Community Bank Risk-Focused Consumer Compliance Supervision Program

I. INTRODUCTION

Overview of the Risk-Focused Framework

The consumer compliance risk-focused supervision program is designed to promote strong compliance risk management practices and consumer protection by ensuring that Federal Reserve-supervised state member community banks comply with consumer protection laws and regulations.[1] The program achieves this goal through processes designed to evaluate whether an organization's consumer compliance risk management program (compliance management program) effectively manages its inherent compliance risk, which includes risks to the institution and its customers. The products and services reviewed during a risk-focused consumer compliance examination will vary based on the inherent compliance risk present in the institution's business lines, products, and services and the effectiveness of the institution's compliance management program.

The purpose of the risk-focused supervision program detailed in this document is to provide a framework that allows examiners to evaluate whether an institution is effectively controlling compliance risk. To accomplish this objective, the program

- incorporates guidelines for evaluating compliance management programs in the context of inherent risk to the organization (including the bank, affiliates, and subsidiaries) as well as to consumers
- requires development of a supervisory strategy that recognizes the risk of noncompliance for business activities at an institution and across institutions
- allows Reserve Banks to tailor supervisory activities to the structure, complexity, and risk of the organization and to adjust these activities over time, thus deploying Federal Reserve resources efficiently and effectively.
- acknowledges the value of timely communication regarding consumer compliance regulatory and supervisory matters by supplementing point-in-time supervisory work with ongoing supervision
- requires coordination with other supervisory disciplines and other regulators, as warranted, to ensure a full understanding of an organization's risk profile and a proper supervisory approach

The framework is

- **Risk-focused.** Evaluates a financial institution's compliance culture and processes for identifying, measuring, monitoring, and controlling risks and its practices regarding the treatment of consumers, the potential for consumer harm, and compliance with consumer protection laws and regulations.
- **Proactive and scalable.** Balances the nature and breadth of supervision with the level of risk to consumers and financial institutions.
- **Efficient.** Incorporates procedures and processes to ensure good stewardship of examiner resources.
- **Clear.** Provides guidance, policies, procedures, and examination findings clearly.
- **Collaborative.** Engages other disciplines and supervisory agencies, as appropriate, to ensure a coordinated supervisory approach.

The risk-focused supervision program outlines standard processes to ensure consistent and effective supervision of Federal Reserve-supervised institutions. This document discusses in detail the following processes depicted in the diagram on page 2:

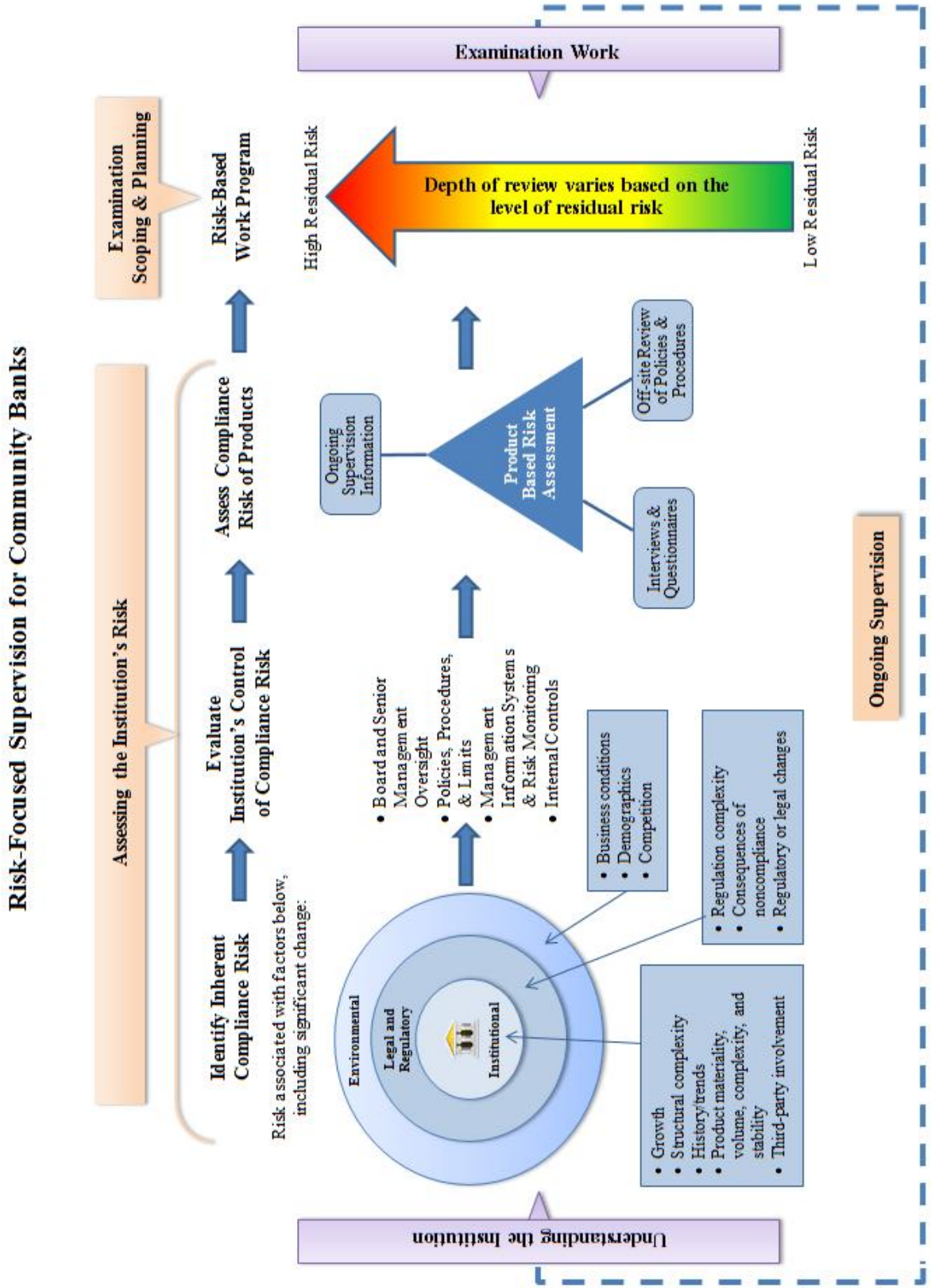
- Understanding the Institution
- Assessing the Institution's Risk
- Examination Scoping and Planning
- Examination Work
- Ongoing Supervision

II. UNDERSTANDING THE INSTITUTION

Overview

The starting point for risk-focused supervision is developing an understanding of the institution, taking into account environmental factors and the legal and regulatory landscape in which it operates. To understand an organization's compliance risks, examiners must understand the types of business it conducts within the institution, its affiliates, and subsidiaries. Examiners must also understand the structure of the organization, including the institution's compliance management program and key personnel in senior management

1. A community bank is a bank with assets of $10 billion or less.


Risk-Focused Supervision for Community Banks
Examination Work
Examination Scoping & Planning
Risk-Based Work Program
High Residual Risk
Depth of review varies based on the level of residual risk
Low Residual Risk
Assessing the Institution's Risk
Identify Inherent Compliance Risk
Evaluate Institution's Control of Compliance Risk
Assess Compliance Risk of Products
Risk associated with factors below, including significant change:
• Board and Senior Management Oversight
• Policies, Procedures, & Limits
• Management Information Systems & Risk Monitoring
• Internal Controls
Ongoing Supervision Information
Product Based Risk Assessment
Off-site Review of Policies & Procedures
Interviews & Questionnaires
Ongoing Supervision
Understanding the Institution
Environmental
Legal and Regulatory
Institutional
• Business conditions
• Demographics
• Competition
• Regulation complexity
• Consequences of noncompliance
• Regulatory or legal changes
• Growth
• Structural complexity
• History/trends
• Product materiality, volume, complexity, and stability
• Third-party involvement

and compliance roles. This step is critical to tailoring the supervisory plan (including examinations, monitoring, and outreach) to align with the risk profile of the organization. The technological, regulatory, and market developments in the financial sector and the speed with which an institution's risk profile can change make it critical for supervisors to keep abreast of material events and changes in strategy that affect the institution's risk profile. Accordingly, consumer compliance examiners should review institution-specific information on an ongoing basis, in accordance with ongoing supervision expectations or in response to material events or changes. Examiners should also stay up to date on environmental and statutory/regulatory changes in order to maintain consumer compliance-specific information for the institutional profile that will communicate the examiners' understanding of that institution and the market(s) in which it operates.

Information about an institution's business model and strategy, major business activities, and associated risk tolerance serves as the foundation for assessing the associated risks and should be captured in the institutional profile. The profile should document the internal changes driven by management decisions or external events that may alter an institution's risk profile.

Preparing the profile begins with gathering and reviewing available information, including examination reports, direct observations gained through monitoring activities, correspondence files, financial databases, information from consumer groups, news outlets, and other information generated by the Federal Reserve and other supervisory agencies. Reviewing this information helps examiners identify both the strengths and the vulnerabilities of the institution.

The following are some documents and sources that are helpful in understanding the institution:

Information about the Institution

- the institution's strategic plan
- board packets or any other information that may be provided by the organization to the Reserve Bank's central point of contact (CPC)
- minutes of board, loan, compliance, Community Reinvestment Act (CRA), audit, risk, or other relevant committees
- organizational chart and compliance management program structure
- policies and procedures
- product offerings by business line
- internal management information system (MIS) reports and compliance and fair lending risk assessments
- compliance testing reports and internal or external audit reports, including the status of corrective actions
- consumer complaint information
- training reports and attendance records
- public filings and annual reports, if applicable
- consumer protection-related litigation and/or investigations by other governmental or regulatory agencies
- information from news outlets and consumer groups
- the institution's website, along with social media

Other Institution Data

- Uniform Bank and Performance Reports (UBPR) and Consolidated Reports of Condition and Income (Call Report)
- market and community demographic data
- Home Mortgage Disclosure Act (HMDA) and CRA data
- electronic loan data

Reserve Bank or Federal Reserve System Information

- current institutional profile, if applicable
- information obtained during ongoing supervision activities or through direct observations, questionnaires, interviews, meetings with management, and/or Reserve Bank correspondence
- supervisory plan and institutional overview developed by Safety & Soundness
- examination reports from other disciplines and/or other agencies
- previous compliance examinations and target reviews, including work papers
- CRA Performance Evaluations
- prior corrective action information, institution responses, and resolution or status information
- applicable risk screening information, including any fair lending screening results
- complaint and correspondence files
- applications and enforcement information
- regulatory and examination procedure updates

Examiners need to contact institution management to develop and maintain an understanding of the institution and the market(s) in which it operates.

Such contact typically involves a specific information request that provides the opportunity to learn about any changes that would affect the profile. These changes might include changes in management personnel, organizational structure, or the institution's strategic direction, including any new products, markets, or delivery channels the institution has introduced or entered or is considering introducing or entering.

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. The profile must draw sufficient attention to key areas and/or changes that contribute to the institution's current and prospective level of consumer compliance risk.

Preparation of the Institutional Profile

The purpose of the institutional profile is to convey an understanding of the institution's present condition and its current and prospective risks, as well as to highlight key issues and supervisory findings. The profile must be updated as part of the risk assessment and scoping process of an examination, again at the conclusion of an examination, and later through ongoing supervision to capture matters of supervisory significance that occur during the supervisory cycle.

The institutional profile must reflect the material events, products, and services and the regulatory environment that affect management decisions. For instance, when introducing a new product or service, senior management should

- conduct proper due diligence
- assess implications of the product's target markets
- evaluate prospective product growth
- consider the product's regulatory implications
- ensure the institution has sufficient staff expertise and capacity to support and deliver the product or service

Institutional Factors

- Organizational Structure
  - *Ownership.* Whether the institution is owned by a bank holding company, and any functions that are centralized at or supported by the holding company.
  - *Operations.* The degree of operational centralization or decentralization.
  - *Affiliates and subsidiaries.* Identification of affiliate structure and/or subsidiaries with activities relevant to the institution's consumer compliance risk.
  - *Structural changes.* Any significant structural changes since the previous examination, or planned changes, such as mergers, acquisitions, divestitures, and pending applications, that would affect the institution's consumer activities.
- Business Model and Strategies
  - *Risk tolerance.* A summary of the scope and complexity of the institution's business model based on consideration of key attributes discussed below, especially in light of the implementation of decisions that change strategy.
  - *Key business lines.* Identification of key business activities along with the stability of the offerings. The identification of key business lines should include an evaluation of management's description of key business areas in comparison to the institution's stated strategy, balance sheet composition, and other publicly available information.
  - *Delivery channels.* Identification of primary delivery channels for the institution's products and services and any nontraditional or complex channels. Consideration should be given to the use of the Internet, mobile applications, social media, brokers, referral sources, and expansion into new or extended channels, especially those that have changed since the previous examination.
  - *Product mix.* A discussion of loan and deposit product mix, as well as the types of products and services offered, considering the level of complexity present in the offerings and the potential for consumer harm associated with the product. Consideration should be given to concerns about consumer protection risk that have been raised by legislative bodies, regulatory/law enforcement agencies, or consumer advocacy groups. To the degree that products or services differ based on targeted customers or geographies, the discussion should identify the variations.
  - *Product and service changes.* Identification of any new or modified products or services, particularly any add-on products or other products with complex features that would increase inherent risk or raise potential for consumer harm, and the level of management expertise and familiarity with the new or modified product or service.
  - *Marketing.* A discussion of marketing strate-

gies, including desired outcomes and an evaluation of targeted products, media outlets, and targeted geographies or customers.

  - *Product volatility.* A discussion of material changes in the institution's asset size, markets, and volume associated with specific products or services. Examiners should pay attention to instances in which volume has significantly increased, which may reflect a change in business strategy or increased risk. Product volume that remains constant may suggest a stable environment, while reductions in volume may point to lower levels of risk. Examiners should select appropriate time intervals for measuring change.
  - *Systems.* A discussion of the capacity of delivery systems as well as consideration of the degree of change due to conversions to new systems or enhancements, including identification of the use of third-party providers or vendors.

- Compliance Management Structure and Personnel
  - *Organizational chart.* A discussion of the compliance function, risk function, and business lines, as applicable. Consideration should be given to the level of independence of functions responsible for compliance oversight and the sufficiency of staffing, including the expertise in relation to the products and services offered.
  - *Committees.* Discussions about board and management committees responsible for compliance risk management.
  - *Hiring, turnover, and succession planning.* A discussion of changes in management (including the board and senior management), compliance, or business line levels that could affect the institution's ability to manage consumer compliance risk.
  - *New product development.* A discussion of any procedures, marketing reviews, and change control processes associated with new product development, including vendor management and the level of involvement of staff who have compliance expertise.
  - *Compliance testing and audit.* A discussion of the coverage and frequency of reviews; the qualifications of staff, whether internal or external; the process for reporting on issues and their resolution; and whether or not there have been any internal review or audit findings of consumer compliance violations or concerns, and if so, a description of the findings and management's response.

- Supervisory Information
  - *Supervisory history.* A description of the recent supervisory history of the institution.
  - *Corrective action.* The status of corrective action for any significant regulatory issues such as Matters Requiring Immediate Attention (MRIA), Matters Requiring Attention (MRA), reimbursements, previously identified consumer risk issues, and any supervisory orders involving civil money penalties.
  - *Areas of concern.* Significant consumer compliance or CRA supervisory issues or concerns and other important supervisory issues.
  - *Enforcement actions.* Identification of any formal or informal actions and the potential impact on consumer compliance risk.
  - *Financial condition.* A discussion of the institution's financial condition, considering its impact on management decisions that would affect the institution's compliance risk tolerance. A discussion of whether the institution is changing or considering changing its products and services based upon the institution's financial condition, including the effect of these changes on compliance controls. Consideration should also be given to the institution's expansion or contraction of markets and geographies.
  - *Other supervisory ratings.* A summary of management and risk management ratings for all supervisory functions that could affect consumer compliance risk.
  - *Complaints.* Any pertinent consumer complaint activity, including a discussion about the quantity and types of complaints and how the institution has resolved them.
  - *Litigation.* Any substantive litigation or other legal concerns, specific to the institution, related to consumer compliance issues, including investigations by other governmental agencies.

Legal and Regulatory Factors

- *Applicability and coverage.* Identification of the level of regulatory complexity, key legal or regulatory developments, and changes that are material and affect the institution, given the institution's product offerings and operations.
- *Litigation.* Consumer compliance-related substantive litigation, other legal concerns, or regulatory

scrutiny in the industry that would potentially relate to the institution's products, services, or practices.

Environmental Factors

- *Market/trade area.* A description of geographic areas or markets served by the institution. The description should include the institution's delineated CRA assessment area and how it compares with its market/trade area, if they are different. The description should also include the identification of areas served and not served, considering minority composition, distressed or underserved areas, and low- and moderate-income individuals and areas.
- *Offices and facilities.* A discussion of the institution's branches, automated teller machines (ATM), and loan production offices (LPO), as applicable, in relation to consumer compliance risk, such as demographic differences across areas served and the degree to which products or services vary by location.
- *Interstate/intrastate structure.* A statement as to whether the institution is an interstate bank, and a listing of the states, metropolitan areas, and Federal Reserve Districts in which it operates.
- *Business conditions.* A discussion of the demand for loans and other products or services in light of employment conditions, housing data, business demographics, local economic conditions, and other demographic considerations.
- *Competition.* A discussion of competition based on market share, including deposit market share, HMDA-reportable activity, and other relevant data sources. The discussion should reflect an evaluation of the level of competition from local and national financial institutions as well as nonbank competitors. The discussion should be adjusted to capture the degree to which competition varies by product or geography.

III. ASSESSING THE INSTITUTION'S RISK

Overview

The institutional profile provides information about the institution's strategy and business activities and the environment in which it operates. The profile also documents the institution's processes for controlling associated risks. Thus, the profile serves as the primary source of information for developing the risk assessment, a vital part of the supervisory process.

The risk assessment presents a comprehensive view of the institution, delineating the areas of supervisory concern, and serves as a platform for the supervisory plan. Inherent risk considers the likelihood and impact of noncompliance with consumer laws and regulations prior to considering any mitigating effects of risk management processes. Risk management and controls are evaluated in the context of their likely effectiveness in achieving compliance with laws and regulations. Residual risk is determined by balancing the overall level of inherent risk of an activity (product or service) with the overall strength of risk controls for that activity.

The risk assessment considers the effectiveness of an institution's overall compliance management program, including four essential elements:

1. board and senior management oversight
2. policies, procedures, and limits
3. risk monitoring and management information systems
4. internal controls

While the risk assessment process evaluates an institution's compliance management program as a whole, the process also evaluates the effectiveness of the institution's compliance risk controls for individual products, services, and business activities. In particular, the levels of inherent consumer compliance risk present in the institution's products, services, and business activities affect the types of risk controls necessary to ensure satisfactory compliance with consumer protection laws and regulations.

Objectives of the Risk Assessment

The goal of the risk assessment is to allow supervisory staff to establish reasonable, but not absolute, assurance that material residual consumer compliance risks are identified. The risk assessment can then be relied upon as the determinant of the scope of examination activities. As a result, examination resources will be focused on areas of elevated residual risk and not on those areas where inherent risk is well controlled and residual risk is limited or low.

Risk Assessment Process

The risk assessment process requires examiners to determine: (1) products, services, and activities that are considered material to the organization; (2) the level of inherent risk associated with these products, services, and activities; (3) the adequacy of management systems used to measure, monitor, and control associated risks; and (4) the residual consumer compliance risk associated with each

material product, service, and activity, as well as for the institution overall, based on the level of inherent risk and the adequacy of risk controls.

Instructions for completing the risk assessment process, including documenting conclusions about inherent risk, controls, and residual risk, are provided in section F of this chapter, Documenting the Consumer Compliance Risk Assessment.

A. Product Management and Materiality

Overview

Product management relates to the institution's ability to identify, measure, monitor, and manage the compliance risk inherent in a particular product. These four essential elements of risk management serve as the foundation for assessing the management of product risk and should be evaluated in the context of the inherent risks associated with specific products or services. Essential factors to consider when evaluating the management of products and services include: (1) knowledge and expertise of the product management team; (2) adequacy of policies and procedures and effectiveness of internal controls; (3) adequacy of resources (for example, staffing, MIS); (4) quality of compliance training; (5) frequency and scope of compliance reviews; (6) recent compliance history (for example, violations noted at prior examinations and recent audit findings); (7) record of responding appropriately to consumer complaints; (8) effectiveness of audit coverage and management's responsiveness to audit findings; and (9) change management (for example, response to changes in laws, regulations, systems, and products).

Product Definition

A product may consist of a group of related products or services that

- share similar features and structure, with differences that are relatively minor (such as different maturities)
- are broadly subject to the same regulations (even if there is a range of risk profiles among the related products)
- are delivered in substantially the same way (for instance, retail loan originations may be treated as a different product than wholesale originations)
- are subject to the same control environment (for example, similar products offered through different legal entities, but having the same control environment, could be considered a single product)

As an example, assume that an institution extends retail mortgages, from simple fixed-rate mortgages to more complex adjustable-rate mortgages, and all retail mortgages share a common consumer compliance control environment. Notwithstanding the range of complexity of the related products, the residual risk of all mortgage loans could be evaluated as a single product; the residual risk would balance the range of inherent risks across all of the related products and the effectiveness of risk controls in the context of the identified inherent risks.

Materiality

Product materiality reflects the relative importance of a product offered by the institution. A product may be material compared to other products; it may also be material based solely on its own significant activity level. Accordingly, a product with low volume (measured by number, dollar volume, or both) compared to other products would likely be considered immaterial, and a product with relatively high volume would be considered material. Nonetheless, a product could be material based solely on its own substantial activity level even if that activity level is comparatively lower than other products' activity levels.

Examination intensity and resources should be commensurate with the consumer compliance risks associated with the institution's material products. Thus, if an institution's material products do not involve significant potential consumer compliance risk, the institution would warrant relatively fewer examination resources, compared to an institution where the products offered pose significant consumer risk. In other words, the absolute risk associated with a product should be considered as well as the risk of a product relative to the other products offered. For example, if an institution is primarily a commercial lender, examiners should not shift increased scrutiny and resources to the review of immaterial consumer products or consumer products that have low residual risk simply because these may have higher consumer risk compared to commercial loans.

An institution's board of directors and management must demonstrate both the willingness and the capacity to comply with all applicable consumer compliance laws and regulations, even in the case of immaterial products. Evidence of willingness and capacity can typically be established by reviewing meeting minutes and policies and procedures and through interviews. Without such evidence, the examination should focus on the assessment of weaknesses in the compliance management program and the changes necessary to ensure and sustain compliance.

Materiality is also a factor to consider when grouping products. In particular,

- when a related product is both complex and material on a stand-alone basis, examiners should consider[2]
  - keeping the same product grouping but focusing on the complex and material products when making scoping decisions, taking into consideration the strength of risk controls
  - segregating these related products, but only when there are questions regarding the quality or capacity of the control environment for such a related product
- add-on or ancillary products or services, when material, may present unique risks or be subject to a different control environment and warrant treatment as a separate product. For example, loan servicing, especially servicing of third-party loans, may be treated as a separate and distinct product.

B. Inherent Consumer Compliance Risk

Overview

Inherent consumer compliance risk is the risk associated with product and service offerings, practices, or other activities that could result in significant consumer harm or contribute to an institution's noncompliance with consumer protection laws and regulations. It is the risk these activities pose absent controls or other mitigating factors. Such risk may be associated with the characteristics of the institution itself, the laws and regulations that apply to its activities, or the environment and market(s) in which it operates. It is important for an institution to effectively identify, measure, monitor, and control its compliance risks to limit any potential adverse consequences of noncompliance.

