SERVICENOW, COMBIZ ABDOLRAHIMI

Proposal and Comment Information

Title: Anti-Money Laundering and Countering the Financing of Terrorism Programs, R-1835

Comment ID: FR-0000-0133-02-C39

Submitter Information

Organization Name: ServiceNow

Organization Type: Company

Name: Combiz Abdolrahimi

Submitted Date: 09/08/2026

The Proposal's core operational demands—codified risk assessment processes, risk-based resource allocation, the establish-and-maintain two-prong effectiveness framework, and the new supervision and enforcement policy—collectively require banks to move beyond static, document-centric compliance programs toward dynamic, data-driven, continuously monitored AML/CFT operations. Our key observations are:

- The two-prong effectiveness framework is clarifying, but examination practice must match the regulatory design. Defining effectiveness as establishing a reasonably designed, risk-based program and maintaining it by implementing that program in all material respects is clearer than a static checklist of pillars. However, banks need certainty that effectiveness will be demonstrated by the strength of design artifacts and implementation evidence—including system-generated audit trails, testing results, resource-allocation analytics, and remediation records—not solely by a narrative program document.
- Codified risk assessment processes require integrated, auditable data architecture. Operationalizing the Proposal's risk assessment requirements at scale demands unified data platforms that aggregate risk signals from across products, services, distribution channels, customers, and geographies—with full audit trail lineage. Workflow orchestration enables banks to connect siloed risk data sources into continuous, traceable processes rather than static annual documents.
- The establish-and-maintain distinction must be preserved at the element level, not only the program level. Without a clear program-versus-element distinction, examiners may treat every component-level finding as a program-establishment failure, collapsing the Proposal's two-prong structure. Integrated program-management systems help by showing, component by component, whether an element exists (establishment) and whether it is operating (maintenance).
- The supervision and enforcement framework needs principled definitions of "significant or systemic failure" and "failure to establish." Banks need to understand the threshold that separates an implementation gap—which the Proposal correctly tolerates if not significant or systemic—from a deficiency that triggers enforcement. The standard should focus on unremediated, material breakdowns, not on the existence of findings.
- Risk-based resource allocation requires dynamic monitoring and scenario analysis. The Proposal's requirement that banks direct more attention and resources toward higher-risk customers and activities requires continuous calibration through technology infrastructure, not static allocation plans.
- The Board's encouragement of innovation should be accompanied by governance guidance. Banks will benefit from Board guidance on how AI-driven analytics, automated transaction monitoring, and workflow automation will be evaluated during examination, particularly regarding model governance, explainability, and auditability.

We elaborate on each below, organized by the Board's specific questions.

servicenow

ServiceNow
www.servicenow.com

2225 Lawson Lane
Santa Clara, CA 95054

Tel +1 (408) 501-8550
Fax +1 (408) 501-8550

ServiceNow, Inc.

September 8, 2026

Mr. Benjamin W. McDonough
Secretary
Board of Governors
The Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, D.C. 20551

Re: Docket No. R–1835 | RIN 7100–AG78 | Anti-Money Laundering and Countering the Financing of Terrorism Programs

Dear Mr. McDonough:

ServiceNow, Inc. ("ServiceNow") respectfully submits these comments in response to the Board of Governors of the Federal Reserve System's ("the Board") proposed rule to amend AML/CFT program requirements for Board-supervised banks under 12 CFR 208.63 (the "Proposal"). The comment period closes September 8, 2026.

ServiceNow is an enterprise AI platform company whose technology is deployed across major financial institutions and regulated entities worldwide to orchestrate workflows, automate processes, manage risk and compliance, and enable cross-functional operational coordination. Our platform enables banks to build and maintain unified data architectures for compliance operations, automate risk assessment and control testing workflows, orchestrate customer onboarding and due diligence processes, and continuously monitor compliance program effectiveness—capabilities directly relevant to this Proposal.

