

Braid



Braid Compliance Readiness Assessment (BCRA)

Initial Consultative Support for Braid implementation in
Banks/Credit Unions



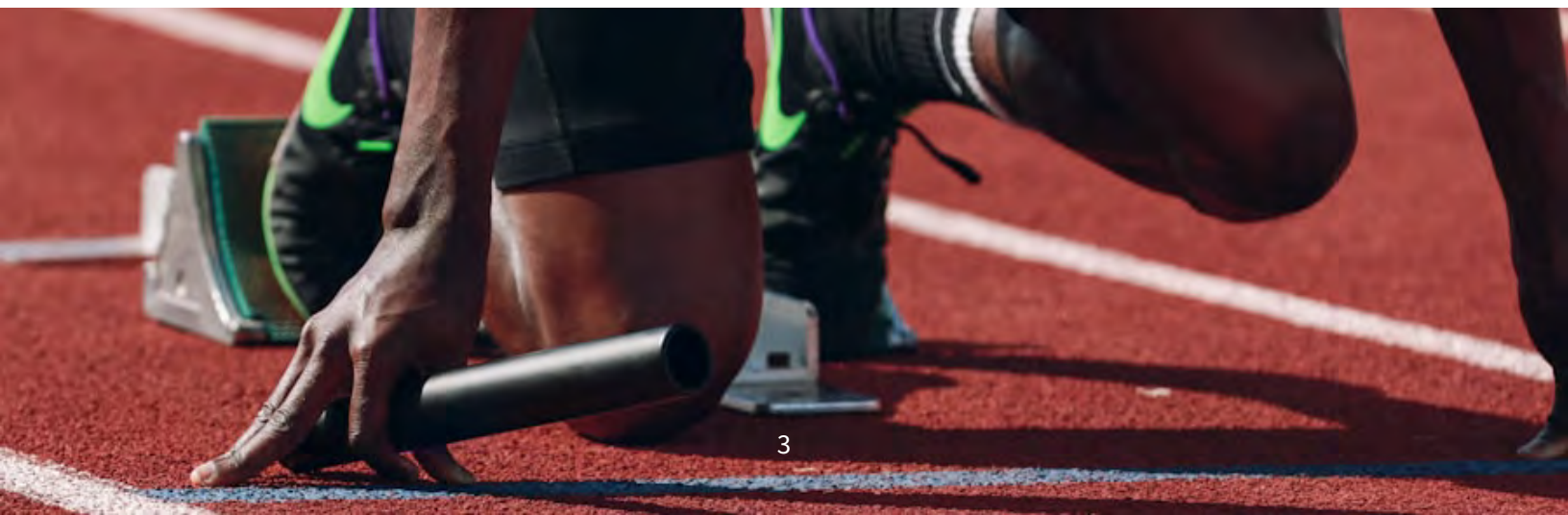
Executive Summary

The Braid Compliance Readiness Assessment (BCRA) is a targeted, risk-based assessment designed to help financial institutions successfully implement the Braid platform to manage higher-risk customers in alignment with regulatory expectations. As banks and credit unions expand services to Fintechs, Money Services Businesses (MSBs), Third Party Payment Processors (TPPPs), Non-Bank Financial Institutions (NBFIs) and other potentially higher-risk customer segments, they face heightened scrutiny and compliance challenges. The BCRA provides a clear, structured approach to evaluating an institution's readiness to meet these challenges—before live transaction processing begins.

The BCRA is a focused assessment that helps financial institutions identify gaps and optimize their AML/CFT and Sanctions Compliance frameworks to fully leverage the enhanced oversight capabilities of the Braid platform. The assessment:

- Pinpoints potential weaknesses in the AML/CFT and Sanctions Compliance Program which may undermine the effectiveness of controls specific to the management of higher-risk customer segments
- Identifies enhancements to governance practices and customer onboarding and monitoring processes to facilitate successful implementation of the Braid platform and oversight of potentially higher-risk customer segments
- Provides leadership with increased confidence in their ability to onboard and oversee higher-risk customers to increase their revenue base

The BCRA report delivers practical, actionable insights, enabling financial institutions to make informed decisions, refine their compliance strategies, and facilitate regulatory alignment—all while positioning themselves for growth in higher-risk market segments.