Consumer compliance risk, in general, is the risk of legal or regulatory sanctions, financial loss, or consumer harm caused by a failure to comply with or adhere to

- consumer protection laws, regulations, or standards
- the organization's own policies, procedures, codes of conduct, and ethical standards
- principles of integrity and fair dealing applicable to the organization's business activities and functions[3]

An institution's failure to manage compliance risk effectively can elevate the risk level or manifest itself as other types of key risks:

- *Legal risk.* Arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a banking organization. For example, failing to follow the terms of consumer loan agreements or to meet strict residential mortgage regulatory requirements will likely increase an institution's legal risk.
- *Operational risk.* Arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected losses. Operational lapses, such as failing to keep confidential customer data secure, could result in losses for both the institution and its customers.

More specifically, noncompliance may expose the organization to fines; civil money penalties; legal damages; voided or unenforceable contracts; reduced franchise value; or rejected expansionary activities, mergers, and acquisitions.

Risk Tolerance

An institution's tolerance for consumer compliance risk is reflected in the choices it makes regarding the scope and complexity of its business activities, including market service areas and the delivery channels for products and services. Institutions that engage in riskier activities demonstrate a higher tolerance for risk and are expected to have a compliance management program commensurate with their risk profile. A higher risk tolerance may be reflected in product offerings that pose greater compliance risk, such as higher-cost products or products targeted to vulnerable or less financially sophisticated consumers. In general, the more willing an institution is to assume inherent compliance risk in its operations, the stronger the controls must be to manage these risks effectively.

Inherent Risk Components and Drivers

A number of factors serve as potential indicators of inherent compliance risk in an institution. All of these factors can also increase legal and operational risk, especially when not managed effectively. In general, inherent compliance risk factors can be grouped into three primary categories: institutional, legal and regulatory, and environmental.

2. A related product would be a single product or service under a more broadly defined product category. For instance, reverse mortgages would be a related product under the broader category of mortgage loans.

3. Business activities are business lines, functions, legal entities, operations in legal jurisdictions, or other business operations.

Institutional Factors

Institutional factors contribute significantly to an institution's overall inherent compliance risk level. Some risk factors derive from the institution's strategic and business decisions; others relate more specifically to the products the institution offers and the risks inherent in these products.

These institutional factors, when considered in conjunction with the extent to which the institution's operations are subject to consumer laws and regulations, will be a significant driver of conclusions about the level of inherent risk. Complex products, decentralized operations, products targeted to vulnerable or less financially sophisticated consumers, failure to serve certain consumer or geographic segments of the market, introduction of substantively new products (rather than slight variations of existing products), multiple delivery channels, and third-party relationships all tend to elevate the level of consumer compliance risk.

Strategic/Business Factors

- *Growth.* Any substantive increase in asset size, change in business focus, or expanded market or geographic presence (resulting from branching, merger, or acquisition activity) may increase compliance risk given the need to manage risk across a larger operation, including additional office locations. Growth may increase risk because an organization may need to respond by changing processes, staffing, or systems. These types of changes often require expanded compliance oversight and knowledge, and may increase compliance risk if not effectively managed.
- *Structural complexity.* The overall complexity of a banking organization's operations, including its branch operations and subsidiary and affiliated relationships, affects compliance risk.

  An institution with an extensive branch network, multiple or nontraditional delivery channels, or a number of subsidiary retail business operations may have more compliance risk to manage than an institution with limited offices or one primary business operation.

  The degree to which an organization, including its related entities, has centralized operations also affects compliance risk. Centralized activities may help limit risk by consolidating knowledge and processes in fewer locations. When centralized operations are handled effectively, the opportunity for error may decrease as a result.

  In general, increased structural complexity and decentralization within an institution tend to increase compliance risk, primarily because the institution has more facilities, staff, products, and overall operations to manage, thus introducing challenges associated with span of control.
- *History/trends.* Whether an institution has effectively managed its compliance risk in the past is a risk factor to consider. Institutions that historically have supported and maintained strong compliance management programs will generally have less risk than institutions that have not exhibited such performance. The significance of this prior performance varies depending on the amount and type of change in an institution's compliance management program and changes to its overall inherent compliance risk profile due to other factors, such as product or regulatory changes, since the previous examination.

Product Characteristics

- *Product volume.* The absolute level of product activity or materiality affects compliance risk. When an institution does not comply with requirements on a high-volume product or service, this error affects more consumers and thus creates more compliance risk for the institution. As with other inherent risk factors, the significance of risk associated with high-volume products depends on the consequences that may result from noncompliance.
- *Product complexity.* As with the institution itself, complexity within products or groups of products significantly affects compliance risk. Several factors affect the complexity of a product, such as
  - the complexity of the product's features, such as numerous conditional requirements, options, or variations
  - over the life cycle of the product, changes are permitted or required that necessitate additional disclosures and/or actions by the institution to comply with legal or regulatory requirements
  - the product targets only certain consumer segments, such as those with certain demographic or credit characteristics (for instance, subprime borrowers), rather than all consumers
  - the complexity of processes surrounding the sale of products, including marketing of specific product features, use of wholesale and retail delivery channels, and the sale of ancillary products or offering of rewards programs

Generally, as the complexity of the product increases, compliance risk may increase because of the need for additional oversight and expertise to manage this increased complexity effectively. Complying with even comparatively noncomplex legal or regulatory requirements may be more challeng-

ing when the product itself has inherent operational complexity. Increased complexity can also be associated with products targeted to a particular segment of the consumer market. Inherent compliance risk may be elevated if marketing efforts, disclosures, and delivery channels do not appropriately consider the sophistication and reasonable expectations of the target audience.

- *Product stability.* Substantial change related to product or service offerings, including changes to existing products and services, is a significant driver of inherent compliance risk. Factors to consider in assessing the compliance risk associated with a product's stability include
  - the length of time the institution has offered the product
  - what, if any, significant product terms have changed
  - whether product volume has grown significantly
  - any significant changes related to product operations, including system changes that would affect product handling or management

Product-related changes may increase compliance risk, primarily because an institution must evaluate these changes to determine whether other corresponding processes or practices need to change to ensure ongoing compliance. A more stable product (one with limited changes and a history of compliance) has a higher likelihood of continued compliance. It should be noted that some changes could lower compliance risk—for example, when an institution eliminates a higher-risk feature.

- *Third-party involvement.* An institution's reliance on third-party providers or vendors may either increase or decrease compliance risk. In all cases, the use of third-party providers requires sufficient controls to manage the relationships. When properly chosen and managed, third-party providers can provide an institution with valuable expertise and service that the institution may find difficult to provide on its own. For example, using a third party to generate loan documents may facilitate consistent delivery of compliant disclosures. Nonetheless, relying on a third party to (1) provide bank-related products or services, such as a loan processing system; (2) generate fee income, such as offering add-on products; (3) assist with compliance management-related services, such as conducting compliance audits; or (4) provide other compliance-related services may increase risk because the institution no longer has direct control over these activities. Accordingly, the institution must have knowledgeable staff and effective processes to oversee these providers to ensure they meet expectations and contractual obligations and comply with legal and regulatory requirements.

Legal and Regulatory Factors

Another primary consideration for determining an institution's inherent compliance risk relates to the types of legal and regulatory requirements that apply to the institution's products and services. Institutions should also evaluate concerns raised by others, including legislative bodies, regulatory or law enforcement agencies, or consumer advocacy groups. The extent of inherent compliance risk related to legal and regulatory requirements is driven primarily by the complexity of the requirements themselves, the level and likelihood of potential consumer harm or other penalties that could result from failing to comply with them, and the extent to which these requirements have changed.

- *Regulation complexity.* The complexity of regulatory and legal requirements relates to the extent of judgment, knowledge, technical skills, or processes needed to understand and effectively implement those requirements. As with product complexity, the increased skill and knowledge needed to comply with more complex regulatory requirements increases inherent compliance risk. Simply put, as regulatory complexity increases, so does the risk that the institution will fail to comply with the requirements.
- *Consequences of noncompliance.* Failure to comply with certain legal and regulatory requirements may have serious consequences for consumers and the financial institution. It is important to consider whether and to what extent failing to comply with the requirement would result in financial, legal, or other harm to consumers. For the institution, failing to comply with regulatory requirements can lead to regulatory sanctions and financial losses. In general, the severity of the consequence, whether harm to consumers or to the institution, and the level of inherent compliance risk associated with noncompliance are directly related.
- *Regulatory or legal changes.* Inherent compliance risk may increase when a new or modified legal or regulatory requirement applies to a financial institution's activities. The effect of any change on inherent risk depends on several factors, which may include
  - the nature and type of the regulatory change
  - the significance of the change relative to the institution's product offerings, processes, or procedures, including
    - the number of products affected
    - whether the change needs to be imple-

mented organizationwide or just in particular business lines

- whether the change has serious consequences for failure to implement and comply effectively
- whether the organization has the expertise to understand and implement the change effectively

When regulations and laws change, an institution may not fully understand the change and hence may fail to implement effective policies, procedures and controls in response, increasing the risk of noncompliance with the new requirement. As discussed, the level of inherent risk posed by any regulatory change depends on the nature of the change and its effect on consumers and the institution.

Environmental Factors

The environment in which the institution operates can affect the level of inherent compliance risk at the institution level and at the product level. Business conditions, the demographic composition of its assessment area(s), and the competition in the institution's markets affect compliance risk.

- *Business conditions.* Market conditions, such as the demand for loans, availability of talent and expertise, unemployment rates, and housing needs, may affect decisions that the institution makes concerning the types and nature of products it offers as well as its capacity to adequately support these products. Consequently, changing business conditions may require an institution to reevaluate its current assumptions and practices. The capacity of an institution's new product approval processes, its change management practices, the robustness of its strategic planning, and the flexibility of its service capacity should be evaluated in the context of the institution's response to changing business conditions. For example, deteriorating business conditions can simultaneously lead to tightening of underwriting standards and a higher default rate on existing loans. Compliance risk potentially increases in both cases, as consistency in underwriting and service levels associated with loss mitigation must be maintained.

  Business conditions may also drive changes to existing products, or the introduction of new products, designed to generate revenue. Institutions operating in communities experiencing economic challenges may have higher inherent risk because of the effect of these challenges on the institution's existing activities or because of actions the institution may take in response to these challenges.
- *Demographics.* The demographics of the institution's market area can also affect inherent compliance risk. Serving a more diverse population requires heightened awareness and responsiveness to ensure that the institution is meeting a potentially broader spectrum of customer needs through its product offerings, marketing efforts, and overall level of service. Without a legitimate business justification, ignoring the needs of certain segments of the population or excluding geographic areas or populations based on demographic composition will likely have adverse consequences for an institution.
- *Competition.* The competitive environment in which an institution operates can affect compliance risk. An institution operating in a highly competitive environment may choose to make frequent product, marketing, or other changes to retain or expand its market share. Competitive factors could also lead an institution to consider offering complex products that fall outside the institution's normal operations or its strategic focus. As with the risks associated with external business conditions, the capacity of an institution's new product approval processes, its change management practices, and the robustness of its strategic planning must be commensurate with the degree or rapidity of change associated with competitive demands. Institutions that operate in a highly competitive environment, particularly smaller institutions, may have greater inherent risk simply because they do not have the capacity to respond effectively to competitive forces.

Assessing Inherent Risk

A variety of factors affect the level of inherent compliance risk in an institution. Effectively identifying and assessing this risk is an important part of the risk-focused examination process.

The institutional profile discusses information about the institution and its community(ies) that is needed to determine the impact of institutional, legal, and environmental factors on the institution's consumer compliance risk level. Considering these factors, examiners will form conclusions about the level of inherent risk for each material product relative to the consumer laws and regulations applicable to such products, as is discussed in more detail later. Taking into account these product assessments, examiners will assign an aggregate inherent risk rating for the institution.

Appendix 2, Guidance for Assessing Inherent Consumer Compliance Risk, is a matrix that should be used when assessing inherent consumer compliance risk. The matrix identifies specific risk components for each of the three broad sources of

risk discussed previously (institutional, laws and regulations, and environmental). While an overall inherent risk rating must be documented only for each material product, the matrix allows for analyzing the potential level of risk associated with each source of risk as well as each of the subsidiary risk components that are detailed in the matrix. Examiners may find that for certain institutions or activities, it makes sense to assign ratings to individual subsidiary risk components first and then work to develop the overall ratings. This level of detail is likely necessary only for larger or more complex organizations and should be reflected in supporting documentation maintained separately from the assessment itself.

Inherent risk should be rated using a five-point rating system.

Inherent Risk Rating
Low (1)
Limited (2)
Moderate (3)
Considerable (4)
High (5)

The following definitions apply to inherent *consumer* compliance risk.

- *Low likelihood of significant negative impact (1)* indicates that consumer compliance risk, prior to considering any mitigating effects of risk management processes, is highly unlikely to have a significant negative impact on the institution or consumers. Expected sanctions or losses due to consumer compliance risk would have little negative impact on the institution.
- *Limited likelihood of significant negative impact (2)* indicates a limited likelihood that consumer compliance risk, prior to considering any mitigating effects of risk management processes, will have a significant negative impact on the institution or consumers. Expected sanctions or losses due to consumer compliance risk are modest and could be absorbed by the institution in the normal course of business.
- *Moderate likelihood of significant negative impact (3)* indicates a moderate likelihood that consumer compliance risk, prior to considering any mitigating effects of risk management processes, will have a significant negative impact on the institution or consumers. Expected sanctions or losses due to consumer compliance risk could adversely affect the institution.
- *Considerable likelihood of significant negative impact (4)* indicates a considerable likelihood that consumer compliance risk, prior to considering any mitigating effects of risk management processes, will have a significant negative impact on the institution or consumers. Expected sanctions or losses due to consumer compliance risk could seriously affect the institution.
- *High likelihood of significant negative impact (5)* indicates a high likelihood that consumer compliance risk, prior to considering any mitigating effects of risk management processes, will have a significant negative impact on the institution or consumers. Expected sanctions or losses due to consumer compliance risk will require significant changes to the management routines and ongoing operations of the institution.

C. Consumer Compliance Risk Management

Overview

Taking and managing risks are fundamental to the business of banking. Accordingly, the Federal Reserve has increasingly emphasized the importance of sound risk-control processes when evaluating the activities of the institutions it supervises. Properly managing risks is critical to ensuring compliance with consumer protection laws and regulations. Effective risk management has become even more important as new technologies, product innovation, and the size and speed of financial transactions have changed the nature of financial services markets. Therefore, it is essential that examiners give significant weight to how effectively the institution's compliance management program manages the inherent risks associated with its consumer-related activities.

An institution's failure to establish a consumer compliance management structure that adequately identifies, measures, monitors, and controls the inherent risks involved in its various products, services, and lines of business is considered unsafe and unsound conduct. Principles of sound risk management should apply to the entire spectrum of compliance-related risks facing a banking organization including, but not limited to, legal and operational risk.

A primary goal of the supervision process is to assess the effectiveness of an institution's compliance management program. Identified violations of consumer protection laws and regulations usually indicate weaknesses in this program. The seriousness of the weaknesses, however, depends on the consequences that result from noncompliance. For example, a substantive violation of a fair lending law or regulation has serious consequences for

consumers and the institution and thus would likely indicate a serious compliance management weakness.

When an error resulting in a violation is identified, the significance of the error must be evaluated not simply by the number of such errors or the percentage of error but in the context of the root cause of the error and actual harm to consumers. The root cause of an error must always be evaluated to determine whether such errors are the result of a systemic control weakness. When systemic issues are identified, the underlying root cause must be addressed. Also, correction of the root cause of an isolated error should be considered if the likelihood of avoiding repeat errors can reasonably be accomplished through modification of business processes and/or by strengthening elements of the compliance management program.

Elements of Risk Management

Elements of a sound risk management system include

- active board and senior management oversight
- adequate policies, procedures, and limits
- adequate risk monitoring and management information systems
- comprehensive internal controls

Each of these elements is described more fully below, along with a list of factors relevant to assessing the adequacy of that element.

Examiners should recognize that the factors specified in these guidelines are intended only to assist in the evaluation of risk management practices and are not intended as a checklist or exhaustive list of requirements for each institution. A carefully devised, implemented, and monitored program provides the foundation for ensuring compliance with consumer banking laws and regulations. All institutions, regardless of size, should maintain an effective compliance management program. The sophistication and formality of the program will typically increase in direct proportion to the complexity of an organization's operations. Examiners should evaluate the adequacy of the compliance management program in the context of inherent risk associated with the institution's complexity, business strategy, activities, and organizational structure. The duties, responsibilities, authority, and independence of compliance personnel will depend on the nature, scope, and complexity of operations.

For smaller institutions that engage solely in traditional banking activities and whose senior managers and directors are actively involved in day-to-day operations, relatively basic risk management systems may be adequate. In such institutions, these systems may consist of an informal compliance program that includes both written and unwritten policies addressing material areas of operations such as lending, basic internal control systems, on-the-job training, and a limited set of management and board reports.

A larger, more complex institution would likely require a more formal and comprehensive program to maintain a satisfactory level of compliance and to provide senior managers and directors with the information they need to monitor and direct day-to-day activities. Because of the diversity of activities and/or the broad geographic dispersion of operations, the compliance risk management processes of more complex banking organizations would typically include

- dedicated compliance staff with specific responsibilities and authority
- detailed policies that set specific prudential limits on acceptable activities and/or the risks associated with specific activities
- sophisticated management reporting to allow senior management to better evaluate and mitigate risks

These reporting systems, in turn, should provide an array of reports that offer sufficient risk-exposure information that is relevant to the duties and responsibilities of individual managers and directors.

For more complex institutions, these reporting systems will naturally require frequent monitoring and testing by independent control areas and internal auditors to ensure the integrity of the information used by senior officials in overseeing compliance with consumer protection laws and regulations. The risk management systems or units of such institutions must also be sufficiently independent of the business lines, in order to ensure adequate separation of duties and avoid conflicts of interest.

Regardless of the size of the institution, an effective process must be in place to manage change. Sometimes change occurs because of an external event, for example, a new compliance regulation. Sometimes change is internal, such as the introduction of a new product, or revision to existing products. Change management should be a structured and disciplined process that is repeatable since change can always be expected. An effective change management process

- requires management and staff from all affected functions—potentially including compliance, accounting, risk, internal audit, and line management—to review and recommend a response or change proposal for senior man-

agement or board approval that clearly articulates expected results. The entire life cycle of a product or service affected by the change must be considered, whether it involves the introduction of a new product or service or a change affecting existing bank operations.

- incorporates appropriate approval processes associated with implementation.
- requires that operating policies and procedures are updated to provide clear guidance to staff on how to comply with all legal or regulatory requirements
- requires that staff be properly trained regarding the change
- incorporates monitoring of the deployment of the new or revised process, product, or service
- requires a post-implementation review to determine whether the actions taken have achieved the expected results

Also, it is important to recognize that while management can appropriately decide to outsource some or all of the operational aspects of a product or service, it cannot outsource the responsibility for complying with laws and regulations. Oversight of vendor actions is particularly important when such actions involve changes to core processing, automated disclosure software, and similar systems, because violations may occur from such changes if not monitored properly. A robust third-party vendor management and oversight process will evaluate all applicable risks, including those related to information security, privacy, and compliance with all applicable laws and regulations.

Board and Senior Management Oversight

Boards of directors have ultimate responsibility for the level of risk assumed by their institutions. Accordingly, the board should approve the institution's overall business strategies and significant policies, including those related to managing and taking risks. The board should also ensure that senior management is fully capable of managing the institution's activities. While all boards of directors are responsible for understanding the nature of the risks significant to their organizations and for ensuring that management is taking the steps necessary to control these risks, the level of technical knowledge required of directors may vary depending on the particular circumstances at the institution.

For institutions with a broad range of technically complex activities, directors must have a clear understanding of the types of risks to which the institution is exposed, even though the board has delegated day-to-day compliance management responsibility to bank officers and staff. For example, the directors of complex institutions should receive reports that identify the size and significance of the risks in terms that are meaningful to them. In fulfilling its risk oversight responsibility, the board of directors should take steps to develop an appropriate understanding of the risks the institution faces—for example, through briefings from auditors and experts external to the organization. Using this knowledge and information, the board of directors should provide clear guidance regarding the level of risk acceptable to the institution and should ensure that senior management implements the procedures and controls necessary to comply with the policies that have been adopted.

Directors of institutions that offer more traditional and less complex products may be more involved with the institution's day-to-day activities and decisionmaking than counterparts at larger organizations. Each director should then have a level of knowledge commensurate with the nature of his or her role in managing the institution's affairs. Nonetheless, senior management is responsible for implementing a program to manage the consumer compliance risks associated with the institution's business model, including ensuring compliance with laws and regulations on both a long-term and a day-to-day basis. Accordingly, management should be fully involved in its institution's activities and possess sufficient knowledge of all major products to ensure that appropriate risk controls are in place and that accountability and lines of authority are clearly delineated. Senior management also is responsible for establishing and communicating a strong awareness of, and need for, effective risk controls and high ethical standards.

In assessing the quality of board of directors and senior management oversight, examiners should consider whether the institution follows policies and practices such as those described below.

- The board and senior management have identified and have established a clear understanding of the types of risks inherent in the institution's activities and make appropriate efforts to stay informed about these risks as financial markets, risk management practices, and the institution's activities evolve.
- The board has reviewed and approved appropriate policies to limit risks inherent in the institution's significant business lines, activities, or products, including ensuring effective oversight of any third-party providers that provide products and services for the institution.
- The board and senior management are sufficiently familiar with and are using adequate

record keeping and reporting systems to measure and monitor the major sources of risk to the institution.

- The board periodically reviews and approves risk exposure limits to conform to any changes in the institution's strategies, addresses new products, and responds to changes in market conditions.
- The board and senior management ensure that businesses lines are managed and staffed by personnel with knowledge, experience, and expertise consistent with the nature and scope of the banking organization's activities.
- The board and senior management ensure that the depth of staff resources is sufficient to operate and manage the institution's activities soundly and that employees have the integrity, ethical values, and competence that are consistent with a prudent management philosophy and operating style.
- The board and senior management at all levels provide adequate supervision of the day-to-day activities of officers and employees, including management supervision of senior officers or heads of business lines.
- The board and management anticipate and respond to risks that may arise from changes in the institution's competitive environment and innovations in its markets and to risks associated with new or changing regulatory or legal requirements.
- Before embarking on new activities or introducing products new to the institution, management identifies and reviews all risks associated with the activity or product and ensures that the infrastructure and internal controls necessary to manage the related risks are in place.

Policies, Procedures, and Limits

Comprehensive and fully implemented policies help to communicate management's commitment and expectations related to compliance. Procedures should provide personnel with guidance that enables them to complete transactions or other processes in accordance with applicable laws and regulations. Such information may include appropriate regulatory references and definitions, sample forms, instructions, and where appropriate, directions for routing, reviewing, and retaining transaction documents. The effectiveness of the procedures in meeting compliance requirements is more important than the degree of formality. However, larger, more complex entities with many employees and products, serving multiple geographic markets, have a greater need for written policies and procedures to ensure compliance with consumer protection laws and regulations.

An institution's directors and senior management should tailor risk management policies and procedures to the types of risks that arise from the institution's activities. Once the risks are properly identified, the institution's policies and its more fully articulated procedures provide detailed guidance for the day-to-day implementation of broad business strategies and generally include limits designed to shield the organization from excessive and imprudent risks. All banking organizations should have policies and procedures that address significant activities and risks; however, the scope and depth of such policies will vary among institutions. A smaller, less complex institution that has effective management heavily involved in day-to-day operations may have less formal policies to address significant areas of operations, but nonetheless, have well-established embedded practices that have proven effective over time for managing consumer compliance risk. In a larger institution, where senior managers rely on large staffs to implement strategies in business lines of varying complexity, much more detailed policies and related procedures would generally be expected. In either case, however, management is expected to ensure that policies and procedures, written or unwritten, address an institution's material areas of risk and that staff modifies these procedures when necessary in order to respond to significant changes in the banking organization's activities or business conditions.