We support the Board's objectives: modernizing the AML/CFT framework to emphasize risk-based, outcome-oriented programs; enabling banks to direct more attention and resources toward higher-risk customers and activities; and clarifying the distinction between program establishment and implementation. These objectives align with the operational capabilities we provide to financial institutions globally.

We write because the Proposal's modernization vision—risk-based resource allocation, codified risk assessment processes, innovation-friendly compliance, and continuous program maintenance—has significant technology infrastructure implications that the Board should consider as it moves toward finalization. Our comments address the Board's specific questions and focus on how enterprise workflow and AI platforms can enable banks to operationalize the Proposal's requirements effectively and at scale.

I. Summary of Position

The Proposal's core operational demands—codified risk assessment processes, risk-based resource allocation, the establish-and-maintain two-prong effectiveness framework, and the new supervision and enforcement policy—collectively require banks to move beyond static, document-centric compliance programs toward dynamic, data-driven, continuously monitored AML/CFT operations. Our key observations are:

- **The two-prong effectiveness framework is clarifying, but examination practice must match the regulatory design.** Defining effectiveness as establishing a reasonably designed, risk-based program and maintaining it by implementing that program in all material respects is clearer than a static checklist of pillars. However, banks need certainty that effectiveness will be demonstrated by the strength of design artifacts and implementation evidence—including system-generated audit trails, testing results, resource-allocation analytics, and remediation records—not solely by a narrative program document.

- **Codified risk assessment processes require integrated, auditable data architecture.** Operationalizing the Proposal's risk assessment requirements at scale demands unified data platforms that aggregate risk signals from across products, services, distribution channels, customers, and geographies—with full audit trail lineage. Workflow orchestration enables banks to connect siloed risk data sources into continuous, traceable processes rather than static annual documents.

- **The establish-and-maintain distinction must be preserved at the element level, not only the program level.** Without a clear program-versus-element distinction, examiners may treat every component-level finding as a program-establishment failure, collapsing the Proposal's two-prong structure. Integrated program-management systems help by showing, component by component, whether an element exists (establishment) and whether it is operating (maintenance).

- **The supervision and enforcement framework needs principled definitions of "significant or systemic failure" and "failure to establish."** Banks need to understand the threshold that separates an implementation gap—which the Proposal correctly tolerates if not significant or systemic—from a deficiency that triggers enforcement. The standard should focus on unremediated, material breakdowns, not on the existence of findings.

- **Risk-based resource allocation requires dynamic monitoring and scenario analysis.** The Proposal's requirement that banks direct more attention and resources toward higher-risk customers and activities requires continuous calibration through technology infrastructure, not static allocation plans.

- **The Board's encouragement of innovation should be accompanied by governance guidance.** Banks will benefit from Board guidance on how AI-driven analytics, automated transaction monitoring, and workflow automation will be evaluated during examination, particularly regarding model governance, explainability, and auditability.

We elaborate on each below, organized by the Board's specific questions.

II. Detailed Comments

A. An "Effective" AML/CFT Program (Questions 1–2)

The Proposal's description of an effective AML/CFT program is a significant improvement over the existing framework. The two-prong test—establishing a reasonably designed, risk-based program and maintaining it by implementing that program in all material respects—correctly separates design quality from operating reality.

What remains unclear in examination practice is the evidence an examiner will accept as proof of "effectiveness." Banks need to know whether effectiveness will be judged by the existence of policies, by outcome metrics (useful SARs, reduced false positives, timely risk-assessment updates, remediation cycle time), or by both. The Board should state that effectiveness is demonstrated by the strength of a bank's design artifacts and implementation evidence—including system-generated audit trails, testing results, resource-allocation analytics, and remediation records—and not solely by a narrative program document.

The Proposal's determination that banks are best placed to identify risks and allocate resources is correct. Operationalizing this principle requires three capabilities that enterprise workflow platforms deliver: (1) risk-tiered workflow routing that automatically directs enhanced due diligence and monitoring resources toward higher-risk customer segments, products, and channels; (2) performance analytics—including real-time dashboards, key performance indicators, and key risk indicators—that demonstrate resource allocation is informed by and consistent with the bank's risk assessment processes; and (3) dynamic rebalancing capabilities that allow banks to adjust allocation as risk profiles change. Continuous monitoring through live operational data, rather than periodic point-in-time assessments, enables banks to maintain a risk picture aligned with current conditions.

