On November 19, 2013, the Board of Governors of the Federal Reserve System released consumer affairs letter, CA 13-19, to community banking organizations to advice of FRB's intention to adopt the Community Bank Risk-Focused Consumer Compliance Supervision Program, on January 1, 2014. The Program outlines a comprehensive risk framework for examiners to evaluate whether a financial institution is effectively controlling compliance risk. By understanding and implementing the requirements of this risk-focused framework, community banks can demonstrate compliance to consumer protection laws and regulations and, thereby, reduces organizational exposure to fines; civil money penalties; legal damages; voided or unenforceable contracts with third-parties; reduced franchise value, brand or reputation; or rejected expansionary activities, mergers, and acquisitions.

FRB designed the framework to be:

- Risk-Focused
- Proactive and Scalable
- Efficient
- Clear
- Collaborative

The framework's risk-based approach evaluates a financial institution's compliance culture and processes for identifying, measuring, controlling, and monitoring risks and its consumer practices, and compliance with consumer protection laws and regulations. The framework also balances the breadth of supervision with the level of risk to consumers and the size of the financial institutions. The framework efficiently incorporates procedures and processes and clearly provides guidance, policies, procedures, and examination findings. Lastly, the framework enables cross-disciplines and supervisory agencies to collaborate.

The risk-focused supervision program outlines five processes, where three of which offer significant insights into activities that may be considered and implemented by financial institutions to comply with the FRB's supervisory process. Figure 1 to the right describes the key processes:

- Understanding the Institution

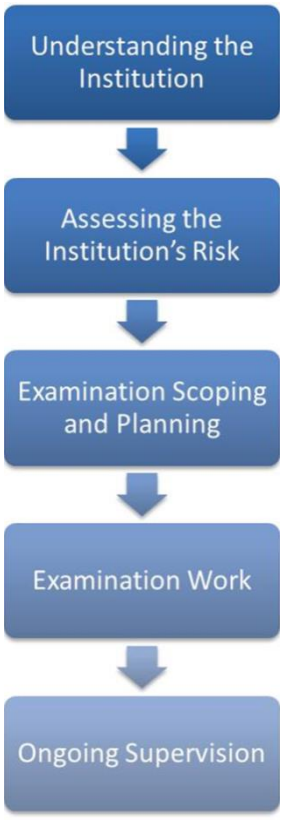

Figure 1: Key Processes of the Risk-focused Supervision Program

- Assessing the Institution's Risk
- Examination Scoping and Planning
- Examination Work
- Ongoing Supervision

Understanding the Institution

The first phase of the process, Understanding the Institution, details the key considerations for the examiners to gain an thorough understanding of the institution, and their role within the legal and regulatory landscape in which it operates, specifically with regard to:

- The types of business the institution and its affiliates and subsidiaries engage.
- The structure of the organization including the board of directors, senior management, and compliance personnel.
- The compliance management program in place at the institution
- Material or significant changes specific to the institution on an ongoing basis that potentially the consumers

The institution profile should be gathered from three possible sources:

- Institution-provided – Covers information including products and services, strategic plan, policies and procedures, compliance reports and audits, consumer complaints, compliance testing, litigations, news, press releases, public filings, social media channels, etc.
- Institution data from oversight agencies – Covers key reports such as Uniform Bank and Performance Reports, Home Mortgage Disclosure Act (HMDA) and CRA data, electronic loan data, etc.
- Reserve Bank or Federal Reserve System Information – Includes past CRA Performance Evaluations, Complaint and correspondence files, examination reports from other disciplines and/or other agencies, etc.

The purpose of the institutional profile is to convey an understanding of the institution's current state addressing regulatory compliancy, stability and its current and prospective risks, as well as to highlight key issues and supervisory findings. The

institutional profile must take into account material events, products, and services and the regulatory environment that affect management decisions. The profile must also consider the institution's staff expertise and capacity to support and deliver product or service, including exercising oversight and review of the institution's third-party providers.

"Simply stated, the institutional profile provides a concise portrait of an institution's structure and business activities that should allow examiners to understand the scope of activities that give rise to potential consumer harm and consumer compliance risk."