Limits are mechanisms designed to prevent an institution from taking unnecessary risks that increase the likelihood of consumer harm, and they should be present and enforced in an institution. An example of a limit is an explicit statement about products or services that the institution deems to be harmful to consumers or contrary to the institution's mission and that the institution chooses not to offer. On a narrower scale, an institution may specifically limit the ability of lending personnel to deviate from established loan pricing guidelines without appropriate approval.

Ongoing education of personnel is essential to maintaining a sound compliance program. The organization should make all personnel aware of consumer protection laws and regulations pertinent to their areas of responsibility and should provide training regarding policies and procedures for those areas.

An institution's training program should be commensurate with the entity's organizational structure and the activities in which it engages. A more formal training program would be expected at an organization that offers complex products or services or operates in multiple or large markets. For

organizations with limited staff turnover and non-complex product offerings, a less formal training program would likely be sufficient.

The following guidelines should assist examiners in evaluating the adequacy of an institution's policies, procedures, and limits:

- The institution's policies, procedures, and limits provide for adequate identification, measurement, monitoring, and control of the risks posed by its activities.
- The policies, procedures, and limits are consistent with the institution's stated goals and objectives.
- Policies clearly delineate accountability and lines of authority across the institution's activities.
- Policies provide for the review of activities new to the financial institution to ensure that the infrastructures necessary to identify, measure, monitor, and control risks associated with an activity are in place before the activity is initiated.
- The institution provides comprehensive, regular training designed to ensure that staff is fully knowledgeable about relevant laws, regulations, policies, and procedures, and that the institution monitors staff's completion of training.

Risk Monitoring and Management Information Systems

Effective risk monitoring requires institutions to identify and manage all significant risk exposures, including compliance risk. Identifying such risk throughout its operations is important to ensure that the institution modifies its compliance management program as needed to respond to any internal or external changes that affect the institution. Risk-monitoring activities must be supported by appropriate MIS that provides senior managers and directors with timely information on the compliance risk exposure of the institution, as well as with regular and sufficient information for line managers engaged in the day-to-day management of the institution's activities.

Banking organizations use MIS to organize and report data to senior management. Compliance issues should be included in the MIS of the organization. Examiners should ascertain whether the MIS is helping ensure that relevant information gets escalated from the business unit level to the compliance function and then on to senior management.

The sophistication of an institution's compliance risk monitoring and MIS should be commensurate with the complexity and diversity of the institution's operations. Accordingly, smaller and less complicated institutions may require only a limited set of management and board reports to support risk monitoring activities. These reports could include results and trends from compliance reviews and consumer complaints, details of lending patterns and approval/denial rates for key lending activities, details of new products or activities and their resultant risk exposure, and similar information. In situations in which there is limited formal reporting for compliance risk monitoring and limited MIS, examiners should have discussions with management to understand the institution's approach and methodology for identifying risk. Management should be able to articulate its understanding of compliance risk in the institution, especially when formal reporting of these risks may be limited. Larger, more complex institutions, however, should have much more comprehensive reporting and monitoring systems that allow for more frequent reporting, tighter monitoring of complex compliance activities, and the aggregation of risks on a fully consolidated basis across all business lines and activities.

A critical element of a strong compliance management program is cultivating a corporate culture that is committed to reevaluating risks on a regular, ongoing basis. The program should ensure that policies and limits are supported by risk monitoring procedures, reports, and MIS that provide management and the board with the information and analyses that are necessary to make timely and appropriate decisions related to compliance controls in response to changing conditions and changes to the institution's operations.

In assessing the adequacy of an institution's measurement and monitoring of risk and its management reports and information systems, examiners should consider whether these conditions exist:

- The institution's risk monitoring practices and reports address all of its material risks.
- Key assumptions, data sources, and systems used in measuring and monitoring risk are appropriate and adequately documented and tested for reliability on an ongoing basis.
- Reports and other forms of communication generated from MIS and other monitoring are consistent with the institution's activities, are structured to monitor exposures and compliance with established limits, goals, or objectives, and as appropriate, compare actual versus expected performance.

- Reports to management or to the institution's directors are accurate and timely and contain sufficient information for decision makers to identify any adverse trends and to evaluate adequately the level of risk faced by the institution.
- Management responds timely and effectively with process or other modifications when warranted by changes in the institution's compliance risks, including risks resulting from changed regulatory or legal requirements or the introduction of new products.

Internal Controls

An institution's internal control structure is critical to the effectiveness of its risk management system. A system of internal controls should include the procedures necessary to ensure timely detection of failure of accountability, and such procedures should be performed by competent persons who have no incompatible duties. Establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate separation of duties, is one of management's more important responsibilities. Effective internal controls are the foundation for the safe, sound, and compliant operation of a financial institution. An institution's board of directors and senior management are responsible for ensuring that the system of internal controls is effective. Their responsibility cannot be delegated to others within or outside the organization. The audit function or other means of compliance testing is an important component of an institution's internal controls. Serious lapses or deficiencies in internal controls may warrant supervisory action, including formal enforcement action.

Audit and internal controls are interrelated, and therefore, frequently confused. In short, internal controls are related to the effectiveness of the overall business process. Appropriate controls assure that the process is effective and are the foundation for the safe and sound operation of the organization. Audit is a method used by management to assure that the operational controls it has designed are effective. As such, audit is a monitoring mechanism and is part, but not all, of a well-designed internal control system. When properly structured, a system of internal controls promotes effective operations and reliable financial and regulatory reporting, safeguards assets, and helps to ensure compliance with applicable laws, regulations, and institutional policies.

At complex organizations, internal controls are tested by an independent internal auditor who reports directly to the institution's board of directors or to its designated committee, which is typically the audit committee. Smaller institutions, whose size and complexity do not warrant a full-scale internal audit function, may rely instead on regular reviews of essential internal controls and compliance testing conducted by bank personnel or by third parties. Ideally, personnel performing these reviews should be independent of the function they are assigned to review. In smaller institutions, this may prove to be a challenge but may be accomplished by having operational staff from one functional area review the work of another functional area. Given the importance of appropriate internal controls to banking organizations of all sizes and risk profiles, the results of audits or compliance testing reviews (whether conducted by an internal auditor or by operational personnel) should be adequately documented, as should management's responses to them. In addition, communication channels should exist that allow negative or sensitive findings to be reported directly to the board of directors or to the relevant board committee.

In evaluating the adequacy of a financial institution's internal controls and audit procedures, examiners should consider whether the following conditions are met.

- The system of internal controls is appropriate for the type and level of risks posed by the nature and scope of the institution's activities.
- The institution's organizational structure establishes clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits.
- Reporting lines provide sufficient independence of the control areas from the business lines and adequate separation of duties throughout the organization.
- Official organizational structures reflect actual operating practices.
- Financial, operational, and regulatory reports are reliable, accurate, and timely; any exceptions are noted and promptly investigated.
- Internal audit or other control review practices provide for independence and objectivity.
- Internal controls and information systems are adequately tested and reviewed on a periodic basis commensurate with risk.
- The coverage, procedures, findings, and responses to audits and review tests are adequately documented.
- Identified material weaknesses are given appropriate and timely high-level attention.
- Management's actions to address material weaknesses are objectively verified and reviewed.

- The institution's audit committee or board of directors regularly reviews the effectiveness of internal audits and other control review activities.
- The institution's change control mechanisms are appropriate for the size and complexity of the institution and reflect sound compliance risk management practices.
- Adequate controls exist to review all facets of vendor management that affect consumer compliance risk.

Vendor management is an increasingly important internal control given the unique challenges presented by third-party relationships. Reliance on vendors has grown as financial institutions seek to gain operational efficiencies by contracting with third parties. Financial institutions use vendors in a variety of ways, often as a way to deliver products and services for which the institution has limited expertise. However, vendors may also perform compliance-related internal control or audit functions. Vendor management is essential because the institution remains responsible for the products and services provided by vendors, but at the same time, is less able to exercise direct control over the delivery or performance of a product or service. Sound vendor management practices require that an institution

- conduct effective due diligence in hiring and overseeing vendors to ensure they have qualified staff, effective processes and controls, a solid reputation in the industry, and sufficient expertise to meet the institution's needs and requirements
- establish contracts with vendors that clearly outline expectations and standards
- identify and understand the products and services provided by vendors for the organization and evaluate the compliance risks associated with offering these products and services
- monitor the vendor's adherence to contractual requirements, including those related to ensuring compliance with consumer protection laws and regulations.

Examiners should refer to the guidance in Appendix 6, Internal Control and Internal Audit Function, Oversight, and Outsourcing. It contains additional information related to the internal control and internal audit functions in general as well as a discussion of outsourcing the internal audit function.

Assessing Effectiveness of Compliance Risk Management

Appendix 2, Guidance for Assessing Consumer Compliance Risk Management, is a matrix that examiners will use as a tool to help assess the quality of compliance risk management. The matrix incorporates the System's standard elements of risk management:

1. board and senior management oversight
2. policies, procedures, and limits
3. risk monitoring and MIS
4. internal controls

The matrix also incorporates a number of subcomponents that examiners should consider, as appropriate, when reaching conclusions about risk management.

For each of the risk management elements, the matrix identifies a number of associated components that provide a more granular analysis of risk management practices. The extent to which these subcomponents are present and must be documented as part of the analysis will vary depending on the sophistication and complexity of each individual institution. Examiners will observe and evaluate many more components at a complex institution that has products or services with higher inherent risk than they will at a less complex institution that has products or services with lower inherent risk and has more informal control processes.

As in the case of inherent risk, examiners may find that for certain institutions or products, it makes sense to assign ratings to individual subsidiary risk components in order to arrive at the overall ratings for inherent risk or risk management. This level of detail and support should be necessary only for larger or more complex organizations, and documentation of this work should be maintained separately from the assessment itself.

In addition, examiners should be particularly aware that the risk-focused supervision program seeks to more effectively utilize organizational risk assessments and the results of audit and internal compliance reviews. These organizational products can be reviewed and used to enhance the consumer compliance risk assessment process. Appendix 6 includes guidance for achieving this objective.

A five-point rating system is used to assess compliance risk management as follows:

Risk Control Ratings
Strong (1)
Satisfactory (2)
Fair (3)
Marginal (4)
Unsatisfactory (5)

The following definitions apply to consumer compliance risk management and should be considered in the context of the inherent risk of the business line, product, or service being evaluated.

- *Strong (1) consumer compliance risk management* exists when management effectively identifies and controls all major consumer compliance risks posed by the institution's activities. Management is fully prepared to address risks emanating from new products and changing market conditions. The board and senior management are forward-looking and active participants in managing risk. Management ensures that appropriate policies and limits exist and are understood, reviewed, and approved by the board. Policies and limits are supported by risk-monitoring procedures, reports, and MIS that provide management and the board with the information and analysis that is necessary to make timely and appropriate decisions in response to changing conditions. Risk management practices and the organization's infrastructure are flexible and highly responsive to changing industry practices and current regulatory guidance. Staff has sufficient experience, expertise, and depth to manage the risks assumed by the institution. Internal controls and audit procedures are sufficiently comprehensive and are appropriate to the size and activities of the institution. There are few noted exceptions to the institution's established policies and procedures, and none is material. Management effectively and accurately monitors the condition of the institution, consistent with the standards for compliance and in accordance with internal and supervisory policies and practices. Consumer compliance risk management processes are fully effective in identifying, measuring, monitoring, and controlling the risks to the institution.
- *Satisfactory (2) consumer compliance risk management* exists when the institution's management of risk is largely effective but is lacking to a modest degree. Management demonstrates responsiveness and an ability to cope successfully with existing and foreseeable risks that may arise in carrying out the institution's business plan. While the institution may have some minor risk management weaknesses, these problems have been recognized and are in the process of being resolved. Overall, board and senior management oversight, policies and limits, risk-monitoring procedures, reports, and MIS are considered satisfactory and effective in maintaining a culture of compliance. Risks are controlled in a manner that does not require more than normal supervisory attention. The institution's risk management practices and infrastructure are satisfactory and generally are adjusted appropriately in response to changing industry practices and current regulatory guidance. Staff experience, expertise, and depth are generally appropriate to manage the risks assumed by the institution. Internal controls may display modest weaknesses or deficiencies, but they are correctable in the normal course of business. Examiners may have recommendations for improvement, but the weaknesses noted should not have a significant effect on the compliance position of the institution.
- *Fair (3) consumer compliance risk management* exists when practices are lacking in some important ways and therefore are a cause for more than normal supervisory attention. One or more of the four elements of sound risk management (active board and senior management oversight; adequate policies, procedures, and limits; adequate risk monitoring and MIS; comprehensive internal controls) is considered less than acceptable and has prevented the institution from fully addressing one or more significant risks to its operations. Certain risk management practices need improvement to ensure that management and the board are able to identify, measure, monitor, and control all significant risks to the institution. Also, the risk management structure may need to be improved in areas of significant business activity (product or service), or staff expertise may not be commensurate with the scope and complexity of business activities. In addition, management's response to changing industry practices and regulatory guidance may need to improve. The internal control system may be lacking in some important aspects, particularly as indicated by continued control exceptions or by a failure to adhere to written policies and procedures. Consumer compliance risk management weaknesses could have adverse effects on the overall compliance position of the institution and result in sanctions or losses if management does not take corrective action.
- *Marginal (4) consumer compliance risk management* exists when practices fail to identify, measure, monitor, and control significant risk exposures in many material respects. Generally, such a situation reflects a lack of adequate guidance and supervision by the board and senior management. One or more of the four elements of sound risk management is defi-

cient and requires immediate and concerted corrective action by the board and senior management. The institution may have serious identified weaknesses, such as a lack of independence or conflicting lines of authority, that require substantial improvement in internal controls or improved adherence to supervisory standards or requirements. Consumer compliance risk management deficiencies warrant a high degree of supervisory attention because, unless properly addressed, they could result in serious sanctions or losses.

- *Unsatisfactory (5) consumer compliance risk management* exists when there is a critical absence of effective risk management practices with respect to the identification, measurement, monitoring, or control of significant risk exposures. One or more of the four elements of sound risk management is considered wholly deficient, and the board and senior management have not demonstrated the capability to address these deficiencies. Internal controls are critically weak and therefore could seriously jeopardize the continued viability of the institution. There is an immediate concern about the reliability of records and regulatory reports and the potential for sanctions or losses if corrective measures are not taken immediately. Deficiencies in the institution's consumer compliance risk management procedures and internal controls require immediate and close supervisory attention.

D. Residual Risk

Residual product risk considers the impact (inherent risk) and probability (risk management) of noncompliance. Residual risk is the risk that remains after determining the level of inherent risk and reaching a conclusion about the effectiveness of risk controls associated with the institution's material products. The residual risk determined for each of the institution's material products should be aggregated to capture the residual risk for the institution as a whole.

After the quality of risk management is factored in, the resulting residual risk rating may be lower or higher than the inherent risk rating. Both inherent risk and risk controls are rated on a five-point scale. Consider these examples:

- The existence of high (5) inherent risk and strong (1) risk management may warrant a considerable (4) or moderate (3) residual risk rating.
- Conversely, where inherent risk is low (1) and risk management is unsatisfactory (5), a limited (2) or moderate (3) residual risk rating could be appropriate.

However, the second scenario (risk management practices are so flawed that they actually increase inherent risk) probably would occur infrequently, such as in cases of willful noncompliance, negligence, or gross negligence. As a general rule, satisfactory risk controls should result in a residual risk rating that is no higher than the inherent risk rating. Finally, when inherent risk is high and risk management appears strong but has not been previously tested, it is generally advisable to test the risk controls to substantiate that they effectively mitigate the high inherent risk. For example, if an institution offers a new product with high inherent risk, examiners generally would be expected to review the product during the current examination to validate the efficacy of the controls. Once the controls have been validated, it may be appropriate at future examinations, in the absence of significant changes, to conclude that the controls effectively mitigate inherent risk.

E. Fair Lending and Unfair or Deceptive Acts or Practices (UDAP)

Additional Guidance Regarding Fair Lending and UDAP

Fair lending (the Fair Housing Act, the Equal Credit Opportunity Act, and Regulation B) and UDAP (Section 5 of the Federal Trade Commission Act and Sections 1031 and 1036 of the Dodd-Frank Act) are two of the most significant risk areas for institutions. Violations in these areas often cause significant consumer harm as well as legal and financial risk to the institution. In addition, both areas may involve complex and fact-specific analysis. As industry practices change over time, fair lending and UDAP risks will also change because institutions can violate fair lending and UDAP laws in many ways. Accordingly, the Board of Governors of the Federal Reserve (Board) established the Fair Lending Enforcement Section to support examiners and ensure that fair lending and UDAP laws are enforced rigorously and consistently across the Federal Reserve System.

Assessing Fair Lending and UDAP Risk

Fair lending and UDAP should always be addressed during the risk assessment and discussed separately in risk assessment documentation. Examiners should identify fair lending and UDAP inherent risks and assess the effectiveness of the institution's risk controls in mitigating these risks, building upon their understanding of the institution, including its credit markets, decision centers, demographics, product lines, loan application and origination volume, credit operations structure, and historical performance. In evaluating fair lending

risk, examiners should consider the risk factors included in the Interagency Fair Lending Examination Procedures and supplemented by applicable Federal Reserve guidance. In addition, examiners should consider any HMDA data screening results distributed by the Fair Lending Enforcement Section. In evaluating UDAP compliance, examiners should pay special attention to products and practices that target vulnerable consumers or pose potential risk to consumers that may not be apparent. In addition, the Board, in conjunction with the Reserve Banks, may periodically provide guidance for Federal Reserve System reviews or emerging risks that should be incorporated into the risk assessment.

In applying a risk-focused approach, examiners should focus on product and service areas that are considered material to the institution's risk profile. If an institution has several material products and services that exhibit moderate or high residual risk, examiners are expected to focus on the products or services that pose the highest risk of consumer harm.

Another factor to consider when assessing both inherent risk and risk controls is whether the institution has received fair lending or UDAP complaints regarding a product, including

- complaints to the Federal Reserve or to the institution
- concerns raised by community contacts during the CRA examination
- complaints to other federal or state agencies
- lawsuits by any party (private or government)
- inquiries or investigations by other federal or state agencies
- complaints generated through Internet websites and/or social media
- press articles raising concerns about the institution's practices

Complaints can be an indicator of areas of potentially heightened inherent risk or they may suggest the need for additional focus on specific risk controls. The role complaints will play in the assessment of risk and development of the examination scope and work plan, however, will depend on the particular issue(s) raised in the complaint(s), viewed in the context of all other examination-related information.

Fair Lending and UDAP Examination Intensity

For UDAP, examiners can determine the appropriate examination intensity using the procedures described in other parts of this document.

For fair lending, as with examiners' evaluation of the overall compliance management program, the level of examination intensity for a particular product should generally be commensurate with the level of residual risk identified in the risk assessment process. However, in circumstances where inherent risk is high, it is advisable to test the risk controls before concluding that they effectively mitigate the high inherent risk. That is, if an institution offers a product with high inherent fair lending risk, examiners generally would be expected to conduct a high intensity review during the examination to test the efficacy of the controls. Once the controls have been tested, it would be appropriate at future examinations, barring significant changes, to conclude that the controls effectively mitigate inherent risk. Finally, even when residual risk is low or moderate, it may nonetheless be appropriate for examiners to provide institutions with guidance on how to mitigate identified risk factors more effectively.

In some instances, determining the fair lending risk of the institution may be quite straightforward. In other instances, the risk assessment may require a balancing of factors. Reserve Banks may contact the Fair Lending Enforcement Section if there are questions about the appropriate level of examination intensity. As with other areas of review, after examiners have determined the work plan, new information may come to light that requires additional examination work. For example, an institution's fair lending risk may initially be deemed moderate risk, with only follow-up interviews planned. The interviews, however, may reveal information that alters the risk assessment and results in the need for further analysis, such as more intensive loan file reviews or more in-depth statistical analysis.

Low Intensity Review

In some instances, examiners may conclude that residual fair lending risk is low and that no additional work beyond the risk assessment is needed. Illustrative examples include the following:

- No fair lending risk factors are present. For example, for pricing, the policies and procedures are clear, with limited or no discretion; loan originator compensation is not based on the terms and conditions of the loans; and there are no disparities for any target group.[4] As another example, for redlining, the institution has an appropriate CRA assessment area that does not reflect illegal discrimination; the branching and marketing do not avoid majority

4. Disparities include "gross disparities," which are differences in pricing between the target group and the control group without controlling for legitimate pricing factors, or "adjusted disparities," which take into account legitimate pricing factors.

minority areas; and there are no large and/or statistically significant disparities in the majority minority areas in the institution's market area.

- Fair lending risk factors are present, but at a previous examination, the examiners tested the institution's risk controls and found that they effectively mitigated the specific risk factors. The risk factors and controls were tested at the previous examination in accordance with the current Federal Reserve System guidance on fair lending risk. In addition, the institution's risk assessment has not changed. Therefore, no further evaluation is called for during the current examination. However, examiners should ensure that they test controls periodically going forward.

Moderate Intensity Review

In some instances, additional analysis beyond the risk assessment may be needed to fully evaluate the fair lending risk. This analysis may include interviewing bank personnel, conducting additional statistical analysis, or obtaining additional information from the institution. Illustrative examples include the following:

- Fair lending risk factors are present, but other analysis performed as part of the risk assessment supports a conclusion that fair lending risk is moderate. For example, bank employees have significant pricing discretion, but no disparities in the annual percentage rate (APR), interest rates, or fees are present. In this instance, the presence of risk factors may affect examiners' view of the adequacy of fair lending policies. Examiners may conduct interviews regarding the institution's pricing policies and controls, and supervisory guidance may be appropriate.
- Examiners identify a practice that raises a concern regarding disparate impact, but consultation with the Fair Lending Enforcement Section and additional information from the institution resolve the concern. For example, after identifying a potential disparate impact issue, the examiners inform the Fair Lending Enforcement Section, and additional information is requested from the institution to better understand the purpose of the practice. Based on the additional analysis, examiners determine that the institution's practice is based on an appropriate business justification and no further analysis is needed.

High Intensity Review

If residual fair lending risk is high, in-depth analysis is appropriate. Illustrative examples include the following:

- Fair lending risk factors are present and have not been resolved through pre-examination statistical analysis. For example, the institution has discretionary pricing for indirect auto loans, and there are disparities in dealer markups. Accordingly, an in-depth analysis with interviews and additional statistical analysis is appropriate.
- Fair lending risk factors are present, and although controls appear satisfactory, they were not tested at a previous examination. For example, the pre-examination statistical analysis shows disparities in interest rates for unsecured consumer loans. The institution has controls in the form of rate sheets and documentation of exceptions, but examiners did not test these controls at the previous examination. Accordingly, an in-depth analysis with interviews, file reviews, and additional statistical analysis is appropriate.

F. Documenting the Consumer Compliance Risk Assessment

When completing the risk assessment of a state member bank, examiners must use the Consumer Compliance Risk Assessment Summary Matrix on page 37 to document and summarize consumer compliance risk.

In the Summary Matrix, for each material product, service, or business line, a rating must be assigned for each inherent risk component, and then a composite inherent risk rating must be assigned. In addition, an aggregate inherent risk rating should be assigned to reflect the overall inherent risk of the institution's product offerings. For these same products, services, or business lines, the Summary Matrix should also document ratings for each of the four risk management elements as well as an aggregate risk-control rating. Based on the balance of inherent risk and the effect of risk controls, a residual risk rating must be assigned for each product, service, or business line and in the aggregate.

The analysis supporting key risk conclusions should be summarized and documented in the risk assessment. Evaluative information reflected in the summary should be provided to support the

assessment of the level of inherent risk, the adequacy of risk controls, and conclusions about residual risk. Examiners will include the following:

Executive Summary

The executive summary highlights the key inherent risks and highest-priority risk management weaknesses (if any) and also identifies risk controls (if any) that are not commensurate with the levels of risk. The executive summary also discusses the primary recommendations for the supervisory plan that were derived from the risk assessment.

