Coalition for Financial Ecosystem Standards

August 5, 2025

Senator Tim Scott, Chairman
Senator Cynthia Lummis
Senator Bill Hagerty
Senator Bernie Moreno
Senate Banking Committee
534 Dirksen Senate Office Building
Washington, D.C. 20510

**Re: The Coalition for Financial Ecosystem Standards Response to the Senate Banking Committee Digital Asset Market Structure Request for Information**

Dear Senators Scott, Lummis, Hagerty, and Moreno,

The Coalition for Financial Ecosystem Standards (CFES) appreciates the opportunity to respond to the Senate Banking Committee's Request for Information (RFI) on digital asset market structure legislation. CFES supports the compliant growth and innovation of financial services through industry-led standards development. Our coalition reflects nearly 20 members, comprising of leading fintechs and community banks. Our work has been covered by Forbes, American Banker, and Politico, and we engage regularly with prudential regulators at the federal and state level.

We write specifically to address your request for comments regarding the establishment of a standards setting organization (SSO), coordination amongst regulators, and options for protecting innovation within a regulatory structure. In short, we propose that Congress contemplate public-private partnerships that allow industry to more closely partner with regulators to align compliance and risk management expectations. Standards, as defined in Section I below, are adaptable, reflective of technological evolutions, and offer greater clarity to market participants.

Over the past year, CFES consulted with a multitude of stakeholders to define a comprehensive set of standards across 54 distinct areas including Anti-Money Laundering (BSA/AML), Compliance Management Systems, Third-Party Risk Management, Complaint Handling, Operational Risk, and Marketing and Product Compliance. These standards utilize a five-level maturity framework (from Rudimentary to Optimized) that accommodates different business models and organizational capabilities while establishing clear benchmarks for progression toward best practices. (See, Appendix A and B).

Through our experiences, we demonstrated that CFES can uniquely keep pace with innovation and emerging best practices by fostering dialogue and developing frameworks that promote competition

and innovation, while the CFES certification process fosters robust risk management and regulatory compliance. We anticipate that this expertise, and the lessons observed through this process, will translate to digital assets partnerships. We believe that industry-led standards can address many of the issues identified in your RFI.

**I. The Case for Standards-Based Digital Asset Regulation**

The rapid evolution of digital asset markets created a critical gap that Congress importantly addressed with its legislative actions. Now that Congress provided statutory clarity, regulators will be left with the important task of operationalizing the statute into evergreen rules and guidance that provide clarity without stifling innovation. This challenge mirrors what CFES has observed and addressed in traditional bank-fintech partnerships where the lack of clear compliance standards undermines operational viability and creates regulatory uncertainty.

While Congressional legislation provides clarity for regulators about their responsibilities, the guidance that regulators release often fails to provide detail to industry participants and business operators In other cases, where regulation is specific enough to deliver market certainty, the rapid evolution of technology may obviate the rules over time. As your counterparts in the House Financial Services Committee recognized in their March 28, 2025 letter to federal prudentials, this problem has a solution: "When financial institutions are given clear expectations and rules that are commensurate to their complexity and risk profiles, the American banking system can thrive."

Our work developing standards for bank–fintech partnerships has shown how legacy regulatory frameworks have a difficult time applying to nonbanks and other modern financial service delivery models. Technology evolves rapidly, and best practices shift in response. When regulation and related guidance lags behind industry innovation, it creates costly ambiguities and weakens the resilience of the banking system. Digital asset markets introduce even more complex technical, operational, and compliance challenges that require specialized expertise. Without a regulatory apparatus that can keep pace with technological change, we risk repeating the same pattern: static rules that quickly become obsolete, leading to regulation by enforcement and discouraging innovation out of fear of deviating from traditional models.

Standards represent detailed, consensus-based frameworks that establish specific criteria for operational practices, risk management, and compliance protocols. Unlike broad regulatory guidance, standards provide granular, implementable requirements that industry participants can follow to achieve consistent outcomes. Standards can provide much needed clarity where technologies and best practices evolve faster than regulators can release rules. What's more, standards can be updated regularly to reflect changes beget by rapidly evolving technology. The details that standards put forth align expectations more clearly for compliance and risk management, while also allowing for innovation and safe growth. And importantly, standards can serve as a force multiplier for regulators and examiners, allowing them to more efficiently and effectively fulfill their responsibilities.

Coalition for Financial Ecosystem Standards

**BSA/AML Compliance: A Deep Dive into Industry-Led Standards**

CFES's ongoing research into BSA/AML compliance in modern financial services illustrates the urgent need for standards-based approaches in digital asset markets.

The Bank Secrecy Act framework, largely developed in the early 2000s for in-person banking relationships, faces growing limitations as financial services migrate toward digital delivery models. As FinCEN has acknowledged, "considerable changes in the way that customers interact with banks and receive financial services" have occurred since key BSA provisions took effect, including remote onboarding, embedded finance, synthetic identities, and rapidly advancing fraud methodologies.

These challenges multiply in digital asset markets, where traditional BSA/AML frameworks struggle to address the unique characteristics of blockchain-based transactions, programmable money, and decentralized protocols. Current regulatory guidance provides high-level principles but lacks the detailed implementation standards necessary for consistent compliance across different business models and technologies.

CFES's existing BSA/AML standards demonstrate how industry-led approaches can bridge these gaps. Our standards provide granular guidance on critical areas such as AML governance, transaction monitoring, customer due diligence, and fraud prevention. An industry-led standard-setting approach for digital assets could build on this foundation by developing:

- Technical standards for transaction monitoring in blockchain environments that account for pseudonymous transactions and programmable compliance
- Risk assessment frameworks tailored to different digital asset business models, from centralized exchanges to DeFi protocols
- Reciprocity agreements for compliance information sharing across intermediaries, enabling more effective suspicious activity detection
- Standardized reporting formats that accommodate blockchain-specific data while maintaining regulatory utility

## II. Industry-Led Standard Setting Organization: How it Works

CFES encourages lawmakers to consider public-private partnerships that would help define standards specifically designed for digital assets. While many models exist, see Appendix C, CFES suggests an approach that represents a middle path that combines industry expertise with regulatory oversight.

### A. Structure and Governance

This organization would follow proven standard-setting models where industry participants fund operations and develop technical standards through consensus processes, while regulators retain discretion over adoption and enforcement. Importantly, the Federal Financial Institutions Examination Council's (FFIEC) role in coordinating examination standards across prudential regulators (OCC, FDIC, Federal Reserve) creates inherent opportunities for collaboration between the standard-setting organization and regulators. Since the FFIEC retains ultimate control over whether to adopt industry standards into examination processes, this structure incentivizes meaningful dialogue and ensures standards can achieve consistency across all banking agencies. This model could serve as an analog for the SEC and CFTC. CFES's experience developing and implementing standards across traditional financial services provides a proven model for this approach. This approach would function through the following operational principles:

- **Industry Leadership:** Industry participants with deep expertise in blockchain technology, digital asset operations, and financial services compliance would develop technical standards
- **Regulatory Oversight:** Federal regulators would retain authority to adopt standards into examination manuals and supervisory processes, similar to how the FFIEC incorporates industry standards into banking supervision
- **Flexible Process:** Standards development would occur outside traditional federal rulemaking procedures, enabling faster adaptation to technological changes while maintaining appropriate stakeholder input
- **Enforcement Through Supervision:** Regulators would integrate standards into existing supervisory frameworks, leveraging proven examination and enforcement processes

### B. Regulatory Participation and Implementation

Regulators should have multiple touchpoints throughout the industry-led standard-setting process. This includes advisory participation in standards development, consultative authority, and the clear ability to incorporate standards into examination manuals or reject those that conflict with statutory requirements. Standards that align with regulatory expectations could be adopted into routine supervisory processes, offering consistent guidance to both industry and examiners. Those that fall short would remain outside supervisory practice, limiting their influence. This optionality creates a meaningful incentive for collaboration, encouraging robust engagement between regulators and industry—similar to how examiners currently assess adherence to industry best practices.

### C. Applicability of Standards to Digital Assets

The CLARITY Act's framework for digital assets is well-suited for a standards-based approach. The Act clarifies Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) jurisdiction over digital assets, creating regulatory structures that could significantly

benefit from industry-led standards. Drawing from our Core Risk and Compliance Standards methodology, such standards could address:

- **Market Infrastructure:** Standards for digital asset exchanges, trading platforms, and intermediaries operating under the new regulatory framework
- **BSA/AML Compliance:** Blockchain-specific monitoring and reporting standards that extend our existing BSA/AML framework to address pseudonymous transactions and cross-chain analysis
- **Consumer Protection:** Disclosure and operational standards for digital asset services, leveraging our Complaint Handling and Marketing compliance standards
- **Custody and Safeguarding:** Standards for digital asset custody arrangements by registered intermediaries and service providers

**III. Conclusion**

The digital asset ecosystem requires sophisticated, technically-informed standards that provide regulatory clarity while enabling continued innovation. CFES believes that an industry-led standard-setting organization represents the most effective approach to achieving these goals, combining industry expertise with appropriate regulatory oversight.

This approach has relevance beyond digital assets as financial services continue to evolve through technological innovation. Traditional financial regulation increasingly struggles to keep pace with technological change, creating uncertainty for innovators and supervisors alike. An industry-led standard-setting model could provide a more adaptive framework for addressing emerging technologies while maintaining appropriate regulatory oversight.

We stand ready to contribute to the development of such an organization and believe that the CLARITY Act's approach to digital asset regulation provides an ideal foundation for this initiative. By learning from both the successes and limitations of existing regulatory approaches, we have an opportunity to create a more effective model for governing emerging financial technologies.

We appreciate the Committee's leadership on these critical issues and welcome the opportunity to discuss our recommendations in greater detail.

This creates a stronger, more comprehensive conclusion by connecting the specific digital asset recommendation to the broader regulatory challenges facing financial innovation.

Sincerely,

CFES

cfes

Coalition for Financial Ecosystem Standards

*Members Include*


**Appendix A: STARC: Standardized Assessment for Risk Management and Compliance**

cfes

Coalition for Financial Ecosystem Standards

MARCH 2025

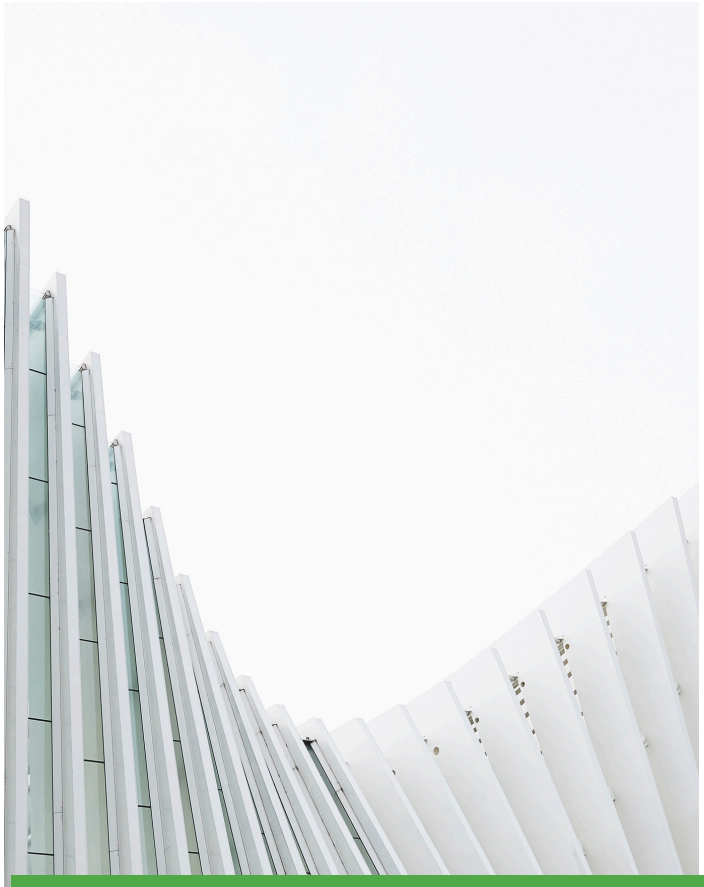
# STARC: Standardized Assessment for Risk Management and Compliance

# About the Coalition for Financial Ecosystem Standards

The Coalition for Financial Ecosystem Standards (CFES) is an organization that supports a competitive and thriving financial services ecosystem that also enables safety, soundness, and consumer protections. In partnership with a wide range of industry leaders, we are enhancing non-bank compliance and risk management practices by developing standards, a certification process, and other supporting services. The standards cover a variety of common controls, processes, and programs that nonbanks are expected or required to maintain.

# Table of Contents





# I. The Case for Standards

The financial services landscape is undergoing a transformation driven by technological innovation and changing consumer expectations. Bank-nonbank partnerships are at the forefront of this evolution, offering unprecedented opportunities for enhanced product offerings, improved customer experiences, and increased financial competition. However, these partnerships also present complex challenges that demand immediate attention and a cohesive regulatory approach.

The current regulatory framework, while robust in many aspects, is challenged by the realities of modern bank-nonbank partnerships. They are unlike traditional vendor models, yet their import to a bank's regulatory mandates are arguably more material. Traditionally, bank regulators have focused their examination efforts on the activities conducted directly by chartered banks. This approach was effective when banks operated primarily as vertically integrated entities, providing most financial services in-house. However, the growth of the bank franchising model and the proliferation of bank-nonbank partnerships have significantly undercut regulators' ability to monitor the full scope of financial services effectively. While the Federal Deposit Insurance Corporation (FDIC) has long been aware of these issues, the recent explosion in bank and nonbank partnerships has lent new urgency to addressing the regulatory challenges posed by these innovative business models.

Clear, standardized guidelines would facilitate more certainty, an environment for innovation, and protect consumers from undue risks. Gaps should be addressed promptly and effectively, and while many call for regulators to expand their budgets, operations, and mandates, we believe that industry must first hold itself accountable. Financial ecosystem participants stand to benefit from standards: banks can enhance risk management and operational efficiency; regulators can achieve more effective oversight; and nonbank partners, including fintechs, can gain operational clarity. Nonbank partners are in a strong position to advance standards by leveraging their collective operational insights and holding themselves accountable via shared incentive alignment.

The Standardized Assessment for Risk Management and Compliance (STARC) provides a framework that operationalizes the vision for industry-led standards. The STARC framework delivers an industry standard, reflecting input from a wide range of market participants, that allows companies to benchmark their compliance and risk management practices. Certifications against the STARC framework ensure that companies are operating with a requisite level of compliance rigor, and demonstrates in a clear and precise manner how their practices perform against a comprehensive set of criteria.

# II. The CFES Approach

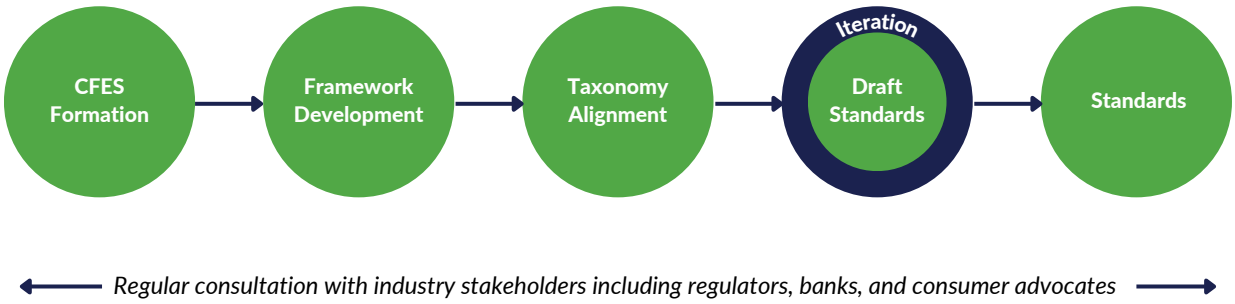
CFES developed the STARC framework to provide clarity into compliance standards for bank- nonbank partnerships, and to facilitate stronger compliance rigor and risk management practices. STARC is modeled off the Federal Financial Institutions Examination Council's (FFIEC) third-party risk management (TPRM) guidelines, and it reflects the feedback and guidance of leaders in the industry. The development of the STARC framework followed a comprehensive, multi-phase process that involved interviews and reviews by multiple banks, fintechs, trade groups, and consumer advocates.

The initial phase focused on establishing the foundational framework, including the matrix approach, compliance categories and program elements, and scoring rubric. This foundational work incorporated extensive feedback from members to ensure the standards reflected real-world operational considerations.

The second phase centered on drafting a comprehensive set of standards that reflected the taxonomy, and then months of refining and validating these standards through robust engagement with stakeholders across the financial ecosystem. This included detailed discussions with banks, banking groups, consumer advocates, and regulators. The feedback from these consultations was instrumental in shaping both the content of the standards and the implementation approach.

In our recently completed phase, we incorporated detailed feedback to refine the scoring criteria and certification methodology, and finalized detailed explanations for rating criteria. This work yielded standards that are both rigorous and practical. The standards released provide an overview of the framework's structure, methodology, and core compliance areas.

*CFES Approach*



# III. STARC: An Introduction

STARC identifies six Core Risk and Compliance Areas, with eight different Risk and Compliance Program Elements that cut across the Core Areas. The different Core Areas and Program Elements were identified in consultation with the interagency guidance on managing risks associated with third-party relationships, the interagency's third-party risk management guide for community banks, and the Office of the Comptroller of the Currency (OCC) Comptroller's Handbook on Compliance Management Systems. The matrix approach enables a thorough model that consistently steps through the Core Areas, with a flexibility to apply the Program Elements as appropriate.

| Core Risk and Compliance Areas | | |
|---|---|---|
| BSA/AML | Compliance Management System (CMS) | Third-Party Risk Management (TPRM) |
| Complaint Handling | Operational Risk | Marketing and Product Compliance |

Each Core Risk and Compliance Area will be assessed across the Risk and Compliance Program Elements, as applicable.

| Risk and Compliance Program Elements | | |
|---|---|---|
| Governance, Oversight and Staffing | Risk Assessment | Training |
| Policies and Procedures | Testing and Monitoring | Issue Management |
| Reporting | Change Management | |

The STARC framework uses a maturity-based rating system, with scores ranging from 5 to 1, where lower numbers indicate higher maturity levels. The ratings progress from Level 5 (Rudimentary) through Level 4 (Documented), Level 3 (Integrated), Level 2 (Strategic), to Level 1 (Optimized). This approach recognizes that organizations at different stages require different levels of sophistication in their risk management and compliance programs.

| Maturity Ratings | |
|---|---|
| 5. Rudimentary | Procedures are usually informal, incomplete, and inconsistently applied. Very little risk capabilities across the compliance area. Lacks understanding of risk management, no documented compliance strategy, reactive, and ad hoc. |
| 4. Documented | Some compliance controls are in place, but they are either not implemented or operationalized across the compliance area. Often limited to certain areas or managed in "silos". Broad view of risks and owners, but no consistent assessment and documentation of risk and control. Risk management applied, but not strategically, siloed and inconsistent. |
| 3. Integrated | Compliance controls and procedures are integrated and standardized across the compliance area. Risk assessments conducted with regular monitoring. Documented risk and compliance framework and processes, lack of visibility across the organization, most processes are consistent. |
| 2. Strategic | Risk management and compliance procedures are integral to business processes, and periodic reviews are conducted to assess program effectiveness. Consistent documentation and some reporting to support risk management, controls, vendor management and incident management. Risk management and compliance embedded across the enterprise, risk management and compliance tools implemented and risk and compliance monitored and improved. |
| 1. Optimized | Regular review and feedback are used to drive a highly sophisticated compliance program supported by substantial investment in robust, enterprise-wide controls; elements are often automated, which are more effective at preventing compliance failures and ultimately less costly than manual controls focusing on detection. Established view of top risks and supporting day-to-day risks, which are reviewed regularly. Strategic risk management and compliance embedded across the enterprise, risk management and compliance tied to value creation and optimized risk-ROI value protection. |

In practice, the framework assesses specific standards within each Core Risk and Compliance Area using the maturity ratings. For example, within BSA/AML, the BSA/AML Governance Standard (1.1), a Governance, Oversight and Staffing Program Element, evaluates how organizations structure and manage their BSA/AML compliance program through leadership and oversight. At its most basic level (5), organizations operate reactively with minimal structure and an inexperienced BSA Officer. As maturity improves, organizations progress through establishing basic documentation and responsibilities (4), implementing a qualified Board-approved BSA Officer with regular reporting (3), developing comprehensive oversight with active Board engagement (2), and ultimately achieving an optimized state (1) where the BSA Officer's

qualifications are third-party validated and there's full integration of BSA/AML considerations into business strategy. The standard emphasizes the importance of clear authority, adequate resources, and collaborative engagement between the BSA Officer, Senior Management, and Board in managing BSA/AML risks effectively.

Importantly, these ratings are not meant to be purely linear or prescriptive. A nonbank may have different maturity levels across different compliance areas based on their business model, risk profile, and stage of growth. This calibrated approach ensures the framework remains meaningful while avoiding unrealistic expectations for automation and sophistication that may not align with an organization's actual risk profile and business requirements.

