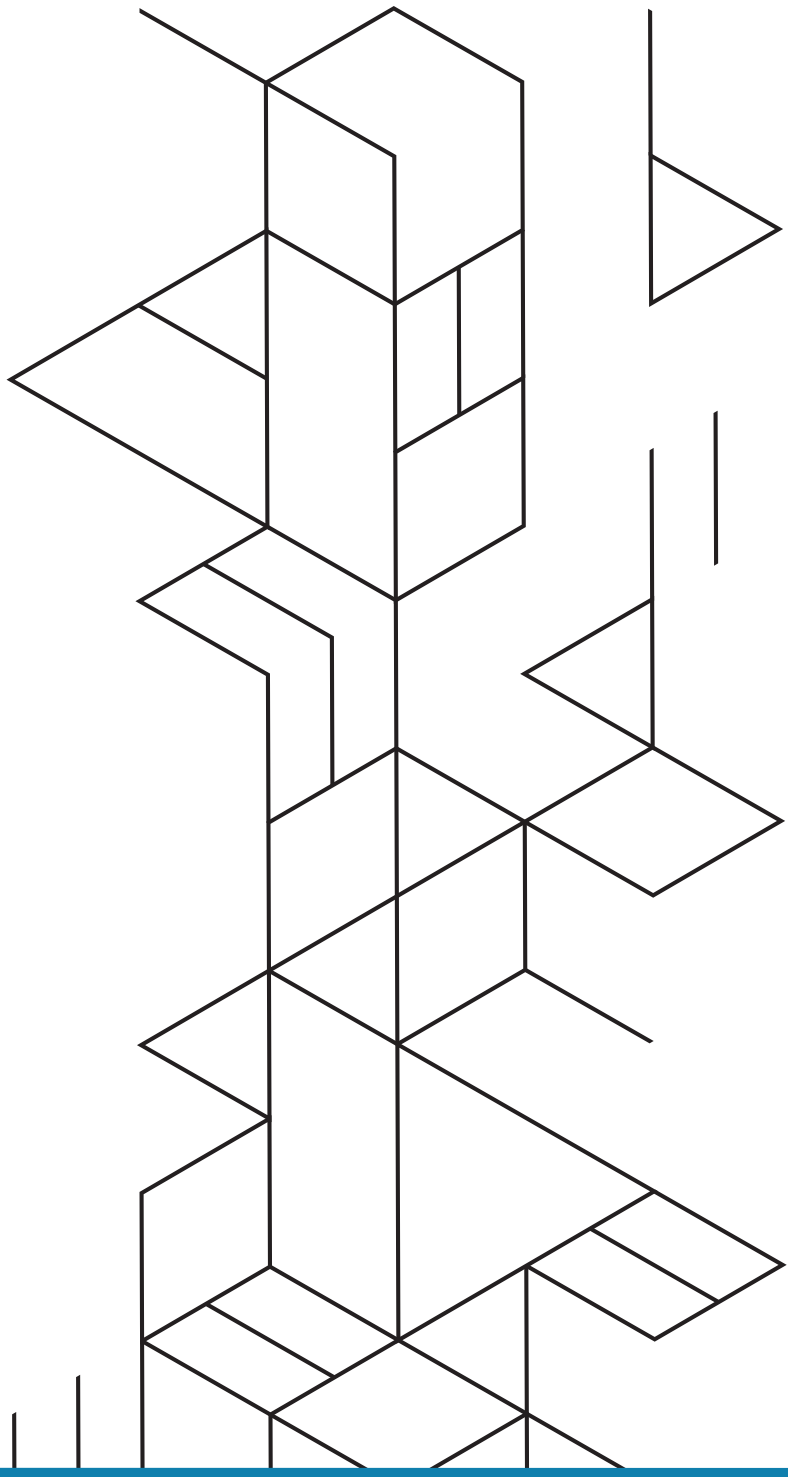
NAFCU *Exam Study Guide*

2020

# NCRM CERTIFICATION



NCRM | NAFCU CERTIFIED RISK MANAGER

***Welcome to the NAFCU NCRM Study Guide!***

This comprehensive manual will provide you with the necessary information you'll need to certify as a NAFCU Risk Manager. We are extremely glad you chose us for your certification needs. Should you have any questions, please do not hesitate to ask any NAFCU staff for assistance.

A special thank you goes to our sponsor whose contributions make these programs a success. Their continued support is greatly appreciated.

Always remember, we believe in you and your mission. That's why we provide the best federal advocacy, education and compliance assistance possible.

Thanks for all you do.