Summary of Inherent Risk

Examiners are to provide an overall rating of inherent risk at the institution that is supported, as necessary, by the ratings on the matrices and reflects an appropriate weighting of products, business lines, or services. In the discussion of the key inherent risks, examiners will identify any relationships between different risks that drive the overall assessment. This summary highlights any areas of heightened inherent risk.

Summary of Risk Management and Controls

This summary discusses the effectiveness of controls, highlights which areas pose the greatest control issues, and provides a high-level summary of the issues or concerns. Examiners also should identify any control-related concerns associated with specific products as well as themes that cut across products, business lines, or services. As part of this discussion, examiners should evaluate the adequacy of management's response to any significant internal review or audit findings that involved consumer compliance matters.

Summary of Residual Risk Assessment

Examiners should summarize conclusions about the overall level of residual risk, with an emphasis on the range of risks across products, business lines, and services, along with an explanation of their weighting of the residual risk associated with each activity. As a general rule, weighting will be consistent with examiner conclusions about the relative materiality of activities and will consider both the number and the dollar volume of each activity.

Recommendations for Supervisory Plan/Strategy

This section is derived from the risk assessment to provide the supporting foundation for development of the supervisory plan and to describe the supervisory planning process, including key priorities. The supervisory plan details all activities that will be necessary to address the risks identified and may include formal examination activities, targeted on- or off-site reviews, outreach, or even recommendations for informal or formal supervisory action.

Consumer Compliance Risk Assessment Summary Matrix

Guidance for assessing inherent risk and risk controls is located in appendixes 2 and 3. Examiners should use the inherent risk and risk-control assessment matrices together when assigning risk ratings for the primary inherent and risk-control components that must be documented in this Consumer Compliance Risk Assessment Summary Matrix or some similar form.

- Inherent Risk—Low, Limited, Moderate, Considerable, or High
- Risk Control Assessment—Strong, Satisfactory, Fair, Marginal, or Unsatisfactory
- Residual Risk—Low, Limited, Moderate, Considerable, or High

Product	Inherent Risk			Risk Controls				Residual Risk
	Institutional Factors	Legal and Regulatory Factors	Environmental Factors	Board and Management Oversight	Policies, Procedures and Limits	Risk Monitoring and MIS	Internal Controls	
Material Business Line, Product, or Service								
Material Business Line, Product, or Service								
Material Business Line, Product, or Service								
Aggregate Risk and Risk Control Assessments								

Updating the Risk Assessment

Pre-examination. Prior to an examination, examiners are required to make a determination as to whether material changes have occurred in the institution's inherent risk and/or in its compliance management program since the most recent risk assessment. This analysis will require examiners to gather information necessary to update the institutional profile. For guidance, refer to the Understanding the Institution section of this document. Significant changes related to the institution's operations and its management of consumer compliance risk should be shown in an updated institutional profile. Relying on the updated profile, examiners will determine whether any changes are material and should be captured in an update to the risk assessment. The goal of the risk assessment is to develop a perspective on risk that can be relied upon to drive supervisory decisionmaking.

Post-examination. The risk assessment must be updated at the conclusion of a consumer compliance examination. Any updates to the risk assessment will reflect changes to the assessment of inherent risk or the effectiveness of controls, consistent with examination findings.

Ongoing supervision. The risk assessment must be updated in conjunction with any mandated ongoing supervision activities. In the case of ongoing supervision, even if no material changes have occurred, examiners are required to affirmatively document completion of the required supervisory event.

Significant risk-profile changes. Finally, the risk assessment must be updated whenever new information indicates a significant change in the organization's risk profile, such as changes in the organization's activities, structure, or financial profile, or in the risk-control environment.

IV. EXAMINATION SCOPING AND PLANNING

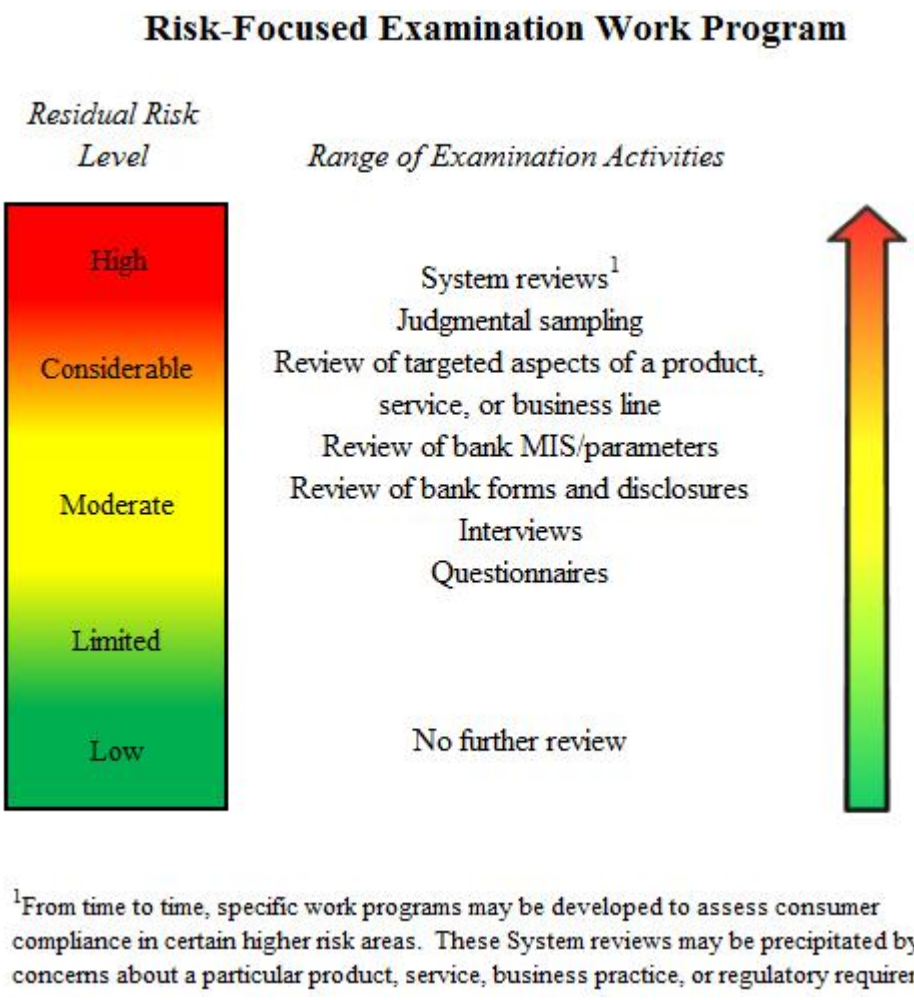
Key Role of the Risk Assessment

Consumer compliance examinations evaluate the effectiveness of an institution's consumer compliance risk management program and assess its level of compliance with applicable consumer protection laws and regulations. Establishing a thorough knowledge of an institution's inherent risk and an understanding of an institution's compliance management program, including the risk controls used to mitigate inherent risk, is a critical part of examination scoping and planning. Ultimately, the risk assessment should drive the scope of activities that will be carried out during the examination.

Objectives of the Scoping Process

Examiners should exercise sound judgment in ensuring that planned examination activities are meaningful, an efficient use of resources, and effective in helping gain reasonable assurance that the institution's compliance management program enables the organization to maintain a satisfactory level of compliance with applicable consumer protection laws and regulations.

The scoping process provides an opportunity to customize examination activities so that they are consistent with the size, complexity, and risk profile of the institution. In this way, it is expected that a broad range of examination activities will be



considered for products, services, and business lines targeted for additional review. Moreover, it is expected that planned activities will involve varying levels of intensity and will be carried out in a way that helps the examination team draw reasonable conclusions about the adequacy of an institution's compliance management program.

Scoping and Planning Considerations

A thorough understanding of the inherent risk and the risk controls for the various products, services, and business lines is the foundation that supports broad conclusions about the institution's overall compliance management program. It is through review of individual products, services, and business lines, particularly those that are material and represent the most significant risk to the organization, that the examination team is better able to assess the effectiveness of the institution's compliance management program.

The examination work program and procedures used to assess the risk management practices of an institution with respect to a particular product or service or across business lines should be commensurate with the level of residual risk identified in the risk assessment process. Thus, the examination work program may include a range of examination activities, as depicted in the diagram above.

Applying a Risk-Focused Approach

The risk-based methodology is flexible regarding the nature and scope of examination activities that may be conducted in a particular product, service, or business line area. Generally, areas deemed to represent the lowest risk should receive lower-intensity reviews or perhaps receive no further review beyond the activities conducted during the risk assessment process. As residual risk increases, however, it is expected that examination coverage and the level of intensity will increase commensurately; nevertheless, the level of review is not prescriptive. Examiners should make prudent decisions regarding the level of review needed,

choosing examination procedures that will most effectively accomplish the stated objective.

For example, inherent risk related to a product area may be considered limited based on associated regulatory requirements, marginal growth, low staff turnover, and a relatively small volume of transactions. If examiners can ascertain that the institution employs strong risk controls, such that residual risk is reduced and deemed low, then no further testing would be required; the examination objectives have already been achieved through the risk assessment process.

In this same scenario, if the institution's limited inherent risk was not effectively mitigated by satisfactory risk controls, examiners might elect to conduct further review of that product. At a minimum, examiners might choose to conduct additional interviews with bank personnel to help assess staff knowledge and understanding of applicable regulations, adherence to internal policies and procedures, the degree of reliance on bank systems, the efficacy of those systems, and the adequacy of the institution's internal control processes. In lieu of or complementing the interviews conducted, examiners may consider reviewing the institution's MIS, computer parameter reports, internal forms, product disclosures, or other documentation. All are permissible options and would help examiners develop a more complete assessment of the institution's risk management processes and their effectiveness. These activities might reveal that the institution's risk controls are indeed adequate for the associated risk. Alternatively, these activities might confirm or reveal significant deficiencies in one or more risk-control areas and indicate a need to increase the depth of review.

At the outset, examiners should be selective when planning examination activities, choosing those that best align with the level of residual risk present in a product, service, or business line. Examiners are not expected to conduct extensive reviews of every business area in order to affirm or refute a working hypothesis regarding the institution's risk management practices. Similarly, it will not be necessary in most cases to test every possible variation of a major product category or business line, especially when such variations are subject to the same control environment. For example, if all time deposit initial disclosures are generated from the same software, it is not expected that every maturity will need to be tested. Instead, testing might include the most popular maturity or the maturity subject to the most complex disclosure rules.

In addition, it may not be necessary to test every transaction for every regulatory requirement to the same degree. More complex regulatory requirements should receive greater scrutiny than other provisions. Further, the need for a baseline evaluation should not prevent examiners from establishing compliance with some regulatory provisions without testing individual transactions if compliance can reasonably be determined by a review of highly automated processes or through interviews and/or the review of forms, disclosures, policies, and procedures. For example, some regulatory and legal requirements, such as APR computations, although typically automated, require manual input for each transaction and thus will require testing of individual transactions, or rather, testing of a particular aspect of the transaction or process. Other business activities, for example, preparing disclosure forms, typically use certain highly automated processes with limited manual input for individual transactions. For these processes, compliance may be established through other means, such as a review of system parameters.

In contrast to the more targeted reviews discussed so far, it is expected that higher-risk areas will be reviewed in greater depth. Although the focus of the examination is on the institution's processes, an appropriate level of transaction testing may be necessary to verify the effectiveness of policies and procedures and the integrity of internal systems. Most commonly, testing may include a judgmentally selected sample of transactions that is used to evaluate various aspects of the institution's products, services, or business lines. Judgmental samples may be larger when overall transaction volume is higher. In certain instances, testing may occur during the scoping and planning stage in order to evaluate the need for additional file reviews on site.

Even in higher-risk areas, examiners may not need to conduct extensive transaction testing. Instead, examiners may begin by reviewing related product forms, agreements, and disclosures or by conducting an in-depth interview regarding institutional processes such as a product life-cycle analysis. Interviews with bank staff and management may prove highly effective in documenting the institution's processes related to the various stages of a product's life cycle, including, for example, its design, marketing, initial interface with the customer, origination/consummation, usage, servicing, or termination. These reviews and discussions alone may satisfy the examination objective or may indicate a need to target a specific process for transaction testing.

Finally, in applying a risk-focused approach, examiners should use sampling methods appropriate for the type of review being conducted. For example, examiners may use judgmental sampling when testing internal controls and statistical sampling when testing the validity of data pursuant to

separate Consumer Affairs (CA) Letter guidance.[5] Examiners should refer to applicable sampling guidelines contained in CA Letters.

Risk-Focused Examination Work Program

After assessing the institution's risk and identifying the areas targeted for additional review, examiners should develop a tailored, risk-focused work program for each product, service, or business line selected, using examination procedures in CA Letters, the Consumer Compliance Handbook, and other Board guidance.

Interagency examination procedures provide examiners with guidance on determining an institution's compliance with applicable consumer protection laws and regulations. Generally, these procedures anticipate two stages to the examination process, captured in management and policy-related examination procedures and transaction-related examination procedures. Examination objectives require examiners to (1) assess the quality of the financial institution's compliance management systems and its policies and procedures, and (2) determine the reliability of the financial institution's internal controls for monitoring the financial institution's compliance.

In many cases, examination objectives for material products or for the overall institution may have been largely met as part of the risk assessment process. For example, if there is a reasonable basis for reliance on the institution's controls, procedures, and monitoring practices and residual risk is limited, examiners may not need to conduct additional work or may conduct only limited follow-up work (such as interviews) during the examination to complete the management and policy-related examination procedures. The level of required work under such circumstances should be clearly conveyed in the scope memorandum.

Management and policy-related examination procedures performed during the risk assessment process may result in the identification of procedural weaknesses or other risks that cannot be addressed effectively through limited follow-up. In such cases, examiners should document the need for transaction testing using the applicable transaction-related examination procedures. As previously discussed, decisions about the scope of testing for any particular product should be driven by the residual risk associated with that product. This decision would include not only a determination about sample sizes but also the extent to which specific features, processes, or regulatory requirements associated with a particular product warrant testing. Examiners should use their judgment in deciding the size of each sample and the scope of testing. The requirement for any testing should be clearly documented in the scope memorandum, limiting testing to what is required by the residual risk associated with the products subject to testing.

Preparing the Examination Plan and Scope Memorandum

Examination scoping and planning should culminate in the preparation of the scope memorandum. The scope memorandum should include an updated institutional profile, risk assessment, and examination plan. The examination plan should detail the overall examination strategy and should also consider and document the following information:

- central objectives of the present examination and anticipated areas of focus
- planned examination activities, including
  - a list of products, services, and business line activities subject to further review
  - the ''risk-focused examination work program,'' which includes the nature and extent of any interviews, documentation reviews, and transaction testing to be conducted, including whether activities will be conducted on site or off site and the level of review as well as the rationale and key drivers behind examiners' decisions
  - the sample size, including the number of transactions that will be tested, as well as the estimated universe of transactions or time period involved, if known
- examiner staffing levels, assignments, and expectations
- examination logistics
- attachments providing additional information, as needed

Completing the scope memorandum sufficiently in advance of the examination start date will assist in identifying staffing needs, assigning staff with the appropriate expertise, and preparing for other examination work. To ensure consistency in the scoping process, Reserve Bank management must implement an approval process that includes a review of the final scope memorandum. This review and approval should be documented. The scoping process should result in communicating to bank management any request for information to be sent to the Reserve Bank or made available on site upon examiners' arrival.

5. CA Letters address significant policy and procedural matters related to the Federal Reserve System's consumer compliance supervisory responsibilities.

Further, an addendum to the scope memorandum should be prepared to document any material changes in the original scope that occur during the examination, but it is not necessary to update the scope memorandum with the examination conclusions. These conclusions should be documented elsewhere in the work papers.

V. EXAMINATION WORK

Examination work begins with updating the institutional profile and risk assessment, continues through the scoping process to the execution of the examination work program, and concludes with the issuance of the consumer compliance rating and the examination report. Supervisory follow-up and ongoing supervision complement examination work.

Examination work may take place at the Reserve Bank or at the state member bank. Examination work that involves information that can be accessed and reviewed at a Reserve Bank may be conducted off site. Transaction testing involving loan and deposit products has typically taken place at the state member bank, although transaction testing may take place at a Reserve Bank if the information is easily accessed and reviewed from the Reserve Bank. In addition, in-person interviews and conversations with business line staff and bank management may be more effective for gathering and exchanging information about higher-risk areas than e-mail communications or telephone conversations.

The following sections set forth general examination expectations regarding examination preparation, communication with Board staff, use of examination procedures, work papers, and communication of examination findings.

Preparing for the Examination

Communication with members of the institution's board of directors (such as a member of the audit committee or compliance committee) and management of the institution in advance of an examination is important in order to

- provide bank management with an understanding of the risk-focused examination process and how it will be applied to the institution
- help examiners gain an understanding of the institution, the level of inherent compliance risk present in products and services offered, and the institution's compliance risk management program and practices

Communications may take the form of telephone conversations, in-person interviews and conversations, e-mails, questionnaires, letters, and examination reports.

Communication and requests for information are likely needed when updating the institution's risk assessment before an examination or when developing the risk-based examination work program. To the extent possible, information requests should avoid asking for information already available, whether it is in the public domain or has already been provided to another area in the Reserve Bank. Further, bank management must be given adequate time to respond to information requests.

Letters written to provide information about a planned examination and request information not available at the Reserve Bank should be tailored to fit the character and profile of the institution being examined and the needs of the Reserve Bank. When examiners are deciding what information should be forwarded to the Reserve Bank for off-site review versus information that should be provided to examiners upon arrival at the institution, the goal should be to maximize the efficiency of the examination process while considering the burden placed on the financial institution. Specific information requests should be in writing to promote a clear understanding of expectations and to provide an examination record.

Communication with Board Staff

Collaboration between Reserve Bank and Board staff is encouraged. Reserve Bank staff may contact Board staff at any time with questions about potential examination issues. In situations involving potential fair lending violations or UDAP, early contact, including during the risk assessment and scoping phase, can result in more efficient supervision. In other situations, Board staff may be notified when follow-up supervisory action is required after examiners make a determination. Board staff are also available when examiners or Reserve Bank management have questions about legal and regulatory requirements or how to interpret them.

Communication with Bank Management during the Examination

At the beginning of the examination, the examiner in charge should meet with the institution's senior management and the compliance officer to discuss the nature and scope of the examination. Because the issues identified in the scoping process and the suggested levels of review may differ from the previous examination, it is important to provide bank management with an understanding of the risk-focused examination process and how it will be applied to the institution. The examination overview should include the assessment of the compliance management program, the type of review for particular loan or deposit products, and specific

areas of the institution to be evaluated. Examiners also should discuss the fair lending portion of the examination, including the areas being reviewed. Finally, management should be informed that the scope of the examination may be adjusted based on examination findings.

Throughout the examination, the examiner in charge should inform bank management of the examination's progress and issues that may have arisen that could result or have resulted in a change to the scope of the examination. The examiner in charge should explain any implications of such a change, especially any need for additional information or access to bank resources, and any extension of the planned time frame for completing the examination. Bank management should be given an opportunity to respond to issues and resolve them if possible, as early in the examination process as is practical.

Use of Examination Procedures

The examination should be conducted consistent with the documented examination scope. In some cases, no additional work, or only limited follow-up, will be required for areas in which residual risk is not elevated. This level of examination work corresponds with the management and policy-related portion of examination procedures, most of which will have been completed during risk assessment and scoping.

Findings during an examination, however, may warrant revision to the planned scope. While performing any on-site management and policy-related examination procedures identified in the scope memorandum, examiners may uncover procedural weaknesses or other risks that require review through testing. As with the scoping and planning phase, examiners should consult with the examiner in charge to determine the appropriate level of transaction testing to be performed. This change in scope must be appropriately documented.

For any specific product, the scope memorandum should specify when the use of transaction testing procedures is necessary and the extent of any testing—including sample sizes, specific features, processes, or regulatory requirements associated with a particular product. Such testing would typically be associated with elevated residual risk and should be conducted consistent with the transaction-related examination procedures.

In some cases, when transaction testing is required in the examination scope, examiners may identify violations or risks related to a product that the risk assessment did not address. In such cases, examiners should consider expanding the scope of transaction testing. The expanded sampling should, in all cases, consider relevant information discerned from the review of files or gathered through interviews, review of policies and procedures, or from other sources that might suggest the underlying root cause of the identified problem. Such information could suggest over- or under-weighting of transactions with certain shared attributes. For example, if an examiner reviewing real estate files identified, among other things, rescission violations, the expanded sample might include more loans subject to rescission compared to other types of loans. Determination of the extent of additional testing should always be made in consultation with the examiner in charge.

Examination Work Papers

It is critical to have well-documented work papers. Supporting documentation is necessary to ensure that consumer compliance examination work papers provide complete information and support examiners' findings and conclusions. Therefore, the final work papers should not contain any unresolved issues or questions.

Examination work papers also provide reference information for use during interim supervisory activities and subsequent examinations or enforcement proceedings.

Minimum Work Paper Guidelines

Work papers should support the examination findings and should be supplemented with copies of specific bank documents as necessary. In addition to the scope memorandum, work papers must include documentation of the work program performed during a supervisory event, including both off-site and on-site activities. Work program documentation must identify the examination procedures conducted, meetings held with management, major risks identified, a summary of findings with conclusions and support for those conclusions, as well as follow-up actions needed, whether MRIAs or MRAs. The written documentation included in the work papers is the basis for preparing the examination report.

Work Paper Standards

At a minimum, the compliance examination work papers must

- identify the examiner responsible for preparing the work papers
- identify the bank personnel responsible for providing information or documents to the examination team
- include a copy of the institutional profile, risk assessment, scope memorandum, and any

documentation that identifies risks or otherwise documents: (1) the work performed, (2) the scope of examination activities, and (3) the examination procedures used, by business line and/or products

- document the depth of the review and the level of intensity and the activities undertaken to achieve this level of review, including questionnaires and pertinent information about interviews, sample sizes, accounts sampled, and other information as appropriate
- document findings. Violations and other weaknesses should be supported by analyses with copies of disclosures, calculations, or interviews that led to conclusions
- identify the examiner responsible for the initial review of the work papers
- be organized so that each element of the examination can be understood

All examination work papers must comply with the secure handling of confidential supervisory material requirements set forth by the Board and the respective Reserve Bank.

Communicating Examination Findings

Final Discussions and Meetings with the Board of Directors

Formal final discussions are held to communicate examination findings and obtain, when necessary, management's commitment for corrective action. The examiner in charge should discuss the findings of the examination with management and, to the extent appropriate, the personnel involved in consumer compliance activities.[6] The final discussion should focus on the overall condition of the institution's consumer compliance and CRA programs (if applicable), any substantive violations of law, required corrective action, and recommendations. In addition to outlining strengths and weaknesses in the compliance management program, examiners should provide management with a list of all identified regulatory violations, including isolated violations. To the extent possible, during this discussion examiners should ask management to explain specific steps that will be taken to correct weaknesses in the compliance management program and to eliminate practices that violate consumer protection laws and regulations, so that the intended corrective action measures can be included in the report of examination.

The board of directors has the ultimate responsibility for operating the institution in compliance with the law and for ensuring that appropriate corrective action is taken. A meeting with the board of directors may be appropriate in certain circumstances, such as if the program weaknesses or legal violations involve the potential for significant administrative and civil liability or if the Reserve Bank is contemplating issuing a formal supervisory action, such as a Written Agreement or a Cease and Desist Order. Typically, a member of Reserve Bank management should attend an examination-related meeting involving the institution's board of directors.

Report of Examination

Supervisory findings are communicated in writing through formal reports and letters summarizing the results of target reviews. These communications, including the Consumer Affairs Report of Examination for community banks, constitute the official record of the examination and are the primary tool for conveying examination findings to the institution's board of directors and senior management.