We acknowledge industry concerns that ratings systems and increased transparency could be misused to penalize organizations that don't achieve "perfect scores." This framework explicitly rejects such an approach. The framework recognizes that innovation in financial services requires thoughtful engagement with risk, not its wholesale elimination. It is risk-calibrated, which by definition contemplates that a small organization’s program warrants different actions to meet standards than a large more complex organization. As such, the scores should be used by banks, nonbanks, and examiners to sharpen their focus on whether appropriate rigor was applied in risk management processes, not to make binary judgments about the inherent risks of innovation. The certification process aims to promote robust risk management practices while avoiding its misuse as a tool for wholesale risk elimination.

Importantly, an organization's voluntary participation in this certification process itself demonstrates a commitment to transparency and rigorous compliance practices. This willingness to undergo independent evaluation signals a mature approach to risk management and compliance - key attributes of sustainable bank partnerships. When properly applied, these metrics should facilitate constructive dialogue about risk management capabilities while supporting continued innovation and growth in bank-nonbank partnerships.

# VI. Looking Ahead

Today's release of the STARC framework marks an important milestone in establishing industry-wide compliance benchmarks. These standards are designed as "open source" resources that banks, nonbanks, and other financial institutions can freely incorporate into their compliance practices. This approach democratizes access to robust compliance frameworks while promoting consistency across the industry.

We're releasing the full scope so that companies have visibility and insight into our certification structure, methodology, and core compliance areas. While this first version serves as a foundational benchmark, we look forward to continuing to build on it and update as industry technology and best practices evolve.

# Appendix: Scoring Criteria

| Program Element | Maturity Rating | | | | |
|---|---|---|---|---|---|
| | 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
| **Governance, Oversight and Staffing** | Governance structure lacks formal compliance framework with undefined risk management accountability, resulting in reactive or missed responses to issues and risk events. | Governance structure incorporates risk and compliance management within existing roles without independence, lacking senior committee oversight and formal accountability frameworks. | Governance structure establishes dedicated compliance framework with clear accountability assigned to independent personnel and officers, supported by defined oversight committees. | Governance structure maintains dedicated roles with executive and ownership buy-in, leveraging specialized third-party expertise for emerging risks while embedding compliance literacy across business units. | Governance structure operates with trained independent professionals, executive champions, and integrated compliance processes. Third-party experts provide specialized assessments and independent validation. Leadership ensures clear segregation between first-line operations, second-line compliance, and third-party assurance. |
| **Risk Assessment** | Compliance risks are poorly understood with minimal assessment or monitoring of risk exposure. Risk management largely reactive, addressing issues only as they arise. | Compliance risks are understood at a basic level but not formally documented or assessed in a systematic way. Risk mitigation efforts are primarily reactive, with a rudimentary understanding of potential compliance risks. Limited resources are allocated to risk assessment activities, resulting in inconsistent and incomplete risk management. | Risk assessments are conducted regularly, though they may lack depth or consistency across all areas. There is a more proactive approach to risk management, with attempts to anticipate potential issues. Risk assessment is beginning to inform business decisions, but integration is not yet comprehensive. | Risk assessments and mitigation plans are completed consistently and in a timely manner. There is strong alignment between risk assessment efforts and overall business strategy. The organization actively uses risk assessment results to inform strategic decision-making. | Risk assessments are completed at least annually against key regulatory risk areas, as well as operational risks. The organization continuously improves its risk assessment methodology, adapting to emerging risks and changes in the business environment. Risk assessment is fully embedded in the organization's culture and decision-making processes at all levels. |
| **Training** | Training program operates without structure, relying on informal and inconsistent learning approaches. | Training program implements basic formal elements with incomplete coverage, resulting in siloed understanding of interdepartmental risks. | Training program delivers regular coverage of key risk areas, fostering a culture of compliance and awareness across all employees. | Training program maintains comprehensive enterprise-wide coverage with specialized content based on emerging risks and specific needs. | Training program leverages automated, compulsory delivery with role-specific content and proactive updates, measuring effectiveness through clear performance metrics. |
| **Policies and Procedures** | Policies exist but may be outdated or incomplete without clear ownership or responsibility. | Policies exist but are not consistently documented, changes typically implemented in reaction to issues. | Policies for key areas documented in consistent format, updated regularly through scheduled cycles. A basic review process exists. Policies easily accessible to employees." | Comprehensive policy documentation with established governance, systematic reviews, and structured change management, including formal tracking of exceptions and effectiveness monitoring. | Legislation, regulatory proposals, and applicable supervisory guidance proactively monitored ensuring timely updates with improvements based on periodic assessments and stakeholder communication. |

| Program Element | Maturity Rating | | | | |
|---|---|---|---|---|---|
| | 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
| **Testing and Monitoring** | Testing and monitoring program operates without formal processes or established testing methodologies, lacking documented plans and designated oversight responsibilities for monitoring activities. | Testing and monitoring program conducts occasional testing with basic documentation but lacks comprehensive planning, consistent methodologies, and systematic follow-up on identified issues. | Testing and monitoring program maintains regular testing activities using defined methodologies for both design and effectiveness testing, supported by documented test scripts and basic sampling approaches. | Testing and monitoring program executes a comprehensive annual testing plan with documented methodologies, clear governance, and regular reporting to senior management, incorporating both design and effectiveness testing with established sampling criteria. | Testing and monitoring program deploys risk-based testing plans with automated workflows, maintains comprehensive test documentation and workpapers, conducts systematic issue tracking and validation, and provides detailed quarterly reporting to board and senior management with escalation protocols. |
| **Issue Management** | Issue management program operates reactively with minimal issue spotting capabilities. | Issue management program identifies issues at business unit level with limited oversight and basic corrective actions. | Issue management program corrects issues with cross-functional input, incorporating root cause analysis and impact tracking. | Issue management program escalates issues immediately for tracking and remediation, maintaining detailed metrics and regular reporting. | Issue management program tracks issues comprehensively from identification to closure, leveraging systematic trend analysis for proactive remediation. |
| **Change Management** | Change management program operates with undefined regulatory taxonomy and reactive approaches, lacking structured processes for managing regulatory and business changes. | Change management program implements basic elements within isolated projects, resulting in varied and inconsistent approaches to regulatory change. | Change management program maintains comprehensive processes across multiple projects, establishing standardized management approaches and consistent documentation. | Change management program deploys company-wide standards and methods, enabling strategic coordination of change initiatives across all departments. | Change management program optimizes processes through enterprise-wide integration, leveraging automated impact assessments and proactive horizon scanning to drive efficient adaptation and value creation. |
| **Reporting** | Limited risk reporting with ad hoc, manual, and siloed regulatory reporting processes. | One-time or on-demand review of data; Basic risk reporting structure, but lacks comprehensiveness. | Establish regular risk reviews with partial automation and some senior management reporting. | Delivers timely, consistent, and largely automated reporting across risk areas to senior management and the board. | Integrates automated risk reporting with business metrics, maintaining comprehensive board and senior management accountability. |

cfes

Coalition for Financial Ecosystem Standards


**Appendix B: Core Risk and Compliance Standards, Version 1.0, March 2025**

cfes
Coalition for Financial Ecosystem Standards

# Coalition of Financial Ecosystem Standard

## Core Risk and Compliance Standards

---

Version 1.0

March 2025

## About CFES

The Coalition for Financial Ecosystem Standards (CFES) is an organization that supports a competitive and thriving financial services ecosystem that also enables safety, soundness, and consumer protections. In partnership with a wide range of industry leaders, we are enhancing non-bank compliance and risk management practices by developing standards, a certification process, and other supporting services. The standards cover a variety of common controls, processes, and programs that nonbanks are expected or required to maintain.

## Overview of CFES Standards

Each standard includes a summary of the expected control, process, or program, along with criteria for rating the quality of a company's application of the standard along a five point scale: Level 5 (Rudimentary), Level 4 (Documented), Level 3 (Integrated), Level 2 (Strategic), and Level 1 (Optimized). For each company being certified, assessors are expected to utilize the rating criteria, along with other industry insights and experience to assign an appropriate certification level for each standard. The CFES expects to periodically update the criteria over time in future releases as needed to capture emerging best practices.

Importantly, these ratings are not meant to be purely linear or prescriptive. A nonbank may have different ratings across different compliance and risk areas based on their business model, risk profile, and stage of growth. This approach ensures the framework provides a meaningful framework for guiding nonbanks to pursue stronger risk and compliance programs while avoiding setting unrealistic expectations for all industry participants. However, as a general rubric, nonbanks early on their journey should strive to consistently achieve ratings of 3-4 while established companies should achieve ratings of 1-3.

## Core Standards

The following 54 standards address a core set of competencies across the following areas: Bank Secrecy Act/Anti-Money Laundering (BSA/AML), Compliance Management System (CMS), Third-Party Risk Management (TPRM), Complaint Handling, Operational Risk, and Marketing and Product Compliance. While we expect to update these core standards to reflect updated best practices, we also expect to release additional modules focused on lending and payments to provide guidance catered toward product specifications.

# Contents

# Cover Sheet

| CFES Standardized Assessment for Risk Management and Compliance (STARC) Cover Sheet | |
|---|---|
| **Purpose** | This cover sheet provides guidance on interpreting and applying the CFES STARC Standards based on organization size and operational maturity. |
| **About STARC** | The Standardized Assessment for Risk Management and Compliance (STARC) provides a framework for evaluating nonbank compliance programs. Key aspects:<br>• Facilitates standardized risk management evaluation<br>• Covers six core compliance areas and ten program elements<br>• Supports regulatory alignment with bank expectations |
| **Framework Principles** | The CFES scoring framework balances three key principles: Consistency: The 5-point maturity scale provides a standardized way to evaluate compliance programs across different organizations, facilitating a thorough evaluation while accounting for company stage. This consistent approach helps banks and certifiers assess nonbanks using common criteria. Comprehensiveness: Scoring covers six Core Compliance Areas and ten Program Elements, ensuring a thorough evaluation of each organization's risk management framework. This comprehensive approach helps prevent gaps while maintaining appropriate focus on areas most relevant to each nonbank's business model. Calibration for Risk: The framework recognizes that effective compliance programs should be tailored to each organization's scale, complexity and maturity. For example, a rapidly growing nonbank may appropriately have different controls than a large established nonbank, even while both maintain sound risk management. This calibrated approach supports continued innovation in financial services while ensuring appropriate safeguards are in place. |

| CFES Standardized Assessment for Risk Management and Compliance (STARC) Cover Sheet | |
|---|---|
| **Maturity-Based Expectations** | Expected Scoring Ranges Based on Maturity of Program:<br>• Launch Phase Programs: 4-5<br>• Early-stage: 3-4<br>• Growth-stage: 2-4<br>• Established companies: 1-3<br><br>These scoring ranges serve as general guidance rather than rigid requirements. Each nonbank's appropriate scoring will vary based on their unique business model, risk profile, transaction volumes, operational maturity, and stage of growth. Not every nonbank should aim for scores of 1-2, as this level of sophistication may be unnecessary or impractical for their business model. The goal is to demonstrate appropriate risk management and controls for the organization's specific context, not to achieve the lowest possible scores across all categories. Banks and evaluators should use this framework as a guide while considering each nonbank's individual circumstances and operational needs.<br><br>This contextual approach ensures standards remain meaningful while avoiding unrealistic expectations for automation and sophistication that may not align with a nonbank's actual risk profile and business requirements.<br><br>**Launch Phase Programs**<br>Companies in early stages of program development, whether pre-launch or newly operational, face unique circumstances when undergoing certification. Since the certification standards are designed for established operational programs, the assessment must be adapted to evaluate readiness and initial implementation rather than historical effectiveness.<br><br>The certification report will document which standards could not be fully assessed due to limited operational history and will detail the company's implementation roadmap for those areas. This includes capturing specific operational milestones, such as when key controls will be activated, when full staff training will be completed, and when regular monitoring and reporting will begin. The report will also evaluate any compensating controls or interim measures the company has implemented during this early stage.<br><br>The assessment considers mitigating factors specific to program maturity - for example, transaction monitoring evaluation will focus on system configuration and rule development rather than historical effectiveness metrics. Similarly, staff training assessment emphasizes initial program design and completion of foundational training rather than ongoing training records.<br><br>**Early-Stage Programs**<br>For early-stage programs, scores of 3-4 indicate appropriate basic compliance foundations are in place. A score of 3 shows maturing processes, with higher scores both expected and appropriate at this stage.<br><br>**Growth-Stage Programs**<br>Growth-stage programs typically show scores of 2-4 reflecting a developing compliance program, while a score of 2 indicates advancing maturity. Mixed scores across different areas are common as automation increases, with emphasis on enhancing controls and monitoring capabilities.<br><br>**Established Programs**<br>Established programs should demonstrate scores of 1-3 reflecting a mature compliance framework. A score of 3 may indicate areas needing enhancement. Lower scores reflect the appropriate sophistication level expected at this stage, including advanced automation and controls.<br><br>**Evaluation Context**<br>Assessors should understand that higher scores (4-5) are entirely appropriate for pre-launch and early-stage companies. The same numerical score requires different interpretation based on company maturity level. Assessment must consider operational maturity and business complexity, as scoring is designed to encourage compliance growth aligned with business scale.<br><br>This framework ensures appropriate risk management while keeping certification accessible across all company stages. It sets realistic expectations for compliance maturity based on organizational size and operational scope, allowing companies to demonstrate adequate controls relative to their stage of development. |

| CFES Standardized Assessment for Risk Management and Compliance (STARC) Cover Sheet | |
|---|---|
| **Core Assessment Areas** | • Bank Secrecy Act/Anti-Money Laundering (BSA/AML)<br>• Compliance Management System (CMS)<br>• Third-Party Risk Management (Vendor Management)<br>• Complaint Handling<br>• Operational Risk<br>• Marketing and Product Compliance |
| **Assessment Structure** | • Complete scoring criteria for each standard<br>• Each core compliance area contains detailed program elements<br>• Review specific scoring criteria for each program element before beginning assessment |
| **Scoring Framework** | The CFES Standards use a 5-point maturity scale:<br>1. Optimized<br>2. Strategic<br>3. Integrated<br>4. Documented<br>5. Rudimentary |

# Business Profile

| | Information | Response |
|---|---|---|
| **Company Information** | Company Name | |
| | Company Background/Overview | |
| | Year Founded | |
| | Amount of Capital Raised (to date) | |
| | Key Investors and Financing | |
| | Board Members | |
| | FinCEN Registration Status- Current registration status (e.g., MSB, non-MSB)- Basis for registration or exemption- Specific regulated activities conducted- Jurisdictions where registered/licensed | |
| | Reputational Risk (e.g., Legal/Regulatory Issues, Media/Public Perception, Founder/Executive Risks) | |
| **Product & Market Overview** | Primary Product/Service Offering | |
| | Primary Customer Segments Targeted (e.g., Retail, Small Business, Enterprise) | |
| | Number of Customers | |
| | Growth Projections | |
| | Geographic Markets Served | |
| | Key Partnerships | |
| **Business Strategy & Economics** | Revenue Model (e.g., Transaction Fees, Subscription, Interest Income) | |
| | Unit Economics (Revenue per Customer, Customer Acquisition Cost, Lifetime Value) | |
| | Current Profitability Status (Pre-revenue, Cash Flow Positive, Profitable) | |
| | Projected Timeline to Profitability | |
| | Burn Rate and Runway | |

| | Information | Response |
|---|---|---|
| **Growth Strategy** | Customer Acquisition Strategy | |
| | Expansion Plans (Product, Geographic, Customer Segments) | |
| | Strategic Partnerships in Development | |
| | Key Milestones for Next 12-24 Months | |
| | Product Roadmap | |
| **Technology** | Core Technology Stack/Platforms | |
| | Cloud Service Providers | |
| | Data Centers/Hosting Locations | |
| | Software/Tools Used for Critical Risk Management Functions | |
| **Security** | Material Vendors | |
| | Cybersecurity Certifications (e.g., ISO 27001, SOC 2) | |
| | Penetration Testing Frequency | |
| | Incident Response Plan | |
| | Business Continuity/Disaster Recovery Plan | |
| **Transaction Volume** | Number of Customers (Prior Year) | |
| | Number of Customers (Projected) | |
| | Overall Monthly Transaction Volume (Prior Year) | |
| | Overall Monthly Transaction Volume (Projected) | |
| | Average Monthly Transaction Volume (Debit) (Prior Year) | |
| | Average Monthly Transaction Volume (Debit) (Projected) | |
| | Average Monthly Transaction Volume (Wire) (Prior Year) | |
| | Average Monthly Transaction Volume (Wire) (Projected) | |
| | Average Monthly Transaction Volume (ACH) (Prior Year) | |
| | Average Monthly Transaction Volume (ACH) (Projected) | |

| | Information | Response |
|---|---|---|
| **Bank Partners** | List of Bank Partners | |
| | Reputational Risk Regarding Bank Partners (e.g. Consent Orders or Other Public Supervisory Findings) | |
| | Average Time for Customer Response/Resolution with Bank Partners | |
| | Real-Time Communication Channels (e.g., Slack, Zoom) Established with Bank Partners | |

# 1. BSA/AML

**1.1 AML Governance**

Nonbanks should maintain a governance structure for its AML program, elements of which may include a designated AML officer with defined responsibilities, management oversight, and board reporting.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Inexperienced AML Officer designated.<br>• Lack of a formal job description.<br>• AML responsibilities are handled reactively.<br>• No clear authority or resources for the AML office or AML program.<br>• Minimal to no engagement from leadership or the Board in AML oversight. | The assessor identified:<br><br>• AML Officer has some related experience but is not a compliance professional.<br>• AML Officer is designated as such in policies approved by the Board.<br>• Initial job description exists, but responsibilities are unclear.<br>• Limited authority and resources invested in the AML program.<br>• Ad-hoc involvement of leadership in AML matters and limited Board awareness. | The assessor identified:<br><br>• Qualified AML Officer or other appropriately designated personnel formally approved by the Board.<br>• Detailed job description with defined AML responsibilities.<br>• Adequate authority and resources to manage the program.<br>• Regular reporting to management on key AML areas.<br>• Regular leadership involvement in the AML Program.<br>• Regular reporting on AML to the Board.<br>• As applicable, AML Program has been subject to independent assessment, material findings have been or are being actively prioritized for remediation. | The assessor identified:<br><br>• Highly qualified AML Officer nominated by CEO, approved by the Board.<br>• Comprehensive role with oversight of the entire AML program.<br>• Strong authority and sufficient resources provided.<br>• Regular, detailed reporting to the Board on AML compliance.<br>• Active engagement of leadership in AML risk management.<br>• The Board demonstrates understanding and involvement in key AML decisions.<br>• As applicable, this area has been subject to independent assessment and the company has established a discipline of addressing material findings timely. Repeat findings rarely occur. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• AML Officer qualifications confirmed by a third-party audit.<br>• Clear, documented authority with direct access to leadership and the Board.<br>• Strategic role, involved in business decisions impacting AML risk.<br>• Ongoing, detailed Board reporting and prompt escalation of issues.<br>• Leads continuous improvement of the AML program.<br>• The Board is fully engaged in AML governance, regularly reviews program effectiveness.<br>• Collaborative approach between BSA Officer, leadership, and the Board in managing AML risks.<br>• As applicable, this area has been subject to independent assessment and the company has established a robust discipline of addressing material findings immediately. Independent assessments consistently validate program effectiveness with no repeat findings. |

**1.2 AML Policies and Procedures**

Nonbanks should document and implement AML policies and procedures, along with processes for maintaining and enhancing AML program documentation over time.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• AML policies and procedures are not customized to the nonbank's products and services.<br>• Policies lack complete or accurate references to relevant guidance or regulations and/or do not address contractual. obligations of the company.<br>• Controls are not adequately described in policies and procedures.<br>• Incomplete process for updating or approving policies and procedures.<br>• Lack of version control or policy history.<br>• Unclear ownership of policy and procedures. | The assessor identified:<br><br>• AML policies and procedures reference nonbank's products and services.<br>• Policies reference the correct regulations and/or contractual requirements.<br>• Controls are referenced in the policies and procedures.<br>• Policies and Procedures were formally approved.<br>• Some version history indicating improvements have been made over time, as appropriate.<br>• Clear ownership of policy and procedures. | The assessor identified:<br><br>• AML policies and procedures are specifically tailored to the nonbank's products and services.<br>• Policies or other artifacts include detailed regulatory applicability analysis.<br>• Procedures are highly customized to the specific controls implemented.<br>• Process in place to regularly update policies and procedures. - Well-documented version history and updates made over time, as appropriate. implemented for procedure updates.<br>• Policies show logical flow between risk issues and policy decisions.<br>• Board-approved policy with defined review cycles. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Robust AML policies, procedures, and desktop manuals have been regularly reviewed and updated.<br>• Consistent Board approval process for policies with documented timeline.<br>• Systematic approach to updating procedures based on operational changes, enhancements, and other guidance.<br>• Policies and procedures have been subject to audits, as well as ongoing testing for company-wide adherence to the Policies and Procedures.<br>• Active oversight by CCO/BSA Officer with regular compliance checks.<br>• Clear articulation of how identified risks and vulnerabilities inform policy decisions.<br>• No outstanding audit findings or other relevant issues to be resolved. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Evidence of a proactive strategy to continuously update AML Policy, Procedures, and Desktop Procedures.<br>• CCO/BSA Officer leads continuous improvement of policies and procedures.<br>• Policies and procedures fully integrated with risk assessment and business strategy.<br>• Testing shows history of compliance with limited to no exceptions.<br>• Regular independent review of policy and procedure effectiveness.<br>• Automated compliance monitoring for policy and procedure adherence.<br>• Policies demonstrate sophisticated understanding of regulatory expectations and industry best practices.<br>• Clear, logical flow from risk assessment to policy decisions to procedural implementation.<br>• Policies proactively address emerging risks and regulatory trends. |