To an institution outsider, the institution profile provides significant insights to the maturity of the institution, its practices to address institutional, legal and regulatory, and environment factors, and the potential inherent consumer compliance risk, as highlighted below:

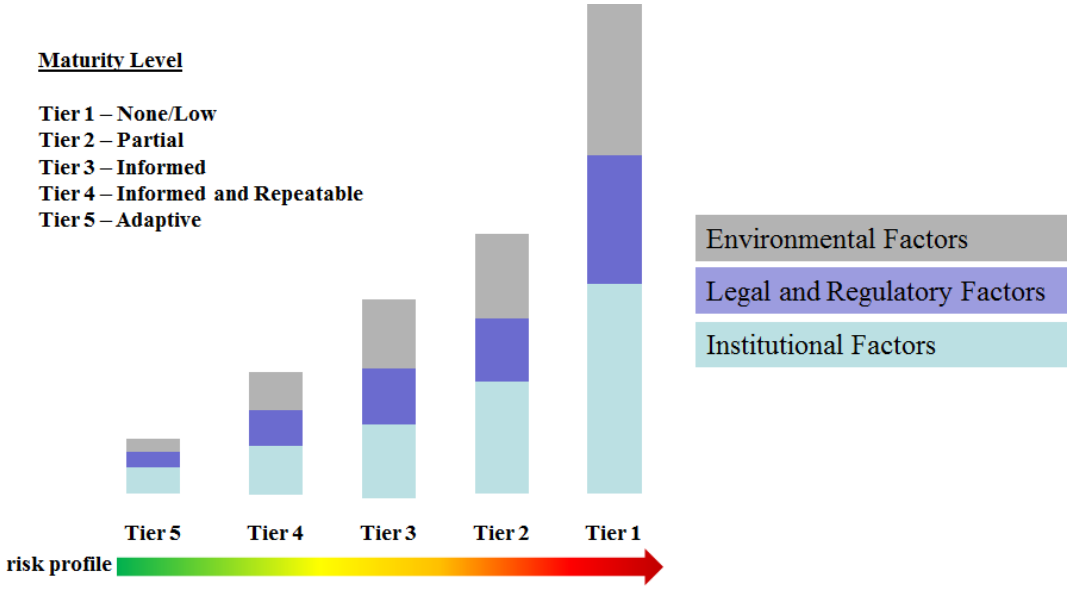

Figure 2: Institution Profile and Inherent Consumer Compliance Risk

How does an institution know what information is critical or important to ensure an accurate and effective development of an institution profile? Consider the following:

1. Organizational Structure – Organizational chart of the organization including the divisions, business units, and key functions such as compliance function, risk function, and business lines, etc. must be well-understood and mapped to the appropriate products, services, and people.

2. Inventory of Key Products, Services and Systems – Products and services provided by the institutions to the consumers must be clearly identified.

Where delivery of products and services rely on the key information systems, the supporting systems must also be documented. The inventory list serves to ensure that accurate and complete consumer compliance impact against the products, services, and systems can be conducted and. The inventory list must contain detailed information (but not limited to):

a. The purpose and type of entities (products, services, vendors, etc.)
b. Primary location
c. The responsible group, within the organizational structure
d. Key individuals including system owners, security officers, etc.
e. Relationship of the system to other systems within the financial institution's network
f. Listing of key devices and major components that establishes the boundaries of the system
g. Key compliance performance metrics (SDLC, control implementation and testing, risk remediation, reporting status)
h. Known residual risks and remediation activities

3. Change Management – Institutions need to identify changes to its business model and strategies, product/service mix, resources, vendors and business associates, policies and procedures, and any other consumer-impacting changes, and to relate those changes to specific products, services, people and/or systems. Change management should also extend to shift in competitive landscape including deposit market share, business and economic conditions such as loans and mortgage products in light of employment, housing data, interest rate, etc.

4. Compliance Management – The institutions must be able to demonstrate effectiveness over compliance testing and audit of controls applicable to the organizational systems. Control testing and audit must also extend to key or volatile controls that require periodic reviews or controls that recently remediated due to issues.

5. Regulatory Reporting – The institutions must meet a variety number of reporting requirements and ad hoc data calls across multiple regulatory agencies, and be able to manage supporting evidence and required documentation for the retention period of the reporting period.

"Centrally management of information plays a crucial role in ensuring accurate and effective development of the institution profile."