The consumer compliance examination evaluates the effectiveness of an institution's compliance risk management program in controlling the inherent risk associated with product and service offerings. The report communicates the effectiveness of the institution's compliance risk management framework, including the risk controls employed to mitigate the inherent risk. It focuses on evaluation of the procedures and processes an institution has in place to identify, measure, monitor, and control its compliance risk.

Conclusions regarding the institution's compliance risk and the quality of its compliance management program should reflect a thorough analysis. While the primary focus is the evaluation of procedures and processes used by the institution to ensure compliance, significant regulatory violations also are important. Explanations of weaknesses noted in the compliance program and violations found during the examination should include a discussion of the cause and severity of the weaknesses or violations found. In the case of violations, the discussion should include the requirements of the regulation or statute.

The report will communicate examination ratings, material findings, significant supervisory issues, and any needed corrective action. MRIAs and MRAs should be discussed in the Executive Summary and Examination Ratings section of the report. To be effective, the communication of supervisory findings must be: (1) written in clear and concise language, (2) prioritized based on degree of importance, and (3) focused on any significant matters that require attention. Information included in the report should enable the institution's board of directors and senior manage-

6. Reserve Bank management should be apprised of these findings prior to the final meeting with the bank.

ment to understand the substance and status of outstanding MRIAs or MRAs and to focus on the most critical and time-sensitive issues.

Other detailed guidance regarding reporting examination findings, consumer compliance ratings, and enforcement actions is in the appendixes to this document.

VI. ONGOING SUPERVISION

Overview

The objective of the ongoing supervision program is 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. Significant changes are changes that immediately heighten the sense of supervisory concern or elevate the level of residual compliance risk of a material product or of the institution as a whole. Understanding key changes to the institution's compliance management program and associated risks will enable examiners to tailor bank examination risk assessments and work programs more effectively and efficiently. The ongoing supervision program also provides an opportunity, if needed, to follow up on supervisory risks or concerns noted at the previous community bank examination.

Supervision between Examinations

Ongoing supervision of an institution between examinations is critical in identifying significant changes or deteriorating trends in a timely manner. Proactive monitoring also confirms whether the institution's board and senior management have appropriately addressed previous examination findings and allows for identification of new product lines, business activities, or other organizational changes.

Ongoing supervision complements the supervision program for state member banks with assets of $10 billion or less and consumer compliance ratings of two or better and CRA ratings of satisfactory or better. For these institutions, an off-site supervisory contact with the institution must occur close to mid-cycle between consumer compliance examinations to identify significant changes to the compliance management program or compliance risks. Key areas that should be considered include the following:[7]

- changes in compliance management structure or staff
- changes in the frequency or scope of audits or internal reviews
- financial condition
- examination ratings (especially risk management ratings)
- new product offerings or changes to existing products
- progress made toward planning and implementing regulatory changes
- geographic expansion/contraction, especially changes in assessment areas
- significant changes in business strategies
- a significant increase or decrease in assets, loans, or deposits.
- changes in the loan portfolio mix.
- changes in indirect or wholesale lending activity
- consumer protection-related litigation and/or investigations by other governmental or regulatory agencies
- complaints

In some cases when the institution's risk profile is high or it changes materially as a result of the addition of more complex or higher-risk strategies, more frequent contacts may be appropriate.

The Ongoing Supervision Questionnaire (appendix 1, following this section) must be used to guide and capture discussions with management that are designed to ascertain key changes. Because institution size, complexity, and markets vary, additional questions may be appropriate for inclusion in the questionnaire. Other System examination tools may also be helpful in identifying relevant key changes.

When information obtained from questionnaire responses, from other interactions with bankers, and from review of relevant internal information indicates no significant changes at the institution, further supervisory action will not be necessary. For example, identification of a new product during an ongoing supervision review does not automatically necessitate additional supervisory work. Examiners should determine on a case-by-case basis if the level of residual risk appears elevated, based on responses to clarifying questions asked when gathering answers to the Ongoing Supervision Questionnaire.

When the level of risk is heightened as a result of an identified significant change, a Reserve Bank may choose from a range of options consistent with the type and level of risk identified. Such options

7. From time to time, Board staff and the Reserve Banks may ask that specific information requests be incorporated into the ongoing supervisory process to collect information across banks. These information requests may be precipitated by concerns about a particular product, service, business practice, or regulatory requirement.

could include off-site/on-site targeted product or service reviews, discovery reviews, on-site advisory visitations, or additional in-depth off-site interviews. In rare cases, it may be appropriate to accelerate the timing of the next examination to fully assess and address the areas of concern.

Significant changes occurring at the institution relating to the key areas outlined above that affect the institutional profile or perceived risk in the institution must be documented in the institutional profile and risk assessment as well as in the corresponding risk controls and ratings in the Compliance Risk Matrix. Changes to the supervisory plan should also be documented in the risk assessment. If there have been no significant changes since the last supervisory activity, it is sufficient to document in the risk assessment the date of the discussion and the individual with whom the information was confirmed.

APPENDIX 1. ONGOING SUPERVISION QUESTIONNAIRE

These are questions that generally can be answered during an interview or discussion with the institution.

Management and Control Environment

1) Explain any changes in the compliance management structure or staff (for example, compliance officer, compliance support staff, senior management, directors).
2) Describe changes in the organization's structure, including the number of bank subsidiaries, locations, lending subsidiaries, and ATMs.
3) Describe changes in the institution's internal control environment (for example, frequency or scope of reviews, internal/external audits, deposit or loan software systems).

Product Mix and Trade Area

4) Has the institution made any changes to, introduced, or discontinued any of the following:
   a) deposit product or service Yes No
   b) loan product or service Yes No
   c) guaranty loan program Yes No
   d) indirect or wholesale lending activity Yes No

   If Yes to any of the above, please describe:
5) Has the institution had any geographic expansion/contraction or made any changes to its
   a) CRA assessment area(s) Yes No
   b) trade area or markets Yes No
   c) business strategy, key business lines, or growth areas Yes No
   d) marketing emphasis or delivery systems Yes No

   If Yes to any of the above, please describe:

For these questions, using other System examination tools may be helpful in identifying relevant key changes. Additional follow-up may be appropriate to assess any changes identified.

Financial Condition

6) Review the institution's financial condition. Has the institution triggered any flags on the surveillance reports or on the risk-screening results? If Yes, please describe and discuss the effect of these issues on the institution's compliance risk management program. Yes No
7) Review the institution's Call Report information. Have there been any significant changes to the institution's loan portfolio mix? If Yes, please describe and discuss the effect of these issues on the institution's compliance risk management program. Yes No
8) Describe significant trends in the institution's portfolio composition, including increases or decreases in assets, loans, or deposits. Yes No
9) Review the most recent Safety and Soundness information. Have there been any significant changes in the CAMELS components that could affect the institution's compliance risk management program? If Yes, please describe and discuss the effect of these issues on the institution's compliance risk management program. Yes No

Risk Management

10) Has the institution had any changes to its Safety & Soundness management and/or risk=management ratings? Yes No

11) Does the institution have an effective change management process for implementing new products and services? Yes No

12) Is the institution a party to any pending consumer-related litigation or the subject of consumer-related inquiries from other agencies (state or federal), or has the institution received consumer compliance-related complaints? Yes No

Supervisory Plan

13) Request the status of examination follow-up on any pending supervisory issues, if applicable.

14) Discuss and document the institution's efforts and progress in areas where significant violations occurred.

Conclusion

15) Based on the information gathered, has the institution's consumer compliance risk profile changed materially, such that a change to the supervisory strategy for the institution is warranted? Yes No

APPENDIX 2. GUIDANCE FOR ASSESSING INHERENT CONSUMER COMPLIANCE RISK

Component	Low	Limited	Moderate	Considerable	High
INSTITUTIONAL FACTORS *Risks associated with the institution's strategic decisions, structure, business lines, products or services, and previous history*					
Strategic/Business Factors					
Growth					
Refers to substantive growth in market share or asset size through branching, merger, acquisition, change in business focus, or geographic expansion.	The institution has had no or minimal growth in market share, asset size, or change in business focus.	The institution has not been involved in any merger or acquisition activity but has experienced modest organic growth. Branch expansion is minimal, with little impact on product volumes or asset size.	The institution has been involved in merger or acquisition activity that has resulted in the institution's market expanding and above-average growth, or the institution has experienced above-average organic growth through branching activities.	The institution has been involved in a major merger or acquisition or has experienced significant organic growth, including significantly expanding its branching network.	There has been significant growth due to merger or acquisition activity, and product volume growth has been strong. As a result of growth or market expansion, the institution's business focus may have changed.
Structural complexity					
Refers to the overall complexity of the institution's operations, including its subsidiary structure, branch networks, and degree of centralization of activities.	The banking organization's operations structure, including its branch operations and subsidiary and affiliated relationships, is noncomplex. The organization has no operating subsidiaries and limited branching activity. Operations are highly centralized.	The banking organization's operations structure, including its branch operations and subsidiary and affiliated relationships, is noncomplex, although the number of branches may be high. The organization has no operating subsidiaries and no shared activities with affiliated entities. Operations may evidence some degree of decentralization.	The banking organization's operations structure, including its branch operations and subsidiary and affiliated relationships, is moderately complex. The institution may conduct consumer business through one or more subsidiaries or divisions and may have a complex branch structure. Businesses may operate with a fair degree of independence from one another.	The banking organization's operations structure, including its branch operations and subsidiary and affiliated relationships, is complex. The institution conducts consumer business through one or more subsidiaries or divisions and may have a very complex branch structure, including substantial interstate operations. Businesses may operate with a substantial degree of independence from one another.	The banking organization's operations structure, including its branch operations and subsidiary and affiliated relationships, is very complex. The institution conducts consumer business through multiple subsidiaries or divisions in a large geographical area. Businesses may operate independently from one another.

Component	Low	Limited	Moderate	Considerable	High
History/trends					
Refers to the extent to which the institution has effectively managed its compliance risk in the past.	The institution has historically managed its compliance risk highly effectively. The compliance management program has historically been adjusted in anticipation of the changing level of compliance risk.	The institution has historically managed its compliance risk effectively. Minor compliance issues may have developed but were not allowed to persist. The compliance management program has typically been adjusted to be commensurate with the level of compliance risk. Nonetheless, minor defects in the program may have persisted for brief periods.	The institution has historically allowed gaps in its management of compliance risk to develop. Some significant compliance weaknesses have developed and have persisted for some time. The institution may be under an informal enforcement action. Timely adjustment of the compliance management program in response to changes in the level of risk has not been routine. Defects in the program may have persisted for long periods.	The institution has gaps in its management of compliance risk that have persisted over time. The institution may be under a formal enforcement action. A number of significant compliance weaknesses have resulted and may currently exist. Correction of weaknesses in the compliance management program generally occurs only after the institution has been cited for noncompliance.	The institution has serious gaps in its management of compliance risk that have persisted over time. The compliance program is ineffective, and the institution is under a formal enforcement action.

Component	Low	Limited	Moderate	Considerable	High
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.	Although not immaterial, the product has low activity. Only a small number of customers have the product.	The product has limited activity, and few customers have the product.	The product has moderate activity. The institution is actively opening new accounts and/or maintains and services a fair number of existing accounts.	The product has significant activity throughout the organization. It is one of the institution's primary products.	The product has very significant activity throughout the organization. It is considered a major product line for the organization.
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.	The institution has a narrow product line, offering basic consumer banking products. It delivers the products through traditional methods.	The institution has a more expansive product line, but consumer banking products are basic. Systems for managing products are not complex. The institution delivers the products through traditional methods.	The institution offers a variety of products, some of which are complex. The institution does not target products to particular consumer segments. Systems for managing products are somewhat complex.	The institution offers an extensive variety of products, many of which are complex. It delivers the products through many different delivery channels and targets some products to particular consumer segments. Its systems for managing these products are complex.	The institution offers almost all types of consumer banking products through all available delivery methods. The product mix includes many products targeted to particular consumer segments. Systems for managing these products are extremely complex.
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.	The institution has had no major changes in products and services.	The institution has made minor changes to the features of existing products and services, but no new complex products or services have been introduced.	The institution has expanded its products or services to include more complex products or has made modest changes to systems related to product handling. Additional expertise is necessary to manage the expanded products and services.	The institution has made major modifications to existing products or services or the systems that manage the products. The product or system changes require new staff to manage them.	The institution has introduced a new high-risk line of business (such as subprime mortgage loans or indirect or brokered loans) or made considerable changes to existing business lines. System changes related to the new business line are extensive.

Component	Low	Limited	Moderate	Considerable	High
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.	Reliance on outsourcing arrangements/ third-party vendors is minimal. Vendors are well-respected industry leaders. The institution has a large, heterogeneous mix of strong vendors that have good industry reputations.	There is moderate reliance on outsourcing arrangements/ third-party vendors for standard, noncomplex services.	The institution has an average number of, and dependency on, third-party vendors. Vendors are a relatively good mix of industry-recognized leaders. Some vendors may be new but show good understanding of the industry and are well run. The institution may rely on vendors that have had previous problems.	The institution relies substantially on outsourcing arrangements/ third-party vendors. Vendors may be new or smaller untested firms for which there is limited financial history.	The institution is entirely dependent on outsourcing arrangements/ third-party vendors for critical services or systems. The institution has a high number of or concentration of work with vendors. Key vendors are largely unseasoned.

Component	Low	Limited	Moderate	Considerable	High
LEGAL AND REGULATORY FACTORS *Legal and financial harm that may result from noncompliance*					
Regulation complexity					
Refers to the amount of judgment, regulatory knowledge, technical skill, or processes required to understand and comply with a law or regulation.	The products and services offered by the institution and the laws and regulations with which it must comply require only a basic level of understanding, judgment, and skill to ensure compliance.	The institution's business lines and the laws and regulations with which it must comply require an enhanced level of judgment, skills, and processes to ensure compliance.	The institution's business lines and the laws and regulations with which it must comply require an intermediate level of judgment, skills, and processes to ensure compliance. The institution offers products within one state only.	The complexity of some of the institution's business lines and some of the laws and regulations with which it must comply require an advanced level of judgment, skills, and processes to ensure compliance. Also, the organization may serve multiple states and therefore must have an understanding of applicable state laws and regulations.	The complexity of the institution's business lines and the various laws and regulations with which it must comply require an expert level of judgment, skills, and processes to ensure compliance. Because it serves multiple states, the organization must have expertise in all applicable state laws and regulations.
Consequences of noncompliance (consumer harm, penalties)					
Refers to the extent to which the institution's failure to comply with legal or regulatory requirements will result in actual or potential financial or legal harm to a consumer or other serious consequences, such as bank penalties or sanctions.	The consequences of noncompliance are minimal.	The consequences of noncompliance may not involve significant monetary costs.	The consequences of noncompliance may involve some monetary costs, legal or regulatory sanctions, or delay in expansion plans.	The consequences of noncompliance involve significant monetary costs, legal or regulatory sanctions, or delay in expansion plans.	The consequences of noncompliance involve substantial monetary costs, legal or regulatory sanctions, or delay in expansion plans.
Regulatory or legal changes					
Refers to new laws, regulations, or amendments or modifications to existing laws or regulations.	The institution does not engage in activities that have been subject to any regulatory changes.	The institution has been subject to some minor regulatory changes as part of the normal course of business.	The institution has been subject to regulatory changes, some of which may have been significant.	The institution engages in a number of activities that are subject to regulatory changes, some of which may have been significant and involve multiple sources of change such as multiple state or local ordinances, court rulings, and federal agencies.	The institution's primary business lines involve activities that are continuously subject to regulatory changes, many of which may be significant and involve multiple sources of change such as multiple state or local ordinances, court rulings, and federal agencies.

Component	Low	Limited	Moderate	Considerable	High
ENVIRONMENTAL FACTORS *External factors that may affect an institution's ability to effectively manage its compliance risk*					
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 are good or stable. Operational changes are not being driven by changes in business conditions, and operational capacity is more than adequate for maintaining a strong compliance position.	Business conditions may show some weakness, but the effect on bank operations is limited or the institution has adequate operational capacity for responding effectively to the changing conditions.	Business conditions are deteriorating, and bank operations have been affected. The institution's capacity to respond to changing conditions is constrained by existing personnel, inadequate processes, and/or the inability to hire or train the personnel necessary to respond to changing conditions.	Business conditions are deteriorating, and bank operations have been significantly affected. The institution's capacity to respond to changing conditions is greatly constrained by existing personnel, inadequate processes, and/or the inability to hire or train the personnel necessary to respond to changing conditions. Compliance resources may be reallocated to address other areas of weakness.	Business conditions are weak, and bank operations have been seriously affected. The institution is not able to respond effectively to changing conditions due to inadequate resources, failing processes, and the inability to hire or train the personnel necessary to respond to changing conditions. Compliance resources have been reallocated to address other areas of weakness.
Demographics					
Refers to the demographic characteristics of the markets in which the institution operates.	The institution serves markets with little demographic diversity. The area is likely predominantly rural. There are few, if any, low- or moderate- income census tracts. The minority population is very low.	The institution serves markets with some amount of demographic diversity. The area is likely still predominantly rural. There are few low- or moderate-income census tracts, but there may be distressed or underserved census tracts. The minority population is limited and there are few, if any, majority-minority census tracts.	The institution serves markets with a moderate amount of demographic diversity. The markets likely include urban areas. There are a number of low- or moderate-income census tracts. The minority population is significant, and there may be some majority-minority census tracts.	The institution serves markets with demographic diversity. The area is likely mostly urban. There are a significant number of low- or moderate-income census tracts. The minority population is substantial, and there are a number of majority-minority census tracts.	The institution serves markets with substantial demographic diversity. The area is likely highly urban. There are a large number of low- or moderate-income census tracts. The minority population is substantial, and there are a significant number of majority-minority census tracts.

Component	Low	Limited	Moderate	Considerable	High
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.	The institution has not made, nor does it plan to make in the near future, any significant changes in response to competitive pressures. New product development and change management processes are deemed adequate given the institution's risk profile.	Competitive factors have had a limited effect on bank operations. While the institution is attuned to its competition, it has not made significant changes to its product offerings, product terms, or marketing; however, it has the operational capacity to respond in the normal course of business.	Competitive factors have had a moderate effect on bank operations. The institution has made some significant changes to product offerings, product terms, or marketing. In making these changes, operational capacity has been strained and some compliance missteps may have occurred.	Competitive factors have had a significant effect on bank operations. The institution has made some substantial changes to product offerings, product terms, or marketing. These changes involve greater complexity and/or the expansion into new products or markets. In making these changes, operational breakdowns have occurred because of inadequate planning, development, and review processes. These breakdowns may have resulted in serious compliance failures.	Competitive factors have had a material effect on bank operations. The institution has made substantial changes to its product offerings, product terms, or marketing. These changes involve substantially greater complexity and/or the expansion into new products or markets without sufficient consideration of whether the changes align with the institution's long-term strategic direction. In making these changes, operational breakdowns have occurred because of inadequate planning, development, and review processes. These breakdowns have resulted in serious compliance failures.

APPENDIX 3. GUIDANCE FOR ASSESSING CONSUMER COMPLIANCE RISK MANAGEMENT

Board and Senior Management Oversight

This element is an evaluation of the adequacy and effectiveness of the board and senior management's understanding and management of risk inherent in the institution's activities, as well as the general capabilities of management. It also includes consideration of management's ability to identify, understand, and control the risks undertaken by the institution, to hire competent staff, and to respond to changes in the institution's risk profile or innovations in the banking sector.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Overall assessment	The board and senior management clearly understand the types of compliance risks inherent in the institution's activities and actively participate in managing those risks and pursuing industry best practices.	The board and senior management have an adequate understanding of the organization's compliance risk profile and provide largely effective oversight of risk management practices.	The board and senior management have a limited understanding of the organization's compliance risk profile, and oversight of risk management practices may be lacking in some important way.	The board and senior management have an inadequate understanding of the organization's compliance risk profile, and oversight of risk management practices reflects a lack of guidance and supervision.	There is a critical absence of effective board and/or senior management oversight.
COMPOSITION					
Board responsibilities	The board fully understands and has approved overall business strategies and significant policies and ensures that senior management is fully capable of managing the activities.	The board generally understands and has approved overall business strategies and significant policies and ensures that senior management is capable of managing the activities.	Weaknesses in one or more aspects of board oversight have prevented the institution from fully understanding or addressing one or more significant legal and compliance risks to the institution.	Ongoing weaknesses in one or more aspects of board oversight have prevented the institution from fully addressing one or more significant legal and compliance risks to the institution.	Critical weaknesses in one or more aspects of board oversight have caused the institution to have significant legal, regulatory and/or compliance issues that have had a major negative effect or consequence.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Management expertise	Management hires staff who possess experience and expertise consistent with the scope and complexity of the organization's business activities. Staffing levels are sufficient to fully and effectively manage the institution's operations and related compliance risks. Management is generally recognized as having considerable expertise in compliance risk management.	Management generally hires staff who possess experience and expertise consistent with the scope and complexity of the organization's business activities. Minor weaknesses may exist in the staffing, infrastructure, or consumer compliance risk management expertise for individual business lines or products.	Management has hired staff who may not be adequate or may not possess experience or expertise consistent with the scope and complexity of the organization's business activities. Identified weaknesses exist in the staffing, infrastructure, or consumer compliance risk management expertise for individual business lines or products.	Management has hired staff who are not adequate or do not possess the experience or expertise needed for the scope and complexity of the organization's business activities. The day-to-day supervision of officer and staff activities, including the management of senior officers or heads of business lines, may be considerably lacking.	Management has not hired staff capable of managing the institution's compliance program. Substantial weakness exists in compliance management expertise for individual business lines or products.
CULTURE					
Ethical values	The board and senior management effectively ensure that employees will exhibit a high level of integrity and ethical values that are consistent with a prudent management philosophy and culture.	The board and senior management communicate an expectation that employees will exhibit a high level of integrity and ethical values that are consistent with a prudent management philosophy and culture.	The board and senior management informally communicate an expectation that employees will exhibit integrity and ethical values that are consistent with a prudent management philosophy and culture.	The board and senior management have failed to communicate an expectation that employees will exhibit integrity and ethical values that are consistent with a prudent management philosophy and culture.	Integrity, ethical values, and competence are not consistent with a prudent management philosophy and culture.
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.	Risk appetite and tolerance levels are generally identified, communicated, and understood throughout the organization.	Risk appetite and tolerance levels may not be clearly identified, communicated, or understood throughout the organization.	Risk appetite and tolerance levels are not clearly identified, communicated, or understood throughout the organization, or the level of risk is not considered prudent.	Risk appetite and tolerance levels are not identified, communicated, or understood throughout the organization, and/or the level of risk jeopardizes the ongoing viability of the organization.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
			EFFECTIVENESS		
Management involvement	The board and senior management are fully informed about compliance matters and provide fully effective supervision of day-to-day activities throughout the organization. Compliance risks are always fully considered in the development of the organization's overall business strategy.	The board and senior management are generally informed about compliance matters. The day-to-day supervision of officers and staff at all levels is generally effective. Compliance risks are generally considered in the organization's overall business strategy.	The board and senior management are inconsistently informed about compliance matters. The day-to-day supervision of officers and staff, including the management of senior officers or heads of business lines or control functions, may be lacking. Compliance risks are occasionally considered in the organization's overall business strategy.	The board and senior management are rarely informed about compliance matters. The day-to-day supervision of officers and staff, including the management of senior officers or heads of business lines or control functions, is lacking. Compliance risks are rarely considered in the organization's overall business strategy.	The board and senior management are not informed about compliance matters, and there is no evidence of day-to-day supervision of officers and staff, including the management of senior officers or heads of business lines and control functions. Compliance risks are not considered in the organization's overall business strategy.
Management responsiveness	The board and senior management respond quickly to changes in the marketplace; proactively identify all compliance risks associated with proposed new activities, services or products offered; and ensure that the appropriate infrastructure and internal controls are established and effective in all business lines before the activities or products are initiated.	The board and senior management ensure that risk management practices are appropriately adjusted in accordance with new activities or enhancements to industry practices and regulatory guidance or expectations.	The board and senior management may adjust risk management practices in accordance with new activities or enhancements to industry practices and regulatory guidance or expectations, although these practices may be lacking in some degree.	The board and senior management rarely adjust risk management practices in accordance with new activities or enhancements to industry practices and regulatory guidance or expectations. Current practices are significantly lacking in varying degrees.	The board and senior management do not adjust risk management practices in accordance with new activities or enhancements to industry practices and regulatory guidance or expectations. Current practices are very ineffective.