**1.3 AML Training**

Nonbanks should educate personnel on an ongoing basis on AML concepts, the company's AML program, and each employee's AML responsibilities.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Training, if any, is ad-hoc and inconsistent.<br>• No formal BSA/AML training program materials in place.<br>• No formal training attendance tracking in place.<br>• Lack of training has created limited awareness of BSA/AML responsibilities across the organization.<br>• Unclear collaboration between HR and Compliance for new hire training.<br>• No documented consequences for non-completion of AML training. | The assessor identified:<br><br>• BSA/AML training exists but is not sufficiently tailored or comprehensive.<br>• Training covers AML laws and regulations.<br>• Annual training occurs but doesn't cover all appropriate employees or isn't updated in a timely manner.<br>• Limited coordination between HR and Compliance for training, including delays in training new employees.<br>• Content is not sufficiently tailored to the company's needs.<br>• Basic documentation of non-completion consequences exists, but enforcement is inconsistent. | The assessor identified:<br><br>• BSA/AML training provided to new employees at or shortly after hiring.<br>• Annual training conducted for all employees in the company.<br>• HR and Compliance collaborate to provide adequate training including coordination with any external training providers if used.<br>• Training content covers essential BSA/AML topics.<br>• Initial tracking of training completion.<br>• Includes assessments or quizzes.<br>• Content reinforces the importance of AML in protecting financial systems and national security.<br>• Documented process for addressing training non-completion with consistent follow-up procedures.<br>• Encourages employees to speak up through a strong whistleblower and reporting framework. | The assessor identified:<br><br>• Comprehensive BSA/AML training program for new hires and ongoing annual training.<br>• Training content tailored to different roles and risk levels within the organization.<br>• Strong collaboration between HR and Compliance to develop and deliver training, including coordination with any training vendor utilized.<br>• Regular review and update of training materials by subject matter experts to reflect regulatory changes and emerging risks.<br>• System for tracking and reporting on training completion.<br>• Assessment of training effectiveness through tests or practical application.<br>• Formal escalation process for non-completion with defined timelines and management accountability.<br>• History of content adjustments based on knowledge gaps and performance. | The assessor identified:<br><br>• Robust BSA/AML training program, confirmed by a third-party audit.<br>• Personalized training paths based on employee roles, experience, and past performance.<br>• Continuous learning approach with regular updates and refresher modules throughout the year.<br>• Advanced collaboration between HR, Compliance, and business units to ensure training relevance, including coordination with training vendor if used.<br>• Use of multiple training methods (e.g., e-learning, workshops, case studies, certifications) to enhance engagement and retention.<br>• Regular independent review of training program effectiveness.<br>• Integration of training performance into employee evaluations and risk management processes.<br>• System integrating automated reminders, manager notifications, performance reviews, and executive escalation for addressing training non-completion.<br>• Proactive adaptation of training to address emerging risks and regulatory changes. |

**1.4 AML Risk Assessment**

Nonbanks should conduct BSA/AML assessments to understand the inherent money laundering risks, control effectiveness, and residual risk of their products and services.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Informal process for assessing and understanding BSA/AML risk.<br>• The lack of an articulable methodology for assessing risks and/or a lack of consistency in how risks are understood and managed.<br>• Overall limited understanding of inherent risks, controls, or residual risks.<br>• No involvement of leadership in the risk assessment process. | The assessor identified:<br><br>• A written BSA/AML Risk Assessment process, including evidence of prior assessments.<br>• Existence of a qualitative methodology.<br>• Refreshes were not performed in a timely manner (annual or upon significant business changes).<br>• Key risks not clearly articulated or described.<br>• Results are not utilized in company decisions (e.g., budgeting and staffing) or tracked to bring risk within tolerance.<br>• Leadership has limited involvement or understanding of the process or results. | The assessor identified:<br><br>• A quality and defensible BSA/AML Risk Assessment process exists.<br>• Evidence that BSA/AML Risk Assessment completed annually and upon significant business changes.<br>• Effectively assesses inherent risk, control effectiveness, residual risk.<br>• Includes quantitative components (when data is available).<br>• Results shared with leadership for review and approval and utilized in company decisions.<br>• Evidence results have been utilized to enhance AML program design and/or effectiveness. | The assessor identified:<br><br>• Comprehensive BSA/AML Risk Assessment process, potentially more frequent than annual.<br>• Sophisticated risk assessment methodology tailored to the company's specific risks.<br>• Takes into account customer, product and service, transaction, channel, and geographic risks.<br>• Detailed analysis of inherent risks, control effectiveness, and residual risks.<br>• Active involvement of leadership in implementing an effective and useful assessment process.<br>• Clear link between risk assessment results and AML program enhancements, where needed.<br>• Regular updates to risk assessment based on emerging threats and business changes. | The assessor identified:<br><br>• Robust BSA/AML Risk Assessment process, confirmed by a third-party audit.<br>• Dynamic, continuous risk assessment approach, not limited to annual reviews.<br>• Comprehensive consideration of all risk factors, including emerging and potential future risks.<br>• Full integration of risk assessment with business strategy and product development.<br>• Leadership and the Board actively engaged in the risk assessment process and in the utilization of the results for decision making purposes.<br>• Automated tools for real-time risk monitoring and assessment.<br>• Regular independent review of risk assessment methodology and effectiveness.<br>• Risk assessment drives proactive enhancements to the AML program and controls.<br>• Risk assessments utilized to establish and assess leadership's performance. |

**1.5 Know Your Customer**

Nonbanks should conduct customer due diligence, including KYC (know your customer) and KYB (know your business) to ensure it verifies the identity and understands the risk each customer poses from an AML risk perspective prior to onboarding and on an ongoing basis.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• AML or KYC policy and procedures are not fully implemented and there is a heavy reliance on manual controls.<br>• The company routinely fails to properly verify customer identity (e.g., accepting unverifiable or unreliable documents).<br>• No risk based approach is utilized.<br>• No oversight of customers' customers (third-party).<br>• No identification of higher risk customers. | The assessor identified:<br><br>• Initial KYC/KYB processes are implemented as per the policy requirements.<br>• Controls lack sophistication or automation.<br>• Unclear how risk based approach is utilized.<br>• Limited view of different types of customers or how customers are to be risk-rated or subjected to increased diligence.<br>• As applicable, heavy reliance on third-parties to perform all checks without involvement or oversight. | The assessor identified:<br><br>• Increased use of commonly utilized tools and/or automation for KYC/KYB processes and escalations.<br>• Documented understanding of risk vectors and higher risk customer types that are attempting to be onboarded.<br>• KYC/KYB procedures and desktop procedures exist and specify how controls are to be operated.<br>• Consistent application of controls, including beneficial owner identification and verification.<br>• As applicable, significant oversight of how third-parties are managing this process. | The assessor identified:<br><br>• Mostly automated and efficient KYC/KYB processes that do not create significant manual review.<br>• Controls do not exhibit a history of regularly onboarding customers outside of risk tolerance.<br>• Comprehensive risk rating and history of clients being escalated for enhanced due diligence.<br>• Customers are subjected to refreshed customer risk rating and ongoing identity verification controls.<br>• Validation and oversight of third-party tools utilized.<br>• History of improvements and calibration of regtechs utilized.<br>• As applicable, robust third-party oversight program with regular monitoring. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Automated KYC/KYB processes, including sophisticated PEP, high risk country/industry, high risk customer identification, and ongoing monitoring controls.<br>• Utilization of source of funds and source of wealth in onboarding and ongoing diligence.<br>• Continuous risk rating process.<br>• Regular identification of higher risk customer types.<br>• Controls are subject to ongoing reporting and oversight.<br>• History of timely customer KYC/KYB refreshes. |

**1.6 Transaction Monitoring and Reporting**

Nonbanks should monitor transactions for unusual activity and escalate that activity in a timely manner according to their regulatory or contractual requirements.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Ad-hoc and manual transaction monitoring processes.<br>• No formal risk scenarios identified for the company's specific products/services.<br>• No case management or structured suspicious activity reporting process.<br>• No history of identifying potentially suspicious activity. | The assessor identified:<br><br>• Regular manual monitoring of Initial scenarios.<br>• Limited evidence suggesting why scenarios were selected or are appropriate.<br>• Some case management or process for reporting suspicious activity.<br>• Some history of identifying and reporting potentially suspicious activity.<br>• Limited feedback loop for root cause or platform changes to prevent similar future activity. | The assessor identified:<br><br>• Automated monitoring using standard industry tools or similarly developed internal tools.<br>• Evidence that scenarios were, at a minimum, selected or developed based on product/service specifics.<br>• Defined process for investigating alerts, case management, and escalating suspicious activity.<br>• Efforts underway to reduce false positives through more sophisticated applications or calibration of rules.<br>• Evidence suggesting an approach to documenting any edits, additions, or removal of rules over time. | The assessor identified:<br><br>• Risk-based approach with scenarios tailored to the company's unique risk profile.<br>• Advanced analytics and machine learning models for detecting unusual patterns.<br>• Behavioral monitoring integrated with transaction analysis.<br>• Heuristics developed based on specific risk scenarios.<br>• Automated case management system for alert investigation.<br>• Subjected to a scenario coverage assessment and calibrated to heuristics based on outcomes.<br>• Comprehensive suspicious activity reporting and record-keeping procedures.<br>• Limited history of backlogs or missing SLAs or other escalation timelines.<br>• Documentation around recurring calibration and quality assurance processes.<br>• Model documentation subjected to conceptual soundness review.<br>• Evidence suggesting significant oversight and testing of rules prior to making edits, additions, or removals. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Real-time adaptive models that evolve with changing behavioral and transaction patterns.<br>• Advanced network analysis to detect complex schemes across user networks.<br>• Integration of diverse data sources for enhanced contextual understanding.<br>• Predictive analytics to anticipate potential high-risk behaviors and transactions.<br>• Automated alert triaging and prioritization based on risk scenarios.<br>• Sophisticated case management and investigation tools.<br>• Streamlined, data-driven escalation process.<br>• Subjected to data validation and quantitative rule calibration assessments.<br>• Regular optimization of monitoring processes based on feedback and outcomes.<br>• Collaboration with other companies and regulators on emerging risks.<br>• Continuous evaluation and integration of innovative monitoring technologies.<br>• No recent history of backlogs, missing SLAs, or quality control issues. |

**1.7 Sanctions Screening**

Nonbanks should implement a risk-based approach to sanctions screening of customers and transactions at onboarding and on an ongoing basis, with appropriate procedures for investigating potential matches and handling blocked transactions.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Policy and procedures are not fully implemented and there is a heavy reliance on manual controls.<br>• No procedures specifying the actual processes employed.<br>• Limited evidence of screening results needed to verify completeness.<br>• Limited evidence of how potential matches were investigated and determined to be false positives.<br>• Lack of ongoing screening. | The assessor identified:<br><br>• Implemented policies and procedures, including controls that indicate customers are screened at onboarding and on an ongoing basis.<br>• Investigation of potential matches occurs, although limited documentation indicating how they were resolved.<br>• Desktop procedures are missing or incomplete.<br>• All key sanctions lists are included in screening criteria. | The assessor identified:<br><br>• Consistent screening of all new customers at onboarding.<br>• Periodic screening of current clients against updated sanctions lists.<br>• Documented investigation process for potential matches.<br>• Evidence of quality and timely reviews.<br>• Documented procedures for match disposition.<br>• Limited or no recent evidence of onboarding sanctioned customers or onboarding/transacting with parties in sanctioned countries.<br>• Evidence confirming correct and most updated lists are utilized. | The assessor identified:<br><br>• Automated screening of all new customers using effective and efficient technology.<br>• Regular ongoing screening of all clients, with clear frequency and scope.<br>• Screening at both customer and transaction level.<br>• Documented desktop procedures for match disposition and blocked/rejected transactions.<br>• Process for reporting confirmed matches and reliable process for blocking transactions or freezing balances.<br>• Strong quality assurance processes with regular testing of screening effectiveness.<br>• Proactive monitoring of sanctions list changes with quick implementation and rescreening. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Auditable evidence of real-time screening at onboarding and ongoing for all client types, with no recent exceptions.<br>• Real-time screening of all transactions, including all identifiable parties involved.<br>• Advanced investigation process to efficiently remove false positives while maintaining compliance standards.<br>• Comprehensive, regularly updated procedures evidencing ongoing process improvements have been implemented.<br>• Regular review and optimization of screening parameters based on performance metrics and risk assessment. |

**1.8 Unusual Activity Reporting**

Nonbanks should report unusual activity in a timely manner to the correct parties based on their regulatory or contractual requirements.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Policy and procedures are not fully implemented.<br>• Minimal evidence of awareness of obligation to report unusual activity.<br>• No designated person(s) for reporting.<br>• No history of reporting unusual activity. | The assessor identified:<br><br>• Some evidence of implementation of reporting controls.<br>• BSA Officer or other appropriately designated personnel aware of responsibility for reporting.<br>• Evidence of occasional reporting. | The assessor identified:<br><br>• Documented reporting process developed by BSA Officer or other appropriately designated personnel.<br>• Quality assurance procedures are in place and evidence suggests reviews occur prior to reporting.<br>• All personnel are aware of duty to report, regardless of where in customer lifecycle activity was identified.<br>• A documented approach to closing or performing ongoing monitoring for reported accounts.<br>• Evidence suggests continuing activity monitoring controls exist.<br>• All personnel are aware of anti-tipping off rules. | The assessor identified:<br><br>• Evidence of cross-functional collaboration on reporting and closing accounts.<br>• Evidence of reporting trends and issues to leadership.<br>• Robust internal investigation procedures.<br>• Evidence of consistent, timely, and quality reporting to the appropriate parties.<br>• For entities with both regulatory and contractual reporting requirements, the company has implemented a process for identifying the correct party to report the activity to based on the unusual activity occurring through a self-licensed component of the program and/or a bank-sponsored component. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• The reporting process is fully integrated with AML, Fraud, and other customer service controls and functions.<br>• Advanced use of reports to enhance activity monitoring and to inform leadership on business decisions.<br>• Evidence of reporting quality and a robust quality assurance process.<br>• No recent evidence of backlogs, missed filing timelines, or missed contractual SLAs.<br>• Proactive communication with bank partner(s) or regulatory agencies on the company's dedication to implementing the necessary solutions to prevent, monitor, and report activity.<br>• Evidence of continuous improvement of the reporting process based on feedback and emerging risks. |

**1.9 Independent Assessment**

Nonbanks should obtain an independent assessment of its BSA/AML program to evaluate the effectiveness of the program, as well as maintain a process for remediating identified issues and reporting to company leadership.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal independent testing process or policy requirement has been implemented.<br>• Testing, if any, is irregular and not truly independent. | The assessor identified:<br><br>• An independent assessment has been performed.<br>• Unclear remediation process for identified issues.<br>• Unclear reporting to leadership or the Board on audit findings or remediation.<br>• Minimal to no engagement from leadership in audit oversight. | The assessor identified:<br><br>• Evidence of independent assessment being conducted annually and on-time.<br>• There is a detailed independent testing process documented.<br>• Testing results flow into a documented remediation and leadership reporting process.<br>• BSA Officer or other appropriately designated personnel oversees remediation of identified issues. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Evidence suggesting leadership has selected an independent assessor based on needs and merit, cleared potential conflicts, and optimized selection for quality over price.<br>• Regular, detailed reporting to leadership and the Board on audit findings and remediation.<br>• Limited or no history of repeat independent assessment findings.<br>• Active engagement of leadership in addressing audit findings.<br>• The Board demonstrates understanding and involvement in overseeing the testing process and results. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Highly qualified, fully independent testing party is utilized.<br>• Proactive remediation process with clear timelines and accountability.<br>• Continuous improvement of testing and remediation processes<br>• Leadership actively participates in addressing audit findings and improving the BSA/AML program.<br>• The Board is fully engaged in overseeing the independent testing process, regularly reviews results, and ensures adequate resources for remediation.<br>• Collaborative approach between BSA Officer or other appropriately designated personnel, leadership, and the Board in managing audit findings and enhancing the overall BSA/AML program. |

**1.10 Quality Assurance**

Nonbanks should maintain an internal quality assurance process or function capable of fostering ongoing improvements in compliance processes and related output.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• QA activities, if any, are performed by BSA/AML operational staff.<br>• QA activities, if any, are not subject to a formal review and feedback process.<br>• No regular reviews or testing of compliance processes.<br>• No personnel with QA responsibilities. | The assessor identified:<br><br>• QA process documented in policies.<br>• Evidence of occasional reviews of compliance processes.<br>• Limited independence in QA function.<br>• Limited role QA plays in employee performance reviews. | The assessor identified:<br><br>• Documented program includes testing scripts and other workpapers.<br>• Performance of regular and statistically significant reviews of key compliance processes.<br>• BSA Officer or other appropriately designated personnel provides some oversight of QA activities. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Evidence of performance improvements over time across team members.<br>• QA reviewers are independent from day-to-day BSA/AML compliance functions.<br>• BSA Officer actively oversees QA activities.<br>• Results play a significant role in team members' performance evaluations.<br>• History of expanding QA function to broader areas of work product. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Highly qualified, independent QA team conducting comprehensive reviews.<br>• Evidence QA results drive strategic enhancements to the BSA/AML program and team performance.<br>• BSA Officer leverages QA insights for program optimization.<br>• Leadership is informed on team performance.<br>• No recent history of major gaps in quality. |

**1.11 Record Retention**

Nonbanks should maintain BSA/AML records in compliance with regulatory and contractual requirements.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal policy or inconsistent record keeping.<br>• No designated responsibility or secure storage capabilities.<br>• Lack of regulatory awareness and required recordkeeping timeframes. | The assessor identified:<br><br>• Policy includes recordkeeping requirements.<br>• Evidence of some recordkeeping in accordance with policy but recordkeeping practices do not allow for full compliance to be confirmed.<br>• Limited leadership oversight of recordkeeping practices. | The assessor identified:<br><br>• Policies and procedures include detailed accounting of recordkeeping requirements and practices.<br>• Evidence of recordkeeping allows compliance to be confirmed.<br>• Recordkeeping aligns with information security practices.<br>• Recordkeeping aligns with data deletion practices that are not in contradiction with requirements. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Policy integrated with overall governance.<br>• Board oversight and regular reviews.<br>• Advanced storage and retrieval systems.<br>• Robust training and audit processes.<br>• No recent history of non-compliance. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Automated retention and disposal schedules.<br>• Advanced encryption and access controls.<br>• Real-time tracking and reporting.<br>• Integration with broader data governance.<br>• Evidence of continuous improvements to retention and oversight. |

**1.12 Information Sharing**

Nonbanks should be prepared to fulfill law enforcement and other lawful document requests in a timely manner, including maintaining appropriate procedures for handling such requests.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal information sharing policy or procedure.<br>• Some evidence that prior requests were fulfilled.<br>• Lack of awareness about information sharing regulations (e.g., 314a/314b).<br>• No designated responsibility for handling information sharing or law enforcement requests.<br>• Responses to prior requests, if any, are inconsistent and untracked. | The assessor identified:<br><br>• Documented policy for responding to law enforcement requests but process specific procedures are missing.<br>• Company-wide awareness of information sharing requirements.<br>• Limited evidence that procedures were followed in fulfilling prior requests.<br>• Limited internal reporting structure from company to the responsible party but BSA Officer or other appropriately designated personnel are aware of responsibility.<br>• Inconsistent tracking of law enforcement requests and responses. | The assessor identified:<br><br>• Documented policy and procedures detail the company's information sharing processes.<br>• Processes for 314a/314b participation, as required.<br>• Clear reporting and escalation process is implemented across the company for requests to reach the correct parties in a timely manner.<br>• Evidence of some tracking of historical requests.<br>• Evidence of timely reviews and responses to requests.<br>• Evidence of compliance with bank escalation requirements, as applicable. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Clear designation of principal contact for law enforcement inquiries based on appropriate role and experience.<br>• Established response SLAs and record retention policies for requests.<br>• Robust logging system for tracking all information sharing and law enforcement requests.<br>• Regular training for relevant staff on information sharing policies and procedures.<br>• Evidence of periodic review and update of information sharing policies and procedures.<br>• Evidence of internal investigations and further actions to assess gaps or risks based on receiving requests.<br>• No recent history of non-compliance or missed SLAs. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Organized systems for logging, tracking, and responding to law enforcement requests.<br>• Clear, documented rationale for information sharing stance (including non-participation decisions).<br>• Regular assessment of potential benefits and risks of participation in voluntary sharing programs.<br>• Advanced analytics for monitoring and reporting on information sharing activities.<br>• Proactive engagement with law enforcement and regulatory bodies on information sharing best practices.<br>• Continuous improvement process based on internal reviews and external feedback.<br>• Integration with broader data governance and privacy protection frameworks.<br>• Evidence of adapting processes in response to risks gleaned from requests. |