Recommendation: The Board should state in the final rule or preamble that effectiveness is demonstrated by the strength of a bank's design artifacts and implementation evidence, and should encourage banks to describe the technology infrastructure they use to ensure resource allocation remains consistent with risk assessment processes over time.

B. Establishing and Maintaining an AML/CFT Program (Questions 3–8)

The Proposal's distinction between "establishing" and "maintaining" an AML/CFT program is clarifying and constructive. However, the operational demands of demonstrating ongoing maintenance—implementation in all material respects—are substantial, and several points warrant clarification.

Program-level versus element-level distinction (Question 5). The final rule should state that a failure to establish one mandatory component—for example, the absence of any independent testing function or the absence of any risk assessment process—is a failure to establish the program. By contrast, a gap in a single control, an overdue training cohort, or a lag in updating one product-risk score should be evaluated as an implementation issue, and rise to an enforcement or significant supervisory matter only if

it is significant or systemic. Without this program-versus-element distinction, examiners may treat every component-level finding as a program-establishment failure, which would collapse the Proposal's two-prong structure. Integrated program-management systems help here because they show, component by component, whether the element exists (establishment) and whether it is operating (maintenance).

"Significant or systemic failure" and "failure to establish" (Questions 6–7, 21–22). These concepts should be described in principles rather than an exhaustive list. A failure to establish an AML/CFT program should mean the bank has not put in place one or more mandatory components in proposed § 208.63(c) in any meaningful form: no risk assessment processes; no designated U.S.-based AML/CFT officer; no independent testing capability; no written policies, procedures, and controls reasonably designed to mitigate identified risks; or no ongoing training program. A weak but existent component is generally a maintenance problem, not an establishment problem.

A significant or systemic failure to implement should mean a deficiency that (i) is widespread across business lines, products, or geographies, or is concentrated in the bank's highest-risk activities; (ii) persists after the bank knew or should have known of it; and (iii) materially impairs the program's ability to identify, assess, or mitigate illicit-finance risk or to produce highly useful information for law enforcement. Isolated exceptions, promptly detected and remediated through the bank's own testing and issue-management process, should not meet that standard.

Recommendation: The Board should confirm that a bank's own detection, documentation, and timely remediation of implementation gaps—particularly through independent testing and integrated issue management—weighs against a finding of significant or systemic failure. The standard should focus on unremediated, material breakdowns, not on the existence of findings.

Harmonization across agencies (Question 8). Program-content requirements—risk assessment processes, resource allocation toward higher-risk activity, CDD, testing, training, and the U.S.-based officer—should be textually aligned across FinCEN, the Board, OCC, FDIC, and NCUA. Banks operate enterprise programs, not agency-specific programs. Divergent wording on the same obligation creates examination inconsistency and forces dual documentation. Where the Board's responsibilities differ from Treasury's—supervision and enforcement of implementation, as distinct from FinCEN's establishment regulations—the Board should say so expressly. The establish/maintain split is the right place to draw that line: FinCEN and the Agencies define what must be established; the Board evaluates whether a Board-supervised bank is maintaining that program in all material respects.

The continuous maintenance obligation requires integrated program management infrastructure connecting risk assessment outputs to policy design, policy design to operational implementation, implementation to testing and monitoring, and monitoring back to risk assessment. When these functions operate in disconnected systems—spreadsheets for risk assessment, document management for policies, separate ticketing for implementation tracking, and standalone audit tools for testing—the bank lacks the integrated view needed to demonstrate that the program is being implemented in all material respects. A connected compliance data model—where

every regulation, policy, control, risk, test, and piece of evidence resides in one system with a traceable line from any regulatory obligation to the control that satisfies it and the evidence that proves it—enables banks to detect and remediate implementation deficiencies before they become significant or systemic failures.