Policies, Procedures, and Limits

This element is an evaluation of the adequacy of an institution's policies and procedures, given the risks inherent in the activities of the consolidated organization and the organization's stated goals and objectives. This component includes an assessment of the institution's training programs to determine if they are comprehensive and appropriate for the size and activities of the organization.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Overall assessment	Compliance policies, procedures, and training are comprehensive and consistent with the institution's business goals and objectives.	Compliance policies, procedures, and training are generally consistent with the institution's business goals and objectives.	Compliance policies, procedures, and training may be somewhat inconsistent with the institution's business goals and objectives.	Compliance policies, procedures, and training do not address significant compliance risks to the institution.	There is a critical absence of effective compliance policies, procedures, and training.
POLICIES AND PROCEDURES					
Formality and approval practices	Policies are appropriate, comprehensive, understood, and regularly reviewed and updated.	Policies are generally appropriate and understood and are regularly reviewed and updated.	Some policies may not be appropriate or understood and are not always regularly reviewed and updated.	Policies may be outdated and inappropriate for current business activities.	Policies are nonexistent or wholly inadequate.
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 institution's activities and between lines of business and associated control or support functions.	Compliance policies cover all significant activities and are adequate. The policies generally provide a clear delineation of accountability and lines of authority across the institution's activities.	Compliance policies cover most activities but may be lacking in specificity. The policies may not provide a clear delineation of accountability and lines of authority across the institution's activities.	Compliance policies are largely ineffective. The policies do not provide a clear delineation of accountability and lines of authority across the institution's activities.	Policies are nonexistent or wholly inadequate.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Sufficiency of procedures	Procedures provide operating personnel with clear and specific guidance in fulfilling their compliance responsibilities.	Procedures provide operating personnel with adequate guidance in fulfilling their compliance responsibilities.	Procedures may not provide operating personnel with sufficient guidance to fulfill their compliance responsibilities. Deficiencies may involve a broad range of activities or may be material to a major business line or activity.	Procedures do not provide operating personnel with sufficient guidance to fulfill their compliance responsibilities. Deficiencies involve a broad range of activities or are material to a major business line or activity.	Procedures are nonexistent or wholly inadequate.
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.	Policies and procedures provide for adequate due diligence before engaging in new activities or products.	Policies may not consistently provide for adequate due diligence before engaging in new activities or products.	Policies and procedures do not provide for effective due diligence before engaging in new activities or products.	Due diligence processes are nonexistent or wholly inadequate.
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.	All appropriate managers and staff have been formally trained on and are generally knowledgeable about the key relevant laws, regulations, policies, and procedures. Training occurs at appropriate frequencies.	Some of the appropriate managers and staff have been formally trained on the key relevant laws, regulations, policies, and procedures, although a wider audience, area of coverage, or increased frequency may be needed. Weaknesses are noted in the level of staff knowledge regarding relevant laws, regulations, policies, and procedures.	Few managers and staff have been trained on relevant laws, regulations, policies, and procedures. Training is informal, not conducted in a meaningful way, or not delivered at appropriate frequencies. Significant knowledge gaps exist among management and staff.	Compliance training does not exist in any meaningful way. Critical knowledge gaps exist among management and staff.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Formality and applicability	Compliance training programs are fully comprehensive and innovative, and results are fully documented.	Training programs are generally effective, and results are sufficiently documented.	Training programs are lacking in some fashion, and results are minimally documented.	Training programs are ineffective or not documented.	Compliance training does not exist in any meaningful way.
Effectiveness	Training is formally tracked, and results are monitored through robust management information systems (MIS).	Training is tracked through some MIS, although areas may need modest improvement.	Training is tracked through only high-level MIS, making it not meaningful.	Training is not tracked through MIS in any meaningful way.	Training is not tracked through MIS.
Accountability	Compensation and performance evaluations consider training attendance and achievement as a significant part of overall performance.	Compensation and performance evaluations may consider training attendance and achievement as a lesser part of overall performance.	Compensation and performance evaluations do not consider training attendance and achievement in any substantive way.	Compensation and performance evaluations do not consider training attendance and achievement in any way.	Compensation and performance evaluations do not consider training records in any way.

Risk Monitoring and Management Information Systems

This element is an evaluation of the adequacy of an institution's risk measurement and monitoring and the adequacy of its management reports and information systems. This analysis will include a review of the assumptions, data, and procedures used to measure risk and the consistency of these tools with the level of complexity of the organization's activities.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Overall assessment	Risk monitoring practices and MIS are comprehensive, timely, and address all material compliance and legal risks.	Risk-monitoring practices and MIS cover major risks and business areas, although they may be lacking in some modest degree.	Weaknesses exist in the institution's risk-monitoring practices or MIS that may involve a broad range of activities.	Inadequate risk-monitoring practices or MIS reports exist that involve a substantial number of business lines or activities.	A critical absence of risk-monitoring and MIS exists.
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.	MIS reports provided to the board and senior management are accurate and timely and broadly identify adverse trends and the level of compliance risks facing the institution, although there may be room for improvement.	MIS reports provided to the board and senior management may not be distributed to appropriate decisionmakers, may not contain significant risks or properly identify adverse trends and compliance risks facing the institution, or may not be distributed in a timely manner.	MIS reports provided to the board and senior management are not distributed to appropriate decisionmakers, do not identify significant adverse trends and compliance risks facing the institution, and are frequently not distributed in a timely manner.	MIS reports provided to the board and senior management are wholly deficient due to inappropriate information, incorrect data, and/or poor documentation.
Effectiveness	MIS reports provided to the board and senior management and other forms of communication are fully efficient, comprehensive, and consistent with all activities.	MIS reports provided to the board and senior management and other forms of communication are generally consistent with the key activities.	MIS reports provided to the board and senior management and other forms of communication may be lacking in some significant way.	MIS reports provided to the board and senior management and other forms of communication are limited and ineffective.	MIS reports provided to the board and senior management are wholly deficient due to inappropriate information, incorrect data, and/or poor documentation.
MONITORING PRACTICES					
Monitoring practices	Strong legal, regulatory, and compliance risk-monitoring programs and associated methodologies are in place.	Satisfactory legal, regulatory, and compliance risk-monitoring programs are in place, but modest improvement is needed.	Weaknesses may contribute to ineffective legal, regulatory, and compliance risk identification or monitoring.	A number of significant legal, regulatory, and/or compliance risks are not adequately monitored or reported.	Legal, regulatory and/or compliance risk-monitoring processes are inadequate.

Internal Controls

This element is an evaluation of the adequacy of an institution's internal controls and audit procedures, including the strength and influence of the internal audit team within the organization. This analysis will also determine whether control functions are independent of management and verify that the scope of the internal audit is commensurate with the organization's complexity.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Overall assessment	The system of internal controls is considered strong for the type and level of compliance risk posed by the nature and scope of the organization's activities.	The system of internal controls adequately covers all major compliance risks and business areas.	Weaknesses exist in the system of internal controls that require more than normal supervisory attention and that affect a broad range of activities or may be material to a major business line or activity.	The institution has a weak internal control system that does not adequately address significant compliance risk to the institution and that may result in inadequate, untimely, or nonexistent compliance risk coverage and/or verification practices.	There is a critical absence of an effective internal control system, which results in completely inadequate or untimely compliance risk coverage and/or verification practices.
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.	The organizational structure generally establishes clear lines of authority and responsibility for adherence to compliance policies and procedures. In general, the control functions are independent from the business lines and there is appropriate separation of duties, but some minor areas of weakness may be noted, although they are correctable in the normal course of business.	Unclear or conflicting lines of authority and responsibility exist. There is a lack of independence between control functions and business activities or ineffective separation of duties.	The institution has conflicting lines of authority and responsibility. There is a lack of independence between control areas and business activities and/or no separation of duties in critical areas.	The institution has completely conflicting lines of authority and responsibility, with no distinction between control areas and business activities or no separation of duties.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
AUDIT					
Independence	Audit or other control review practices provide for clear independence and objectivity.	In general, audit or other control review practices provide for independence and objectivity.	Audit or other control review practices are lacking some independence and objectivity.	Audit or other control review practices lack independence.	Audit or other control review practices completely lack independence, and the audit or control practices are so ineffective that examiners cannot rely on them.
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.	The risk methodology, frequency, and coverage are generally sufficient, although some modest weaknesses may be noted.	The risk methodology, frequency, and coverage do not properly address some key compliance risk areas.	The risk methodology, frequency, and coverage do not properly address the compliance risk areas in a substantive and meaningful way.	The risk methodology, frequency, and coverage are highly flawed and do not properly address the compliance risk areas.
Documentation	Coverage, procedures, findings, and responses to audits and review tests are all well documented.	Coverage, procedures, findings, and responses to audits and review tests are all generally well documented, although some areas for improvement may exist.	Documentation for work performed in some areas is lacking.	Documentation for work performed in numerous areas is lacking.	Documentation for work performed is completely absent.
Follow-up and reporting	When exceptions or material weaknesses are noted, they are promptly investigated and corrected. Management's actions to address material weaknesses are objectively reviewed and verified.	In most cases, exceptions and identified material weaknesses are given appropriate and timely attention. Any weaknesses or deficiencies that have been identified are modest in nature and are in the process of being addressed. Management's actions to address material weaknesses are reviewed and verified.	In some cases, exceptions and identified material weaknesses are not given appropriate and timely attention. Management's actions to address material weaknesses are not always reviewed and verified or are not reviewed and verified in a timely manner.	In most cases, exceptions and identified material weaknesses are not given appropriate and timely attention. Management's actions to address material weaknesses, when identified, are not verified or are not reviewed in a timely manner.	No management review exists to ensure the correction of exceptions or identified weaknesses.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Oversight	The board or its audit committee regularly reviews the results of material audits and findings, as well as the effectiveness of audits and other control review activities.	The board or its audit committee routinely reviews the results of some audits and the overall effectiveness of the audit program and other control review activities, although some recommendations for improvement may exist.	Oversight of audit and other control mechanisms by the board or its audit committee is generally insufficient.	Oversight of audit and other control mechanisms by the board or its audit committee is lacking in material and substantive ways.	The board or its audit committee has no oversight of audit and other control mechanisms.
SYSTEMS AND AUTOMATION					
Sufficiency and testing	Systems and automation are thoroughly tested and reviewed. They are effectively aligned with policies and procedures. Updates and changes are reviewed by compliance, audit, or legal staff as appropriate.	Systems and automation are adequately tested and reviewed. They are generally aligned with policies and procedures. Updates and changes are generally reviewed by compliance, audit, or legal staff as appropriate.	Systems and automation are not regularly tested and reviewed. They do not completely align with policies and procedures. Updates and changes are reviewed only by the business line.	Systems and automation are not tested or reviewed once established. They do not align with policies and procedures in significant areas. Controls over system updates and changes are lacking in some meaningful way.	Systems and automation have not been tested or reviewed. They do not align with policies and procedures. No monitoring of system updates and changes exists.
Accuracy and level of interfacing/ controls	Bank systems effectively interface. Management ensures that financial, operational, legal, compliance, and regulatory reports are reliable, accurate, and timely.	Bank systems generally interface, although a modest degree of operational adjustment is needed. Generally, management ensures that financial, operational, legal, compliance, and regulatory reports are reliable, accurate, and timely.	Bank systems generally interface, but weaknesses exist. Management does not ensure that financial, operational, legal, compliance, and regulatory reports are reliable, accurate, and timely. Some records may be inaccurate.	Bank systems do not interface. Inaccurate records or financial, operational, or legal, compliance, or regulatory reporting exist.	Bank systems conflict. Records or legal, compliance, or regulatory reporting are completely inaccurate or nonexistent.

Component	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
			COMPLIANCE REVIEW AND TESTING		
Scope and depth of compliance review and testing programs	The institution has in place a fully robust compliance review and testing program. Fully documented risk assessments are in place that identify and rate all applicable laws and regulations based on risk.	The institution has in place a compliance review and testing program. Risk assessments are in place that generally identify and rate applicable laws and regulations based on risk.	The compliance review program is lacking in ways that make it not fully effective. Risk assessments may not be in place or may not identify and rate applicable laws and regulations based on risk.	The compliance review program is lacking in substantive ways, and it is not considered effective. Risk assessments are not in place or do not identify and rate applicable laws and regulations based on risk.	The compliance review program is wholly lacking or completely ineffective. Risk assessments do not exist.
Documentation and follow-up practices	Results of compliance reviews and testing programs are fully documented, and robust MIS is created and appropriately distributed. The institution takes quick corrective actions to fully address any identified issues or exceptions.	Results of compliance reviews and testing programs are adequately documented, although some minor areas may need improvement or MIS may be in place but is lacking in some minor way. The institution generally takes corrective actions in a timely manner to address major issues or exceptions.	Results of compliance reviews and testing are not always adequately documented and need improvement. The institution may not take corrective actions in a timely manner, or the actions may not address major issues or exceptions.	Results of compliance reviews and testing are poorly documented. The institution does not take corrective actions, or its actions are ineffective.	Results of compliance reviews and testing are not documented. The institution does not take corrective actions, or its actions are wholly ineffective.
			OPERATIONAL CONTROLS		
Scope and depth of controls	A robust system of operational controls to mitigate compliance risk is an integral part of daily operations of business lines or activities.	An adequate system of operational controls to mitigate compliance risk is an integral part of daily operations of business lines or activities.	The institution's system of operational controls is not fully effective or does not address all key areas of compliance risk in daily operations of business lines or activities.	The institution's system of operational controls is inconsistent and yields ineffective results.	The institution has no system of operational controls, or the system is wholly ineffective.
Follow-up practices	Identified errors or issues are immediately corrected, and processes are adjusted to prevent future errors.	Identified errors or issues are corrected in a timely manner, but preventive measures are not always taken.	If errors are identified, they may or may not be corrected, and no preventive measures are taken.	Errors are not consistently identified or corrected, and no preventive measures are taken.	Errors are rarely identified or corrected, and no preventive measures are taken.

APPENDIX 4. REPORT OF EXAMINATION

The report should convey information to the bank about the conduct of the examination, examiner findings and conclusions (including conclusions about CRA performance, as applicable), and the bank's rating.

Report Format

The report consists of an open section provided to the institution and a confidential section used by the Federal Reserve. Reserve Banks are free to modify the report to reflect unique situations or to adapt the format to reflect their own programs.

All report-related documents must conform to the Board's Information Security Manual (ISM) classification requirements. Report-related documents will be classified as Restricted FR.

Timely transmittal of examination-related documents is an important part of the examination process. The Consumer Affairs Report of Examination and CRA Performance Evaluation (where applicable) will be transmitted to state member banks and the Board no later than 60 calendar days following the close of an examination. As part of this process, the Reserve Bank will transmit copies of the following to the Board, as applicable:

- transmittal letter
- report of examination
- CRA performance evaluation
- scope memoranda and scope addendum, as applicable
- institutional profile and (post-examination) risk assessment
- pertinent correspondence for institutions rated 3, 4, or 5

Relevant information will be entered into national exam data (NED) within three business days of transmitting the examination report and CRA Performance Evaluation to the Board and the institution. A copy of the report also should be forwarded to the appropriate state banking department. The Reserve Bank will retain a copy of the examination report, along with any relevant correspondence.

Open Section

Table of Contents

If necessary, Reserve Banks may modify the table of contents to reflect unique situations or adapt the format to reflect their own program. At a minimum, however, the table of contents will include the following sections and their corresponding page numbers in the report:

- executive summary and examination ratings
- scope of the examination
- evaluation of the consumer compliance risk management program
- evaluation of the fair lending program
- violations of laws and regulations (if applicable)[8]
- CRA assessment (if applicable)

Executive Summary and Examination Ratings

The executive summary provides a brief overview of the examination report findings. The effectiveness of this page depends on the accuracy, brevity, and clarity of the discussion. When complex issues or other matters are included, the summary should discuss the general nature of these matters in a few sentences, prioritized by the significance of the issues, and should refer the reader to the appropriate section of the report for a more detailed discussion.

This section of the report contains the institution's name and date of examination, a list of Reserve Bank and state member bank officers and staff who attended the exit meeting, and a discussion of the following matters:

- examiners' conclusions regarding the institution's compliance and CRA programs and applicable ratings
- a discussion of significant issues and required corrective action (Matters Requiring Immediate Attention (MRIA) and Matters Requiring Attention (MRA))

Each of these areas is discussed in more detail below.

1. Examiners' conclusions regarding the bank's compliance and CRA programs and applicable ratings. This section includes both the compliance and the CRA ratings, along with their accompanying standardized descriptions from the Uniform Interagency Consumer Compliance Rating System. This section also includes a brief description of the effective-

8. It is not necessary to include in the table of contents an exhaustive list of all consumer banking statutes and regulations reviewed during the examination. To focus attention on the most important examination findings, only those laws and regulations with substantive violations should be listed under the violations of laws and regulations section in the table of contents. For example, if an institution was not subject to Regulation M, then that regulation would not be listed in the table of contents. Likewise, if the bank was subject to Regulation M, but no violations related to that regulation were included in the report, Regulation M would not appear in the table of contents.

ness of the institution's compliance program and the primary factors that contributed to the assigned compliance and CRA ratings.

2. A discussion of significant issues and required corrective action. This section discusses significant issues identified during the examination that require corrective action. Both MRIAs and MRAs will be discussed in the section, along with a time frame within which the banking organization must complete the corrective actions. In many circumstances, it may be appropriate to require the banking organization to submit an action plan that identifies remedial actions to be completed within specified time frames.

Scope of Examination

The scope of examination section contains the following information:

- compliance areas reviewed, by business line or product, as identified through the risk assessment and scoping processes (examination activities utilized, extent of transaction testing, as applicable, and reliance on compliance management program)
- CRA examination method (small bank, intermediate small bank, large bank, etc.)
- statement that CRA community contacts were conducted (do not include names).

While the name of the institution and the date of the examination may also be included, this information is not necessary if it is included in the Executive Summary.

Evaluation of the Compliance Risk Management Program

The evaluation focuses on the effectiveness and comprehensiveness of the institution's compliance management program as it relates to the institution's consumer-related activities. The discussion should support examiners' conclusions regarding the compliance rating assigned to the institution. Comments in this section are to be evaluative rather than descriptive. In addition, this section will discuss any significant changes in the institution's level of compliance since the last examination. Examiners should factor in the causes of violations into the overall assessment of the compliance management program.

Examiners will evaluate the institution's compliance management program, including assessing how the program manages and controls fair lending and UDAP risk, in the context of the elements of risk management, including: board and senior management oversight, policies, procedures, and limits; risk-monitoring and management information systems; and internal controls.

Evaluation of the Fair Lending Program

This section includes a summary of the fair lending risk assessment, including a discussion of the presence of any fair lending risk factors, an evaluation of the fair lending program, and conclusions regarding fair lending risk. If examiners identified and evaluated a fair lending focal point (s), the discussion should also summarize the examination work by describing the following:

- type of analysis (for example, pricing or redlining)
- time period reviewed
- product(s) reviewed
- market(s) reviewed
- decision center(s) reviewed
- target group(s) reviewed
- sample sizes used
- conclusion(s)

This section will also include a description of any violations of the anti-discriminatory provisions of the Equal Credit Opportunity Act/Regulation B and the Fair Housing Act (FHA) and should contain any advisory comments deemed necessary.

Violations involving other provisions of Regulation B and the FHA usually involve technical aspects of these regulations and should be discussed in the Violations of Laws and Regulations section of the examination report. Likewise, violations of HMDA and the Fair Credit Reporting Act should be presented in the Violations of Laws and Regulations section and not in the Fair Lending section of the examination report.

Violations of Laws and Regulations (if applicable)

While all regulatory violations are important, the examination report must direct management's attention to those violations that represent the highest degree of risk to the institution or its customers and to those that require immediate corrective action. Violations included in the report of examination are often characterized by one or more systemic or procedural weaknesses. Such violations usually or potentially affect a large number of transactions or customers. Violations that represent repeat deficiencies or a condition or practice that, when combined with other regulatory violations, reflects unfavorably on the effectiveness of an institution's compliance management program should also be included in the report of

examination. Moreover, violations that have significant consequences to consumers, such as violations resulting in restitution, or to institutions, such as violations of the flood insurance rules, are generally included in the report of examination.

Examiner judgment and a thorough understanding of the circumstances surrounding the violations are critical in determining whether they should be included in the report. Other than for fair lending and UDAP, isolated violations that are inadvertent errors or other errors not indicative of bank practice are not generally included in the report of examination. A large number of isolated violations, however, may indicate weaknesses in an institution's compliance management program and, when considered together, could elevate the violations to a more serious level. In those cases, the violations would likely be discussed in the examination report.

All violations, regardless of whether or not they are included in the report of examination, must be discussed with bank management, thoroughly documented in the examination work papers, and entered in the Federal Reserve's examination database.

1. Organization of violations. This section of the report may be organized by regulation or statute, or by function (loan or deposit type), branch, or in any other logical order. Whatever method is used, the aspects of the institution's activities with the most significant violations should be listed first. For example, if the violations of Regulation Z were the most important, then those violations should be listed first. Likewise, if the findings were organized by function, and credit card violations were the most significant, this area should be listed first.
2. Description of violations. The scope of the review for a particular regulation or statute should be discussed before the violations for that regulation or law are presented. This discussion may include a listing of what the examination reviewed (e.g., policies, procedures, disclosures, or other matters), the number of loans sampled, and a short summary of examiners' findings. Comparisons to the last examination may also be included here.

To draw attention to the violations, a citation to the relevant law or regulation will be highlighted. This may be done by placing the cite in the margin, at the beginning of the discussion, or on a line above the discussion. It is not necessary to begin a new page for each regulation or statute. The discussion of a violation must include

- a description of the problem, the extent of the problem, and how the institution's situation differs from the law's requirement or prohibition
- the cause of the problem, if it can be determined
- required corrective action, recommendations, and the institution's response (if available)

It is not necessary to specify corrective action for a particular violation if corrective action is implicit in the description of the violation. Appropriate recommendations should address changes to the institution's internal controls, procedures, or other elements of the compliance management program that are needed to prevent similar violations from occurring. It may also be appropriate to give broad recommendations in the executive summary rather than in the discussion of individual violations.

CRA Assessment (if applicable)

This section of the report is limited to information related to the institution's CRA performance that is not suitable for the CRA Performance Evaluation. This section should not reiterate the information contained in the performance evaluation and should not be included in the report if there is no relevant information to be discussed.

This section should begin with the following statement: "The discussion of the institution's CRA performance in this examination report supplements the public performance evaluation. To obtain an understanding of an institution's overall CRA performance, the CRA examination summary report must be read in conjunction with the public performance evaluation."

Information in this section may include, but is not limited to, lending restrictions, supervisory actions that have not been made public, or comments regarding Reserve Bank follow-up activities.

Confidential Section

The primary purpose of the confidential section of the examination report is to provide Reserve Bank and Board staff with confidential or administrative information. This information is not shared with management of the institution. As a result, the confidential pages of the examination report are not included in the report transmitted to the institution.