# 2. Compliance Management System (CMS)

**2.1 Compliance Policy and Procedures**

Nonbanks should document and implement compliance policies and procedures, along with processes for maintaining and enhancing compliance program documentation over time to maintain regulatory compliance across the organization's operations, products, and services.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Policy and procedure documentation outdated or missing.<br>• No policy review or approval process.<br>• Missing regulatory applicability or risk assessment framework to determine in scope compliance areas.<br>• No designated ownership of discrete compliance areas.<br>• Policies lack regulatory references. | The assessor identified:<br><br>• Regulatory applicability or assessment.<br>• Full suite of policies and procedures in alignment with assessment.<br>• Policies and procedures lack version control or history of regular updates.<br>• Ownership of the majority of policies unreasonably. consolidated with few personnel.<br>• Minimal regulatory references.<br>• Policies and procedures lack complete tailoring to the business and processes.<br>• Procedures updated infrequently and reactively. | The assessor identified:<br><br>• Full suite of policies and procedures with clear objectives, requirements, and responsibilities outlined in each.<br>• Policies and procedures are appropriately designated to experienced personnel with bandwidth to cover their responsibilities.<br>• Version control with evidence of ongoing updates and improvements.<br>• Evidence of strong awareness and buy-in across all levels of the organization to compliance.<br>• Board-approved policy with defined review cycles.<br>• Procedures updated annually or when significant changes occur. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Evidence that policy and procedures are aligned with overall organizational risk management strategy and tolerance.<br>• Evidence of a proactive and not reactive approach to identifying and mitigating compliance risks and making process improvements.<br>• Advanced monitoring and automated reporting processes accompany policies and procedures.<br>• Evidence of regular review and updates based on emerging risks and business changes.<br>• Key Performance Indicators (KPIs) established for measuring effectiveness. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Real-time visibility into compliance tasks and performance.<br>• Integration of compliance data with other risk management systems.<br>• Regular leadership reporting with evidence of its impact on business decisions.<br>• Strong compliance leadership in place.<br>• Frequent engagement with bank partner(s) and/or regulators on compliance best practices.<br>• No recent history of material compliance gaps.<br>• Regular independent review of policy and procedure effectiveness. |

**2.2 Compliance Training Program**

Nonbanks should educate personnel on an ongoing basis on compliance concepts, the company's compliance program, and each employee's compliance responsibilities.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Training, if any, is ad-hoc and inconsistent.<br>• No formal compliance training program materials in place.<br>• No formal training attendance tracking in place.<br>• Lack of training has created limited awareness of compliance responsibilities across the organization.<br>• Lack of documented collaboration between HR and Compliance for new hire training. | The assessor identified:<br><br>• Compliance training exists but is not comprehensive.<br>• Training covers essential laws and regulations.<br>• Annual training occurs but doesn't cover all appropriate employees or isn't updated in a timely manner.<br>• Limited coordination between HR and Compliance for training, including delays in training new employees.<br>• Content is not sufficiently tailored to the company's needs. | The assessor identified:<br><br>• Compliance training provided to new employees at or shortly after hiring.<br>• Annual training conducted for all employees in the company.<br>• HR and Compliance collaborate to provide adequate training including coordination with any external training providers if used.<br>• Training content covers essential compliance topics.<br>• Initial tracking of training completion.<br>• Includes assessments or quizzes.<br>• Content reinforces the importance of compliance in protecting financial systems and customers.<br>• Encourages employees to speak up through a strong whistleblower and reporting framework. | The assessor identified:<br><br>• Comprehensive compliance training program for new hires and ongoing annual training.<br>• Training content tailored to different roles and risk levels within the organization.<br>• Strong collaboration between HR and Compliance to develop and deliver training, including coordination with any training vendor utilized.<br>• Regular review and update of training materials by subject matter experts to reflect regulatory changes and emerging risks.<br>• System for tracking and reporting on training completion.<br>• Assessment of training effectiveness through tests or practical application.<br>• History of content adjustments based on knowledge gaps and performance. | The assessor identified:<br><br>• Robust compliance training program, confirmed by a third-party audit.<br>• Personalized training paths based on employee roles, experience, and past performance.<br>• Continuous learning approach with regular updates and refresher modules throughout the year.<br>• Advanced collaboration between HR, Compliance, and business units to ensure training relevance, including coordination with training vendors if used.<br>• Use of multiple training methods (e.g., e-learning, workshops, case studies, certifications) to enhance engagement and retention.<br>• Regular independent review of training program effectiveness.<br>• Integration of training performance into employee evaluations and risk management processes.<br>• Proactive adaptation of training to address emerging risks and regulatory changes. |

**2.3 Monitoring and Testing Program**

Nonbanks should review and validate its compliance practices, including maintaining systems and procedures for monitoring key business processes.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Any testing or monitoring is informal and undocumented.<br>• No evidence of internal requirements for testing or monitoring key compliance processes.<br>• No evidence of processes for monitoring new or emerging risks. | The assessor identified:<br><br>• Evidence of occasional testing or monitoring.<br>• Monitoring and testing activities that are informal and not well-documented.<br>• Unstructured approach or schedule for monitoring and testing.<br>• Limited evidence that prior testing yielded findings or improvements.<br>• Limited evidence of follow-up on identified issues.<br>• Incomplete coverage across compliance areas.<br>• Some evidence of monitoring of new and emerging risks. | The assessor identified:<br><br>• Regular monitoring and testing program in place.<br>• Clear and comprehensive documentation of monitoring and testing results.<br>• Head of Compliance or other appropriately designated personnel involved in establishing testing programs.<br>• Some evidence that results were used to improve or enhance the program.<br>• Programmatic monitoring of new and emerging risks. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• A fully developed monitoring and testing plan.<br>• Monitoring and testing that covers all key compliance areas and processes.<br>• Regular reporting of monitoring and testing results to leadership.<br>• Evidence that results are used to inform compliance program updates and remediation activities.<br>• Independent monitoring and testing is incorporated, at least periodically. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Continuous monitoring of emerging risks and internal processes.<br>• Automated systems for tracking and reporting.<br>• Evidence that monitoring and testing of programs is tailored to each area's size and maturity.<br>• Proactive risk mitigation based on monitoring and testing results.<br>• Seamless integration of monitoring and testing with business operations.<br>• Demonstrated leadership commitment to timely remediation and other necessary investments. |

**2.4 Regulatory Applicability and Risk Identification**

Nonbanks should independently identify and monitor the regulatory obligations relevant to their products and services, along with any unique compliance risks that flow from those obligations.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Incomplete or outdated inventory of regulatory requirements.<br>• Lack of awareness of related risks of non-compliance.<br>• No clear ownership of the regulatory applicability or risk quantification process.<br>• Limited awareness of regulatory applicability or compliance risks across the organization. | The assessor identified:<br><br>• Inventory exists but is not comprehensive or detailed to serve as a useful tool for the company.<br>• Ownership of the process is missing.<br>• Inconsistent regulatory applicability or risk awareness across different departments. | The assessor identified:<br><br>• Documented process for ongoing regulatory applicability and risk mapping.<br>• A current inventory of regulatory requirements.<br>• A current understanding of the risk of non-compliance with each requirement.<br>• Clear ownership of the process within the company.<br>• Culture of regulatory awareness and evidence of frequent conversations across the company on regulations and compliance risks. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Systematic process for regularly reviewing and updating regulatory and risk awareness across the organization.<br>• Frequent Legal and Compliance involvement in applicable business conversations and decision making.<br>• Sufficient internal and external resources for proactive and systematic regulatory applicability and compliance risk initiatives.<br>• Strong risk awareness culture throughout the organization.<br>• Detailed state level regulatory applicability mapping. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Continuous Legal and Compliance collaboration in applicable business decisions.<br>• Advanced, data-driven compliance risk identification processes.<br>• Real-time updates to the regulatory obligations inventory.<br>• Clear accountability and enterprise-wide engagement in the process.<br>• Predictive risk identification capabilities.<br>• No recent history of significant gaps in regulatory applicability mapping or compliance risk identification. |

**2.5 Change Management**

Nonbanks should diligently manage product changes affecting compliance with regulations and contractual obligations.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Incomplete or informal change management program in place.<br>• Reactive approach to addressing how changes may affect regulatory compliance.<br>• Lack of clear oversight and approval process for changes. | The assessor identified:<br><br>• Change management policy and processes exist but are not capable of adequately controlling the risk a change may cause a compliance failure.<br>• Limited change management history logged throughout the company.<br>• Limited company-wide controls to prevent changes may cause a compliance failure. | The assessor identified:<br><br>• Changes are routinely tracked throughout the company (e.g., product, technology, customer service).<br>• An internal process for assessing risk of change.<br>• An internal process or approval workflow.<br>• Limited evidence of compliance assessments prior to approval.<br>• Limited evidence of Compliance and Legal involvement in approving changes.<br>• Limited evidence of implementation testing.<br>• Limited evidence of backout or contingency plans.<br>• Limited post-change performance monitoring.<br>• Limited or informal change management reporting. | The assessor identified:<br><br>• Limited history of non-compliance with change management processes.<br>• Detailed change management history and record-keeping.<br>• Diverse change management approval structure, such as a committee with Legal and Compliance representation.<br>• Internal and external communications plan.<br>• Thorough implementation testing.<br>• Detailed backout or contingency planning.<br>• Post change monitoring and reporting processes.<br>• History of assessments and regulator or bank pre-approvals, where required. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• No recent history of changes causing significant compliance gaps.<br>• Limited negative customer, employee, or vendor post-change feedback from a compliance perspective.<br>• Documented history of refreshing audits and other compliance program components, such as policies and procedures needed to reflect changes.<br>• Documented history of regular assessment and improvement of the change management program's effectiveness. |

**2.6 Compliance Risk Assessment**

Nonbanks should conduct compliance assessments to understand the inherent compliance risks, control effectiveness, and residual risk of their products and services.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Informal process for assessing and understanding compliance risk.<br>• The lack of an articulable methodology for assessing risks and/or a lack of consistency in how risks are understood and managed.<br>• Overall limited understanding of inherent risks, controls, or residual risks.<br>• No involvement of leadership in the risk assessment process. | The assessor identified:<br><br>• A written Compliance Risk Assessment process, including evidence of prior assessments.<br>• Existence of a qualitative methodology.<br>• Refreshes were not performed in a timely manner (annual or upon significant business changes).<br>• Key risks not clearly articulated or described.<br>• Results are not utilized in company decisions (e.g., budgeting and staffing) or tracked to bring risk within tolerance.<br>• Leadership has limited involvement or understanding of the process or results. | The assessor identified:<br><br>• A quality and defensible Compliance Risk Assessment process exists.<br>• Evidence that Compliance Risk Assessment completed annually and upon significant business changes.<br>• Effectively assesses inherent risk, control effectiveness, residual risk.<br>• Includes quantitative components (when data is available).<br>• Results shared with leadership for review and approval and utilized in company decisions.<br>• Evidence results have been utilized to enhance compliance program design and/or effectiveness. | The assessor identified:<br><br>• Comprehensive Compliance Risk Assessment process, potentially more frequent than annual.<br>• Sophisticated risk assessment methodology tailored to the company's specific risks.<br>• Takes into account customer, product and service, transaction, channel, and geographic risks.<br>• Detailed analysis of inherent risks, control effectiveness, and residual risks.<br>• Active involvement of leadership in implementing an effective and useful assessment process.<br>• Clear link between risk assessment results and compliance program enhancements, where needed.<br>• Regular updates to risk assessment based on emerging threats and business changes. | The assessor identified:<br><br>• Robust Compliance Risk Assessment process, confirmed by a third-party audit.<br>• Dynamic, continuous risk assessment approach, not limited to annual reviews.<br>• Comprehensive consideration of all risk factors, including emerging and potential future risks.<br>• Full integration of risk assessment with business strategy and product development.<br>• Leadership and the Board actively engaged in the risk assessment process and in the utilization of the results for decision making purposes.<br>• Automated tools for real-time risk monitoring and assessment.<br>• Regular independent review of risk assessment methodology and effectiveness.<br>• Risk assessment drives proactive enhancements to the compliance program and controls.<br>• Risk assessments utilized to establish and assess leadership's performance. |

**2.7 Compliance Reporting**

Nonbanks should monitor and report key performance metrics to stakeholders that provide insights into the compliance program's effectiveness and the company's risk exposure.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Limited history of reporting, if any.<br>• No internal standards or format on reporting processes.<br>• Few or no metrics identified or established for compliance reporting.<br>• No compliance reporting to partners, regulators, or third parties.<br>• No personnel have responsibilities for providing compliance reporting. | The assessor identified:<br><br>• Limited internal standards or format for reporting.<br>• Internal reporting cadence established in policies.<br>• Limited metrics established, but not consistently tracked or reported.<br>• Limited evidence of leadership receiving, reviewing, or utilizing reports in business decisions.<br>• Employees have reporting responsibilities.<br>• Some history of key risks and issues reported, but not comprehensively identified or followed up on. | The assessor identified:<br><br>• Regular reporting to leadership and other stakeholders based on a risk-based schedule.<br>• Structured report covering all key areas.<br>• Comprehensive metrics established and regularly utilized.<br>• Evidence that leadership regularly reviews and utilizes reports in business decisions. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Key risks, major developments, issues, and compliance incidents appear to be thoroughly reported.<br>• Reporting includes recommendations and updates from prior reports and prior report feedback.<br>• Clear, prioritized recommendations for follow-up provided.<br>• Seamless integration of reporting across internal stakeholders and bank partner(s), as applicable. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Real-time and dynamic reporting structure utilizing advanced data visualization.<br>• Comprehensive, risk-based metrics with predictive analytics.<br>• Quarterly or annual refreshes to metrics.<br>• Automated tracking and reporting of risks, developments, issues, and incidents.<br>• Reporting includes actionable, prioritized recommendations with clear ownership and timelines.<br>• Continuous improvement of reporting based on stakeholder feedback and emerging best practices. |

**2.8 Corrective Action/Issues Management Program**

Nonbanks should maintain processes for documenting, tracking, and validating outstanding issues and remediation efforts.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal program for issues management or risk assessment.<br>• Remediation efforts are reactive and not tracked.<br>• Minimal cross-organizational collaboration on corrective action projects. | The assessor identified:<br><br>• Issue management policy and program is in place.<br>• Limited evidence of formally tracking issues via the process.<br>• Limited root cause analysis performed on issues.<br>• Limited tracking and management of remediation efforts. | The assessor identified:<br><br>• Complete policy and structured processes in place that are routinely utilized across the company.<br>• Mechanisms in place to comprehensively source issues from audits, customer complaints, internal escalations, etc.<br>• Compliance and Legal involvement in reviewing root cause analyses performed by business.<br>• Proactive identification and mitigation of potential issues. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Effective cross-organizational collaboration for issue correction, remediation, and validation.<br>• Methodology for ranking and prioritizing issues by customer impact and risk exposure, among other factors.<br>• Seamless cross-organizational collaboration with clear accountability. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Strategic Compliance oversight of root cause analysis process.<br>• Sophisticated analytics and predictive modeling.<br>• Continuous improvement from analyzing trends in past issues to strengthen internal control. |

**2.9 Internal Audit/Third-Party Compliance Testing**

Nonbanks should obtain an independent assessment of its compliance program to evaluate the effectiveness of the program, as well as maintain a process for remediating identified issues and reporting to company leadership.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal independent testing process or policy requirement has been implemented.<br>• Testing, if any, is irregular and not truly independent. | The assessor identified:<br><br>• Formal Internal Audit Policy and plan.<br>• An independent assessment has been performed.<br>• No systematic approach to analyzing and remediating testing findings.<br>• Unclear reporting to leadership or the Board on audit findings or remediation.<br>• Minimal to no engagement from leadership in audit oversight.<br>• Leadership responses to identified issues are reactive and often delayed. | The assessor identified:<br><br>• Evidence of independent assessment being conducted annually and on-time.<br>• There is a detailed independent testing process documented.<br>• Testing results flow into a documented remediation and leadership reporting process.<br>• Compliance Officer or other appropriately designated personnel oversees remediation of identified issues. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Evidence suggesting leadership has selected an independent assessor based on needs and merit, cleared potential conflicts, and optimized selection for quality over price.<br>• Regular, detailed reporting to leadership and the Board on audit findings and remediation.<br>• Limited or no history of repeat independent assessment findings.<br>• Active engagement of leadership in addressing audit findings.<br>• The Board demonstrates understanding and involvement in overseeing the testing process and results. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Highly qualified, fully independent testing party is utilized.<br>• Dynamic Internal Audit plan that adapts to changing risks and business environment.<br>• Proactive remediation process with clear timelines and accountability.<br>• Continuous improvement of testing and remediation processes.<br>• Leadership actively participates in addressing audit findings and improving the compliance program.<br>• Board fully engaged in overseeing the independent testing process, regularly reviews results, and ensures adequate resources for remediation.<br>• Collaborative approach between Compliance Officer or other appropriately designated personnel, leadership, and the Board in managing audit findings and enhancing the overall compliance program. |

# 3. Third Party Risk Management (Vendor Management)

**3.1 TPRM Policy and Procedures**

Nonbanks should document and implement risk management policies and procedures to maintain oversight across the organization's third-party relationships.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Policy and procedure documentation outdated or missing.<br>• No policy review or approval process.<br>• Missing lists of all third parties.<br>• No designated ownership of third-party oversight. | The assessor identified:<br><br>• Documented policy for TPRM program but process specific procedures are missing.<br>• Limited version control or history of regular updates.<br>• Lists of vendors exist but they have not been risk rated.<br>• Limited oversight of third-party relationships.<br>• Standardized processes for vendor lifecycle management.<br>• Vendor due diligence conducted, but inconsistently applied.<br>• Company-wide awareness of third-party risks.<br>• Procedures updated infrequently and reactively. | The assessor identified:<br><br>• Documented policy and procedures detail the company's TPRM program.<br>• Full suite of policies and procedures with clear objectives, requirements, and responsibilities outlined in each.<br>• Higher risk vendors have been subject to thorough and well-documented diligence and ongoing oversight.<br>• Policies and procedures are appropriately designated to experienced personnel with bandwidth to cover their responsibilities.<br>• Version control with evidence of ongoing updates and improvements.<br>• Evidence of vendor due diligence and risk assessment allows compliance to be confirmed.<br>• Regular monitoring of third-party relationships.<br>• Procedures updated annually or when significant changes occur.<br>• Board-approved policy with defined review cycles. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Evidence of a proactive and not reactive approach to identifying and mitigating third-party risks and making process improvements.<br>• Advanced monitoring and automated reporting processes accompany policies and procedures.<br>• Evidence of regular review and updates based on emerging risks and business changes.<br>• Key Performance Indicators (KPIs) established for ongoing monitoring and measuring the performance of the third party/vendor.<br>• Strong awareness and buy-in for TPRM across all levels of the organization.<br>• Integration with other risk management systems. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Real-time visibility into third-party performance.<br>• Integration of third-party risk data with other risk management systems.<br>• Regular leadership reporting with evidence of its impact on business decisions.<br>• Strong third-party risk management leadership in place.<br>• Frequent engagement with bank partner(s) and/or regulators on third-party risk management best practices.<br>• Regular independent review of policy and procedure effectiveness.<br>• No recent history of material third-party risk management program gaps. |

**3.2 Due Diligence Process**

Nonbanks should conduct comprehensive due diligence on its third parties, including processes for evaluating operational, financial, compliance, and security risk dimensions.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal due diligence process or evidence that diligence has been performed.<br>• Due diligence, if performed, is inconsistent and ad-hoc.<br>• No differentiation in diligence between high and low-risk vendors.<br>• No designated employee responsible for vendor assessment.<br>• No contract review process by Legal or Compliance teams.<br>• Due diligence materials not retained or centrally stored. | The assessor identified:<br><br>• Due diligence process is documented but lacks evidence that the process is consistently followed.<br>• Limited consideration of service provider risk in the selection process.<br>• Evidence of due diligence conducted.<br>• Due diligence depth varies widely across the company.<br>• Minimal contract review process with inconsistent Legal involvement.<br>• Due diligence records are maintained but not centrally accessible. | The assessor identified:<br><br>• Routinely followed and consistent due diligence processes across the company.<br>• Due diligence process that addresses operational, financial, compliance, and security dimensions.<br>• A designated employee has clearly defined responsibilities for vendor oversight.<br>• Consistent contract review process with Legal involvement.<br>• Regular review of each third party's internal policies and procedures, when necessary.<br>• Due diligence documentation centrally stored with appropriate retention periods.<br>• Evidence from relevant departments routinely provided input during the due diligence process. | The assessor identified:<br><br>• Risk-based due diligence approach integrated into service provider lifecycle management.<br>• Comprehensive assessment of service provider policies, procedures, and controls.<br>• Standardized contract review involving Legal, Compliance, and business stakeholders.<br>• Regular reviews and updates of due diligence procedures based on regulatory changes.<br>• Due diligence results directly inform contract terms and monitoring requirements.<br>• Evidence of declining service providers that failed to meet risk standards.<br>• No recent history of working with vendors of poor quality or reputation. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Due diligence process fully integrated with enterprise risk management framework.<br>• Advanced risk assessment models determine appropriate due diligence scope.<br>• Automated workflow tools support efficient and thorough due diligence execution.<br>• Continuous monitoring capabilities supplement initial due diligence assessment.<br>• Due diligence data integrated with other risk management and procurement systems.<br>• Regular reporting to leadership and the Board on due diligence program effectiveness and new high risk vendors. |

