Supervisory Letter

NCUA | Office of Examination & Insurance
1775 Duke Street, Alexandria, VA 22314
www.ncua.gov

SL No. 17-01
March 29, 2017

TO: **All Field Staff**

SUBJECT: **Evaluating Compliance Risk – Updated Compliance Risk Indicators**

ENCL: **Updated Compliance Risk Indicators**
AIRES Compliance Risk Questionnaire

This supervisory letter provides an updated list of Compliance Risk Indicators (see Appendix A) that are a part of NCUA's Risk-Focused Examination program. Also enclosed is the updated AIRES questionnaire for Compliance Risk.[1] The guidance in this document applies whenever field staff evaluates compliance risk in a federally insured credit union. Field staff will begin using the updated list of Compliance Risk Indicators for any supervisory evaluations of Compliance Risk started on or after March 31, 2017.[2]

The updated list of Compliance Risk Indicators builds upon the current set of indicators and provides additional guidance for field staff in assigning the compliance risk rating – one of the existing seven risk categories in the Risk-Focused Examination program. The update reflects transformations in technology, business models, and members' banking habits since the list of Compliance Risk Indicators were originally developed in 2002. The update results in a more comprehensive, integrated and transparent framework in evaluating a credit union's ability to manage its risk of violations and non-compliance with applicable laws and regulations.

[1] The questionnaire will be incorporated into AIRES by June of 2017.
[2] March 31, 2017, is also the effective date for the revised Federal Financial Institutions Examination Council (FFIEC) Uniform Interagency Consumer Compliance Rating System. NCUA, as an FFIEC member agency, has incorporated the principles of the revised Consumer Compliance Rating System into the Compliance Risk Indicators. The supervisory evaluation of compliance is ordinarily conducted as part of NCUA's risk-focused examinations of credit unions, not as a separate examination.

The updated list of Compliance Risk Indicators does not create a new compliance rating, does not separate consumer compliance from overall compliance, and does not impose any new or higher supervisory expectations for credit unions.

Exam Procedures

NCUA's assessment of compliance risk encompasses all of the federal consumer financial protection laws and regulations NCUA enforces, as well as other relevant laws and regulations that govern the operation of credit unions, such as the Bank Secrecy Act, the Flood Disaster Protection Act, and the SAFE Act. Field staff will continue to reflect their conclusion about a credit union's compliance risk, and management of that risk, in the compliance risk rating,[3] the Management CAMEL component rating, and the CAMEL composite rating as appropriate.[4]

NCUA's approach to examining a credit union's compliance with applicable laws and regulations remains risk-focused with appropriate consideration given to a credit union's size, complexity, and risk profile. Field staff will draw on their professional judgment to target their efforts to the areas of greatest existing and potential risk. Field staff's supervisory evaluation will typically focus primarily on evaluating the sufficiency of a credit union's overall approach to managing compliance risk– also referred to as a compliance management system. As reflected in the updated Indicators, compliance risk is best managed by an institution when its compliance management systems are proactive; that is, they promote self-identification and self-correction of any identified compliance deficiencies.

Field staff's evaluation will also routinely include specific and/or in-depth reviews of some areas of special emphasis based on statutory requirements,[5] changes to laws or regulations, broad trends, or institution specific risk factors.[6] The supervisory evaluation of compliance need not, and typically does not, include specific or in-depth evaluations of compliance with all applicable laws and regulations or extensive transaction testing.

The updated framework incorporates and adds detail to the current Compliance Risk Indicators to aid field staff in evaluating compliance risk. The updated Compliance Risk Indicators framework has three broad categories: Board and Management Oversight; Compliance Programs; and Violations of Law and Consumer Harm. Each category has several factors, (briefly summarized below). Field staff will assess the first two with consideration given to a credit union's size, complexity, and risk profile. In particular, field staff will consider:

1. **Board and Management Oversight**
   - Commitment to the credit union's compliance management system.

---

[3] NCUA's Letter to Federal Credit Unions 02-FCU-09, "Risk-Focused Examination Program" discusses the seven categories of risk, including compliance risk, that comprise a credit union's risk profile. Based on field staff's evaluation of the risk, each risk category is assigned a risk level of low, moderate, or high.
[4] See NCUA Letter to Credit Unions 07-CU-12 regarding the CAMEL rating system.
[5] For example, NCUA is required by law to review compliance with the Bank Secrecy Act and the Flood Disaster Protection Act at all examinations of insured credit unions.
[6] Field staff should continue to refer to the annual Exam Scope instruction for requirements for each type of federally insured credit union examination.