The confidential section must include

- the current compliance rating and CRA rating, including date(s)
- the previous compliance rating and CRA rating, including date(s)
- the name of the examiner in charge

- a list of other examiners participating on the examination
- if fair lending violations are identified, a discussion of any pertinent information not included in the open section of the report.
- a listing of community contacts made as part of the CRA examination

In addition, where such information may shed additional light on the current examination or inform future examinations, the examiner may consider also including

- material deemed unsuitable for the open section of the report because of privacy issues
- information, such as tentative institution plans or strategies, that may affect the scope or conduct of the next compliance examination or other issues to be targeted or considered for review during scoping, monitoring, or other future supervisory events
- CRA-related information deemed unsuitable for the open section of the report, such as tentative institution plans or strategies that may affect the scope or conduct of the next CRA examination

With respect to information necessary for monitoring, scoping, or other future supervisory events, examiners will include comments on outstanding or recommended enforcement actions, recommended Reserve Bank follow-up activities, a target date for the next examination or supervisory event, recommended interim advisory visits, and suggestions for the focus of future examinations.

The confidential section will also include a discussion of issues that affect the institution's overall compliance level or position. Examples might include anticipated changes in certain management positions, ownership of the institution, or the effect of potential reimbursements on the institution's capital. If appropriate, comments on this page could also include the names of individuals or other sources responsible for substantive violations. Finally, information on pending consumer litigation that might affect the institution's compliance management program may also be included here.

Transmittal Letter

While Reserve Banks may exercise some discretion with the format, the following may provide useful advice in drafting portions of the transmittal letter.

The letter transmitting the examination report must draw attention to the most significant issues identified in the report's Executive Summary. To this end, the letter will include the compliance and CRA ratings, as applicable. The transmittal letter must be sent to the institution's board of directors or to the institution's president with a requirement that it be shared and discussed with the board and must include a statement that it is considered confidential supervisory information.

The letter must also require the board to respond formally to any significant findings noted in the examination report, including the specific actions that will be taken to address the weaknesses. If corrective action is required as a result of an examination, the transmittal letter should identify a specific time frame or due date by which the institution must detail and forward to the Reserve Bank an explanation of the actions it has taken or plans to take and should include any request for supporting documents, when warranted. If appropriate, an action plan that identifies remedial actions to be completed within specified time frames may be requested. Action plans with intermediate- and long-term time frames that span more than a 12-month period should include interim progress targets. The board should be allowed sufficient time to respond to the examination findings.

Requiring a response to the examination report, however, is not always necessary. For example, if the examiners identify a few minor violations during the examination but no major issues that need to be addressed, no response from the institution would be necessary. If the institution takes corrective action on the violations identified during an examination before the conclusion of the examination, and if examiners confirm the corrective action and note it in the report, a formal response to that aspect of the report would not be necessary.

The transmittal letter will also include information concerning the timing and availability of the institution's CRA performance evaluation, as applicable, and explaining the institution's option to include in its public file any comments it may have regarding the performance evaluation.

APPENDIX 5. RATINGS AND ENFORCEMENT

Ratings

The primary purpose of the rating system is to draw conclusions about the effectiveness of an institution's consumer compliance risk management program. In assigning a consumer compliance rating, examiners must evaluate all relevant factors related to the effectiveness of an institution's compliance management program. The rating descriptions below provide basic guidance for reaching conclusions about the effectiveness of an institution's compliance risk management practices. This should not be interpreted to mean that in order to attain a specific rating an institution needs to demonstrate all of the factors listed in the definition. In addition, the levels of sophistication and formality of the compliance management program should be viewed in the context of the scope and the complexity of the organization.

The Uniform Interagency Consumer Compliance Rating System is based upon a scale of 1 through 5 in increasing order of supervisory concern. Thus 1 represents the highest rating and consequently the lowest level of supervisory concern, and 5 represents the lowest, most critically deficient level of performance and therefore the highest degree of supervisory concern. Each of the five ratings is described below.

Rating 1

An institution in this category is in a strong compliance position. Management is capable of and staff is sufficient for effectuating compliance. An effective compliance program, including an efficient system of internal procedures and controls, has been established. Changes in consumer statutes and regulations are promptly reflected in the institution's policies, procedures, and compliance training. The institution provides adequate training for its employees. If any violations are noted, they relate to relatively minor deficiencies in forms or practices that are easily corrected. There is no evidence of discriminatory acts or practices, reimbursable violations, or practices resulting in repeat violations. Violations and deficiencies are promptly corrected by management. As a result, the institution gives no cause for supervisory concern.

Rating 2

An institution in this category is in a generally strong compliance position. Management is capable of administering an effective compliance program. Although a system of internal operating procedures and controls has been established to ensure compliance, violations have nonetheless occurred. These violations, however, involve technical aspects of the law or result from oversight on the part of operating personnel. Modification in the institution's compliance program and/or the establishment of additional review/audit procedures may eliminate many of the violations. Compliance training is satisfactory. There is no evidence of discriminatory acts or practices, reimbursable violations, or practices resulting in repeat violations.

Rating 3

Generally, an institution in this category is in a less than satisfactory compliance position. It is cause for supervisory concern and requires more than normal supervision to remedy deficiencies. Violations may be numerous. In addition, previously identified practices resulting in violations may remain uncorrected. Overcharges, if present, involve few consumers and are minimal in amount. There is no evidence of discriminatory acts or practices. Although management may have the ability to effectuate compliance, increased efforts are necessary. The numerous violations discovered are an indication that management has not devoted sufficient time and attention to consumer compliance. Operating procedures and controls have not proven effective and require strengthening. This may be accomplished by, among other things, designating a compliance officer and developing and implementing a comprehensive and effective compliance program. By identifying an institution with marginal compliance early, additional supervisory measures may be employed to eliminate violations and prevent further deterioration in the institution's less than satisfactory compliance position.

Rating 4

An institution in this category requires close supervisory attention and monitoring to promptly correct the serious compliance problems disclosed. Numerous violations are present. Overcharges, if any, affect a significant number of consumers and involve a substantial amount of money. Often, practices resulting in violations and cited at previous examinations remain uncorrected. Discriminatory acts or practices may be in evidence. Clearly, management has not exerted sufficient effort to ensure compliance. Its attitude may indicate a lack of interest in administering an effective compliance program, which may have contributed to the seriousness of the institution's compliance problems. Internal procedures and controls have not proven effective and are seriously

deficient. Prompt action on the part of the supervisory agency may enable the institution to correct its deficiencies and improve its compliance position.

Rating 5

An institution in this category is in need of the strongest supervisory attention and monitoring. It is substantially in noncompliance with the consumer statutes and regulations. Management has demonstrated its unwillingness or inability to operate within the scope of consumer statutes and regulations. Previous efforts on the part of the regulatory authority to obtain voluntary compliance have been unproductive. Discrimination, substantial overcharges, or practices resulting in serious repeat violations are present.

Adverse Ratings and Enforcement Actions

Institutions with consumer compliance ratings of 3, 4, or 5 are considered to need more than normal supervisory attention. CA Letter 81-5 contains specific actions that are required for institutions in these rating categories, as detailed below.

Fair Rating—3

A rating of 3 indicates an institution whose compliance position is borderline between being acceptable and unacceptable. Weaknesses exist that require prompt management attention. The prompt use of effective remedial measures can arrest deterioration in the institution's compliance position. A primary advantage of the 3 classification is that supervisory resources are focused on problems and deficiencies before they have seriously undermined an institution's compliance efforts.

While institutions with consumer compliance ratings of 3 require corrective action, a distinction should be made between those 3-rated institutions that show a deteriorating or stagnant situation and those institutions exhibiting a positive trend in consumer compliance. While both situations require ongoing management and Reserve Bank attention, the supervisory response will, to some degree, depend on the trend of the institution under review.

An improving 3-rated institution may require nothing more than time and continued management vigilance. A deteriorating or stagnant 3-rated institution should receive closer attention from the Reserve Bank, since this situation often indicates the absence of an adequate management response in correcting the institution's weaknesses. In order to facilitate adequate management attention, it is essential to clearly define all the weaknesses and properly fashion the corrective programs. This should normally be achieved by executing a Memorandum of Understanding (MOU) between the state member bank's board of directors or management and the Reserve Bank. Reserve Banks should execute an MOU as part of the examination follow-up procedures for each 3-rated institution, unless the institution's consumer compliance position is improving or unless other individual circumstances rule out the appropriateness or feasibility of using this supervisory tool. For institutions whose 3 rating reflects an improving trend, it may be sufficient to keep the institution's management apprised of problem areas through explicit transmittal letters, follow-up examinations, telephone contacts, and/or follow-up educational/advisory visits or discussions.

The MOU is not a formal written agreement as contemplated by the Financial Banks Supervisory Act of 1966 (such as those discussed with respect to institutions rated 4). It represents, instead, a good faith understanding between the state member bank and the Reserve Bank concerning the institution's principal problems and the proposed remedial plans for correcting those problems. The MOU should be prepared and executed by the Reserve Bank and the institution under examination. Board approval is not generally required, although the Board's staff is available for consultation on any matters relating to implementing this procedure. A copy of any such MOU, however, must be entered into the Federal Reserve's supervisory document repository, the Central Document and Text Repository (CDTR).

While the MOU is meant to be a flexible supervisory tool, it should, at a minimum, include the following:

- a brief listing and summary of the principal problems and deficiencies
- a brief outline of management's and/or the directors' plans for remedial action, including any audits, training, or procedural changes
- a provision for periodic progress reports to be sent to the Reserve Bank
- the signatures of the directors, indicating their review, agreement, and approval of the terms
- the signature of the relevant Reserve Bank official, indicating only that the remedial program appears reasonable in light of the institution's compliance problems

Remedial plans, as set out in the MOU, should be realistic and specific enough to gauge the institution's progress. If possible, they should be designed after consultation with the institution, since bank directors and management have the ultimate responsibility for designing and implementing a program of corrective action. Appropriate Reserve

Bank personnel should visit the institution to develop and present an MOU whenever feasible.

Even though penalties cannot be imposed for bank management's failure to make a good faith effort to implement the provisions of the MOU, its failure to do so might constitute future grounds for considering a formal supervisory action (Written Agreement or Cease and Desist Order). The use of MOUs will not preclude the use of Written Agreements or Cease and Desist Orders for certain 3-rated institutions when very serious compliance program deficiencies or violations of law have been identified or when management has failed to undertake necessary corrective action. Reserve Bank staff should undertake appropriate follow-up action to ensure that bank management takes necessary corrective action in a timely manner.

In the event that the policy outlined in this statement is believed to be inappropriate or not feasible with respect to a 3-rated institution, a detailed explanation should be incorporated into the confidential section of the report of examination or in a separate letter or memorandum to the Oversight Section of the Division of Consumer and Community Affairs (DCCA). However, consideration should be given to other types of informal enforcement action that include the following:

- *Board resolutions* generally represent a number of formal commitments made by the institution's full board of directors and are incorporated into the institution's corporate minutes. The Reserve Bank will draft the board resolution and may request in the examination transmittal letter that the institution provide it with a signed copy of the corporate resolution. Alternatively, Reserve Bank management may deliver the board resolution to the institution's directors and direct its adoption.
- *Commitment letters* are generally used to correct minor problems or to request periodic reports addressing certain aspects of an institution's operations. Commitment letters may be used when there are no significant violations of law or unsafe or unsound practices and when the institution and its officers and directors are expected to cooperate and comply. Commitments are generally obtained by the Reserve Bank sending a letter to the institution outlining the request and asking for a response and an indication that the commitments are accepted.

Marginal Rating—4

A 4 rating indicates that the institution's management and directors may lack the interest or ability to produce and maintain an effective consumer compliance program. Internal routines and controls are either ineffective or nonexistent. Repeat violations, discriminatory practices, and overcharges may all be present.

Formal supervisory action, in most cases a formal Written Agreement, should be pursued for 4-rated institutions. The Written Agreement should require that management put in place a comprehensive remedial program dealing with each of the institution's principal problem areas. In addition, requirements such as an internal audit program, training programs, forms review, hiring a qualified compliance officer, and development of a written lending policy should be considered. An analysis of the relevant facts and recommendations regarding the provisions that should be included in the Written Agreement should be sent to the Board's staff to prepare the necessary documentation. In addition, the Reserve Bank is expected to submit the examination report in draft to Board staff, as appropriate, when formal enforcement action against an institution is expected.

Note that Written Agreements and Cease and Desist Orders concerning violations of law cannot be issued under delegated authority and can only be issued by the Board. The primary consideration in choosing between a Cease and Desist Order and a formal Written Agreement lies in the severity of the violations and bank management's willingness or ability to correct them. Appropriate Reserve Bank officials should attend the meeting of the institution's board of directors at which the Written Agreement or Cease and Desist Order is presented, in order to underscore the seriousness of the matter and to elicit full support for the terms of the agreement. In appropriate cases, Board personnel will attend the meeting.

The seriousness of the problems of an institution rated 4 for consumer compliance cannot be overstated. In light of the seriousness of the problems of 4-rated institutions, the Reserve Bank should make sure that follow-up examinations are conducted in accordance with current policy. Reports of examination for follow-up examinations, any other correspondence with the subject institution, and internal memoranda describing meetings with the institution's management or board of directors must be posted to CDTR.

If the Reserve Bank believes that a departure from the policy outlined in this statement regarding an institution rated 4 for consumer compliance is warranted, it should explain the need for the departure in detail and submit recommendations for alternative action in a letter to the director of DCCA. With the division director's concurrence, the Reserve Bank may undertake alternative ap-

proaches to the institution's problems not prescribed by this policy statement.

Unsatisfactory Rating—5

An institution in this condition has demonstrated its unwillingness or inability to comply with the law. Generally, previous efforts to obtain compliance by such an institution have been unsuccessful. Discrimination and/or substantial overcharges may exist. Such an institution requires a strong supervisory response and continual close monitoring.

Formal supervisory action, in most cases the imposition of a Cease and Desist Order, is warranted. The Cease and Desist Order should require that management put in place a comprehensive remedial program dealing with each of the institution's principal problem areas. In addition, requirements such as an internal audit program, training programs, forms review, hiring a qualified compliance officer, and development of a written lending policy should be considered.

An analysis of the relevant facts and recommendations regarding the provisions that should be included in the Cease and Desist Order should be sent to the Board's staff for preparation of the necessary documentation. As is the case with Written Agreements, Cease and Desist Orders concerning violations of law cannot be issued under delegated authority and can only be issued by the Board. For consent to Cease and Desist Order proceedings, appropriate Reserve Bank officials should, whenever possible, attend the meeting of the institution's board of directors at which the order is presented. The goal is to indicate to the institution that this is a very serious matter to the Reserve Bank and to encourage a strong commitment by the board of directors to see that the terms of the order are met. In appropriate cases, Board personnel will also attend the meeting.

In light of the seriousness of the problems of institutions with a 5 rating for consumer compliance, the Reserve Bank should make sure that follow-up examinations are conducted in accordance with current policy. Reports of examination for follow-up examinations, any other correspondence with the subject institution, and internal memoranda describing meetings with the institution's management or board of directors must be posted to CDTR.

If the Reserve Bank believes that a departure from the policy outlined in this statement with respect to an institution rated 5 for consumer compliance is warranted, it should explain the need for the departure in detail and submit recommendations for alternative action in a letter to the Director of DCCA. With the division director's concurrence, the Reserve Bank may undertake alternative approaches to the institution's problems not prescribed by this policy statement.

APPENDIX 6. INTERNAL CONTROL AND INTERNAL AUDIT FUNCTIONS, OVERSIGHT, AND OUTSOURCING

The information in this appendix is intended to assist examiners' understanding of internal control and internal audit, and the differences between the two. The appendix also provides specific guidance on how to assess internal control and internal audit and how to leverage internal audit in the scoping process. Tools for assessing outsourced internal audit arrangements are included in the discussion of internal audit.

The information in this appendix draws heavily on the following three sources:

1. *Commercial Bank Examination Manual,* Section 1010.1, Internal Control and Audit Function, Oversight, and Outsourcing
2. *Commercial Bank Examination Manual,* Section A.1010.1, Internal Control: Supplement on Internal Auditing
3. Supervision and Regulation (SR) Letter 03-5, Amended Interagency Guidance on the Internal Audit Function and its Outsourcing

Examiners are encouraged to review each of these source documents for additional information and guidance related to internal controls and auditing.

Overview

This section sets forth the principal aspects of effective internal controls and internal audit. It assists examiners in understanding and evaluating the objectives of and the work performed by internal auditors. It also sets forth the general criteria examiners should consider when determining whether the work of internal auditors may be relied on as part of the examination. To the extent that audit records may be relied on, they should be used to determine the appropriate scope of the examination. In situations where audit records may not be relied upon, additional supervisory activities such as interviews or limited transaction testing may be appropriate, depending on the residual risk of the product or service.

Effective internal controls are the foundation for the safe, sound, and compliant operation of a financial institution. The board of directors and senior management are responsible for ensuring that the system of internal controls is effective. Their responsibility cannot be delegated to others within or outside the organization. An internal audit function is an important element of an effective system of internal control. When properly structured and conducted, internal audit provides directors and senior management with vital information about the condition of the system of internal control, and it identifies weaknesses so that management can take prompt remedial action. Examiners should review an institution's internal audit function as it relates to consumer compliance and recommend improvements, if needed.

In summary, internal controls are designed to provide reasonable assurance that the institution will achieve the following objectives: efficient and effective operations, including safeguarding of assets, reliable financial reporting, and *compliance with applicable laws and regulations.* Internal controls consist of five primary components: the control environment, risk assessments, control activities, information and communication, and monitoring activities. The effective functioning of these components, which is brought about by an institution's board of directors, management, and other personnel, is essential to achieving the internal controls objectives. This description of internal controls is consistent with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 1992 report, *Internal Control—Integrated Framework*.[9]

Community banks should adopt a recognized internal control framework that is appropriate for their needs and for safe and sound operations. COSO's framework is an example of one such method that many banks have found to be useful. Although this framework is used by multi-billion-dollar financial institutions, it is flexible enough to work effectively at a bank with only $25 million in total assets as well.

As noted, internal audit and internal controls are interrelated and therefore are frequently confused. In short, internal control is related to the effectiveness of the overall business process. Appropriate controls assure that the process is effective and is the foundation for the safe and sound operation of the organization. Audit is used by management to assure that the operational controls it has designed are effective. Thus, audit is a *monitoring* mechanism and part of a well-designed internal control system.

Objectives of Internal Control

The three objectives of internal control relate to operations, reporting, and compliance. In order to achieve these objectives, a system of internal control should include those procedures necessary to ensure timely detection of failure of accountability, and such procedures should be performed by competent persons who have no incompatible

9. In May 2013, COSO issued an updated version of its internal control framework. The original 1992 framework will remain available during the transition period but will be superseded effective December 15, 2014.

duties. The following standards are encompassed within the description of internal control:

Existence of Procedures

Existence of prescribed internal control procedures is necessary but not sufficient for effective internal controls. Prescribed procedures that are not actually performed do nothing to establish control. Consequently, examiners must give thoughtful attention not only to the prescribed set of procedures but also to the practices actually followed. This attention can take the form of inquiry, observation, testing, or a combination of these approaches.

Competent Performance

For internal controls to be effective, competent persons must perform the required procedures. Evaluation of competence undoubtedly requires some degree of subjective judgment because attributes such as intelligence, knowledge, and attitude are relevant. Thus, examiners should be alert for indications of employees who have not performed their duties effectively and should ask questions about their abilities.

Independent Performance

If employees who have access to assets also have access to the related accounting records or perform related review operations (or immediately supervise the activities of other employees who maintain the records or perform the review operations), they may be able to both perpetrate and conceal defalcations. Therefore, duties concerned with the custody of assets are incompatible with recordkeeping duties for those assets, and duties concerned with the performance of activities are incompatible with the authorization or review of those activities.

Understanding Internal Controls

In order to understand internal controls, it is important to start with a focus on the business process or the distribution of the product or service. This understanding is the basis for assessing the potential failures in the process, which could result in negative outcomes. As mentioned above, the COSO framework may be used to systematically analyze how the business process is controlled. The COSO framework focuses attention on five components: control environment, risk assessment, control activities, information and communication, and monitoring activities.

The *control environment* component includes an assessment of the culture of control in the organization. It deals with questions about the degree of concern that the organization has for assuring that operations will meet financial and operational goals and also result in compliance with applicable laws and regulations.

Risk assessment describes the process that the board and senior management goes through to consider risk. It also involves determining the organization's risk tolerance and establishing appropriate risk-measurement practices.

Control activities are the actions and procedures built into the business process to assure that an organization gets the business outcomes it desires. These control activities often are erroneously viewed as being all that constitutes a system of internal control. Common control activities include such specific processes as: having employees bonded and insured; having appropriate authorizations to initiate transactions; having pre-numbered documents to assure completeness of records; separation of critical duties such as custody, authorization, and recordkeeping; and incorporating mechanical and software controls into processes.

Information and communication are the ways in which the organization organizes and reports information about risks and their control to decision-makers. These are important elements of a control system, and the degree to which they are incorporated into an organization's business process will determine the outcomes of the business.

Monitoring activities test the quality of information or the effectiveness of controls. Monitoring activities may be part of the normal business process, such as managers reviewing daily work, or they may be special activities like internal or external audits that assess controls.

Examiners should review the adequacy of the internal control system for each business line or process under review. This assessment can be accomplished through reviews of established procedures or compliance audit/review work papers, through discussions with line management, or by testing actual transactions. Examiners' review should determine whether the organization's internal controls are working properly.

Assessing the Adequacy of Internal Control

The COSO framework provides broad guidance on the components that should be considered in assessing a system of internal control. Since the controls are designed to assure that a business process is meeting its objectives to provide reliable financial information, compliance with relevant laws and regulations, and effective and efficient opera-

tions, it is useful to consider internal control in light of business processes affected by consumer regulations.

In order to adequately assess the effectiveness of the internal control structure in an institution's lending and deposit operations, examiners first need to understand the institution's structure, business lines, and products offered. Specifically, this includes understanding the entire loan or deposit account origination process, from the initial application to consummation. Examiners must also be aware of events that occur throughout the life of the product, which may trigger additional consumer rules or subsequent disclosure requirements. By understanding (''mapping'') the entire product process from beginning to end, examiners will become more familiar with the internal control checkpoints, which are crucial to ensuring that compliance-related disclosures are accurate and delivered to the consumer in a timely manner. When violations are identified, often the root cause of the violation can be traced back to a breakdown in or lack of controls at one or more of these checkpoints. Understanding the root cause and the full scope of the errors will help examiners determine whether or not the violations noted represent a pattern or practice. The following internal controls are present at many of the control checkpoints:

- policies and procedures
- use of automated systems
- use of checklists
- segregation of duties
- periodic testing by the compliance officer or compliance staff

Policies and Procedures

Policies provide a framework for more detailed operating procedures that may be used as a reference source or as training material for bank personnel. Comprehensive and fully implemented policies help to communicate the board of directors' and senior management's commitment to and expectations for compliance. Procedures should provide personnel with specific guidance that helps them complete transactions in accordance with applicable laws, regulations, and supervisory guidance. Such information may include appropriate regulatory citations and definitions, sample forms, instructions, and where appropriate, directions for routing, reviewing, and retaining transaction documents.

The degree to which compliance policies and procedures are formalized is not as important as their effectiveness and the consistency with which they are performed. This distinction is especially true in smaller institutions, where established compliance practices may not be in writing but are nonetheless effective if fully communicated to the staff, performed on a regular basis, and periodically monitored. Conversely, at larger, more complex institutions that have many employees and multiple locations, the need for more formalized written policies and procedures will be greater.

Use of Automated Systems

This control is software that is programmed to automate aspects of both the lending and deposit functions by creating, among other things, compliance-related disclosures based on information input from a customer's application and other related sources. Institutions usually purchase these programs from third-party vendors that warrant the disclosures will be correct if the software is used in accordance with instructions. In addition, institutions rely on the third-party vendor to provide software updates when changes to any laws or regulations occur. If used properly and validated when changes occur, automated software programs help to achieve compliance consistency on an ongoing basis.