Sincerely,

B. Dan Berger

President & CEO

## TABLE OF CONTENTS

## NAFCU NCRM STUDY GUIDE

Welcome to the 2020 NAFCU Virtual Risk Management Seminar! This study guide is designed to assist in preparing for the NCRM exam. The exam contains 50 questions. To obtain the NCRM designation you must receive a score of 76 percent or higher. This guide, along with the presentations, will provide all the information necessary to review and pass the exam.

Risks have been around longer than credit unions have been in business. One might even say credit unions are in the business of risk. From giving out loans, to offering new products and services, credit unions are faced with a number of different risks. NAFCU's program is designed to strengthen and enhance an understanding of general risk principles as expected by the financial institution regulators.

## REGULATORS

Credit unions are expected by various regulators to manage the risks associated with operations. These are the main regulators responsible for examination and risk guidance for credit unions.

1. The National Credit Union Administration (NCUA) is the independent federal agency created by the United States Congress to regulate, charter and supervise federally insured credit unions (FICUs). As a prudential regulator, NCUA is tasked with managing risks to the National Share Insurance Fund and has broad authority to determine if FICUs are operating in a safe and sound manner.
2. The Consumer Financial Protection Bureau (CFPB) is a regulatory agency charged with overseeing financial products and services that are offered to consumers. The CFPB writes and enforces rules for financial institutions, examines both bank and non-bank financial institutions, monitors and reports on markets, as well as collects and tracks consumer complaints. Notably, the CFPB only has direct supervisory authority for credit unions that are 10 billion dollars or more in assets.
3. The Federal Financial Institutions Examination Council (FFIEC) is a formal U.S. government interagency body that includes five banking regulators—the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller (OCC), NCUA and the CFPB.
4. The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury charged with the prevention and punishment of criminals and criminal

networks that participate in money laundering. Specifically, FinCEN issues guidance and regulations implementing the Bank Secrecy Act.

5. State chartered credit unions are also regulated by their state regulator, such as a Department of Financial Institutions or similar.

## WHY THIS MATTERS, RISK FOCUSED EXAMS

NCUA is authorized by the Federal Credit Union Act (FCU Act) to examine all FICUs. A key goal of NCUA exams is to protect the share insurance fund while also determining whether a credit union is in compliance with applicable laws and regulations. For most credit unions, the agency utilizes risk-focused exams to meet its statutory obligation to oversee FICUs. Chapter One of the NCUA Examiners Guide states:

*"A risk-focused program is a forward-thinking approach that allocates resources to the credit unions and areas exhibiting weaknesses or adverse trends. Examiners allot time to reviewing areas containing the most risk for an individual credit union. Activities posing the highest risk receive the most scrutiny.*

*In the risk-focused program, distinctions between examination and supervision blur. Examination and supervision efforts may, at times, be a continuum to the extent that examiners will call a particular contact an examination, rather than supervision simply because the time frame requires an examination.*

*Supervision is the ongoing monitoring of a credit union's financial and operational condition. During supervision in the risk-focused program, the examiner looks forward at the direction a credit union takes and the decisions it makes. Examiners can then anticipate when those decisions could result in the credit union assuming undue risk or failing to manage the risk it has taken. Examiners may determine or adjust the timing of the examination based on conditions revealed during the supervision process."*

NCUA uses the CAMEL rating system, which is based upon an evaluation of five critical elements of a credit union's operations: Capital Adequacy, Asset Quality, Management, Earnings and Liquidity/Asset-Liability Management. This internal rating system is used for evaluating the soundness of credit unions, the degree of risk to the National Credit Union Share Insurance Fund (NCUSIF) and to identify those credit unions needing additional supervisory attention. It is designed to consider and reflect all significant financial, operational and management factors of a credit union's performance and risk profile. In connection with the risk focused examination, CAMEL quantifies the impact material risk has on the credit union's

soundness. Examiners rate each of the five elements on a scale from 1 to 5 (1 being the best). The credit union also receives an overall composite rating from 1 to 5. The performance and capability of management is a significant factor in the overall risk profile of a credit union and the examiner will give special consideration to the management rating when assigning the overall composite rating.

The risk focused exam aims to hone an examiner attention and resources on areas showing weaknesses and adverse trends. The examiner generally will derive these high-risk areas from previous examinations, his or her review of the credit union's call report, and general downward trends in the industry. New products and services will likely be considered a higher risk to the credit union than those with which the credit union has vast experience. This risk-focused process provides examiners with flexibility to focus on areas they see as exhibiting current or potential risk to the credit union and the overall system. However, there are three things each examination must include:

- Reviewing the accuracy of the 5300 Call Report data;
- Reviewing the supervisory committee audit; and
- Reviewing the credit union's compliance with the Bank Secrecy Act.