### 3.3 Third Party Risk Assessment

Nonbanks should conduct a third-party risk assessment to understand the risks of their service provider relationships.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal risk assessment process for third-party vendors and service providers.<br>• Service provider risk is not systematically evaluated at onboarding or thereafter.<br>• No classification system for Servicers.<br>• Risk factors like access to customer PII or direct customer interaction are not consistently considered.<br>• No process for storing risk assessment results. | The assessor identified:<br><br>• Risk assessment process exists but is inconsistently applied.<br>• Evidence of risk evaluation at onboarding, but limited or no ongoing or periodic reassessment.<br>• Classification of servicers exists, but criteria are not well-defined.<br>• Some consideration of key risk factors, but not comprehensive.<br>• Tracking of risk assessment results.<br>• Leadership has limited involvement or understanding of the process, results, and risks of key service providers. | The assessor identified:<br><br>• Evidence that third-party risk assessment for servicers completed at onboarding and periodically thereafter.<br>• Clear classification system for servicers based on defined key factors.<br>• Effectively assesses inherent risk, control effectiveness, residual risk.<br>• Includes quantitative components (when data is available).<br>• Results shared with leadership for review/approval.<br>• Evidence indicates leadership utilizes results in company decisions.<br>• Evidence that past results have been utilized to enhance third-party risk management program design and/or vendor selection/offboarding. | The assessor identified:<br><br>• Comprehensive third-party risk assessment process fully integrated into third-party management lifecycle.<br>• Classification system with multiple tiers and granular risk categorization.<br>• Regular schedule for periodic reassessments with flexibility for event-driven assessments.<br>• Risk assessment results actively inform decision-making and risk mitigation strategies.<br>• Detailed analysis of inherent risks, control effectiveness, and residual risks.<br>• Active involvement of leadership in implementing an effective and useful assessment process.<br>• Regular updates to third-party risk assessment based on emerging risks and business changes. | The assessor identified:<br><br>• Robust risk assessment process is a key component of overall risk management strategy.<br>• Dynamic risk classification system that adapts to changing risk profiles<br>• Comprehensive set of risk factors with weighted scoring based on business impact.<br>• Full integration of risk assessment with business strategy and product development.<br>• Continuous monitoring and reassessment of Servicer risks.<br>• Automation used to enhance risk assessment accuracy and efficiency<br>• Integration of risk assessment data with other enterprise risk management and business intelligence systems.<br>• Regular independent review of risk assessment methodology and effectiveness.<br>• Leadership oversight and reporting on third-party risk assessments.<br>• Proactive approach to identifying and mitigating emerging third-party risks.<br>• Risk assessments utilized to establish and assess leadership's performance. |

**3.4 Written Contracts**

Nonbanks should establish and maintain service provider agreements with appropriate contractual protections, including provisions for security, compliance, performance standards, and termination rights.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Contracts, when used, lack specific and clear expectations.<br>• Legal is rarely or never involved in contract review.<br>• No standard process for contract creation or management.<br>• Contracts do not consistently address protections for the company and its assets (e.g., data processing agreements). | The assessor identified:<br><br>• Some contracts include specific expectations, but clarity and comprehensiveness vary.<br>• Informal responsibility for contract establishment, not clearly designated.<br>• Occasional involvement of Legal in contract review, but not consistent.<br>• Initial process for contract creation, but lacks standardization.<br>• Limited consideration of company and asset protection in contracts.<br>• Limited retention/storing of contracts. | The assessor identified:<br><br>• Evidence that contracts include specific and clear expectations.<br>• Clear ownership of the process within the company.<br>• Legal is engaged to review each servicer contract.<br>• Consistent focus on ensuring adequate protections for the company and its assets.<br>• Process is documented and followed across the organization.<br>• Designated individuals who are the only authorized signatories. | The assessor identified:<br><br>• Contracts consistently include detailed, clear, and tailored expectations for each servicer.<br>• Clear ownership and accountability for contract management across different roles.<br>• Evidence of proactive engagement of Legal throughout the contract lifecycle.<br>• Robust protections for the company and its assets, regularly updated based on risk assessments.<br>• Contract terms align with overall vendor management and risk mitigation strategies.<br>• Regular review and update of contract templates and processes. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Contract management process fully integrated with overall risk and vendor management.<br>• Adaptive contracting process that anticipate and address emerging risks and business needs.<br>• Automation used for contract creation, management, and compliance monitoring.<br>• Legal integrated into the contract process, providing strategic input.<br>• Continuous monitoring of contract performance and compliance.<br>• Regular board-level reporting on contract management effectiveness.<br>• No recent history of sound processes not being followed. |

### 3.5 Ongoing Due Diligence and Oversight

Nonbanks should monitor third-party relationships for performance, compliance, and risk issues and escalate concerns in a timely manner according to their governance framework and contractual requirements.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal process for ongoing monitoring and oversight of servicer relationships.<br>• Due diligence and oversight activities, if any, are sporadic and inconsistent.<br>• No consideration of criticality, risk, complexity, or volume of outsourced activities.<br>• No designated responsibility for ongoing due diligence and oversight.<br>• Lack of awareness about the need for continuous monitoring of servicers.<br>• Reactive approach to servicer issues or concerns. | The assessor identified:<br><br>• Ongoing due diligence and oversight policy and processes exists, but are not capable of adequately controlling the risk a third-party presents.<br>• Limited oversight activities and, if any, they primarily focus on reacting to major issues or incidents.<br>• Limited designation of responsibility for ongoing due diligence, not clearly designated.<br>• Application of due diligence efforts across different servicers is limited.<br>• Minimal documentation of ongoing monitoring activities. | The assessor identified:<br><br>• Consistent process for ongoing monitoring and oversight of all servicer relationships.<br>• Due diligence and oversight activities are commensurate with the criticality, risk, complexity, and volume of outsourced activities.<br>• Clear ownership of the process within the company.<br>• Regular monitoring activities are conducted and documented.<br>• Evidence of reporting on ongoing due diligence and oversight activities.<br>• Some evidence that results were used to improve or enhance the program. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Risk-based approach to ongoing due diligence and oversight.<br>• Tailored monitoring plans for each servicer based on detailed risk assessments.<br>• Clear criteria for determining the depth and frequency of oversight activities.<br>• Integration of ongoing due diligence results with overall vendor management strategy.<br>• Regular review and update of the oversight process based on emerging risks and business changes.<br>• Advanced reporting and analytics on servicer performance and risk trends.<br>• Proactive identification and mitigation of potential servicer issues. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Ongoing due diligence and oversight process fully integrated with enterprise risk management.<br>• Continuous monitoring of servicer performance and risk indicators.<br>• Dynamic adjustment of oversight activities based on changing risk profiles and performance metrics.<br>• Seamless integration of servicer data with business operations.<br>• Board-level visibility and reporting on ongoing due diligence and oversight activities.<br>• Collaborative approach with servicers to drive continuous improvement.<br>• Demonstrated leadership commitment to timely remediation and other necessary investments.<br>• No recent history of significant third-party service provider issues. |

# 4. Complaint Handling

**4.1 Complaint Policy and Procedures**

Nonbanks should maintain a documented policy that establishes the framework for receiving, tracking, responding to, and analyzing customer complaints.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal complaint policy in place.<br>• Complaints are handled inconsistently and reactively.<br>• No requirements for documentation of complaint resolutions.<br>• No defined escalation process for complex issues.<br>• Minimal requirements for reporting complaints to management or bank partner(s), as applicable. | The assessor identified:<br><br>• Consistency in complaint handling, but processes not fully standardized.<br>• System for logging complaints, but tracking is incomplete.<br>• Documentation of complaint resolutions, often inconsistent.<br>• Informal escalation process for complex issues.<br>• Limited reporting on complaints to management and bank partner(s), as required. | The assessor identified:<br><br>• Standardized processes for handling various types of complaints.<br>• Centralized system for logging and tracking complaints.<br>• Consistent and auditable documentation of complaint resolutions.<br>• Defined escalation process for complex issues.<br>• Complaint categorization methodology (e.g., tiered approach).<br>• Regular reporting on complaints to management and bank partner(s), as required.<br>• Measures in place to assess customer satisfaction with complaint resolution.<br>• Board-approved policy with defined review cycles.<br>• Clearly designated employee responsible for complaint oversight and reporting. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Evidence that the complaint program is regularly reviewed and updated.<br>• System for logging, tracking, and analyzing complaints.<br>• Thorough documentation of all complaint resolutions.<br>• Clear escalation matrix for complex issues with designated responsible parties.<br>• Comprehensive reporting on complaints to management and bank partner(s), including trend analysis.<br>• Requires regular, in-depth complaint root cause analysis and evidence of its use to drive process improvements.<br>• Multiple channels available for customers to submit complaints.<br>• Proactive measures to assess and improve customer satisfaction with complaint resolution. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Comprehensive complaint policy that adapts to changing regulatory requirements and customer needs.<br>• Highly efficient, customer-centric processes for handling complaints, including IVR, live agents, and use of automation for quality control.<br>• Comprehensive documentation of complaint resolutions with insights for process improvement.<br>• Dynamic escalation process that adapts based on complaint complexity and customer impact.<br>• Real-time reporting and dashboards on complaints for management and bank partner(s), as applicable.<br>• Regular optimization of complaint handling processes based on feedback and outcomes.<br>• Omnichannel approach for complaint submission, including integration with social media and emerging platforms.<br>• Proactive identification and resolution of potential issues before they become complaints.<br>• No recent history of complaint management issues. |

**4.2 Complaint Procedure**

Nonbanks should document and implement complaint procedures that detail the day-to-day operations of the complaint handling process, including intake, classification, tracking, and response to consumer complaints.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No procedures specifying the actual processes employed.<br>• Limited evidence of how complaints are intake, classified, tracked, or responded to.<br>• Complaint handling is inconsistent and varies by individual.<br>• No structured intake process or classification system.<br>• Complaints are tracked manually, if at all.<br>• Response times are inconsistent and often delayed.<br>• No version control for procedures.<br>• No regular updates to procedures. | The assessor identified:<br><br>• Implemented procedures, including controls that indicate complaints are properly intaken, classified, tracked, and responded to.<br>• Limited evidence suggesting how complaints are responded to.<br>• Some consistency in complaint handling, but significant variations remain.<br>• Simple intake process with Initial classification (e.g., product type).<br>• Complaints tracked in a spreadsheet or database.<br>• General guidelines for response times, but often not met.<br>• Procedures updated infrequently and reactively. | The assessor identified:<br><br>• Standardized processes for intake, classification, tracking, and response.<br>• Defined intake channels and classification system (e.g., severity, product type).<br>• Centralized complaint tracking system with limited reporting capabilities.<br>• Specific timeframes established for complaint acknowledgment.<br>• Specific timeframes established for complaint resolution.<br>• Version control with change logs.<br>• Procedures updated annually or when significant changes occur. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Evidence of consistent processes across all complaint types and channels.<br>• Multi-faceted classification system (e.g., severity, product, root cause).<br>• Advanced complaint tracking system with automated alerts and reporting.<br>• Tiered response time targets based on complaint severity and type.<br>• Integration with other compliance and customer service systems. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Automated processes for intake, classification, and initial response.<br>• AI-assisted classification and routing of complaints.<br>• Real-time complaint tracking and analytics system with predictive capabilities.<br>• Automated escalation and dynamic response time targets based on multiple factors.<br>• Full integration with all relevant business systems (e.g., CRM, product development).<br>• Proactive identification and resolution of potential complaints before they arise. |

**4.3 Root Cause Analysis**

Nonbanks should maintain processes for analyzing complaint patterns to identify underlying issues and translate insights into operational improvements.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal root cause analysis process for complaints.<br>• Analysis of complaints, if any, is superficial and reactive.<br>• No systematic identification of underlying issues or trends.<br>• Minimal to no use of complaint data to drive improvements.<br>• No designated responsibility for root cause analysis.<br>• No reporting on insights from root causes to leadership. | The assessor identified:<br><br>• Cause identification performed on some complaints but not all, without following standard steps.<br>• Evidence of attempts to identify underlying issues, but analysis lacks depth.<br>• Limited use of complaint data to suggest improvements for product teams.<br>• Informal responsibility assignment for root cause analysis.<br>• Occasional, ad-hoc reporting on insights from root causes to leadership. | The assessor identified:<br><br>• Step-by-step process followed for all complaints using standard templates and categories.<br>• Evidence of regular identification of underlying issues and trends.<br>• Systematic categorization of root causes.<br>• Some use of complaint data to drive improvements in products and processes.<br>• Designated responsibility for conducting root cause analysis.<br>• Regular reporting on insights from root causes to leadership. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• End-to-end analysis process that examines multiple factors (people, process, systems) and links directly to the case management system.<br>• In-depth analysis of underlying issues, trends, and systemic problems.<br>• Clear methodology for prioritizing and addressing identified root causes.<br>• Regular use of complaint data to drive significant improvements.<br>• Cross-functional team involved in root cause analysis and improvement initiatives.<br>• Regular reporting on root causes and resulting improvements to leadership. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Advanced root cause analysis process potentially leveraging data analytics and AI.<br>• Proactive identification of potential issues before they lead to complaints.<br>• Continuous, real-time analysis of complaint data to identify trends and root causes.<br>• Integration of insights from root cause analysis into product development and process improvement.<br>• Regular third-party audits of root cause analysis process effectiveness.<br>• Root cause analysis results are directly tied to strategic planning and resource allocation.<br>• Evidence suggests competence in utilizing analysis to solve issues, without repeat issues. |

**4.4 Complaint Intake Channels**

Nonbanks should establish and maintain multiple channels for receiving customer complaints, with clear guidance on the complaint submission process.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Limited complaint intake channels (e.g., only email).<br>• No formal guidance on how to file a complaint on customer-facing platforms.<br>• Inconsistent monitoring of established channels.<br>• No process for handling complaints from non-standard channels (e.g., social media).<br>• No regular checks on the accessibility and reasonableness of complaint channels. | The assessor identified:<br><br>• Reasonable complaint intake channels established (e.g., email and live agent).<br>• Limited guidance on how to file a complaint available on the main website.<br>• Irregular monitoring of established channels.<br>• Ad-hoc process for handling complaints from non-standard channels.<br>• Infrequent checks on the sufficiency of complaint channels. | The assessor identified:<br><br>• Multiple complaint intake channels established (e.g., email, phone, web form, chat).<br>• Publicly listed dedicated email address for receiving complaints.<br>• Regular monitoring of third-party complaint aggregators (e.g., CFPB, Better Business Bureau).<br>• Clear guidance on how to file a complaint available on all major customer-facing platforms.<br>• Regular monitoring of established channels.<br>• Process for handling complaints from non-standard channels.<br>• Quarterly checks on the sufficiency of complaint channels.<br>• Tracking of complaint volume by channel. | The assessor identified:<br><br>• Comprehensive set of complaint intake channels (e.g., email, phone, web form, chat, mobile app).<br>• Detailed guidance on how to file a complaint prominently displayed on all customer-facing platforms.<br>• Consistent monitoring of all established channels.<br>• Detailed processes for handling complaints from all potential channels.<br>• Monthly checks on the sufficiency of all complaint channels.<br>• Detailed tracking and analysis of complaint volume and types by channel.<br>• Limited recent history of complaints that include difficulty in submitting complaints or obtaining assistance. | The assessor identified:<br><br>• Omnichannel approach to complaint intake (including emerging platforms).<br>• Interactive, user-friendly guidance on complaint filing processes across all platforms.<br>• Real-time monitoring of all complaint channels.<br>• Sophisticated process for handling complaints from any source, with AI-assisted routing and prioritization.<br>• Advanced analytics on complaint data across channels to inform business decisions.<br>• Integration of complaint channels with CRM and other relevant systems.<br>• Proactive identification and resolution of potential complaints through predictive analytics.<br>• Continuous optimization of channels based on customer preferences and complaint data.<br>• No recent history of complaints that include difficulty in submitting complaints or obtaining assistance. |

**4.5 Complaint Tracking**

Nonbanks should implement systems and processes for documenting, classifying, and monitoring complaints throughout their lifecycle.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal complaint classification system.<br>• Complaint tracking is manual and inconsistent.<br>• Minimal information recorded for each complaint.<br>• No centralized database; complaints tracked in disparate locations.<br>• No standardized process for updating complaint status.<br>• No reporting capabilities. | The assessor identified:<br><br>• Complaint classification system (e.g., high, medium, low priority).<br>• Evidence of complaints tracked in a spreadsheet or simple database.<br>• Some key information recorded, but not comprehensive.<br>• Centralized tracking, but not easily accessible by all relevant staff.<br>• Initial process for updating complaint status, but often inconsistent.<br>• Limited reporting capabilities (e.g., limited to count of complaints). | The assessor identified:<br><br>• Defined complaint classification system (e.g., Tier 1, 2, 3).<br>• Complaints tracked in a dedicated database.<br>• Standardized complaint form/template that captures date received, receiving method, customer information, complaint description, actions taken, root cause, and resolution date.<br>• Complaint log maintained that documents intake through resolution.<br>• Evidence information consistently recorded for each complaint.<br>• Evidence indicating how resolution was communicated to the customer.<br>• Centralized database accessible by relevant staff.<br>• Standardized process for updating complaint status.<br>• Initial reporting capabilities (e.g., complaint volumes by type, status). | The assessor identified:<br><br>• Comprehensive complaint classification system with clear criteria.<br>• Robust complaint tracking database with advanced search and filtering.<br>• Evidence of all required information consistently recorded, including detailed resolution steps.<br>• Automated status updates based on actions taken.<br>• Advanced reporting capabilities (e.g., trend analysis, response time metrics).<br>• Integration with other relevant systems (e.g., CRM, customer service platform). | The assessor identified:<br><br>• Sophisticated classification system that adapts to emerging complaint types and regulatory changes.<br>• Comprehensive information captured for each complaint, including predictive insights.<br>• Fully integrated, cloud-based database with secure access from any device.<br>• Automated workflow management with smart routing and escalation.<br>• Advanced analytics and reporting with predictive modeling and AI-driven insights.<br>• Full integration with all relevant business systems.<br>• Automated compliance checks and alerts for regulatory reporting requirements.<br>• Continuous improvement based on analysis of tracking data and user feedback.<br>• No recent history of repeat complaints or other evidence the company failed to follow up or close out complaints due to tracking issues. |

**4.6 Complaint Reporting**

Nonbanks should analyze and communicate complaint data to stakeholders, tracking key metrics and providing insights to drive improvements.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal complaint reporting process.<br>• Limited history of reporting, if any.<br>• No internal standards or format on reporting processes.<br>• Few or no metrics identified or established for complaint reporting.<br>• No complaint reporting to partners, regulators, or third parties.<br>• No personnel have responsibilities for providing complaint reporting. | The assessor identified:<br><br>• Limited internal standards or format for reporting.<br>• Internal reporting cadence established in policies.<br>• Limited metrics established, but not consistently tracked or reported.<br>• Limited evidence of leadership receiving, reviewing, or utilizing reports in business decisions.<br>• Employees have reporting responsibilities.<br>• Some history of key complaint data and issues reported, but not comprehensively identified or followed up on. | The assessor identified:<br><br>• Regular reporting to leadership and other stakeholders based on a risk-based schedule.<br>• Structured report covering all key complaint data.<br>• Comprehensive metrics established and regularly utilized.<br>• Evidence that leadership regularly reviews and utilizes reports in business decisions. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Key complaint data, findings, risks, issues, and incidents appear to be thoroughly reported.<br>• Reporting includes recommendations and updates from prior reports and prior report feedback.<br>• Clear, prioritized recommendations for follow-up provided.<br>• Integration of reporting across internal stakeholders and bank partner(s), as applicable. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Real-time and dynamic reporting structure utilizing advanced data visualization.<br>• Comprehensive, risk-based metrics with predictive analytics.<br>• Quarterly or annual refreshes to metrics.<br>• Automated tracking and reporting of risks, developments, issues, and incidents.<br>• Reporting includes actionable, prioritized recommendations with clear ownership and timelines.<br>• Continuous improvement of reporting based on stakeholder feedback and emerging best practices. |