Scope and Limitations 5

Audience 6

BCRA Report 8

Governance, Regulatory Engagement, and Strategic Leadership 9

AML/CFT and Sanctions Enterprise Risk Assessment 11

Key Areas of Evaluation 11

Customer Onboarding and Account Monitoring 13

Key Areas of Evaluation 13

AML/CFT Transaction Monitoring Program 14

Key Areas of Evaluation 14

Sanctions Filtering Program 16

Key Areas of Evaluation 16

Conclusion 18





Scope and Limitations

The BCRA is a targeted, risk-based evaluation designed to support banks and credit unions in integrating the Braid platform within their existing AML/CFT and Sanctions compliance framework. The scope is limited to AML/CFT and Sanctions compliance considerations as outlined in this document, specifically those related to the implementation of the Braid platform and the institution's capacity to mitigate financial crime risks associated with servicing higher-risk customers.

The BCRA is not an audit, certification, or assurance engagement and does not replace regulatory examinations, independent reviews, or other legally required compliance obligations. Instead, it is a strategic assessment that highlights key compliance considerations related to Braid platform implementation, helping institutions proactively refine policies, procedures, and controls to support sustainable growth.

This work is conducted within a fixed budget range and a clearly defined scope, applying a risk-based approach to review and reporting. While the BCRA may identify additional areas warranting attention, addressing those matters—or expanding the scope beyond what is outlined—would require a separate engagement.



Audience

The BCRA is designed to support key stakeholders involved in the strategic implementation and oversight of the Braid platform. This assessment helps provide decision-makers across risk, compliance, and business leadership have the clarity and confidence needed to integrate higher-risk customer segments into their institution's AML/CFT and Sanctions Compliance framework.

Stakeholders Responsible for Implementation and Oversight

- **Board of Directors:** Provides governance, ensures alignment with the institution's risk appetite, and sets strategic direction regarding AML/CFT and Sanctions Compliance readiness
- **Chief Risk Officer (CRO):** Assesses whether the institution's risk management framework and controls are prepared to manage the unique risks and oversight responsibilities associated with higher-risk customer segments
- **Chief Compliance Officer (CCO):** Reviews the institution's compliance program, regulatory obligations, and operational readiness to support a smooth and compliant Braid platform implementation
- **AML/CFT and Sanctions Officer/Director:** Assesses the institution's operational capacity, resource adequacy, and internal alignment with the institution's AML/CFT and Sanctions Risk Assessment and compliance objectives
- **Financial Institution Teams Directly Managing Implementation:** Align Braid platform capabilities with the institution's customer onboarding, transaction monitoring, and compliance workflows to effectively manage Fintechs, MSBs, TPPPs, and NBFIs



Braid's Implementation and Referral Team

Supports the institution in assessing its operational and compliance readiness to effectively integrate the Braid platform while meeting regulatory expectations and achieving the institution's objectives

Regulatory Considerations

While regulators are not the direct audience for the BCRA, financial institutions must ensure that their governance, risk management, and compliance frameworks align with the expectations of FinCEN, OFAC, and their primary federal regulators. Regulatory examiners may review BCRA-related reports, recommendations, or processes during routine examinations—especially when institutions expand services to higher-risk customer segments or extend agency relationships to third parties.

Risk-Based Execution

The scope and depth of review are tailored based on the institution's size, complexity, growth strategy, and current level of high-risk customer exposure. Institutions at earlier stages may receive foundational assessments, while those further along may undergo more detailed governance, leadership, and regulatory communication evaluations.