6. Regulatory Applicability and Coverage – Applicable regulations must be identified against systems to be evaluated, including regulation updates.

7. Finding and Corrective Action Management – Institutions must have in place fundamental mechanisms to manage risks including capabilities to:

    a. Identify risks
    b. Assess and evaluate risks
    c. Treat risks
    d. Monitor and review risks

    Risk reviews should include past supervisory history, corrective actions from internal and external audits, changes to institution's financial condition, and other supervisory ratings or issues raised as part of enforcement actions, complaints, and litigations.

Key Challenges of Information Gathering

For most institutions, information may already exist in forms of spreadsheets, electronic documents (Word or PowerPoint), reports (printed and scanned), images, other electronic data, etc., disparately locate across the enterprise. In some cases, information may reside on specific workstations of certain users based on their roles within the organization. Institutions have attempted to overcome this disparate state of information by adopting a centralized approach to data management either through the use of enterprise collaboration tools such as Sharepoint, or through the use of shared folders within a network. These bits of information, or artifacts, serve as bodies of evidence to support a compliance position, or statement in the development of the institution profile. These artifacts must be manually maintained by the end-users when updated to ensure accuracy of information.

Due to the competitive and regulatory landscape information related to the institution is expected to change over time. The changes must be managed in a standardized approach to ensure data integrity and to meet the requirements of organization's policies and procedures. The same expectation also extends to compliance review and testing, and the management of findings and corrective actions as they potentially increase the consumer compliance risks. This challenge can be met effectively only through the use of enterprise governance, risk and

compliance (GRC) solutions due to the large number of regulations.

Another challenge that must also be addressed by the institutions to ensure accurate institution profile is the assurance of data accuracy and integrity of the centrally managed information as the same data may be editable by multiple users, possibly without or limited use of audit trails or version control. This challenge may be overcome by using a combination of user group and file access permissions and to limit the scope of write access to a smaller group of users.

To understanding the institution, regardless of the challenges, centrally management of information plays a crucial role in ensuring accurate and effective development of the institution profile.

Figure 3: Risk Assessment Process

Assessing the Institution's Risk

The second phase of the process of the Risk-focused Program addresses the risk assessment of the institution to determine the effectiveness of an institution's overall compliance management program. This process is both costly and time-consuming to implement and demonstrate for financial institutions due to the combination of methodical evaluation against a pre-defined standards and the vigorous approach to document of compliance evidence.

The assessment process, as shown in Figure 3, commences with a listing or inventory of products, services and activities that may be material to the institution. The task of organizing the required contents can be overwhelming and time-consuming for the institution as the required contents may include purpose, product volume (in term of dollars, units, or both), boundaries, SLAs, MOUs, critical diagrams, points of contact of the responsible organizational unit and supporting vendors, and assets/devices associated with the inventory. The details of the content directly correlate to the materiality of the product, service or activity under review, and may warrant a more or less in-depth assessment.

TrustedAgent significantly reduces the effort required to capture and organize the contents. Data templates from TrustedAgent accelerate the setup of inventory and development of the institutional profile, allowing loading and updating of content within TrustedAgent from external sources. Assets (hardware/software/devices) can also be loaded using data templates or import directly from vulnerability assessment (VA) results from common VA tools such as Nessus. Once imported, standard

product enumerations of the assets are determined, as applicable, using the NIST National Vulnerability Database (NVD).

Through security categorization process, financial institutions can establish the level of materiality for the product, service or activity under review. Optionally, with TrustedAgent, financial institutions can define their own evaluation criteria for materiality based on internal policies, procedures, and risk tolerance to ensure consistency in assessment of their inventory. Depending on the outcome of the security categorization, more or less controls should be considered in the determination of the inherent risk for the product, service, or activity.