However, overreliance on vendors can lead to complacence on the part of staff responsible for compliance. A strong vendor management program, as discussed throughout this supervision program, is a key control for ensuring that automated tools serve as an effective control mechanism.

Use of Checklists

Checklists are very good tools to help ensure that all procedures to originate a loan or set up a deposit account are performed. These are no more than the organization's policies and procedures condensed into a summary document. Checklists not only prompt employees to complete all necessary steps for a given transaction but also are used by the organization to document its compliance with a law or regulation.

Segregation of Duties

Segregation of duties occurs when an employee not involved with the particular transaction at hand verifies the work of another employee. The classic example is having one employee enter information from an application into an automated system and a second employee review the accuracy of the input by comparing information on an application to a report (for example, the new loan report) generated from the automated system.

Periodic Testing by the Compliance Officer or Compliance Staff

Sometimes referred to as compliance reviews, these tests are performed periodically on key, or high-risk, areas to ensure ongoing compliance. This testing can be accomplished by having the compliance officer judgmentally select loan or deposit accounts and test, for example, the accuracy of the finance charge and annual percentage rate. Periodic testing can also be an effective means of monitoring new products to ensure compliance with laws, regulations, and supervisory guidance as well as the institution's own policies and procedures.

The Role of Internal Audit

Internal auditing is an independent assessment function established within an institution to examine and evaluate its system of internal controls and the efficiency with which the various units of the institution carry out their assigned tasks. The objective of internal auditing is to assist the board and senior management in discharging their responsibilities effectively. To this end, internal auditing furnishes management with analyses, evaluations, recommendations, counsel, and information concerning the activities reviewed.

Accordingly, an institution's internal audit function provides essential independent validation of its compliance risk management framework. Internal audit has a unique responsibility to the board of directors and senior management regarding the compliance culture and sound operational practices. The function is enterprise-wide in nature, and its products provide a basis for understanding risks, transactions, operations, and the internal control environment.

An Institution's Board or a Committee of the Board Should Actively Oversee the Audit Function

While monitoring of operational risks can be delegated to others in the institution and the internal audit function may be completely or partially outsourced, ultimate responsibility cannot be delegated. According to the Federal Deposit Insurance Corporation Improvement Act, each institution with total assets of $1 billion or more, as of the beginning of the fiscal year, is required to have an audit committee, the members of which must be outside directors who are independent of the institution's management.[10] Institutions with total assets of at least $500 million but less than $1 billion, as of the beginning of the fiscal year, must have an audit committee, the members of which are outside directors and the majority of whom must be independent of the institution's management. For publicly traded companies, all audit committee members must be independent. The committee must have at least three members, with at least one qualifying as an "Audit Committee Financial Expert." For insured institutions with total assets of more than $3 billion, the audit committee must (1) have members with banking or related financial management expertise, (2) have access to outside legal counsel, and (3) not include any large customers of the institution.

Smaller, less complex institutions often do not have an audit committee, and the audit function is supervised by the full board. In addition, these institutions may have only one board member experienced in preparing or analyzing financial information.

Active boards or audit committees have clearly identified responsibilities, members with appropriate skills and interests, active meeting attendance, and robust discussions about risk and risk management. In addition, the board or audit committee should have the opportunity to meet with the head of the audit function without members of management present. Audit also should have the authority and funding to engage consultants or legal experts as necessary to meet its responsibilities. Finally, information packages should provide the board or the audit committee with sufficient information to monitor the effectiveness of the audit function. This information should include the results of audits completed since the last meeting, the status of unresolved exceptions, and status reports on the audit plan.

The Audit Function Should Be Independent and Adequately Staffed

The audit function should demonstrate an independent, skeptical approach and be free of undue influence from management. Functionally, audit should report to the board or audit committee and, ideally, should report administratively to an executive officer who can influence behavior throughout the institution. In addition, staff performing audit functions should not have management or operational responsibilities that could interfere with their independence, including direct involvement in an institution's compliance risk management process. The audit function should not be restricted from receiving information from any area of the institution. Finally, staff performing audit functions should have the necessary competence and access to ongoing training.

Larger, more complex institutions typically have an audit department with a full-time director. Job descriptions for all levels of audit staff include

10. FDICIA, 12 C.F.R. Part 363.

minimum qualifications, including education and certification. Specialized skills (such as knowledge about mortgage banking or fair lending analyses) are developed internally or outsourced to competent third-party providers to ensure adequate coverage of more complex business lines and processes.

Smaller institutions may not have an internal audit department but should have an audit function appropriate for their size and the nature and scope of their activities. At a minimum they should implement a comprehensive set of independent reviews of significant internal controls. The audit function may be assigned to an officer with other nonaudit responsibilities who nevertheless can maintain independence from the areas being audited. This individual may have no formal audit credentials but should have significant operational experience and knowledge of internal controls. Audit activities at smaller institutions can be performed by individuals from various operational areas who have limited audit duties but are independent of the areas being audited.

The Audit Function Should Identify and Assess Risks

The risk identification and assessment process is one of the most critical elements in an effective internal audit function. A flawed methodology can negatively affect every other audit activity, including planning, execution, and reporting. The highest risk to the audit function itself is failure to identify a risk or to properly assess the severity and priority of a given risk. Risk assessment results provide the board, senior management, and the audit department with an opportunity to view risks and risk management from both a departmental and an enterprisewide perspective.

Risk identification and assessment should be a dynamic process that includes line management, senior management, and internal audit. Ongoing risk-identification and assessment processes should include a continuous evaluation of inherent risks and the controls to mitigate those risks. Risk assessments should be updated to reflect changes in business lines, products, processes, people, systems, and structures and should include external as well as internal factors.

In larger, more complex institutions, audit risk assessment is typically an enterprisewide process that involves senior management, line management, and internal audit. The risk assessment process has a defined methodology and criteria for assigning risk ratings that have been reviewed and approved by the board or the audit committee. Risk ratings may be assigned judgmentally, by the use of statistical methods, or by a combination of the two. Assessment results are provided to the audit committee. In smaller institutions, the risk assessment process is generally less formal and less extensively documented and generally may be performed annually rather than on an ongoing basis.

Banks Should Conduct Comprehensive Audit Planning

Audit plans help the audit committee and senior management determine whether the function is meeting its stated goals. An audit plan that does not include adequate or timely review of issues can negatively affect the audit function's ability to identify and report compliance and internal control weaknesses. Audit planning should be risk focused, and the areas chosen for coverage and the audit frequency should be based on the level of risk identified in the risk assessment. The plan should consider all auditable entities, business lines, and processes within the institution, including potential acquisitions and planned new products and services. It should also include areas for which audit work is expected to be outsourced and should include provisions to monitor and follow up on any audit work conducted by third parties. It should be used for budgeting and resource allocation. Finally, the audit plan should be approved by the board and provide a mechanism for reporting deviations from the plan to the board and senior management.

At larger, more complex institutions, formal audit plans are approved by the audit committee. The audit committee approves deviations from plan and has the authority to request additional audits or follow-up audits. It is notified of any request for special internal audit projects that would affect the department's ability to meet its audit plan. At smaller institutions, risk assessments and audit plans may be less formal, but board members should have a good understanding of the relationship between the institution's risks and the audit processes being performed.

Audit Programs Should Have Relevant Content and Should Be Consistently Executed

Audit program content should keep pace with changes in the institution's processes, products, people, and systems. Audit procedures should focus on validating the effectiveness of internal controls, identifying control weaknesses, and testing compliance with applicable laws and regulations. They should consider exceptions from prior audits, concerns of management, issues identified in regulatory examinations, and comments from the external auditor's management letter. Consistency in execution and the overall effectiveness of the

audit program can be enhanced by having audit procedure and work paper standards, as well as by having independent reviews of work papers (by a quality assurance function or external audit).

Audit Findings Should Be Effectively Reported

Effective communication of audit findings enhances management's ability to respond to and correct exceptions. Audit policies should establish clear reporting standards, including timelines, consistent terminology for ratings and opinions, and reporting procedures. For each area audited, reports should clearly identify the scope, findings, any necessary corrective action to be taken by management, and an overall rating or opinion. There should be a system for classifying findings by severity (for example, low/moderate/high or recommended vs. required actions). In addition, repeat exceptions should be clearly identified, with ratings adjusted to reflect the existence of unresolved or recurring exceptions. Finally, reports should be distributed to all management affected by the noted exceptions. At larger, more complex institutions, the audit policy may establish formal timelines for the reporting process. The timeline may include the time established to complete fieldwork, issue the report, and receive management's response, as well as a time frame for presenting the report to the audit committee. Smaller institutions may have less formal guidelines for issuing audit reports.

Audit Exceptions Should Be Promptly Resolved

Business lines or departments should track exceptions and corrective action measures until the internal audit function has validated the effectiveness of corrective action. Procedures should include provisions for escalating unresolved exceptions to higher levels in the institution. Management's response to exceptions should include the date the exception will be corrected and the person responsible for correcting the exception. In addition, internal audit should follow up on high-risk exceptions shortly after the planned correction date. Finally, information on open audit items should be reported to the board or audit committee.

Audit Outsourcing Arrangements

Management may choose to outsource its compliance audit program. The principles outlined in SR Letter 03-5 are helpful in evaluating the outsourced relationship. A summary of these concepts is discussed below.

As with any vendor relationship, outsourced audit may be effective if managed properly. Moreover, it can potentially reduce compliance risk by providing a higher-quality audit program. Senior management is responsible for ensuring that the institution's system of internal controls operates effectively. One way to meet this responsibility is by contracting with outside third parties to perform audit procedures on behalf of management.

However, while the audit work can be delegated to outside parties, managing the relationship and any identified findings is the ultimate responsibility of the board of directors and senior management. This responsibility cannot be delegated to others. Furthermore, it is important that communication between the audit function, the audit committee, and senior management not diminish because the institution engages an outside vendor. Senior management also should ensure it has a contingency plan for addressing any vendor performance issues.

Examples of Internal Audit Outsourcing Arrangements

An outsourcing arrangement is a contract between an institution and a vendor to provide internal audit services. Outsourcing arrangements take many forms and are used by institutions of all sizes. Some institutions consider entering into these arrangements to enhance the quality of their control environment by obtaining the services of a vendor with the knowledge and skills to critically assess their internal control systems and recommend improvements. The contracted internal audit services can be limited to helping internal audit staff members with assignments for which they lack expertise. Such an arrangement is typically under the control of the institution's manager of internal audit, and the outsourcing vendor reports to him or her. Institutions often use outsourcing vendors for audits of areas requiring more technical expertise, such as mortgage banking or fair lending analyses. Such uses are often referred to as ''internal audit assistance'' or ''audit co-sourcing.''

Some outsourcing arrangements may require an outsourcing vendor to perform virtually all the procedures or tests of the internal control system. Under such an arrangement, a designated manager of internal audit oversees the activities of the outsourcing vendor and typically is supported by internal audit staff. The outsourcing vendor may assist the audit staff in determining risks to be reviewed and may recommend testing procedures, but the internal audit manager is responsible for approving the audit scope, plan, and procedures to be performed. Furthermore, the internal audit manager is responsible for the results of the outsourced audit work, including findings, conclu-

sions, and recommendations. The outsourcing vendor may report these results to the audit committee jointly with the internal audit manager.

Additional Considerations for Internal Audit Outsourcing Arrangements

Even when outsourcing vendors provide internal audit services, the board of directors and senior management are responsible for ensuring that both the system of internal control and the internal audit function operate effectively. In any outsourced internal audit arrangement, the institution's board of directors and senior management must maintain ownership of the internal audit function and provide active oversight of outsourced activities. When negotiating an arrangement with an outsourcing vendor, an institution should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. The outsourcing arrangement should not increase the risk that a breakdown in internal controls will go undetected.

To clearly distinguish its duties from those of the outsourcing vendor, the institution should have a written contract, often taking the form of an engagement letter. Contracts between the institution and the vendor typically include provisions that

- define the expectations and responsibilities under the contract for both parties
- set the scope and frequency of, and the fees to be paid for, the work to be performed by the vendor
- set the responsibilities for providing and receiving information, such as the type and frequency of reporting to senior management and directors about the status of contract work
- establish the process for changing the terms of the service contract, especially for expansion of audit work if significant issues are found, and stipulations for default and termination of the contract
- state that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related work papers it deems necessary, and that employees authorized by the institution will have reasonable and timely access to the work papers prepared by the outsourcing vendor
- specify the locations of internal audit reports and the related work papers
- specify the period of time (for example, seven years) that vendors must maintain the work papers[11]
- state that outsourced internal audit services provided by the vendor are subject to regulatory review and that examiners will be granted full and timely access to the internal audit reports and related work papers prepared by the outsourcing vendor
- prescribe a process (arbitration, mediation, or other means) for resolving disputes and for determining who bears the cost of consequential damages arising from errors, omissions, and negligence
- state that the outsourcing vendor will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of a member of management or an employee

Vendor Competence

Before entering into an outsourcing arrangement, the institution should perform due diligence to satisfy itself that the outsourcing vendor has sufficient staff who are qualified to perform the contracted work. The staff's qualifications may be demonstrated, for example, through prior experience with financial institutions in the compliance function, or certifications such as being a former commissioned federal bank examiner with a consumer compliance specialty, Certified Regulatory Compliance Manager (CRCM), Certified Risk Professional (CRP), Chartered Bank Auditor (CBA), or Certified Financial Services Auditor (CFSA). Because the outsourcing arrangement is a personal-services contract, the institution's internal audit manager should have confidence in the competence of the vendor's staff and receive timely notice of key staffing changes. Throughout the outsourcing arrangement, management should ensure that the outsourcing vendor maintains sufficient expertise to effectively perform its contractual obligations.

Management of the Outsourced Internal Audit Function

Directors and senior management should ensure that the outsourced internal audit function is competently managed. For example, larger institutions should employ enough competent staff members in the internal audit department to assist the manager of internal audit in overseeing the outsourcing vendor. Small institutions that do not employ a full-time audit manager should appoint a competent employee, who ideally has no managerial responsibility for the areas being audited, to oversee the outsourcing vendor's performance

11. If the work papers are in electronic format, contracts often call for the vendor to maintain proprietary software that enables the institution and examiners to access the electronic work papers for a specified period of time.

under the contract. This person should report directly to the audit committee for purposes of communicating internal audit issues.

Communication When an Outsourced Internal Audit Function Exists

Communication between the internal audit function and the audit committee and senior management should not diminish because the institution engages an outsourcing vendor. All work by the outsourcing vendor should be well documented, and all findings of control weaknesses should be promptly reported to the institution's manager of internal audit. Decisions not to report certain findings of the outsourcing vendor to directors and senior management should be the mutual decision of the internal audit manager and the outsourcing vendor. In deciding what issues should be brought to the board's attention, the concept of ''materiality,'' as the term is used in financial statement audits, is generally not a good indicator of which control weakness to report. For example, when evaluating an institution's compliance with laws and regulations, any exception may be important.

Contingency Planning to Ensure Continuity of Outsourced Audit Coverage

An institution may increase its operational risk when it enters into an outsourcing arrangement or significantly changes the mix of internal and external resources used by internal audit. Because an outsourced arrangement may be terminated suddenly, the institution should have a contingency plan to mitigate any significant disruption in audit coverage, particularly for high-risk areas.

Using Audit in the Supervisory Process

Audits and internal control reviews are designed to test whether the institution has adopted a business process that is operating as it should be and that complies with applicable consumer protection laws and regulations.[12] An examiner's goal in reviewing audits is to draw conclusions about the ability of an organization to identify, monitor, and resolve compliance problems with its business process at an early stage and thereby reduce the risk that such problems could pose to the institution. Examiners evaluate the audit program and determine the degree to which the audit function's assessment of the quality of internal controls can be considered as evidence of the effectiveness and consistency of the compliance management program. In that regard, examiners should ensure that management implements preventive controls and that the audit or compliance review programs test the controls. Management should not rely on the detective audit or compliance reviews in place of its ongoing preventive controls. To the extent the audit function is deemed reliable, the compliance audits should be used to help set the scope of the examination.

Conducting the Review of Audit

Examiners should have complete and timely access to an institution's internal audit resources, including personnel, work papers, risk assessments, work plans, programs, reports, and budgets. A delay may require examiners to widen the scope of their examination work and may subject the institution to follow-up supervisory actions. Examiners should assess the quality and scope of an institution's internal audit function, regardless of whether it is performed by the institution's employees or by an outsourcing vendor. Specifically, examiners should consider

- *Quality of board of directors' audit oversight.* Does the board
  - ensure it has open communication with and receive periodic reports from audit?
  - provide adequate resources to the audit function?
  - review and approve audit risk assessments?
  - assure compliance weaknesses are fully corrected in a timely fashion?
  - review the audit program periodically to ensure it remains comprehensive and effective?
  - review the effectiveness of the compliance management program periodically to ensure it is effective and properly positioned within the organization and that the compliance officer has sufficient authority within the organization?
- *Independence from management and business functions and adequacy of staffing to meet current and anticipated audit needs.* Is the audit function
  - independent of management?
  - impartial and not influenced by managers of day-to-day operations? Any internal staff used for audits or internal reviews should be independent of the area being reviewed.
  - located in the organizational structure so it does not report to the management of any areas for which it has audit or review responsibilities?

12. In this context, the term ''reviews'' refers to internal reviews that are conducted independent of the business line. For example, they may include reviews of specific business lines conducted by the independent compliance function. The term does not include reviews of a business line conducted by compliance staff located in the particular business line.

  - adequately staffed with qualified and experienced individuals who exhibit knowledge of applicable compliance regulations, are forward looking, and are engaged in continuous quality improvement?
  - able to absorb reasonable turnover and provide training of less experienced audit staff?
- *Identification and assessment of risks.* Does the audit function employ a risk-focused methodology that includes a risk assessment process commensurate with the institution's size and complexity?

In considering the quality of audit and the part it plays in assuring the integrity of the compliance function, examiners should review the nature of the institution's approach to risk-based or risk-focused auditing. Internal audit functions often use a risk-focused approach that focuses on high-risk areas and reduces the resources devoted to low-risk areas. With a risk-focused audit program, the institution should ensure it periodically assesses low-risk areas because these areas may be frequently excluded from internal audit's testing work.

In these circumstances, the examiners should review internal audit's methodology for confirming the risk assessment for all areas. The risk assessment process should incorporate periodic reviews of low-risk areas and include a process to reconfirm risk levels previously identified. In addition, the methods used should consider factors such as regulation risk, the effect of noncompliance, the control environment, and institutional and product complexity.

Finally, examiners should be aware that a risk-focused approach taken by audit or review staff may result in the need for enhanced levels of monitoring and testing by other control functions (such as business lines or the compliance function).

- *Comprehensiveness of audit planning and coverage.* Are the audit scope, coverage, and frequency comprehensive and based on the risk assessment?

  Do the scope and coverage

  - give appropriate consideration to all areas based on the nature, complexity, and risk of the institution's activities?
  - devote resources to the highest-risk areas?
  - respond to changes in identified risks?
  - give appropriate consideration to lower-risk areas?
  - appropriately consider whether large numbers of customers would be affected if errors were noted, there is a high transaction volume, or there are noted violations or weaknesses?

  Is audit frequency

  - commensurate with risk and periodically reassessed?
  - In considering the adequacy of audit frequency, some rules of thumb may be helpful. For example, there are regulations, which, regardless of the specific characteristics of the institution, presumptively pose a higher degree of compliance risk. Products or business lines subject to these regulations in general should be tested more frequently.
  - Conversely, there are instances in which frequent testing would not be necessary given a product's materiality, an established record of management competence, and product stability. Examiners also should consider risk factors that might change the appropriate frequency, such as regulatory changes, prior problems identified in an institution's systems or procedures, or changes in products that require new platform enhancements or new management skills and procedures.

  Does the sampling methodology

  - give appropriate consideration to the size and nature of the operation, previous problems, volume of activity and regulatory risk, to name a few?
  - ensure that statistical sampling is employed when appropriate for high-risk areas or when problems are identified within a smaller judgmental sample?

  Are contingency plans

  - in place in the event that the audit schedule cannot be completed as planned?
- *Reporting of auditing findings and resolution of exceptions.*
  - Are audit reports and work products sufficiently documented, with conclusions clearly stated and supported by work papers?
  - Is management responsive to findings, taking prompt corrective action?

Review of Audit Work Papers

Unless otherwise prohibited, the examiners' internal audit evaluation should include a review of work papers created in the course of an audit or internal review, when appropriate.[13]

13. The report or results of the self-test that a creditor

If the work papers appropriately support the audit or review findings, examiners may be able to leverage the findings and perform minimal or no additional transaction testing during the examination. However, if the work paper review reveals weaknesses in the quality of the audits or reviews performed, these weaknesses increase the institution's compliance risk and should be factored into examination scoping decisions.

Examination Concerns about the Effectiveness of the Internal Audit Function

If examiners conclude that the institution's internal audit function, whether or not it is outsourced, does not sufficiently meet the institution's internal audit needs or is otherwise ineffective, they should determine whether the scope of the examination should be adjusted. Examiners also should discuss these concerns with the internal audit manager or other person responsible for reviewing the system of internal controls. If these discussions do not resolve the examiners' concerns, the matters should be brought to the attention of senior management and the board of directors or audit committee. If examiners find material weaknesses in the internal audit function or the internal control system, they should discuss them with Reserve Bank management to determine the appropriate actions to take to ensure that the institution corrects the deficiencies. These actions may include formal and informal enforcement actions.

The institution's rating should reflect examiners' conclusions regarding the institution's internal audit function. The report of examination should contain comments concerning the effectiveness of this function, significant issues or concerns, and recommended corrective actions.

Scoping Determinations

Once examiners have reviewed the broad components of the internal audit program, which may include the audit work papers, and have drawn conclusions regarding the effectiveness of the internal audit function, a determination must be made as to how the audits should affect the scope of the examination.[14] In general, the level of transaction testing should be based on the residual risk associated with each specific product. Audit is only one of many factors to consider when establishing the level of residual risk; examiners should follow the risk assessment and scoping process outlined in this program. The matrix on the following page can assist examiners with how to consider the audit program in making judgments about residual risk.

---

voluntarily conducts (or authorizes) are privileged as defined under section 202.15 of Regulation B. The privilege under this section applies to the report or results of the self-test, data or factual information created by the self-test, and any analysis, opinions, and conclusions pertaining to the self-test report or results. The privilege covers work papers or draft documents as well as final documents.

14. When evaluating risk controls and setting the examination scope, examiners may make an initial determination of the extent to which audit may be relied upon, based on interviews, audit procedures, audit reports, and follow-up responses by management. Audit work papers may then be reviewed on site, if deemed necessary, to confirm that audits were conducted consistent with the initial determination. In the absence of significant changes to critical components of the audit program, examiners may be able to rely on a prior determination regarding the effectiveness of audit but should consider reviewing work papers when regulatory requirements have changed.

Audit Evaluation Matrix

Quality of testing	Low inherent risk	High inherent risk
Weak	• Auditors did not test, or tests were ineffective; the audit function is not considered effective. • Risk is low or limited. • **Conclusion:** The examiner should consider the effectiveness of other control mechanisms to establish whether residual risk remains low or limited.	• Auditors did not test, or tests were ineffective; the audit function is not considered effective. • Risk is moderate, considerable, or high. • **Conclusion:** Residual risk may remain elevated unless adequately mitigated through other control mechanisms.
Strong	• Auditors did test, and tests were effective; the audit function is considered effective. • Risk is low or limited. • **Conclusion:** In the absence of weakness in other controls, residual risk will be low or limited.	• Auditors did test, and tests were effective; the audit function is considered effective. • Risk is moderate, considerable, or high. • **Conclusion:** An effective audit program should result in a lower residual risk rating.

Inherent risk