C. Internal Policies, Procedures, and Controls and Risk Assessment Processes (Questions 9–16)

Changes to existing internal policies (Question 9). Most banks already have BSA policies, but many still treat the risk assessment as an annual document, resource allocation as a budget exercise, and implementation evidence as material assembled for the examination. The Proposal's "risk-based" and "reasonably designed" language, combined with the prompt-update and maintain-in-all-material-respects obligations, will push banks to convert those artifacts into living processes: mapped controls, workflow-driven change management, continuous testing, and auditable resource-allocation monitoring. That is a process and infrastructure change, not merely a policy rewrite.

Risk assessment processes (Questions 10–11). The Proposal's use of the term "risk assessment processes" (plural) is significant and welcome. In practice, the data that informs risk assessment is distributed across multiple operational systems: transaction monitoring platforms, customer information systems, payments infrastructure, and counterparty databases. Synthesizing these inputs into a coherent risk picture requires workflow orchestration that connects source systems, normalizes data, and maintains audit trails. Platforms purpose-built for integrated risk management address this by enabling banks to centralize risk assessment workflows, map controls to regulatory requirements, automate control testing, and maintain continuous, auditable documentation.

The listed criteria—products, services, distribution channels, customers, and geographic locations—plus the AML/CFT Priorities and prompt updates for significant change are the right mandatory set. The Board should not expand the mandatory list. Additional factors that many banks already consider, and that technology platforms can ingest—delivery-channel digitalization, third-party and fintech partnerships, correspondent and nested activity, product velocity, and typologies identified through 314(b) sharing or law-enforcement feedback—are better left as examples in guidance, not as additional regulatory elements.

Incorporating risk assessment results (Question 12). In a manual environment, incorporating a completed assessment into policies, monitoring scenarios, due-diligence procedures, and training often takes a full quarter or more, and sometimes waits for the next annual cycle. That lag is the operational problem the "promptly" standard is meant to solve. In a workflow-integrated environment, high-impact findings can be converted into owned change tasks within days, with control and scenario updates following on a risk-tiered schedule: immediate for newly identified high-risk exposures, longer for documentation and training refresh. The Board should not set a numeric deadline. It should recognize that "incorporation" is a set of risk-prioritized actions with audit trails, not a single republished binder.

AML/CFT Priorities (Questions 13–14). The principal difficulty in incorporating AML/CFT Priorities is translation. National Priorities are strategic statements; a bank's risk assessment is an institution-specific map of products, customers, channels, and geographies. Banks struggle when they treat Priorities as a separate chapter rather than as a lens applied to existing risk factors. A second difficulty is timing: Priorities may change on a cycle that does not match the bank's assessment calendar, which collides with a prompt-update standard if the process is annual and manual.

Useful guidance would (i) confirm that incorporation means the bank has considered each Priority against its own business model and documented why a Priority is material, partially material, or not applicable; (ii) confirm that "as appropriate" does not require every Priority to generate a new control; and (iii) provide examples of how a Priority can be reflected in customer risk rating, product risk, monitoring scenarios, or resource allocation without becoming a parallel program. The Board should not publish a mapping template that examiners then treat as mandatory.

Prompt updates (Question 15). The Proposal's requirement for prompt updates upon significant changes to ML/TF risks (proposed § 208.63(c)(1)(i)(C)) creates an operational challenge best addressed through automated monitoring and workflow triggers. Regulatory change management capabilities—where regulatory intelligence feeds are auto-ingested, mapped against existing controls and obligations through AI-driven impact assessment, and translated into change tasks with clear ownership and deadlines, prior to final human review and validation—represent the type of infrastructure that operationalizes the prompt update requirement at scale.

Recommendation: The Board should clarify that banks may use automated, workflow-driven risk monitoring and escalation systems to satisfy the prompt update requirement. The Board should confirm that banks using multiple integrated risk assessment processes—connected through a unified workflow platform with audit trail capabilities—satisfy the documentation requirements without producing a standalone, consolidated risk assessment document. The Board should not set a numeric deadline for incorporation; it should recognize that incorporation is a set of risk-prioritized actions with audit trails.