BCRA Report

The findings from this assessment will be incorporated into the BCRA Report, which serves as a roadmap for the financial institution's readiness to implement the Braid platform from an AML/CFT and Sanctions perspective while helping to maintain regulatory compliance. Specifically, the report will:

Summarize Key Findings

Identify gaps and opportunities for enhancement in AML/CFT and Sanctions governance, regulatory engagement, strategic leadership, risk assessment, customer onboarding and account monitoring, transaction monitoring and sanctions screening

Where identified, highlight areas requiring policy, procedure, or control updates to align with regulatory expectations

Provide Risk-Based Recommendations

Offer tailored recommendations for addressing identified compliance risks associated with onboarding and monitoring higher-risk customers such as Fintechs, MSBs, TPPPs, and NBFIs

Suggest strategies to improve regulatory communication and oversight to facilitate proactive engagement with regulators

Assist alignment with Strategic Implementation Goals

Assess whether the financial institution can integrate the Braid platform without disrupting existing AML/CFT and Sanctions Compliance frameworks

Suggest improvements supporting a structured approach to scaling compliance resources and controls in alignment with growth in high-risk customer segments

Support Decision-Making and Implementation

Assist leadership (Board, CRO, CCO, and AML/CFT and Sanctions Compliance Officer) to develop a roadmap of AML/CFT and Sanctions compliance initiatives based on risk and operational readiness to integrate the Braid platform



Governance, Regulatory Engagement, and Strategic Leadership

A strong governance framework is essential for the effective implementation of the Braid platform and oversight of higher-risk customer segments, including Fintechs, MSBs, TPPPs, and NBFIs.

Objectives and Evaluation Areas

This assessment evaluates:

- Governance readiness to support Braid platform implementation and higher-risk customer oversight
- Leadership accountability for integrating compliance into business strategy
- Regulatory engagement practices aligned with evolving risk profile, operational changes and supervisory expectations

Governance Practices

- **Strategic Alignment:** Assess whether governance structures—including Board and senior management oversight—are positioned to support Braid-related activities and high-risk customer management
- **Approval and Oversight:** Evaluate whether formal processes exist for approving new customer segments, product offerings, technology, and customers, ensuring alignment with the institution's risk appetite
- **Operational Readiness:** Confirm governance mechanisms are in place to monitor ongoing performance and compliance effectiveness
- **Compliance Capacity:** Consider, at a high level, whether the AML/CFT and Sanctions Officer and supporting compliance team appear to have sufficient authority, access, and baseline resources to support risk oversight and decision-making related to Braid implementation.



Leadership Accountability

- **LOB Sponsorship:** Confirm whether a designated executive is responsible for managing higher-risk customer segments and overseeing Braid-related initiatives
- **Role Definition:** Evaluate the clarity of leadership responsibilities, reporting lines, and collaboration with compliance and risk functions
- **Scalable Strategy:** Assess whether leadership plans account for compliance capacity and risk management needs as services expand

Regulatory Engagement

- **Communication Strategy:** Evaluate whether the institution has a structured approach for informing regulators of material business changes
- **Proactive Outreach:** Confirm plans for maintaining constructive regulatory relationships as risk exposure increases
- **Risk Anticipation:** Evaluate the institution's awareness of likely regulatory focus areas and its preparedness to respond effectively

Compliance Culture and Awareness

- **Training:** Confirm whether the Board, Executives and key staff have received or will be receiving additional AML/CFT and Sanctions training appropriate to the institution's evolving risk exposure





AML/CFT and Sanctions Enterprise Risk Assessment

A robust enterprise AML/CFT and Sanctions Risk Assessment is the foundation of a risk-based compliance program. It enables financial institutions to proactively identify, measure, and mitigate risks associated with higher-risk customer segments, such as Fintechs, MSBs, TPPPs, and NBFIs in line with regulatory expectations, while ensuring operational controls remain aligned with business expansion.

However, many institutions lack the necessary risk segmentation, control validation, and technological integration to support a scalable, real-time risk assessment process. This targeted evaluation identifies gaps, inefficiencies, and opportunities for enhancement to prepare the institution to manage risks associated with the implementation of the Braid platform.