To determine the inherent consumer compliance risk associated with the products, services or activities, the institutions may leverage one or more controls set including FFIEC Examiner Controls, OCC guidance, etc. to determine the extent of control implementation and effectiveness for the entity using TrustedAgent. The determination considers the following factors:

- Institutional Factors
- Legal and Regulatory Factors
- Environment Factors

TrustedAgent addresses the requirements relating to institutional, regulatory and environmental factors as follow:

Institutional Factors	How TrustedAgent supports Requirements
Strategic/Business Factors	
Structural Complexity Refers to the overall complexity of the institution's operations, including its subsidiary structure, branch networks, and degree of centralization of activities.	Provides the ability for institutions to organize its operations into organizational hierarchy where one or more product, service, or activity is assigned to the corresponding organizational unit owner. The same hierarchy also extends to the dashboard and reporting further simplifies the complexity of information across the institution, its subsidiaries, regions, operations, functions, and, if required, to the branches.
Growth Refers to substantive growth in market share or asset size through branching, merger, acquisition, change in business focus, or	For each product, service, or activity (i.e., collectively managed as entities within TrustedAgent), the organizational unit owner

geographic expansion.	can maintain several attributes and supporting artifacts. Market share or asset size year to year can be added as artifacts and automatically incorporated into regulatory documentation.
History/Trends Refers to the extent to which the institution has effectively managed its compliance risk in the past.	TrustedAgent's dashboard comprehensively supports the tracking and review of risk performance over time of an institution. Risk performance can be filtered into smaller organizational units, and by product, service or activity (i.e., by entity). Multiple attributes of risk performance are available including control implementation and effectiveness by risk level, identified risks, risk by assets, corrective actions by remediation status, etc.
Product/Service Characteristics	
Product Volume Refers to the level of product activity and the number of consumers potentially negatively affected if the institution fails to comply with regulatory requirements.	Volume of activities for each product, service, or activity can be maintained as artifacts.
Product Complexity Refers to the intricacies of a product related to: (1) the complexity of the product's characteristics, (2) whether the product targets specific consumer segments, and (3) processes concerning the institution's products, including delivery channels and marketing, account opening, loan origination, servicing, and loss mitigation practices or processes.	By leveraging the template authoring capability and attributes built into TrustedAgent, details of the product's characteristics and the consumer segment support can be documented. Supporting evidence such as diagrams and artifacts can also be maintained along with applicable policies and procedures.
Product Stability Refers to recent changes in products or services, either new product or service offerings or modifications to existing products or services, including system changes that would affect product handling or management.	Changes to the profile of product, service, or activity such as growth, volume, or additional offerings can be maintained as new entity or modification to details of existing entity.
Third-Party Involvement Refers to the use of third-party vendors to provide bank-related products or services, including assistance with compliance management-related functions.	TrustedAgent supports vendors as entities and offer the capability to conduct review of the vendors using third-party vendor assessment frameworks such as BITS, Shared Assessments or ISO standards.

Legal and Regulatory Factors	How TrustedAgent supports Requirements
Regulation Complexity Refers to the amount of judgment, regulatory knowledge, technical skill, or processes required to understand and comply with a law or regulation.	TrustedAgent provides the ability for the institution to methodically and consistently evaluate its products and services against various regulatory requirements using standards and guidance from FFIEC, FDIC, OCC<

	and other government agencies.
Regulatory or Legal Changes Refers to new laws, regulations, or amendments or modifications to existing laws or regulations.	Changes due to laws, regulations, etc. can be incorporated and updated against the control sets. Controls previously implemented and assessed can be reset for review due to the changes. Changes that impact policies and procedures can be disseminated across the enterprise users

Environmental Factors	How TrustedAgent supports Requirements
Business Conditions Refers to the business environment in which the institution operates, including factors such as overall market conditions, loan demand, employment rates, and housing needs.	Business conditions, demographics and competition utilized in defining the attributes of the entity, its consumer inherent risk's position may be maintained as artifacts for detailed description, or as artifacts to specific control reviewed of the entity.
Demographics Refers to the demographic characteristics of the markets in which the institution operates.	Refer to previous requirement.
Competition Refers to the level of competition in the institution's market(s) and the nature of activities engaged in by the institution's competitors.	Refer to previous requirement.