- Effectiveness of change management processes.
- Risk management associated with products, services, and activities.
- Self-identification efforts and corrective actions taken.

2. Compliance Program

- The effectiveness of a credit union's compliance management system.
- Policies and procedures, training, monitoring and audit programs, and complaint resolution.

3. Violations of Law and Consumer Harm (if applicable)

- Pervasiveness of the violation.
- Root cause of the violation.
- Severity of the violation or any consumer harm.
- Duration of the violation.

In assigning a Compliance Risk rating, field staff consider the totality of the Compliance Risk Indicators. Any single or small subset of Compliance Risk Indicators is not necessarily determinative of the existence of lower or higher risk. An effective risk assessment is a composite of multiple factors. Depending upon the circumstances, certain factors - such as the quality of the credit union's overall approach to compliance management, or the existence of pervasive or severe violations - may be weighted more heavily than others.

See Appendix A for the full chart of Compliance Risk Indicators.

If you have any questions on the material in this letter, please direct them to your immediate supervisor or regional management.

Sincerely,

/s/

Larry Fazio
Director
Office of Examination & Insurance

Appendix A: Compliance Risk Indicators

Factor	Low	Moderate	High
Board and Management Oversight Board and management oversight factors should be evaluated commensurate with the credit union's size, complexity, and risk profile. Compliance expectations below extend to third-party relationships.			
Oversight and Commitment	Board and management fully understand all aspects of compliance risk and exhibit a clear commitment to compliance. Commitment is communicated throughout the credit union. Board and management demonstrate strong commitment and oversight to the credit union's compliance management system. Significant compliance resources are provided, including systems, capital, and human resources. Staff is knowledgeable, empowered and held accountable for compliance with consumer laws and regulations. Management conducts comprehensive and ongoing due diligence and oversight of third parties consistent with NCUA expectations to ensure that the credit union complies with consumer protection laws and regulations. Where appropriate, the credit union exercises strong oversight of third parties' policies, procedures, internal controls and training to ensure consistent oversight of compliance responsibilities.	Board and management reasonably understand the key aspects of compliance risk. Commitment to compliance is reasonable and satisfactorily communicated. Board and management provide satisfactory oversight of the credit union's compliance management system. Compliance resources are adequate and staff is generally able to ensure the credit union is in compliance with consumer laws and regulations. Management conducts adequate and ongoing due diligence and oversight of third parties to ensure that the credit union complies with consumer protection laws and regulations. They adequately oversee third parties' policies, procedures, and internal controls, and training to ensure appropriate oversight of compliance responsibilities.	Board and management does not understand, or has chosen to ignore key aspects of compliance risk. The importance of compliance is not emphasized or communicated throughout the organization. Management has not established or enforced accountability for compliance performance. Board and management oversight, resources, and attention to the credit union's compliance management system are deficient or non-existent. Compliance resources are inadequate or seriously deficient and are ineffective at ensuring the credit union's compliance with consumer laws and regulations. Management does not adequately conduct due diligence and oversight of third parties to ensure that the credit union complies with consumer protection laws and regulations, nor do they adequately oversee third parties' policies, procedures, internal controls, and training to ensure appropriate oversight of compliance responsibilities.
Change Management	Management anticipates and responds promptly to changes in applicable laws and regulations, market conditions and products and services offered by evaluating the change and implementing responses across impacted lines of business. Management conducts due diligence in advance of product changes, considers the life cycle of a product before implementing the change, and reviews the change after implementation to determine whether actions taken have achieved planned results.	Management responds timely and adequately to changes in applicable laws and regulations, market conditions, and products and services offered by evaluating the change and implementing responses across impacted lines of business. Management evaluates product changes before and after implementing the change.	Management does not respond adequately or timely or fails to respond to changes in applicable laws and regulations, market conditions, and products and services offered.