Key Areas of Evaluation

Risk Assessment Review & Gap Analysis

- Review the institution's documented AML/CFT and Sanctions Risk Assessment to evaluate whether it requires enhancement to effectively evaluate the risks introduced by the Braid platform and higher-risk customers
- Identify potential weaknesses in inherent risk calculations, such as:
 - Lack of risk segmentation by product, service, channel, customer type, counterparty, or geography
 - Absence of quantitative inputs, leading to subjective or inconsistent risk determinations
 - Combining AML and Sanctions Risk Assessments without distinct evaluations which may lead to gaps in risk identification, control testing, and regulatory alignment
 - Limited focus on emerging criminal typologies (e.g., fraud, cybercrime, human trafficking, and other evolving risks)

- Identify potential weaknesses in the control testing process, such as:
 - Risk conclusions are based on process-level assumptions of effective operation rather than control effectiveness testing of individual controls in the process
 - Absence of documented evidence of control testing and validation
 - Confirm whether the institution has implemented controls for customer risk assessment at onboarding, initial and ongoing due diligence, and transaction monitoring

Regulatory Alignment and Risk-Based Compliance Preparedness

- Evaluate the institution's preparedness for emerging regulatory requirements, including FinCEN's Notice of Proposed Rulemaking (NPRM RIN 1506-AB52), which will implement the AML Act of 2020 legal requirement that financial institutions:
 - Perform an AML/CFT Risk Assessment as part of an effective, risk-based, and reasonably designed AML/CFT program
 - Incorporate consideration of the National AML Priorities into the risk assessment to ensure the assessment addresses the financial crime threats which impact national security
- Recommend updates to the risk assessment framework to facilitate alignment with both regulatory expectations and the operational realities of onboarding higher-risk customers

Technology and Data-Driven Risk Assessment Enhancements

- Assess whether the institution's current risk assessment processes can:
 - Scale efficiently with increased transaction volumes and customer complexity
 - Leverage automation and advanced analytics to improve risk identification and mitigation
 - Support real-time risk adjustments based on transaction behaviors, regulatory changes, and external risk intelligence
- Identify gaps in technology, data integration, or reporting capabilities that may limit the institution's ability to maintain an agile, risk-based approach

Customer Onboarding and Account Monitoring

Serving higher-risk customer segments, such as Fintechs, MSBs, TPPPs, and NBFIs, often necessitates enhancements to the institution's customer onboarding and account monitoring processes, including policies and procedures for performing customer due diligence (CDD), enhanced due diligence (EDD), and on-going due diligence (ODD), and for identifying customers' Beneficial Ownership (BO). Robust customer onboarding and account monitoring processes are essential to enable the institution to identify and mitigate risks while ensuring compliance with regulatory requirements.

This assessment evaluates whether the institution's customer onboarding and account monitoring processes, including CDD, EDD, ODD, and BO identification, supports effective risk management for onboarding and monitoring higher-risk customers.

Key Areas of Evaluation

Policy and Practice Evaluation

- Review the institution's customer onboarding and account monitoring processes, including its CDD, EDD, ODD, and UBO identification policies and procedures, to assess alignment with their risk profile as defined by their AML/CFT and Sanctions Risk Assessment
- Identify gaps or weaknesses for managing risks associated with higher-risk customers which may negatively impact implementation of the Braid platform
- Evaluate whether additional tools may be needed to enable the institution to assess customer risk



AML/CFT Transaction Monitoring Program

A risk-responsive transaction monitoring program is critical for detecting, assessing, and responding to suspicious activity—especially when serving higher-risk customer segments. Institutions must ensure that monitoring processes:

- Align with their enterprise AML/CFT and Sanctions Risk Assessment, ensuring controls effectively mitigate the risks posed by their customer base
- Adapt to evolving threats and regulatory expectations, rather than relying on outdated monitoring logic
- Support compliance and business goals simultaneously, providing the agility needed to scale responsibly

This targeted evaluation assesses whether the institution has the right structures, technology, and governance practices to support effective transaction monitoring for higher-risk customers.