The FRB Risk-Focus program also requires an assessment of the management and the management systems for the institution to assess consumer compliance risk management. Factors for consideration include:

- Board and Senior Management Oversight
- Policies, Procedures, and Limits
- Risk Monitoring and Management Information Systems
- Internal Controls

For each of the above factors, TrustedAgent supports the adequacy of management systems for the institutions as follow:

Board and Senior Management Oversight	How TrustedAgent supports Requirements
Management Expertise Management hires staff with experience and	Key points of contact (POCs) can be maintained

expertise consistent to the complexity of the organization's business activities. Also maintain staff level appropriate to the resource demand of the organization.	for each entity by specific role. The POCs can subsequently be used in regulatory documentation.
Risk Appetite/Risk Tolerance Risk appetite and tolerance levels are fully and clearly identified, communicated, and understood, from board and senior management levels throughout the organization.	TrustedAgent supports both qualitative and quantitative risk methods. Under the qualitative method, control and finding risks are classified as Low, Moderate or High. Customizable risk scoring impact based on numerical scoring can be leveraged to determine the control risk. Additionally, industry scoring method such as CVSS is supported for risks identified against asset through vulnerability scanning tools. Acceptable risk tolerance can be communicated through combination of memo or policy or procedures. Acknowledgement of review can also be enforced.
Management Responsiveness Refers to management pro-activeness in handling of consumer compliance risks associated with current and proposed activities, services or products offered, and ensure that the appropriate infrastructure and internal controls are established for the institution.	TrustedAgent provides a risk management approach to consistently support institution's processes of identify and remediation of risks. The application provides internal controls to ensure that risk handling is consistent to organization's plicies and procedures. TrustedAgent's dashboard and management reporting provide the mechanisms to ensure that risk management practices are appropriately adjusted in accordance with new activities or enhancements to industry practices and regulatory guidance or expectations. The dashboard provides real-time indications of risk metrics at an enterprise level, at organizational unit level and specific entity.

Policies, Procedures, and Limits	How TrustedAgent supports Requirements
Policies and Procedures	
Formality and Approval Practices Policies are appropriate, comprehensive, understood, and regularly reviewed and updated.	Policies and procedures can be managed in a central repository, and communicate to end users when change. User acknowledgement can also be enforced.
Applicability, Depth, and Coverage of Policies Compliance policies provide for effective identification, measurement, monitoring, and control of the compliance risks posed by all activities. The policies clearly delineate accountability and lines of authority across the	TrustedAgent allows policies or procedures to be distributed to users across the enterprise, or to specific small organizational unit.

institution's activities and between lines of business and associated control or support functions.	
Sufficiency of Procedures Procedures provide operating personnel with clear and specific guidance in fulfilling their compliance responsibilities.	TrustedAgent's Policy Management module allows comprehensive development of new policies or procedures or from existing Word format. Ownership for policies and procedures can also be established as well as authoring and editing capabilities.
New Activities A comprehensive review of new activities and products is performed to ensure that the infrastructure necessary to identify, monitor, and control compliance risks is in place and fully effective before the activities or products are initiated.	TrustedAgent enables a new entity to be created and evaluated for compliance to specific regulatory and security requirements/standards. The required policies and procedures can be conducted as part of the assessment.
Training	
Coverage and Frequency All managers and staff have been formally trained on and are fully knowledgeable about the relevant laws, regulations, policies, and procedures. Training occurs at appropriate frequencies.	A training program can be setup as an entity within TrustedAgent and be assessed for compliance to training requirements of the risk-focused program.
Formality and Applicability Compliance training programs are fully comprehensive and innovative, and results are fully documented.	The assessment of the entity includes a evidentiary review of results from training across a subset of employees and the related documentation.
Effectiveness Training is formally tracked, and results are monitored through robust management information systems (MIS).	Effectiveness determination of the training program is fully supported by TrustedAgent's assessment process.

Risk Monitor and Management Information Systems	How TrustedAgent supports Requirements
Board and Senior Management Level Reporting	
Sufficiency and Timeliness MIS reports provided to the board and senior management are accurate and timely and contain all the information necessary to identify adverse trends and adequately evaluate the level of compliance risks facing the institution.	TrustedAgent's dashboard and management reporting capabilities support management review and reporting in real-time. Information can be filtered down to smaller organization unit by various risk performance metrics.
Effectiveness MIS reports provided to the board and senior management and other forms of communication are fully efficient, comprehensive, and consistent with all activities.	TrustedAgent provides multi-level reports enabling management and business owners to understand the ongoing regulatory activities of the institution. Where built-in reports may not contain the required information, ad hoc

