OCC. *Policies and Procedures Manual – PPM 5310-3 (Subject: Bank Enforcement Actions and Related Matters)* (November 2018).
- OCC. OCC Bulletin 2020-94, Sound Practices to Strengthen Operational Resilience (October 2020).
- The White House. Presidential Actions: Executive Order on Ensuring Responsible Development of Digital Assets. (March 2022).

Other Supervisory Guidance and Secondary Sources:

- Bank for International Settlements – Basel Committee on Banking Supervision. *Consultative Document: Principles for Operational Resilience* (August 2020).

- Bank for International Settlements – Basel Committee on Banking Supervision. *Discussion Paper: Designing a Prudential Treatment for Crypto-Assets* (December 2019).

- U.K. Financial Conduct Authority's *Policy Statement 19/22: Guidance on Cryptoassets – Feedback and Final Guidance to CP 19/3* (July 2019).

Appendix B. Abbreviations

ALLL	Allowances for Loan and Lease Losses
BIS	Bank of International Settlements
AML/CFT	Bank Secrecy Act/Anti-Money Laundering
CAMELS	Capital Adequacy, Asset Quality, Management, Earnings, and Liquidity
CFPB	Consumer Financial Protection Bureau
CMP	Civil Monetary Penalty
CMS	Compliance Management System
DD	Digital Asset Depository (under Nebraska's NFIA)
DLT	Distributed Ledger Technology
EIC	Examiner in Charge
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
FinTech	Financial Technology
ICO	Initial Coin Offering
InfoSec	Information Security
IT	Information Technology
ITCC	Information Technology, Trust, Consumer Compliance, and Community Reinvestment Act
KYC	Know-Your-Customer
MIS	Management Information Systems
MOU	Memorandum of Understanding
MRBA	Matter Requiring Board Attention
NFIA	Nebraska Financial Innovation Act
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
RAS	Risk Assessment System
RMA	Risk Management Association
ROCA	Interagency uniform supervisory rating system for federal branches and agencies. ROCA integrates ratings from four component areas: risk management, operational controls, compliance, and asset quality. These components represent the major activities or processes of a branch or agency that may raise supervisory concern.
SEC	Securities and Exchange Commission
UDAAP	Unfair, deceptive, abusive acts and practices
UITRS	Uniform Interagency Trust Rating System
URSIT	Uniform Rating System for Information Technology