Key Areas of Evaluation

Transaction Monitoring Processes and Tools

- Evaluate whether the institution's description of its transaction monitoring processes and tools indicates that they are suitably designed to enable the institution to timely identify and evaluate suspicious activity commensurate with the risks identified in the institution's risk assessment
- Establish whether the institution has documented processes to calibrate transaction monitoring rules and thresholds to the institution's unique risk profile, as defined in its risk assessment
- Establish whether written protocols exist for the investigation, resolution, and reporting of suspicious activity, ensuring consistent escalation and decision-making





Ongoing Effectiveness and Risk Adaptation

- Establish whether the institution has mechanisms to regularly test the effectiveness of the detection scenarios and underlying rules, threshold values, parameters and assumptions - particularly as it introduces higher-risk customers
- Identify whether the institution has procedures in place to adjust transaction monitoring based on new risks, regulatory guidance, and emerging criminal typologies
- Provide recommendations to improve the agility and responsiveness of transaction monitoring processes to ensure continuous alignment with evolving threats

Governance and Oversight

- Verify that governance practices are in place to ensure end-to-end, pre- and post-implementation testing of the transaction monitoring system, which may include the institution's reviews of governance, data mapping, transaction coding, detection scenarios logic, model validation, data input, and program output
- Verify that governance practices are in place to oversee system changes, including changes to detection scenarios and rule updates, periodic tuning, and threshold adjustments
- Confirm processes are in place to ensure that all program updates, changes, and enhancements are documented, approved by compliance leadership, and communicated to senior management and the Board



Sanctions Filtering Program

A risk-based sanctions filtering program is essential for identifying, mitigating, and preventing prohibited transactions involving sanctioned entities, individuals, and jurisdictions. Institutions serving higher-risk customer segments—such as Fintechs, MSBs, TPPPs, and NBFIs—must ensure that their sanctions filtering systems are tailored to their risk exposure and regulatory obligations.

Beyond regulatory compliance, effective sanctions screening safeguards institutions from financial crime, enforcement actions, and reputational harm. This assessment evaluates the institution's sanctions filtering processes and tools, governance structure, and ability to adapt to evolving risks, particularly in light of the implementation of the Braid platform.

Key Areas of Evaluation

Sanctions Filtering Processes and Tools

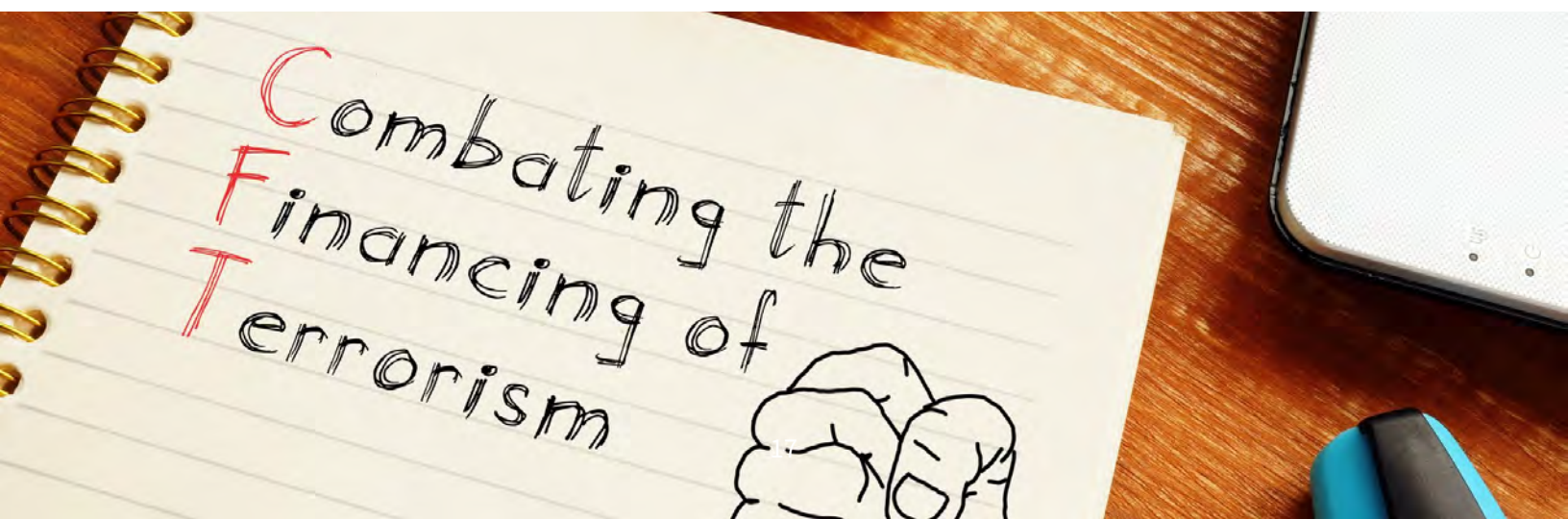
- Assess whether the institution's description of its sanctions filtering processes and tools indicates that they are suitably designed to enable it to interdict transactions that are prohibited by OFAC and whether they are commensurate with the risks identified in the institution's risk assessment
- Evaluate coverage of key sanctions regimes and lists, including OFAC sanctions lists