	reporting can be leveraged to produce the required communications and reports for the board or senior management.
Monitoring Practices	
Monitoring Practices Strong legal, regulatory, and compliance risk monitoring programs and associated methodologies are in place.	TrustedAgent supports regulatory monitoring through its continuous monitoring module where key controls can be reset to re-assess for changes due to remediation, regulatory changes, etc. Where devices are required to be periodically monitored as with IT assets, TrustedAgent allows periodic vulnerability scanning to be scheduled, conducted, and identified findings be automatically imported into the tool. Identified findings can be tracked and remediation can be monitored through a combination of alerts and dashboard board indications.
Reporting Lines	
Reporting Lines The organizational structure establishes clear lines of authority and efficient communication regarding responsibility for adherence to legal and compliance policies and procedures. Reporting lines provide clear independence of the control functions from the business lines and separation of duties throughout the organization.	TrustedAgent supports multi-level role-based access to information managed within the application. The role can be based on reporting lines and functions to limit and control access of key information to specific users. Any large number of roles can also be developed using custom profiles to best support the governance structure of the organization.
Audit	
Independence Audit or other control review practices provide for clear independence and objectivity.	To support independence and objectivity of controls, the workflows for control implementation and assessment, and related documentation within TrustedAgent are based on the roles of the users as follow: 1. Control owner(s) – Responsible for the control implementation and supporting evidence to demonstrate that the controls have been implemented per policies, procedures and specifications of the organization and governing regulations. This role is the responsibility of the respective product, service, or activity owner. 2. Control assessor(s) – Independent reviewers of the controls to assess that

	the control implementation is accurate, effective and met the applicable assessment objectives defined for the control. Typically this role is assigned to internal or external regulatory auditors.
Scope and Frequency	
A robust risk methodology is in place that appropriately identifies high-risk areas and activities and properly sets review frequency and coverage. The bank fully adheres to its review schedule.	Risk management with TrustedAgent is flexible allowing frequency of control testing to vary from on-demand through annually basis or extended as far as two additional years into the future. On-demand testing can be employ
Effectiveness	
Training is formally tracked, and results are monitored through robust management information systems (MIS).	Effectiveness determination of the training program is fully supported by TrustedAgent's assessment process.

Documenting the Assessment

TrustedAgent documents the risk assessment as happens in real-time. In the FRB Risk-focus program, the results of the assessment must be made available to senior management, compliance staff, and examiners. TrustedAgent thoroughly support the complete life cycle of control documentation from control implementation, artifact and evidence collection, control assessment, and control reporting.

Control implementation documents the implementation details, any deviations

Figure 2: Control Implementation Process

such as exception or use of compensating, along with any supporting evidence to meet the required control objective. In addition to uploaded artifacts, the compliance description also supports hyperlinks allowing the users to provide links to existing policies and procedures managed within TrustedAgent as evidence to having met the requirements of the control. The hyperlinks can also be directed to external (outside of TrustedAgent) as well other Web sources, as required.

Optionally, the implemented controls can be reviewed for effectiveness using institutional-defined test cases or test cases based on standards or best practices

defined by FFIEC. TrustedAgent also supports conformity assessment enabling organizations to independently confirm the controls using independent assessors.

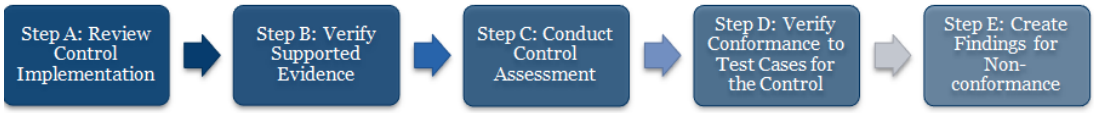

Figure 3: Control Assessment Process

Once assessed, the control documentation is automatically updated with control effectiveness information.

For any of the controls that fail to demonstrate minimum compliance identified either during control implementation or assessment, findings are created with specific risk level, business impact, recommended mitigation action to track identified issues. The findings represent un-mitigated residual consumer risk of the inventory with higher residual risk associating to higher risk levels and the presence of a larger number of findings. Conversely, a lower residual consumer risk associates to a small number of findings of low risk level.