D. Independent Testing, AML/CFT Officer, Training, Written Program, and Approval (Questions 17–20)

Independent testing (Question 17). The Proposal's retention of the independent testing requirement is appropriate. Automated, continuous control testing—where indicators collect data to monitor controls and risks, detect non-compliant conditions in near real time, and generate automated alerts when critical controls fail—should be recognized as complementary to, and in some cases more effective than, periodic manual audits. The Board should confirm that banks may use technology-enabled continuous testing approaches, provided they are independent and appropriately documented.

AML/CFT officer and offshore personnel (Question 18). The U.S.-located officer requirement is clear and should be retained. Personnel outside the United States can and do perform supporting AML/CFT functions. The Board should confirm that workflow platforms, case-management systems, and audit-trail tools may be accessed by

offshore staff for permitted functions without converting those staff into the designated officer, and without authorizing SAR access beyond existing limits (foreign head office or controlling company in limited circumstances). System access controls, role-based permissions, and immutable logs are how banks operationalize that line. No further geographic restriction on technology hosting or vendor support is necessary in this rule, provided SAR confidentiality and access limitations are enforced.

Written program requirement (Question 19). Enterprise workflow platforms maintain program documentation as structured, version-controlled digital records integrated with implementation evidence. A bank's compliance program may be more accurately represented by the strength of its configured workflows, policies, procedures, controls, testing protocols, and associated audit trails within an enterprise platform than by a single narrative document. The Board should confirm that system-generated, electronically maintained program documentation satisfies the "written" requirement.

Board or senior-management approval (Question 20). Approval should attach to the overall program framework and to material revisions of that framework—risk-assessment methodology, governance structure, monitoring architecture at the design level, officer designation, and testing structure. Approval should not be required for parameter-level monitoring thresholds, individual procedure edits, or routine control-testing schedules. Requiring governing-body approval of every configuration change would freeze the dynamic maintenance the Proposal intends to encourage.

"Appropriate senior management" is a useful alternative or complement to the board for mid-cycle material revisions at large organizations, provided the board or equivalent retains at least annual oversight of the program framework. The Board should not eliminate the approval requirement—oversight is part of establishment—but should allow the bank to define the approval path in the written program and to evidence it through the same system of record that holds the program itself.

E. Supervision and Enforcement (Questions 21–26)

FinCEN consultation provisions (Question 23). ServiceNow takes no position on the allocation of examination authority between the Board and FinCEN. From an operational standpoint, banks benefit when the agencies that examine the same program apply the same concepts of effectiveness, materiality, and "significant or systemic" failure. If the Board remains outside the consultation framework the other Agencies proposed, it should still commit in the preamble to coordinated interpretations of those shared concepts so that a bank's program is not "effective" under one agency's reading and deficient under another's.

"Significant AML/CFT supervisory action" definition (Questions 24–26). The term "any written communication" is too broad if it captures ordinary examination observations, matters requiring attention that are not AML-specific, or informal feedback. If the definition is used to trigger consultation, information-sharing, or heightened consequences, it should be limited to written communications that (i) conclude the bank has failed to establish an AML/CFT program or has significantly or systemically

failed to implement one, or (ii) impose or propose a formal enforcement remedy grounded in the BSA or the Board's AML/CFT rule.

Including "unsafe or unsound practices or conditions" in an AML/CFT-specific definition risks mixing safety-and-soundness vocabulary with BSA program vocabulary. If the Board retains the phrase, it should state that an AML/CFT program deficiency is not per se unsafe or unsound, and that the AML/CFT rule's own significant-or-systemic standard governs AML/CFT enforcement.

F. Tailoring, Innovation, and Effective Date (Questions 28–29)

Tailoring by size and complexity (Question 28). The rule text should remain principle-based for all Board-supervised banks: reasonably designed, risk-based, established, and maintained in all material respects. Formal tailoring of the legal obligation by asset size would create cliff effects and examination arguments about which tier a bank occupies. What should be tailored is implementation expectation.