On-going Effectiveness of Sanctions Filtering Processes and Tools

- Establish whether the institution has mechanisms to test the ongoing effectiveness of the algorithms and underlying rules, threshold values, parameters, and assumptions used by its filter program detection scenarios for name and account matching, particularly as it introduces higher-risk customers
- Provide recommendations to enhance the institution's responsiveness to evolving risks and regulatory guidance and to improve its agility in implementing changes in its sanctions filtering operations

Governance and Documentation

- Verify that governance practices are in place to ensure end-to-end, pre- and post-implementation testing of the sanctions filtering system. These governance practices may include, as relevant, the institution's review of governance, data mapping, transaction coding, filter screening logic, model validation, data input, and program output
- Verify that governance practices are in place to oversee system changes, including changes to detection scenarios for name and account matching, periodic tuning, and threshold adjustments
- Establish whether the program and changes made to it are documented, approved by appropriate compliance personnel, and communicated to the institution's senior management and Board, in accordance with regulatory expectations



Conclusion

The BCRA is a risk-based evaluation designed to help financial institutions prepare for the successful implementation of the Braid platform and onboarding and management of higher-risk customers on the platform. By assessing compliance readiness within the institution's existing AML/CFT and Sanctions framework, the BCRA provides leadership with the insight and information to implement the Braid platform with confidence.

Expanding services to higher-risk customer segments provides both opportunity and responsibility. Regulatory expectations, risk management, and operational preparedness must align to support sustainable growth. The BCRA serves as a prudent, proactive measure—providing financial institutions with a clear understanding of the potential impact of Braid implementation on their compliance posture as they integrate the platform as part of their existing control framework.

MSB Compliance Inc. is your trusted partner in this process. Leverage our expertise, risk-based approach, and deep industry knowledge to help ensure that your institution is positioned for both regulatory alignment and operational success.

Take the next step. To discuss how the BCRA can support your institution's goals, contact us today. Let's build a compliance strategy that supports growth while maintaining sound risk management.

 info@msbcomplianceinc.com |  www.msbcomplianceinc.com

Disclaimer

The Braid Compliance Readiness Assessment (BCRA) is a targeted, risk-based evaluation intended to support banks and credit unions in preparing for implementation of the Braid platform and managing higher-risk customer segments. It is not a compliance audit, certification, independent review, or assurance engagement and does not replace independent reviews, regulatory examinations or other legally required processes.

MSB Compliance Inc. is not a law firm, and no communications or reporting provided as part of the BCRA are intended to constitute legal advice. Institutions should consult legal counsel for any matters of legal or regulatory interpretation.

Recommendations provided through the BCRA are advisory in nature; all final compliance responsibilities, including the implementation of recommendations and mitigation strategies, rest solely with the financial institution.