Factor	Low	Moderate	High
Comprehension, Identification and Management of Risk	The credit union has a strong control culture that has proven effective. Compliance management systems are sound and minimize the likelihood of excessive or serious future violations. Management has a good understanding and effectively identifies compliance risks, including emerging risks, in the credit union's products, services, and other activities. Management effectively manages those risks, including through comprehensive self-assessments.	Compliance management systems are adequate to avoid significant or frequent violations or noncompliance. Management understands and adequately identifies compliance risks, including emerging risks, in the credit union's products, services, and other activities. Management adequately manages those risks including through self-assessments.	Compliance management systems are deficient, reflecting an inadequate commitment to risk management. Management does not understand or identify compliance risks, including emerging risks, in the credit union's products, services, and other activities.
Corrective Action and Self-Identification	Management proactively identifies issues and promptly responds to compliance risk management deficiencies and any violations of laws or regulations, including taking corrective action.	Management adequately responds to and corrects deficiencies and/or violations, including adequate corrective action, in the normal course of business.	Management does not adequately respond to compliance deficiencies and violations including those related to corrective action, or those responses, including those relating to examination findings that are seriously deficient.
Compliance Program Compliance Program factors should be evaluated commensurate with the credit union's size, complexity, and risk profile. Compliance expectations below extend to third-party relationships.			
Policies and Procedures	Compliance policies and procedures and third-party relationship management programs are strong, comprehensive, and provide standards to effectively manage compliance risk in the products, services, and activities of the credit union.	Compliance policies and procedures and third-party relationship management programs are adequate to manage the compliance risk in the products, services, and activities of the credit union.	Compliance policies and procedures and third-party relationship management programs are inadequate (or absent) at managing the compliance risk in the products, services and activities of the credit union.
Training	Compliance training is comprehensive, timely, and specifically tailored to the particular responsibilities of the staff receiving it, including those responsible for product development, marketing, and customer service. The compliance training program is updated proactively in advance of the introduction of new products or new consumer protection laws and regulations to ensure that all staff are aware of compliance responsibilities before roll out.	Compliance training outlining staff responsibilities is adequate and provided timely to appropriate staff. The compliance training program is updated to encompass new products and to comply with changes to consumer protection laws and regulations.	Compliance training is not adequately comprehensive, timely, updated, or appropriately tailored to the particular responsibilities of the staff. Compliance training may be seriously deficient or absent.

Factor	Low	Moderate	High
Monitoring and/or Audit	Compliance monitoring practices, management information systems, reporting, compliance audit, and internal control systems are comprehensive, timely, and successful at identifying and measuring material compliance risk management throughout the credit union. Programs are monitored proactively to identify procedural or training weaknesses to preclude regulatory violations. Program modifications are made expeditiously to minimize compliance risk.	Compliance monitoring practices, management information systems, reporting, compliance audit, and internal control systems adequately address compliance risks throughout the credit union.	Compliance monitoring practices, management information systems, reporting, compliance audit, and internal control systems are absent or do not adequately address risks involving products, services or other activities including, timing and scope.
Consumer Complaint Response	Processes and procedures for addressing consumer complaints are strong. Consumer complaint investigations and responses are prompt and thorough. Management monitors consumer complaints to identify risks of potential consumer harm, program deficiencies, and customer service issues and takes appropriate action.	Processes and procedures for addressing consumer complaints are adequate. Consumer complaint investigations and responses are generally prompt and thorough. Management adequately monitors consumer complaints and responds to issues identified.	Processes and procedures for addressing consumer complaints are deficient, absent, or inadequate. Consumer complaint investigations and responses are not thorough or timely, or are deficient, or absent. Management does not adequately monitor consumer complaints, monitoring is seriously deficient, or management exhibits a disregard for complaints or preventing consumer harm.
Violations of Law and Consumer Harm			
Root Cause	Violations are the result of minor weaknesses, if any, in the compliance risk management system.	Violations are the result of modest weaknesses in the compliance risk management system.	Violations are the result of material weaknesses, or serious or critical deficiencies in the compliance risk management system.
Severity	Type of consumer harm, if any, resulting from the violations would have minimal impact on consumers.	Type of consumer harm resulting from the violations would have limited impact on consumers.	Type of consumer harm resulting from the violations would have considerable or serious impact on consumers.
Duration	Violations and resulting consumer harm, if any, occurred over a brief period of time.	Violations and resulting consumer harm, if any, occurred over a limited period of time.	Violations and resulting consumer harm, if any, occurred over an extended period of time, or have been long-standing or repeated.
Pervasiveness	Violations and resulting consumer harm, if any, are isolated in number.	Violations and resulting consumer harm, if any, are limited in number.	Violations and resulting consumer harm, if any, are numerous, or widespread in multiple products or services.