The preamble and any accompanying supervisory guidance should state expressly that community and regional banks may satisfy the same legal standard with simpler processes, qualitative assessments, and fewer systems, while complex firms are expected to have more formalized, data-connected processes. The Board's existing statement that new technology is not required, particularly for smaller banks, should be repeated in the final preamble and carried into examiner instructions. Enterprise-platform capabilities are a means by which larger and more complex firms can meet the standard at scale; they are not a template for every state member bank.

Innovation (Question 28, continued). The Board's encouragement of responsible AML/CFT innovation—including machine learning, generative AI, digital identity, blockchain monitoring and analytics, and APIs—is a significant and welcome signal. However, the value of the innovation safe harbor depends on the clarity of what "responsible" incorporation means in examination practice.

The governance architecture we believe the Board should encourage includes several key elements: enterprise-wide AI policy enforcement that defines which AI models and providers are permitted for which compliance functions; continuous monitoring of AI model outputs for drift, bias, and false positive rates, with automated alerts and remediation workflows when thresholds are breached; decision audit trails that log every material AI-driven action with full traceability for supervisory review; data privacy controls that protect sensitive information as it flows through AI-enabled compliance workflows; and human-in-the-loop oversight protocols that route material AI decisions to accountable human owners before execution. This type of governed, auditable AI deployment—where AI capabilities operate within a compliance governance framework rather than as standalone tools—represents the responsible innovation approach the Board should encourage.

Recommendation: The Board should issue supplementary guidance articulating expectations for AI governance within AML/CFT programs, including model validation, performance monitoring, bias testing, explainability, and human oversight requirements.

Such guidance would give banks the confidence to adopt innovative technologies consistent with the AML Act's stated purpose of encouraging technological innovation.

Effective date (Question 29). The proposed 12-month implementation period is reasonable for most program alignment activities. However, banks undertaking technology modernization to satisfy the Proposal's operational requirements—particularly the integration of risk assessment processes with resource allocation monitoring and continuous program maintenance—may require additional time. We recommend the Board provide flexibility for banks actively implementing technology infrastructure to support compliance, for example by allowing a phased approach where program establishment requirements take effect at 12 months and full implementation demonstration requirements take effect at 18 months.

III. Conclusion

ServiceNow supports the Board's objectives in modernizing the AML/CFT regulatory framework to emphasize risk-based, outcome-oriented compliance programs. The Proposal's two-prong effectiveness framework, codified risk assessment processes, risk-based resource allocation standard, and innovation-friendly posture represent meaningful progress toward the AML Act's modernization goals.

We urge the Board to ensure that examination practice matches regulatory design—in particular, by defining "significant or systemic failure" in principled terms, preserving the establish/maintain distinction at the element level, confirming that effectiveness is demonstrated by the strength of implementation evidence rather than narrative documents alone, and providing governance guidance for AI and innovative technologies in AML/CFT programs.

The shift from static, document-based compliance to dynamic, continuously monitored AML/CFT programs, the resource allocation demands of risk-based prioritization, the integrated governance requirements of the establish-and-maintain framework, and the need for responsible AI innovation governance all point to the central role that enterprise workflow and compliance platforms will play in making this Proposal operational. Banks that invest in integrated technology infrastructure—connecting risk assessment, policy management, control testing, regulatory change monitoring, and resource allocation within a unified, auditable system—will be better positioned to meet the Proposal's requirements and, more importantly, to achieve the BSA's core purpose of generating highly useful information for law enforcement and national security agencies.

We appreciate the opportunity to submit these comments and welcome further engagement with Board staff on the operational and technical dimensions of this rulemaking. If you have any questions, please feel free to contact me at: +1 (202) 795-0883.

Sincerely,

Combiz Abdolrahimi
Vice President and Global Head, Government Affairs and Public Policy
ServiceNow, Inc.