**4.7 Training**

Nonbanks should educate personnel on an ongoing basis on complaint handling concepts, the company's complaint program, and each employee's responsibilities in the complaint process.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Training, if any, is ad-hoc and inconsistent.<br>• No formal complaint handling training program materials in place.<br>• No formal training attendance tracking in place.<br>• Lack of training has created limited awareness of complaint handling responsibilities across the organization.<br>• Lack of documented collaboration between HR and complaint team for new hire training. | The assessor identified:<br><br>• Complaint handling training exists but is not comprehensive.<br>• Some new hires receive training, but not consistently.<br>• Annual training occurs but doesn't cover all appropriate employees or isn't updated in a timely manner.<br>• Limited coordination between HR and complaint team for training, including delays in training new employees.<br>• Content is not sufficiently tailored to the company's needs. | The assessor identified:<br><br>• Complaint handling training provided to new employees at or shortly after hiring.<br>• Annual training conducted for all employees in the company.<br>• HR and complaint teams collaborate to provide adequate training including coordination with any external training providers if used.<br>• Training content covers essential complaint handling topics.<br>• Limited tracking of training completion.<br>• Includes assessments or quizzes. | The assessor identified:<br><br>• Complete complaint handling training program for new hires and ongoing annual training.<br>• Training content tailored to different roles and risk levels within the organization.<br>• Strong collaboration between HR and complaint teams to develop and deliver training, including coordination with any training vendor utilized.<br>• Regular review and update of training materials by subject matter experts to reflect regulatory changes and emerging risks.<br>• System for tracking and reporting on training completion.<br>• Assessment of training effectiveness through tests or practical application.<br>• History of content adjustments based on knowledge gaps and performance. | The assessor identified:<br><br>• Robust complaint handling training program, confirmed by a third-party audit.<br>• Personalized training paths based on employee roles, experience, and past performance.<br>• Continuous learning approach with regular updates and refresher modules throughout the year.<br>• Advanced collaboration between HR, complaint team, and business units to ensure training relevance, including coordination with training vendor if used.<br>• Use of multiple training methods (e.g., e-learning, workshops, case studies, certifications) to enhance engagement and retention.<br>• Regular independent review of training program effectiveness.<br>• Integration of training performance into employee evaluations and risk management processes.<br>• Proactive adaptation of training to address emerging risks and regulatory changes. |

**4.8 Record Retention**

Nonbanks should maintain complaint records in compliance with regulatory and contractual requirements, ensuring secure storage and appropriate access to complaint documentation.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal policy requiring complaint record retention.<br>• Inconsistent and haphazard record keeping.<br>• No designated responsibility for record retention.<br>• Lack of secure storage for complaint records.<br>• Evidence of limited awareness of regulatory requirements for complaint record retention.<br>• No process for record disposal or destruction.<br>• No defined retention periods. | The assessor identified:<br><br>• A policy includes complaint record retention standards.<br>• Some evidence of complaint records are retained, but not consistently.<br>• Limited security measures for stored records.<br>• Limited evidence of oversight of the record retention process.<br>• Inconsistent process for record disposal. | The assessor identified:<br><br>• Complaint record retention policy with clear retention standards, timelines, and location of data.<br>• Evidence of retention of all complaints, research documents, response correspondence, and supporting documentation.<br>• Designated personnel responsible for record retention oversight.<br>• Secure storage system implemented for complaint records.<br>• Records maintained in a form capable of being accurately reproduced for later reference.<br>• Records accessible to persons who are legally entitled to access them.<br>• Process for record deletion at the end of retention period.<br>• Consistent application of retention policies across all complaint types.<br>• Regular monitoring of record retention compliance. | In addition to the criteria identified in 3. Integrated, the assessor identified:<br><br>• Complaint record retention policy integrated with overall data governance strategy.<br>• Leadership oversight and regular reviews of record retention practices.<br>• Advanced storage (e.g., backups) and retrieval processes for complaint records.<br>• Regular internal audits of record retention practices.<br>• Comprehensive process for secure record disposal and destruction.<br>• Clear protocols for handling records related to ongoing investigations or litigation.<br>• No recent history of non-compliance with retention requirements. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Automated retention and disposal schedules for complaint records.<br>• Advanced encryption and access controls for stored records.<br>• Real-time tracking and reporting of record retention status.<br>• Integration with broader data governance and privacy compliance frameworks.<br>• Continuous improvement process based on regulatory changes and best practices.<br>• Automated classification and management of complaint records.<br>• Regular third-party audits of record retention practices.<br>• Seamless integration with complaint management and reporting systems.<br>• Proactive adaptation to emerging data protection and privacy regulations. |

# 5. Operational Risk

**5.1 Information Security and Data Privacy**

Nonbanks should implement systems, processes, and controls to protect customer data confidentiality, integrity, and availability.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal information security program in place.<br>• Policy and procedure documentation outdated or missing.<br>• Limited to no awareness of privacy laws and regulations.<br>• No regular penetration testing or security certifications.<br>• Reactive approach to security incidents.<br>• No designated CISO or equivalent role overseeing Information Security and Privacy programs.<br>• Employees receive minimal or no security training.<br>• Data protection measures are inconsistent or non-existent. | The assessor identified:<br><br>• Information security policies and procedures exist but may be outdated or incomplete.<br>• Awareness of privacy laws, but compliance is inconsistent.<br>• Occasional penetration testing, but not on a regular schedule.<br>• Security measures in place, but not comprehensive.<br>• CISO role exists but may lack authority or resources.<br>• Initial security training provided to some employees.<br>• Limited data protection measures implemented.<br>• Procedures updated infrequently and reactively. | The assessor identified:<br><br>• Information security program covering key areas.<br>• Evidence of understanding and compliance with major privacy laws (e.g., GLBA, CCPA).<br>• Regular penetration testing conducted, but may not cover all systems.<br>• Some relevant certifications (e.g., SOC 2) obtained and maintained.<br>• CISO or other appropriately. designated personnel lead the security efforts with support from the IT team.<br>• Regular security training provided to most employees.<br>• Data protection measures cover most critical assets.<br>• Version control with evidence of ongoing updates and improvements.<br>• Procedures updated annually or when significant changes occur. | The assessor identified:<br><br>• Comprehensive information security program aligned with industry standards.<br>• Evidence of full compliance with all applicable privacy laws and regulations.<br>• Regular, comprehensive penetration testing across all critical systems.<br>• All relevant certifications obtained and actively maintained.<br>• CISO has clear authority and resources to implement security strategies.<br>• Tailored security training provided to all employees based on roles.<br>• Robust data protection measures implemented across the organization.<br>• Security and privacy considerations integrated into business processes.<br>• Evidence that the security program is regularly reviewed and updated.<br>• No outstanding audit findings or other relevant issues to be resolved. | The assessor identified:<br><br>• Advanced, risk-based information security program with continuous improvement.<br>• Proactive approach to privacy compliance, staying ahead of regulatory changes.<br>• Continuous security monitoring and testing, including third-party assessments.<br>• Industry-leading certifications maintained, often exceeding standard requirements.<br>• CISO is a key strategic leader, involved in all relevant business decisions.<br>• Security culture embedded throughout the organization, with ongoing awareness programs.<br>• Regular independent review of policy and procedure effectiveness.<br>• Policies demonstrate sophisticated understanding of regulatory expectations and industry best practices.<br>• Security and privacy by design principles applied to all new initiatives.<br>• Advanced threat intelligence and incident response capabilities.<br>• Regular Board-level reporting and oversight of information security and privacy matters.<br>• Policies proactively address emerging risks and regulatory trends.<br>• No recent history of issues or data breaches. |

**5.2 Data Classification and Management**

Nonbanks should implement a structured approach to categorizing and protecting information assets based on sensitivity levels, with appropriate policies, controls, and oversight in place for managing data across the organization.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal data classification policy or scheme in place.<br>• Limited or no awareness of different levels of data sensitivity.<br>• No distinction between public, internal, confidential, or restricted data.<br>• Inconsistent or non-existent data handling practices.<br>• No clear roles or responsibilities for data classification.<br>• Lack of employee training on data classification.<br>• No consideration of legal or regulatory requirements in data handling.<br>• High risk of data mishandling or unauthorized disclosure. | The assessor identified:<br><br>• Data classification scheme exists with incomplete or inconsistent application.<br>• Evidence of limited awareness of different data sensitivity levels (e.g., public vs. confidential).<br>• Limited guidelines for handling different types of data.<br>• Limited roles defined for data classification with unclear responsibilities.<br>• Minimal employee training on data classification concepts.<br>• Limited consideration of legal requirements lacking comprehensiveness.<br>• Inconsistent labeling and handling of sensitive data. | The assessor identified:<br><br>• Data classification policy with defined categories (e.g., Public, Internal Use, Confidential, Restricted).<br>• Clear definitions and examples for each data classification level.<br>• Guidelines for handling data at each sensitivity level.<br>• Defined roles and responsibilities for data classification and handling.<br>• Regular employee training on data classification policy and procedures.<br>• Consideration of major legal and regulatory requirements in classification schemes.<br>• Consistent labeling of sensitive data, with some automated classification tools in use. | The assessor identified:<br><br>• Comprehensive data classification policy integrated with overall information security strategy.<br>• Detailed classification levels with clear criteria and numerous examples.<br>• Thorough guidelines for data handling, storage, transmission, and destruction for each level.<br>• Well-defined roles and responsibilities, including data owners and custodians.<br>• Regular, role-specific training on data classification and handling.<br>• Full alignment with legal, regulatory, and contractual requirements.<br>• Automated classification tools widely used, with manual override capabilities.<br>• Regular audits of data classification practices and effectiveness. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Advanced data classification policy that adapts to changing business and regulatory environments.<br>• Dynamic classification levels that consider context and use cases.<br>• Context-aware guidelines for data handling throughout the data lifecycle.<br>• Clearly defined and widely understood roles, with data classification embedded in all relevant job functions.<br>• Continuous, interactive training and awareness programs on data classification.<br>• Proactive alignment with emerging legal and regulatory requirements.<br>• Real-time monitoring and enforcement of data handling based on classification.<br>• Regular third-party audits and continuous improvement of classification practices.<br>• Data classification integrated into all business processes and decision-making.<br>• Culture of data awareness and responsible handling throughout the organization.<br>• Evidence data management provides critical advantages to various parts of the company. |

**5.3 Fraud Prevention and Detection**

Nonbanks should implement capabilities for preventing, detecting, and responding to fraudulent activities during customer onboarding, including systems, procedures, and oversight to protect against new account fraud and identity theft.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Fraud and identity theft prevention program not fully implemented.<br>• Lack of a Red Flags program.<br>• No identity verification systems for new accounts.<br>• Minimal or no systems for fraud detection and prevention.<br>• No structured process for responding to fraudulent activities during account opening.<br>• Employee training on fraud detection and prevention is non-existent or ad hoc.<br>• No clear responsibility for fraud prevention within the organization.<br>• Reactive approach to fraud incidents. | The assessor identified:<br><br>• Fraud and identity theft prevention policies in place.<br>• Red Flags program in place but is limited to simple identity verification concepts.<br>• Fraud detection systems provide limited coverage.<br>• Fraud handling procedures are lacking detail.<br>• Occasional employee training on fraud detection without regular or comprehensive approach.<br>• Head of Risk Management or equivalent identified with limited resources or authority.<br>• Fraud prevention efforts are siloed and lack cross-functional coordination. | The assessor identified:<br><br>• Fraud and identity theft prevention program covers all key areas of customer onboarding.<br>• Evidence the Red Flags program is operational and proving useful for new accounts.<br>• Systems in place for detecting and preventing common types of fraud.<br>• Procedures for responding to fraudulent activities during account opening.<br>• Regular employee training on fraud detection and prevention.<br>• Head of Risk Management, or equivalent leads fraud prevention efforts with a dedicated team.<br>• CRO, or equivalent, provides oversight and reports to the Board or leadership periodically.<br>• Most staff are aware of their responsibility to report potential fraud. | The assessor identified:<br><br>• Comprehensive fraud and identity theft prevention program aligned with industry standards.<br>• Robust Red Flags program for customer verification actively monitored and updated.<br>• Advanced systems implemented for identity verification and fraud detection and prevention across all business areas.<br>• Detailed, well-documented procedures for detecting, preventing, and responding to identity theft and account opening fraud.<br>• Regular, role-specific training on fraud detection and prevention for all employees.<br>• Fraud Prevention Team works cross-functionally to implement and improve strategies.<br>• CRO, or equivalent, regularly reports to the Board on fraud prevention strategies and outcomes.<br>• Strong culture of fraud awareness and reporting throughout the organization. | The assessor identified:<br><br>• Advanced fraud and identity theft prevention program with evidence of continuous improvement.<br>• Red Flags program is proactive, leveraging advanced analytics to identify emerging threats in customer verification.<br>• Cutting-edge identity verification and onboarding fraud detection systems using AI and machine learning.<br>• Dynamic, adaptive process for fraud prevention that evolves with new threats.<br>• Fraud Prevention Team collaborates with external experts and law enforcement.<br>• CRO is a key strategic leader, involved in all relevant business decisions.<br>• Fraud prevention is embedded in organizational culture, with staff at all levels actively engaged.<br>• Regular third-party audits of fraud prevention program effectiveness.<br>• Fraud prevention strategies directly tied to overall risk management and business strategy.<br>• No recent history of material fraud losses or other related issues. |

**5.4 Fraud Monitoring, Transaction Processing and Funds Transfer**

Nonbanks should implement robust approaches to monitoring for fraudulent activity in existing accounts, processing and monitoring funds transfers, ensuring compliance with relevant regulations, implementing appropriate system controls, and maintaining oversight of transaction activities.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal policies or procedures for funds transfers and transaction processing.<br>• Limited awareness of relevant regulations (Regulation E, CC, J, NACHA rules).<br>• No systematic fraud monitoring for ongoing customer transactions after account opening.<br>• No fraud alerts or notification systems for suspicious transaction activity.<br>• Manual and inconsistent transaction processing.<br>• Minimal recordkeeping, often incomplete or disorganized.<br>• No clear roles or responsibilities for regulatory compliance.<br>• No systems in place for timely processing of transactions.<br>• High risk of regulatory non-compliance and processing errors. | The assessor identified:<br><br>• Policies and procedures exist for funds transfers with incomplete or outdated elements.<br>• Limited awareness across the company of relevant regulations.<br>• Semi-automated transaction processing requiring significant manual intervention.<br>• Basic fraud monitoring with limited rules-based detection for existing accounts.<br>• Minimal process for investigating suspicious transactions and activity patterns.<br>• Some compliance recordkeeping in place but evidence is limited.<br>• COO or equivalent aware of compliance requirements with limited implementation.<br>• Systems in place for transaction processing not optimized for timeliness.<br>• Occasional compliance checks without systematic approach. | The assessor identified:<br><br>• Policies and procedures covering key areas of funds transfers.<br>• Evidence of compliance with major regulations (Regulation E, CC, J, NACHA) is mostly achieved.<br>• Automated systems in place for most transaction processing.<br>• Fraud monitoring systems covering common transaction fraud patterns and scenarios.<br>• Established processes for investigating and responding to suspicious account activities.<br>• Customer notification for suspicious transactions and account activity.<br>• Evidence of a structured recordkeeping system implemented.<br>• Evidence demonstrating all required authorization requests were obtained and storage requirements are met.<br>• COO or equivalent actively implements policies for regulatory compliance.<br>• Operations team maintains transaction processing systems.<br>• CCO involved in ensuring regulatory alignment.<br>• Internal or external audit function conducts regular compliance assessments.<br>• CRO begins to assess transaction risks. | The assessor identified:<br><br>• Comprehensive policies and procedures aligned with all relevant regulations.<br>• Evidence demonstrates readiness to fully comply with Regulation E, CC, J, and NACHA rules, as applicable.<br>• Highly automated and efficient transaction processing systems.<br>• Advanced fraud monitoring with transaction and behavior analysis capabilities.<br>• Comprehensive fraud investigation and response protocols for account activity.<br>• Multi-channel fraud monitoring and detection capabilities for existing accounts.<br>• Regular reporting on fraud metrics and patterns to leadership.<br>• Robust recordkeeping with easy accessibility and auditability.<br>• COO leads strategic initiatives for regulatory compliance in funds transfers.<br>• Operations team continuously improves transaction processing systems.<br>• CCO actively involved in interpreting and implementing regulatory requirements.<br>• Regular, thorough compliance audits conducted by Internal Audit.<br>• CRO assesses transaction risks and reports to the Board periodically.<br>• Clear roles and responsibilities established across all relevant departments. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Transaction processing systems with real-time monitoring and error detection.<br>• AI and machine learning-based transaction fraud detection systems.<br>• Predictive fraud analytics to identify emerging transaction-related threats.<br>• Integration of fraud controls with customer experience throughout the account lifecycle.<br>• Minimal false positives with high detection rates for transaction monitoring.<br>• Advanced recordkeeping with data analytics for trend analysis and risk detection.<br>• COO drives innovation in funds transfer processes and compliance strategies.<br>• Continuous compliance monitoring and real-time auditing capabilities.<br>• CRO provides sophisticated risk analysis of transaction patterns to the Board.<br>• Regular third-party audits.<br>• Integration of compliance, risk management, and operational efficiency.<br>• Proactive identification and mitigation of potential regulatory and operational risks.<br>• No recent history of transaction issues, such as unreasonably high return rates. |

**5.5 Business Continuity Policy**

Nonbanks should establish and maintain policies and procedures for preparing for and managing significant business disruptions, ensuring the ability to maintain critical operations during this time, and swiftly recovering from these events with limited customer disruptions.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal Business Continuity Policy in place.<br>• Limited awareness of business continuity needs.<br>• No clear identification of critical business processes or applications.<br>• IT infrastructure not evaluated for disaster recovery.<br>• No designated responsibility for business continuity.<br>• Lack of training on business continuity procedures.<br>• No Incident Response Team or unclear leadership.<br>• Reactive approach to disasters with no precautionary measures. | The assessor identified:<br><br>• Business Continuity Policy exists with incomplete or outdated elements.<br>• Some critical business processes and applications identified lacking comprehensive coverage.<br>• Limited assessment of IT infrastructure for disaster recovery or other testing.<br>• CISO or equivalent role exists without full authority over business continuity.<br>• Minimal training provided on business continuity procedures.<br>• Ad hoc Incident Response Team with unclear roles.<br>• Some precautionary measures in place lacking systematic approach.<br>• Limited post-incident assessment process. | The assessor identified:<br><br>• Documented Business Continuity Policy covering key areas.<br>• Most critical business processes and applications identified and documented.<br>• IT infrastructure assessed for disaster recovery, with limited plans in place.<br>• CISO, or equivalent oversees Business Continuity Program with clear authority.<br>• Regular training provided on business continuity procedures.<br>• Established Incident Response Team with CISO, or equivalent as leader.<br>• Defined precautionary measures implemented for common scenarios.<br>• Key vendor and partner contacts are logged and are easily accessible.<br>• Initial post-incident assessment process in place. | The assessor identified:<br><br>• Comprehensive Business Continuity Policy aligned with industry standards.<br>• Evidence of all critical business processes and applications thoroughly documented and prioritized.<br>• IT infrastructure disaster recovery plans in place and regularly tested.<br>• Regular, role-specific training on business continuity for all employees.<br>• Well-structured Incident Response Team with defined roles and responsibilities.<br>• Comprehensive precautionary measures covering a wide range of scenarios.<br>• Thorough post-incident assessment process with clear follow-up actions.<br>• No recent history of unreasonably burdensome business continuity issues. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Advanced mapping of business processes, applications, and their interdependencies.<br>• IT infrastructure with real-time replication and failover capabilities.<br>• CISO, or equivalent is a key strategic leader, driving innovation in business continuity practices.<br>• Ongoing, interactive business continuity training integrated into operations.<br>• Highly skilled Incident Response Team with regular drills and scenario planning.<br>• Proactive and adaptive precautionary measures based on emerging threats.<br>• Sophisticated post-incident assessment with analysis and recommendations.<br>• Regular third-party audits of business continuity program effectiveness.<br>• Business continuity considerations embedded in all new business initiatives.<br>• Continuous monitoring and improvement of recovery time objectives (RTOs) and recovery point objectives (RPOs).<br>• Integration of business continuity with overall risk management and business strategy. |