Identified findings undergo risk mitigation review where the institution's compliance staff and inventory's owner either risk accept the findings without mitigation, or remediate the findings as corrective actions. Corrective actions contrast to findings by representing risks that would be removed if the defined remediation activities are implemented effectively. Accordingly the difference between the sum of the risk level of the risk-accepted findings and the sum of the corrective action being remediated represents the expected residual risk for the institution against any given product, service or activity. The aggregation of the residual risks across all products, services, and activities represent the overall residual risk for an institution.

Regulatory Reporting

The outcome of the completed assessment is a concise demonstration of implementation for all applicable controls along with control effectiveness, if applicable, documented in a security plan for the product, service or activity. Identified findings for any failed controls are automatically captured and documented in the security assessment report. Security plan, security assessment report, and any other templates are fully customizable and centrally managed to meet organization requirements, thereby enforces consistency and compliant to

policies/procedures while eliminating duplication of editing and errors relating to change management across the organization.

These two core documents contain both the institution profile details along with the overall level of residual risk for the product, business line, service, or activity. The documents enable management and external examiners to gain an understanding of the overall rating of inherent risk at the institution and the adequacy of controls in place or management's response to any significant internal review or audit findings that involved consumer compliance matters.

TrustedAgent offers a comprehensive management reporting framework that includes filter-enable drill-down graphical dashboard of key metrics in real-time and historical trends, a plethora of built-in reports, and on-demand (ad hoc) reports using organization-defined criteria/queries to support regulatory reporting or data calls required by the organization.

TrustedAgent's dashboard organizes key metrics into views relating to Authorization, Inventory, Assets, Controls, Findings, and Corrective Actions. These views presents information in real-time with filters and drillable details allowing visualization of information in an easy to understand manner. As previously discussed, the determination of overall residual risk derives from the Findings and Corrective Actions views.

Ongoing Supervision

The FRB Risk-focus program discusses a requirement for an ongoing supervision program intended to identify significant changes that have occurred in the compliance management program or in the level of consumer compliance risk in the institution since the previous supervisory activity. Using TrustedAgent's template authoring capability, ongoing supervision questionnaire can be incorporated into the risk assessment template, enabling the institutions to continuously update key changes or information related to:

- Management and control environment
- Product mix and trade area
- Financial condition
- Risk management
- Previous Supervisory Findings

New product, service, or activity can be added to list of inventory and be managed through an assessment. Changes to compliance management structure or staff, ownership can also be applied to existing inventory and be retested. Controls specific to changes in regulations, geographic expansion/contraction, business strategies, etc. can be reset and re-evaluated to determine if the changes have a significant impact on the institution's overall residual risk. Optionally, the institution may programmatically identify key controls and configure the controls to be retested periodically on an annual basis for up to a three-year monitoring period.

Additional continuous monitoring activities can be managed within TrustedAgent including:

a. Vulnerability assessments from vulnerability assessment tools
b. Annual assessment reports and metrics
c. Updated findings and corrective actions from ongoing remediation activities.

As changes are implemented, TrustedAgent's dashboard reflects the current information allowing management and compliance staff to gain timely understanding of the impact to the inherent risk, adequacy of controls, and the derived overall residual risk.

Conclusion

FRB Risk-focus program places significant obligations on financial institutions to demonstrate that the institutions have strong risk management and consumer protection practices in place for its products, services, and activities. By leveraging TrustedAgent, financial institution can scale and customize its compliance program to meet and comply with the requirements of the program while maintaining a balance between cost, expected requirements, and implementation time.

Trusted Integration is a leading provider of Governance, Risk and Compliance (GRC) management solutions for government and commercial organizations. TrustedAgent is an adaptive, scalable GRC solution for organizations to standardize business processes, reduce complexities, and lower costs in the management, analysis, and remediation of risks across the enterprise to meet the challenging, complex, and ever-changing requirements of PCI, SOX, HIPAA, NERC, ISO, COBIT, FISMA, and many others.

TrustedAgent provides an unparalleled and cost-effective enterprise solution that enables organizations to inventory, assess, remediate, and manage risks and regulatory requirements before detrimental loss are sustained by the organization.

Trusted Integration, Inc.
525 Wythe Street
Alexandria, VA 22314
703-299-9171 Main
703-299-9172 Fax
www.trustedintegration.com