**5.6 Incident Response Team and Action Plans**

Nonbanks should establish and maintain a structured and effective incident response function, with clear procedures, roles, reporting mechanisms, and documented action plans for managing incident recovery and responding to various disruption scenarios.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal Incident Response Team (IRT) in place.<br>• Lack of monitoring for Operational and Enterprise Data Protection (EDP) Disaster and Business Resumption Plans.<br>• No designated leadership for the disaster recovery process.<br>• No regular meetings or reporting structure for incident response.<br>• No clear responsibility for roles, responsibilities, succession planning, or action plan development during disasters.<br>• No documented response plans for various business disruptions (natural disasters, malware attacks, stolen credentials, etc.).<br>• Staff unaware of how to respond to different types of disruptions, with a purely reactive approach to incidents. | The assessor identified:<br><br>• Incident Response Team exists lacking formal structure.<br>• Some monitoring of disaster and business resumption plans without comprehensive coverage.<br>• CISO or equivalent identified as IRT leader with unclear roles and responsibilities.<br>• Irregular IRT meetings with limited documentation.<br>• Minimal reporting to leadership.<br>• Limited succession planning and preparedness for common disaster scenarios.<br>• Initial action plans exist but are generic, incomplete, or outdated with limited consideration of different disruption types.<br>• Some staff have general knowledge of response procedures, but plans are rarely reviewed or updated. | The assessor identified:<br><br>• Incident Response Team with defined membership.<br>• Regular monitoring of Operational and EDP Disaster and Business Resumption Plans.<br>• CISO, or equivalent, leads the IRT with defined responsibilities for disaster recovery.<br>• Annual IRT meetings conducted with limited documentation.<br>• Reporting to leadership occurs annually.<br>• Defined succession plan for IRT leadership with action plans covering major disruption types.<br>• Recognition and specific plans for common disruption scenarios (e.g., natural disasters, malware attacks).<br>• Most staff are aware of response procedures for common disruptions, with plans reviewed and updated periodically. | The assessor identified:<br><br>• Well-structured Incident Response Team with clear roles and responsibilities.<br>• Comprehensive monitoring of all aspects of disaster and business resumption plans.<br>• CISO, or equivalent, effectively leads the IRT with full authority over disaster recovery processes.<br>• Regular IRT meetings (more than annually) with thorough documentation.<br>• Detailed reporting to leadership with actionable insights.<br>• Robust succession plan for IRT leadership with detailed action plans for a wide range of disruption types.<br>• Staff well-trained on scenario-specific response procedures for various disruption types (natural disasters, malware attacks, stolen credentials, etc.).<br>• IRT actively involved in developing and improving comprehensive disaster recovery plans with clear roles, responsibilities, and communication protocols.<br>• No recent history of unreasonable long response or recovery periods following outages or other events. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Highly skilled and adaptive Incident Response Team integrated across the organization.<br>• Continuous, proactive monitoring of disaster and business resumption plans.<br>• CISO, or equivalent is a strategic leader, driving innovation in incident response and disaster recovery.<br>• Frequent IRT meetings with advanced scenario planning, simulations, and drills for all staff.<br>• Real-time reporting capabilities to leadership.<br>• Dynamic succession planning with integrated action plans that leverage AI/predictive analytics to anticipate and refine responses.<br>• Comprehensive coverage of known and potential disaster scenarios with automated incident response systems and detailed, tested responses.<br>• Regular third-party audits of IRT effectiveness and preparedness.<br>• Incident response strategies and action plans fully integrated with overall risk management, business continuity planning, and other business processes.<br>• Culture of preparedness embedded throughout the organization with continuous improvement based on lessons learned and emerging threats. |

**5.7 Business Impact Analysis**

Nonbanks should conduct thorough assessments of potential business disruptions, using appropriate methods to identify critical functions, analyze dependencies, and measure potential impacts.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal business impact analysis conducted.<br>• Lack of identification or prioritization of business functions.<br>• No analysis of interdependencies among business processes and systems.<br>• Absence of established metrics for assessing disruption impact.<br>• No structured risk assessment process in place.<br>• Limited awareness of potential disruptions and their impacts. | The assessor identified:<br><br>• Business impact analysis exists but is lacking sufficient detail or is otherwise incomplete.<br>• Some business functions identified with unclear or inconsistent prioritization.<br>• Limited analysis of interdependencies focusing only on obvious connections.<br>• Rudimentary metrics established for assessing disruption impact without consistent application.<br>• Rudimentary risk assessment process primarily reactive to known issues.<br>• Some awareness of potential disruptions with superficial impact analysis. | The assessor identified:<br><br>• Business impact analysis covering most critical business functions.<br>• Business functions are prioritized, but criteria may need refinement.<br>• Analysis of key interdependencies among major business processes and systems.<br>• Established metrics for assessing disruption impact, consistently applied to major functions.<br>• Structured risk assessment process in place, covering main areas of operation.<br>• Awareness of common potential disruptions with limited impact analysis. | The assessor identified:<br><br>• Complete business impact analysis covering all business functions.<br>• Clear prioritization of business functions based on well-defined criticality criteria.<br>• Thorough analysis of interdependencies across all business processes and systems.<br>• Robust metrics for assessing disruption impact, applied consistently across the organization.<br>• Well-structured risk assessment process, proactively identifying potential disruptions.<br>• In-depth analysis of potential disruptions and their impacts across various scenarios.<br>• Regular review and update of business impact analysis and risk assessment. | The assessor identified:<br><br>• Advanced business impact analysis integrated with overall business strategy.<br>• Dynamic prioritization of business functions, adaptable to changing business environments.<br>• Advanced modeling of interdependencies, including cascading effects and hidden connections.<br>• Metrics established for disruption impact, leveraging real-time data and predictive analytics.<br>• Continuous scenario planning and impact analysis for a wide range of potential disruptions.<br>• Real-time updates to business impact analysis and risk assessment based on internal and external factors.<br>• Integration of risk assessment results into all levels of decision-making.<br>• Regular third-party audits to ensure best-in-class risk management and assessment processes.<br>• Culture of risk awareness embedded throughout the organization. |

**5.8 Continuity Strategies**

Nonbanks should implement appropriate resources, systems, and procedures to maintain operational resilience and ensure business recovery capabilities in the event of disruptions.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal continuity strategies in place.<br>• Lack of defined resilience and recovery objectives.<br>• No guidelines for business continuity.<br>• CISO, or equivalent role undefined or not involved in continuity planning.<br>• Inadequate or non-existent off-site location for software and documentation.<br>• Limited or no data backup procedures.<br>• No off-site infrastructure for recovery systems.<br>• No engagement with third-party service providers regarding disaster scenarios. | The assessor identified:<br><br>• Initial continuity strategies exist but are incomplete.<br>• Limited resilience and recovery objectives.<br>• Limited guidelines for business continuity without evidence of consistent adherence.<br>• CISO or equivalent aware of continuity responsibilities with insufficient authority or resources.<br>• Backup or off-site facilities in place.<br>• Inconsistent data backup procedures.<br>• Limited off-site infrastructure for recovery without full functionality.<br>• Minimal discussion with third-party providers about disaster scenarios. | The assessor identified:<br><br>• Continuity strategies covering key areas.<br>• Defined resilience and recovery objectives for major systems.<br>• Established guidelines for business continuity, generally followed.<br>• CISO, or equivalent involved in continuity planning with some authority.<br>• Functional off-site infrastructure for most critical software and documentation.<br>• Regular data backup procedures in place for key systems.<br>• Off-site infrastructure available for critical recovery systems.<br>• Evidence CISO engages in limited discussions with major third-party providers about disaster scenarios. | The assessor identified:<br><br>• Complete set of continuity strategies aligned with business objectives.<br>• Clear, measurable resilience and recovery objectives for all systems.<br>• Robust guidelines for business continuity, consistently implemented.<br>• CISO, or equivalent, has clear authority and resources for continuity planning.<br>• Well-maintained, comprehensive off-site infrastructure for all software and documentation.<br>• Systematic data backup procedures covering all systems.<br>• Fully functional off-site infrastructure for all recovery systems.<br>• CISO regularly discusses detailed disaster scenarios with all third-party providers.<br>• No recent history of continuity issues across key systems. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Advanced continuity strategies integrated with overall business strategy.<br>• Dynamic, adaptive resilience and recovery objectives that evolve with the business.<br>• CISO, or equivalent is a key strategic leader in continuity planning and disaster preparedness.<br>• Innovative off-site infrastructure with real-time updates and version control.<br>• Automated, continuous data backup with multiple redundancies.<br>• Advanced off-site infrastructure with instant failover capabilities.<br>• CISO leads collaborative scenario planning with third-party providers, including joint drills.<br>• Use of AI/predictive analytics to anticipate and mitigate potential disruptions.<br>• Regular testing and optimization of all continuity strategies.<br>• Continuity strategies seamlessly integrated with risk management and incident response.<br>• Culture of resilience embedded throughout the organization.<br>• Regular third-party audits to ensure best-in-class continuity practices. |

**5.9 Business Continuity/Disaster Recovery Training**

Nonbanks should develop and implement comprehensive training programs that prepare personnel at all levels to effectively execute their business continuity and disaster recovery responsibilities.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Training, if any, is ad-hoc and inconsistent.<br>• No formal business continuity training program materials in place.<br>• No formal training attendance tracking in place.<br>• Lack of training has created limited awareness of BCP/DR responsibilities across the organization.<br>• Unclear collaboration between HR and BCP/DR team for new hire training. | The assessor identified:<br><br>• BCP/DR training exists but is not sufficiently tailored or comprehensive.<br>• Training covers fundamental BCP/DR concepts.<br>• Annual training occurs but doesn't cover all appropriate employees or isn't updated in a timely manner.<br>• Limited coordination between HR and BCP/DR team for training, including delays in training new employees.<br>• Content is not sufficiently tailored to the company's needs. | The assessor identified:<br><br>• BCP/DR training provided to new employees at or shortly after hiring.<br>• Annual training exercises conducted for all employees in the company.<br>• HR and BCP/DR collaborate to provide adequate training including coordination with any external training providers if used.<br>• Training content covers essential BCP/DR topics.<br>• Rudimentary tracking of training completion.<br>• Includes assessments or quizzes. | The assessor identified:<br><br>• Detailed BCP/DR training program for new hires and ongoing annual training.<br>• Training content tailored to different roles and risk levels within the organization.<br>• Strong collaboration between HR and BCP/DR team to develop and deliver training, including coordination with any training vendor utilized.<br>• Detailed information on disaster preparedness policies readily accessible.<br>• Regular, scenario-based training exercises conducted.<br>• Regular review and update of training materials by subject matter experts to reflect regulatory changes and emerging risks.<br>• System for tracking and reporting on training completion.<br>• Assessment of training effectiveness through tests or practical application.<br>• History of content adjustments based on knowledge gaps and performance. | The assessor identified:<br><br>• Advanced BCP/DR training program, confirmed by a third-party audit.<br>• Personalized training paths based on employee roles, experience, and past performance.<br>• Continuous learning approach with regular updates and refresher modules throughout the year.<br>• Advanced collaboration between HR, BCP/DR team, and business units to ensure training relevance, including coordination with training vendor if used.<br>• Use of multiple training methods (e.g., e-learning, workshops, case studies, certifications) to enhance engagement and retention.<br>• Regular independent review of training program effectiveness.<br>• Integration of training performance into employee evaluations and risk management processes.<br>• Proactive adaptation of training to address emerging risks and regulatory changes. |

**5.10 Disaster Exercises and Tests**

Nonbanks should regularly validate their business continuity procedures through appropriate exercises and tests, ensuring recovery capabilities are effective and operational.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal disaster exercises or tests conducted.<br>• Lack of Board and leadership involvement in business continuity validation.<br>• No verification that business continuity procedures support objectives.<br>• Absence of any type of exercise (Full-Scale, Limited-Scale, or Tabletop).<br>• No consideration of company size or maturity in approach to testing.<br>• Business Continuity Plan not validated through exercises or tests.<br>• No documentation of exercise results or lessons learned. | The assessor identified:<br><br>• Occasional, unstructured disaster exercises or tests.<br>• Minimal Board and leadership involvement in continuity validation.<br>• Limited verification of business continuity procedures' effectiveness.<br>• Infrequent Tabletop Exercises (walkthroughs) conducted, if any.<br>• Limited consideration of company size and maturity, but not reflected in the testing approach.<br>• Partial validation of the Business Continuity Plan through initial exercises.<br>• Minimal documentation of exercise results with no formal follow-up. | The assessor identified:<br><br>• Regular Tabletop Exercises conducted, with some Limited-Scale Exercises.<br>• The Board and leadership provide limited oversight of continuity validation.<br>• Some verification that procedures support business continuity objectives.<br>• Exercises used to validate key aspects of the Business Continuity Plan.<br>• Testing approach generally aligned with company size and maturity.<br>• Documentation of exercise results with some follow-up actions.<br>• Annual review of exercise effectiveness by leadership. | The assessor identified:<br><br>• Program with a mix of exercises including Tabletop, Limited-Scale, and some Full-Scale Exercises.<br>• Active Board and leadership involvement in planning and reviewing exercises.<br>• Thorough verification that procedures support business continuity objectives.<br>• Exercises systematically validate all major aspects of the Business Continuity Plan.<br>• Testing approach well-tailored to company size and maturity.<br>• Detailed documentation of all exercises with formal follow-up and improvement processes.<br>• Regular reporting to the Board on exercise results and Business Continuity Plan effectiveness. | The assessor identified:<br><br>• Complete program with a mix of Tabletop, Limited-Scale, and Full-Scale Exercises.<br>• The Board and leadership champion and actively participate in continuity exercises.<br>• Continuous validation and improvement of business continuity procedures.<br>• Exercises rigorously test and validate all aspects of the Business Continuity Plan.<br>• Dynamic testing approach that evolves with company growth and maturity.<br>• Advanced documentation and analysis of exercise results using data analytics.<br>• Real-time adjustments to the Business Continuity Plan based on exercise outcomes.<br>• Use of advanced technologies (e.g., AI, VR) to enhance exercise realism and effectiveness.<br>• Cross-functional and cross-departmental involvement in all levels of exercises.<br>• Inclusion of external stakeholders (e.g., key vendors, regulators) in appropriate exercises.<br>• Continuous learning culture with immediate integration of lessons learned.<br>• Third-party audits of exercise program effectiveness.<br>• Exercises simulate complex, multi-faceted disaster scenarios.<br>• Integration of exercise outcomes into overall risk management and strategic planning. |

**5.11 Wind Down Plan**

Nonbanks should develop and maintain plans for potential cessation of regulated activities, ensuring compliance with relevant requirements and protection of customer interests during wind-down.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal wind-down plan in place.<br>• Limited awareness of regulatory requirements for business cessation.<br>• No clear strategy for handling customer assets during wind-down.<br>• Lack of consideration for permissible activities and regulatory obligations.<br>• No plan for vendor relationships management.<br>• High risk of disorderly wind-down and regulatory non-compliance. | The assessor identified:<br><br>• A wind-down plan exists, lacking comprehensiveness.<br>• Some awareness of regulatory requirements with gaps in understanding.<br>• General idea of customer asset handling without detailed procedures.<br>• Limited consideration of permissible activities and regulatory obligations.<br>• Initial plan for vendor relationships management.<br>• Minimal consideration of vendor relationships during wind-down. | The assessor identified:<br><br>• Documented wind-down plan covering key areas.<br>• Understanding of major regulatory requirements for business cessation.<br>• Procedures in place for handling customer assets during wind-down.<br>• Consideration of permissible investments and major regulatory obligations.<br>• Defined process for vendor relationships management.<br>• Initial categorization of critical and non-critical vendors. | The assessor identified:<br><br>• Comprehensive wind-down plan aligned with regulatory requirements.<br>• Clear understanding and incorporation of all applicable laws and regulations.<br>• Well-defined DRI roles with clear responsibilities and decision-making authority.<br>• Detailed procedures for protecting and returning customer assets.<br>• Robust management of permissible investments throughout the wind-down process.<br>• Strategic approach to vendor relationship management during wind-down.<br>• Regular review and updates of the wind-down plan, coupled with analysis of financial position, runway, and financing strategies. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Comprehensive wind-down plan integrated with overall business strategy.<br>• Proactive alignment with evolving regulatory landscapes.<br>• DRIs are key strategic leaders with full authority and resources.<br>• Advanced systems for immediate return of customer assets.<br>• Continuous testing and refinement of wind-down procedures.<br>• Integration with risk management and business continuity planning.<br>• Regular third-party audits of wind-down plan effectiveness.<br>• Complete view of runway, likelihood of wind-down, and plans for managing associated tasks.<br>• No history of failing to maintain a complete financial picture or an adequate financial runway. |

**5.12 Account Reconciliation**

Nonbanks should implement effective systems and procedures for managing custodial account records, ensuring accurate recordkeeping, appropriate access, and compliance with partner bank requirements.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No comprehensive recordkeeping system for custodial accounts.<br>• Incomplete or inconsistent records of individual account owners.<br>• Reconciliations performed sporadically, not daily.<br>• Limited or no access provided to bank partner(s) for records.<br>• No specific data formatting system for bank partner(s) requirements.<br>• Lack of alignment with FDIC data formatting requirements.<br>• No clear internal controls for determining beneficial ownership.<br>• Absence of continuity plans for disruption scenarios.<br>• Vague or non-existent contractual agreements with bank partner(s) regarding recordkeeping.<br>• No independent validations of records and processes. | The assessor identified:<br><br>• Rudimentary recordkeeping system is in place, though not comprehensive.<br>• Records of individual account owners exist, yet may be incomplete.<br>• Reconciliations are performed regularly, rather than daily.<br>• Limited access is provided to bank partner(s) for records, as applicable.<br>• Simple data formatting system exists, though not fully aligned with bank partner(s) requirements.<br>• There is partial alignment with FDIC data formatting requirements.<br>• internal controls exist for determining beneficial ownership.<br>• Initial continuity plans are established, though not comprehensive.<br>• Records and processes undergo occasional, ad-hoc validations. | The assessor identified:<br><br>• Functional recordkeeping system covering most custodial accounts.<br>• Detailed records of individual account owners maintained for most accounts.<br>• Daily reconciliations performed for the majority of accounts.<br>• Bank partner(s) have access to most records, but may not be continuous.<br>• Data formatting system largely aligns with bank partner(s) requirements.<br>• Substantial alignment with FDIC data formatting requirements.<br>• Established internal controls for determining beneficial ownership.<br>• Continuity plans cover main disruption scenarios.<br>• Clear contractual agreements with bank partner(s), defining essential roles and responsibilities.<br>• Regular independent validations of records and processes, with some results shared. | The assessor identified:<br><br>• Comprehensive recordkeeping system for all custodial accounts.<br>• Detailed, accurate records of all individual account owners.<br>• Daily reconciliations performed consistently for all accounts.<br>• Bank partner(s) have direct, continuous access to most records.<br>• Data formatting system fully aligns with bank partner(s) requirements.<br>• Complete alignment with FDIC data formatting requirements.<br>• Robust internal controls for determining beneficial ownership.<br>• Comprehensive continuity plans for various disruption scenarios.<br>• Detailed contractual agreements with bank partner(s), clearly defining all roles and responsibilities.<br>• Regular, thorough independent validations, with results consistently shared with bank partner(s).<br>• No recent history of material account reconciliation issues. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Comprehensive, fully automated recordkeeping system for all custodial accounts.<br>• Real-time, highly detailed records of all individual account owners.<br>• Continuous, automated reconciliations with instant error detection and correction.<br>• Bank partner(s) have direct, continuous, and unrestricted access to all records through secure, redundant systems.<br>• Proactive alignment with evolving FDIC data formatting requirements.<br>• Collaborative, technology-enabled contractual agreements with bank partner(s), allowing real-time updates and transparency.<br>• Continuous, independent validations using advanced analytics, with real-time reporting to bank partner(s).<br>• Machine learning algorithms employed to predict and prevent reconciliation issues.<br>• Regular third-party audits to ensure best-in-class recordkeeping and reconciliation practices.<br>• Integration with broader risk management and compliance systems. |

# 6. Marketing and Product Compliance

**6.1 Marketing Policy**

Nonbanks should establish and maintain a comprehensive marketing policy that ensures compliance with applicable regulations and provides clear oversight for managing marketing practices across channels.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal marketing policy exists.<br>• Marketing practices are inconsistent and not reviewed for compliance.<br>• No designated responsibility for marketing reviews prior to distribution.<br>• No awareness of regulatory requirements for financial service marketing (e.g., UDAAP, FCRA, CAN-SPAM, TCPA).<br>• No process for reviewing or approving marketing materials. | The assessor identified:<br><br>• Initial marketing policy exists with incomplete or outdated elements.<br>• Some awareness of regulatory requirements with inconsistent application.<br>• Limited oversight of marketing materials for compliance.<br>• Reactive approach to addressing compliance issues in marketing.<br>• Minimal training on compliant marketing practices.<br>• Some institutional understanding of some key regulations (e.g., UDAAP) alongside gaps in knowledge of others.<br>• Limited evidence of reviewing marketing materials prior to distribution. | The assessor identified:<br><br>• Documented marketing policy covering key regulatory requirements.<br>• Process in place for reviewing and approving marketing materials.<br>• Defined responsibility for marketing compliance oversight.<br>• Regular review of marketing materials for compliance.<br>• Some collaboration between compliance and marketing departments.<br>• Fundamental training provided on compliant marketing practices.<br>• Awareness of major regulations (UDAAP, FCRA, CAN-SPAM, TCPA) and attempts to comply.<br>• Some consideration of social media and third-party marketing.<br>• Board-approved policy with defined review cycles. | The assessor identified:<br><br>• Comprehensive marketing policy aligned with all relevant regulations.<br>• Clear ownership and accountability for marketing compliance.<br>• Formal review and approval process for all marketing materials.<br>• Regular training on marketing compliance for all relevant staff.<br>• Proactive monitoring of regulatory changes affecting marketing practices.<br>• Metrics tracked on marketing compliance complaints.<br>• Detailed procedures for different marketing channels (email, social media, telemarketing).<br>• Documented process for handling customer complaints related to marketing.<br>• Clear guidelines for endorsements and testimonials.<br>• Evidence that the marketing compliance program is regularly reviewed and updated.<br>• No recent history of marketing distribution prior to receiving all required pre-approvals. | The assessor identified:<br><br>• Fully integrated marketing compliance program aligned with business strategy.<br>• Automated workflows for review and approval of marketing materials.<br>• Real-time compliance checking tools integrated into marketing processes.<br>• Advanced analytics used to predict and prevent potential compliance issues.<br>• Continuous improvement based on performance metrics and industry benchmarks.<br>• Regular audits and third-party assessments of marketing compliance program.<br>• Comprehensive training program with role-specific modules.<br>• Detailed archiving and documentation practices for all marketing materials.<br>• Robust process for monitoring and managing third-party marketing activities.<br>• Integration with overall risk management and compliance frameworks. |

**6.2 Marketing Compliance Review and Approval Process**

Nonbanks should implement a structured process for the internal review and approval of all marketing materials to ensure regulatory compliance before distribution to customers. When applicable, nonbanks should also establish a formal process for obtaining and documenting bank partner approvals for marketing materials in accordance with partner requirements and contractual obligations.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal review process for marketing materials.<br>• Compliance review occurs sporadically, if at all.<br>• No designated responsibility for compliance review.<br>• Marketing materials are often published without compliance input.<br>• High risk of non-compliant materials being distributed.<br>• No documentation of the review process or decisions.<br>• No awareness of bank partner's requirements for marketing materials review (as applicable).<br>• No process for escalating materials to bank partner(s) for review (as applicable). | The assessor identified:<br><br>• Review process exists with inconsistent application.<br>• Some awareness of the need for compliance review without formal procedures.<br>• Limited collaboration between marketing and compliance teams.<br>• Some marketing materials may still be published without proper review.<br>• Minimal documentation of the review process.<br>• Limited awareness of the need for a bank partner(s) review with incomplete understanding of requirements (as applicable).<br>• Inconsistent process for escalating materials to bank partner(s) (as applicable). | The assessor identified:<br><br>• Documented review process for customer-facing marketing materials.<br>• Designated responsibility for compliance review, typically Head of Compliance or other appropriately designated personnel/Marketing Compliance.<br>• Most marketing materials undergo compliance review before publication.<br>• Some collaboration between marketing and compliance teams.<br>• Rudimentary framework established for managing compliance requirements.<br>• Process documentation exists, but may lack detail.<br>• Bank partner's requirements for marketing materials review are identified (as applicable).<br>• Process established for escalating materials to bank partner(s) and documenting review outcomes (as applicable).<br>• Procedures updated annually or when significant changes occur. | The assessor identified:<br><br>• Comprehensive review process covering all customer-facing marketing materials.<br>• Clear ownership and accountability for compliance review.<br>• Structured back-and-forth between marketing and compliance teams.<br>• Goal-oriented process aimed at producing effective and compliant materials.<br>• Regular updating of review framework to reflect changing regulations.<br>• Detailed documentation of the review process and decisions.<br>• Metrics tracked on review process efficiency and effectiveness.<br>• No recent history of material complaint volume related to deceptive marketing or campaigns.<br>• Comprehensive understanding of bank partner's review requirements and criteria (as applicable).<br>• Regular communication with bank partner(s) about the review process and metrics tracked on review outcomes (as applicable). | The assessor identified:<br><br>• Fully integrated and automated review process.<br>• Proactive collaboration between marketing and compliance teams.<br>• Real-time compliance checking tools integrated into marketing workflows.<br>• Continuous improvement of the review process based on metrics and feedback.<br>• Advanced analytics used to predict potential compliance issues.<br>• Comprehensive training for both marketing and compliance teams on the process.<br>• Regular audits of the review process to ensure effectiveness.<br>• Integration with overall risk management and compliance frameworks.<br>• Ability to quickly adapt processes for new marketing channels or regulatory changes.<br>• Proactive engagement with bank partner(s) with automated systems for review escalation (as applicable).<br>• Integration of bank partner's review criteria into internal processes with advanced tracking and continuous improvement based on feedback (as applicable). |

**6.3 Regulatory Change Management**

Nonbanks should maintain a system for monitoring and responding to regulatory changes affecting their product and/or operations.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal process for monitoring regulatory changes.<br>• Unaware of regulatory updates affecting products, services, or operations.<br>• Existing products not reviewed for compliance with new regulations.<br>• No designated responsibility for regulatory change management<br>• High risk of non-compliance due to outdated products and processes.<br>• No system for updating products, services, or documentation based on regulatory changes. | The assessor identified:<br><br>• Awareness of the need to monitor regulatory changes that affect products.<br>• Sporadic checks for regulatory updates without systematic approach.<br>• Some attempt to review existing products when major regulatory changes occur.<br>• Limited understanding of how regulatory changes impact products.<br>• Informal responsibility assignment for monitoring regulatory changes. | The assessor identified:<br><br>• Regular monitoring of regulatory changes affecting all product aspects.<br>• Head of Compliance or other designated personnel assigned responsibility for identifying regulatory updates.<br>• Process in place to review existing products when regulatory changes occur.<br>• System for tracking regulatory changes and their potential impact across the organization.<br>• Evidence of proactive updating of products, services, and documentation based on regulatory changes.<br>• Documentation of regulatory change management process. | The assessor identified:<br><br>• Comprehensive system for monitoring regulatory changes.<br>• Process for assessing impact of regulatory changes on existing products and services.<br>• Regular, scheduled reviews of all products for regulatory compliance.<br>• Metrics tracked on identification and implementation of necessary changes.<br>• Cross-functional team involved in addressing regulatory changes.<br>• Proactive approach to updating products before regulatory changes take effect. | The assessor identified:<br><br>• Advanced regulatory intelligence system providing real-time updates.<br>• Automated impact assessment of regulatory changes on existing product portfolio.<br>• Predictive analytics used to anticipate potential regulatory changes.<br>• Integration of regulatory updates into the product development and review process.<br>• Continuous monitoring and immediate flagging of non-compliant products or features.<br>• Agile process for quickly updating products, services, and documentation across all channels.<br>• Comprehensive training program on regulatory change management.<br>• Integration with overall risk management and compliance frameworks. |

**6.4 Truth in Savings Compliance**

Nonbanks should maintain compliance with Truth in Savings Act (TISA), implemented by Regulation DD through a number of controls related to ensuring accurate deposit account terms, rates, and fees.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Minimal awareness of Truth in Savings Act (TISA) and Regulation DD requirements.<br>• No formal TISA policy or inconsistent implementation.<br>• Account disclosures missing key terms, fees, or APY information.<br>• Inaccurate or misleading disclosures regarding deposit account features.<br>• No process for updating disclosures when terms change.<br>• Advertising lacks required TISA disclosures or contains prohibited terminology.<br>• No designated responsibility for TISA compliance oversight. | The assessor identified:<br><br>• TISA policy exists but implementation is inconsistent.<br>• Account disclosures cover minimum regulatory requirements but lack detail.<br>• Some standard APY calculations but inconsistent application.<br>• Limited process for ensuring advertising includes required disclosures.<br>• Evidence of notifications to customers when account terms change, but not consistently within required timeframes.<br>• Limited coordination between product, marketing, and compliance teams.<br>• Minimal training for staff on TISA requirements. | The assessor identified:<br><br>• Comprehensive TISA policy with detailed procedures for disclosures and advertising.<br>• Complete account disclosures with accurate information on fees, terms, and APY.<br>• Standardized APY calculation methodology consistently applied.<br>• Process for timely notification to customers at least 30 days before adverse changes take effect.<br>• Marketing materials reviewed for TISA compliance before publication.<br>• Prohibition on using terms like "free" or "no cost" for accounts with maintenance or activity fees.<br>• Regular training for staff on TISA requirements.<br>• Evidence of coordination between product, marketing, and compliance teams. | The assessor identified:<br><br>• Robust TISA compliance program integrated with product development and marketing processes.<br>• Detailed and consumer-friendly account disclosures that exceed regulatory requirements.<br>• Automated APY calculations with quality control checks.<br>• Proactive monitoring of deposit terms and timely customer notifications of changes.<br>• Comprehensive review process for all marketing materials with TISA-specific checklists.<br>• Clear processes for time account maturity notices and disclosure updates.<br>• Advanced training for relevant staff customized by role.<br>• Regular auditing of TISA compliance with documented improvements.<br>• No recent history of TISA-related compliance issues. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Integration of TISA compliance into the earliest product design phase with compliance participation.<br>• Sophisticated tracking of disclosure delivery and customer acknowledgment.<br>• Systems that automatically trigger notices of term changes and maturity dates.<br>• Advanced monitoring of competitor practices to benchmark disclosure quality.<br>• Regular independent review of TISA program effectiveness.<br>• Continuous improvement of disclosure language based on customer feedback and comprehension testing.<br>• Leadership regularly updated on TISA compliance metrics and program enhancements.<br>• Proactive adaptation to regulatory changes and emerging best practices. |

**6.5 E-Sign Compliance**

Nonbanks should maintain compliance with the E-Sign Act by implementing processes for consent, delivery, and record retention.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal E-Sign policy or inconsistent implementation.<br>• Limited awareness of E-Sign Act requirements.<br>• Inadequate disclosure of hardware/software requirements.<br>• No clear process for customers to withdraw consent for electronic records.<br>• Inconsistent records of customer consent for electronic delivery.<br>• Limited capability to provide paper copies upon request.<br>• No designated responsibility for E-Sign compliance oversight. | The assessor identified:<br><br>• E-Sign policy exists but implementation is inconsistent.<br>• Some standardized consent collection for electronic delivery.<br>• Limited disclosure of hardware/software requirements for accessing electronic records.<br>• Process for customers to request paper copies.<br>• Minimal tracking of customers who have consented to electronic delivery.<br>• Limited or inconsistent retention of electronic consent records.<br>• Some designated responsibility for E-Sign compliance but limited oversight. | The assessor identified:<br><br>• Comprehensive E-Sign policy with detailed procedures.<br>• Clear disclosures of hardware/software requirements before consent.<br>• Standardized process for collecting and documenting electronic consent.<br>• Established process for customers to withdraw consent or request paper copies.<br>• Consistent retention of electronic consent records.<br>• Regular monitoring of electronic delivery processes.<br>• Clear responsibilities assigned for E-Sign compliance oversight.<br>• Evidence of coordination between technology and compliance teams. | The assessor identified:<br><br>• Robust E-Sign compliance program integrated with document management systems.<br>• Detailed and easily understandable hardware/software requirement disclosures.<br>• Technology that confirms customer ability to access electronic records.<br>• User-friendly mechanisms for consent withdrawal and paper copy requests.<br>• Advanced tracking of electronic consent status across all customer touchpoints.<br>• Regular auditing of E-Sign compliance with documented improvements.<br>• No recent history of E-Sign related compliance issues.<br>• Processes designed to accommodate customers with diverse technological capabilities. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Advanced E-Sign platform with real-time verification of customer access capabilities.<br>• Sophisticated consent tracking that integrates with all customer systems.<br>• Proactive monitoring of customer electronic access patterns to identify potential issues.<br>• Regular independent review of E-Sign program effectiveness.<br>• Continuous improvement based on customer feedback and technological developments.<br>• Leadership regularly updated on E-Sign compliance metrics and program enhancements.<br>• Integration with broader digital experience and accessibility initiatives. |

### 6.6 Accessibility

Nonbanks should maintain compliance with the Americans with Disabilities Act (ADA) by applying controls to ensure deposit account interfaces and services are accessible to persons with disabilities.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal ADA policy for digital banking services.<br>• Limited awareness of accessibility requirements for deposit accounts.<br>• Digital interfaces not designed with accessibility considerations.<br>• No testing for accessibility compliance.<br>• No alternative access methods for persons with disabilities.<br>• No designated responsibility for accessibility oversight.<br>• No process for addressing accessibility-related complaints. | The assessor identified:<br><br>• Accessibility policy exists but implementation is inconsistent.<br>• Some awareness of ADA requirements for digital banking.<br>• Limited evidence of testing of digital interfaces for accessibility.<br>• Minimal alternative access methods available but not well communicated.<br>• Initial process for handling accessibility complaints but not comprehensive.<br>• Limited training for staff on accessibility requirements.<br>• Some designated responsibility for accessibility but limited oversight. | The assessor identified:<br><br>• Comprehensive accessibility policy with detailed procedures.<br>• Digital interfaces designed with accessibility features.<br>• Evidence of regular testing for compliance with WCAG standards for all new and recently edited screens or websites.<br>• Alternative access methods clearly communicated to customers.<br>• Established process for addressing accessibility complaints.<br>• Regular training for relevant staff on accessibility requirements.<br>• Clear responsibilities assigned for accessibility oversight.<br>• Evidence of coordination between product, technology, and compliance teams. | The assessor identified:<br><br>• Robust accessibility program integrated with product development and customer experience design.<br>• Digital interfaces designed for optimal accessibility, meeting or exceeding WCAG standards.<br>• Comprehensive testing protocols including automated and manual accessibility testing.<br>• Multiple alternative access methods tailored to different disability types.<br>• Regular auditing of accessibility compliance with documented improvements.<br>• No recent history of ADA-related complaints or issues.<br>• Processes for quickly implementing accessibility enhancements.<br>• Clear authority delegated to qualified personnel for accessibility program oversight. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Innovative approaches to digital accessibility that exceed regulatory requirements.<br>• Integration of accessibility considerations into earliest product design phases.<br>• Engagement with disability advocacy groups for feedback and testing.<br>• Advanced technologies employed to enhance accessibility features.<br>• Regular independent review of accessibility program effectiveness.<br>• Continuous improvement based on user feedback and evolving standards.<br>• Leadership regularly updated on accessibility metrics and program enhancements.<br>• Proactive monitoring of emerging technologies and techniques for improving accessibility. |

### 6.7 FDIC Insurance Disclosure

Nonbanks should maintain compliance with FDIC insurance disclosure standards by frequently reviewing the accuracy of claims and disclosures.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• Inconsistent or inaccurate representations of FDIC coverage.<br>• Limited awareness of FDIC disclosure requirements.<br>• No clear delineation between insured and non-insured products.<br>• Missing or inadequate FDIC disclosures in marketing materials.<br>• No process for reviewing FDIC-related statements.<br>• No designated responsibility for FDIC disclosure oversight. | The assessor identified:<br><br>• Some standardized language for FDIC insurance statements.<br>• Limited distinction between insured and non-insured products in marketing.<br>• Limited review process for FDIC references, but not comprehensive.<br>• Minimal training on FDIC insurance coverage and disclosure requirements.<br>• No unlawful use of FDIC logo and statement usage.<br>• Some designated responsibility for FDIC disclosure compliance but limited oversight. | The assessor identified:<br><br>• Clear, accurate statements about FDIC insurance coverage across all channels.<br>• Consistent disclosures including bank partner(s) information and coverage limits.<br>• Established review process for all FDIC-related statements and logos.<br>• Clear distinction between insured and non-insured products.<br>• Regular training for relevant staff on FDIC disclosure requirements.<br>• Monitoring of marketing materials for accurate FDIC representations.<br>• Clear responsibilities assigned for FDIC disclosure oversight.<br>• Evidence of coordination between marketing and compliance teams. | The assessor identified:<br><br>• FDIC disclosure program integrated with product development and marketing processes.<br>• Consumer-friendly explanations of FDIC coverage that maintain accuracy.<br>• Clear visual distinction between insured and non-insured products in all materials.<br>• Comprehensive review process with FDIC-specific checklists for all customer-facing content.<br>• Advanced training customized by role with regular updates.<br>• Regular auditing of FDIC disclosure compliance with documented improvements.<br>• No recent history of FDIC disclosure-related compliance issues. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Integration of FDIC disclosure considerations into earliest product design phases.<br>• Advanced monitoring of compliance with bank partner(s)' FDIC disclosure requirements.<br>• Regular independent review of FDIC disclosure effectiveness.<br>• Continuous improvement based on customer feedback and regulatory developments.<br>• Processes to quickly incorporate FDIC rule changes into disclosures.<br>• Clear authority delegated to qualified personnel for FDIC disclosure oversight. |

**6.8 Dormant Account Management**

Nonbanks should maintain a process for managing inactive and dormant accounts to align with AML standards, fraud risk strategies, and state unclaimed property laws, among others.

| 5. Rudimentary | 4. Documented | 3. Integrated | 2. Strategic | 1. Optimized |
|---|---|---|---|---|
| The assessor identified:<br><br>• No formal policy for dormant account management.<br>• Limited awareness of applicability to AML, Fraud, and state unclaimed property laws.<br>• No systematic tracking of account inactivity.<br>• Inconsistent or absent customer notifications about dormant status.<br>• No clear process for escheatment of abandoned accounts.<br>• No designated responsibility for dormant account oversight.<br>• Limited record-keeping of escheatment activities. | The assessor identified:<br><br>• Dormant account policy exists but implementation is inconsistent.<br>• Some awareness of applicability to AML, Fraud, and state unclaimed property laws.<br>• Limited tracking of account inactivity periods.<br>• Limited customer notifications about dormant status but not comprehensive.<br>• Simple escheatment process but not fully aligned with all state requirements.<br>• Minimal record-keeping of escheatment activities.<br>• Some designated responsibility for dormant account management but limited oversight. | The assessor identified:<br><br>• Comprehensive dormant account policy with detailed procedures.<br>• Clear understanding of applicability to AML, Fraud, and state unclaimed property laws.<br>• Systematic tracking of account inactivity periods.<br>• Systematic tracking of dormant account reactivation to limit fraud and AML exposure.<br>• Regular customer notifications at key intervals before escheatment.<br>• Established procedures for escheatment that comply with state requirements.<br>• Consistent record-keeping of all dormant account and escheatment activities.<br>• Clear responsibilities assigned for dormant account management.<br>• Evidence of coordination between operations, customer service, and compliance teams. | The assessor identified:<br><br>• Robust dormant account program integrated with account management systems.<br>• Sophisticated tracking of account activity that identifies potential dormancy before official status.<br>• Proactive account closing processes to limit Fraud and AML issues related to dormant accounts.<br>• Proactive customer engagement strategies to prevent dormancy.<br>• Comprehensive notification process with multiple contact methods.<br>• Advanced procedures for multi-state escheatment compliance.<br>• Detailed record-keeping and reporting of all dormant account activities.<br>• Regular auditing of dormant account management with documented improvements.<br>• No large dormant account customer base. | In addition to the criteria identified in 2. Strategic, the assessor identified:<br><br>• Advanced analytics to identify patterns of inactivity and trigger early interventions.<br>• Sophisticated customer outreach strategies with high reactivation success rates.<br>• Automated systems for tracking dormancy across multiple jurisdictions.<br>• Regular independent review of dormant account program effectiveness.<br>• Continuous improvement based on performance metrics and regulatory developments.<br>• Leadership regularly updated on dormancy metrics and program enhancements.<br>• Proactive monitoring of legislative changes affecting escheatment requirements.<br>• Integration with broader customer retention and relationship management initiatives. |

**Appendix C: Standard-Setting Models Analysis**

CFES identified three potential models for digital asset standard-setting, each with distinct advantages and limitations:

**Option 1: Government-Mandated Self-Regulatory Organization**

Similar to the Public Company Accounting Oversight Board (PCAOB) or the Financial Industry Regulatory Authority (FINRA), this model would establish a government-created entity with statutory authority to develop and enforce standards. These organizations have mandatory membership requirements and clear enforcement powers—FINRA, for example, requires all broker-dealers to be members and has disciplinary authority over them. While providing clear regulatory backing and enforcement power, this approach may lack the technical expertise and agility necessary for rapidly evolving digital asset markets. The formal federal rulemaking process could also slow adaptation to technological changes.

**Option 2: Voluntary Membership Organization**

Following models like The Clearing House, this approach would create a voluntary membership organization that develops industry standards and best practices. The Clearing House, owned by major banks, develops payment system standards, operational procedures, and risk management frameworks that members can choose to adopt. This model offers industry expertise and flexibility but faces significant limitations in scope and adoption. The voluntary nature may create competitive disadvantages for compliant participants and limit comprehensive market coverage, particularly in emerging sectors where participation incentives remain unclear.

**Option 3: Industry-Led Hybrid Standard-Setting Organization**

This model represents a middle path that combines industry expertise with regulatory oversight. Under this approach, industry participants would fund and develop standards outside the federal rulemaking process, enabling faster adaptation to technological changes. Critically, the enforcement mechanism would remain with government regulators through existing supervisory frameworks, similar to how banking examiners incorporate industry best practices into examination processes.