Once the minimum requirements have been met, examiners may turn towards areas that reveal pertinent risk characteristics.

NCUA states the goals for a risk focused approach to exams will assist with reducing the time it takes examiners onsite and with ensuring that the riskiest areas for each individual credit union are addressed. The foundation for risk focused exam success is the credit union's risk management program.

## RISK MANAGEMENT PROGRAM

Each credit union is unique; its risk management program needs to reflect that quality. The program should be designed around the market factors that affect the institution and the fields of membership it serves. There is no one-size fits all risk management program that can work for all credit unions. Each organization has factors, products and services that make such a system impossible.

**Study Tip!** It is extremely important, when designing and implementing a risk management program, to design the program around the size, scope and complexity of the organization.

### *Risk Impact*

If one is unsuccessful at managing risk, the credit union can suffer a risk impact. A risk impact refers to the cost or disruption experienced by the organization should the risk occur. Risk impacts can occur in the form of direct loss of money, regulatory or legal noncompliance violations, and cleanup projects to correct errors.

### *Silo Approach*

When reviewing and evaluating risks at an organization, there are several different approaches to take. An independent and uncoordinated risk management program could result in a silo approach. This tends to lead to gaps in an assessment of the overall risk to the organization.

## NCUA RISK MANAGEMENT PROGRAM FOUNDATIONS

While there is no uniform risk management program, there are a number of common processes that NCUA expects credit unions to employ to ensure risks are being accurately monitored. The NCUA Examiners Guide highlights these common processes as:

1. **Policies** reflect the board's intent and commitment in pursuing desired results. Effective management requires written policies that the credit union adheres to in practice. Policies set standards and courses of action to pursue, implement, and enforce specific objectives. Good policies link with, and reflect, a credit union's underlying mission, values, and principles. They also clarify the credit union's tolerance for risk. Credit unions should have mechanisms in place to trigger a review of policies in the event activities or tolerances change.
2. **Processes** include the procedures, programs, and practices governing how a credit union will pursue its objectives and define how it will carry out its daily activities. Good processes demonstrate consistency with the underlying policies, efficiency, and adequacy of internal control checks and balances.

3. **Personnel** encompass the staff and managers executing or overseeing performance of the processes. Qualified, competent managers and staff should perform as a conscientious board expects. They must understand the mission, values, policies, and processes.
4. **Control systems** are tools and information systems managers use to measure performance, assist in decision-making, and assess the effectiveness of existing processes. Sound control systems require timely, accurate, and informative feedback devices. In turn, management must implement reporting systems by which they communicate necessary and sufficient information to the directors.

## WHAT ARE THE RISK FACTORS?

NCUA has defined seven categories of risks for credit unions to monitor. These seven factors can be present in products and services the credit union offers. The categories are assigned a risk level, which will be reflected in the appropriate CAMEL codes. The seven risk categories are **Credit**, **Interest Rate**, **Liquidity**, **Transaction**, **Reputation**, **Compliance** and **Strategic**. These risks are not mutually exclusive either; a risk may fit into any number of the seven identified risks. For example, the credit union may suffer a data breach of its core processor. The risk posed by the data breach could make the credit union susceptible to transaction risk, by using the stolen data to perpetrate fraud. In addition, the credit union could suffer reputation risk by having the story of the data breach on the front page of a national newspaper, or worse.

The next section outlines the seven categories of risk as defined by NCUA. As a credit union navigates managing risks, one of the tenants of successful risk management is agreeing on language. A credit union often adapts definitions to these risk categories that make sense to its specific organization, while also keeping NCUA's guidance and definitions in mind. Please use this provided information as a reference.

## NCUA IDENTIFIES SEVEN RISK CATEGORIES

**Credit Risk**: The current and prospective risk to earnings or capital arising from an obligor's failure to meet terms of any contract with the credit union or otherwise fail to perform as agreed. Credit risk exists in all activities where the credit union invests or loans funds with the expectation of repayment.

In short, these are risks to a credit union's earnings that are due to a failure of its investments or a portion of its loan portfolio.

**Interest Rate Risk**: The risk that changes in market rates will adversely affect a credit union's capital and earnings. Interest rate risk arises from:

1. Differences between the timing of rate changes and the timing of cash flows (repricing risk),
2. Changing rate relationships among different yield curves affecting credit union activities (basis risk),
3. Changing rate relationships across the spectrum of maturities (yield curve risk), and
4. Interest-related options embedded in credit union products (options risk).

Not only can a move in interest rates affect the price of investments, it also has an effect on the value of the loan portfolio and on fee income, which is sensitive to changes in interest rates.

The assessment of interest rate risk should consider risk from both an accounting perspective (i.e., the effect on the credit union's accrual earnings, including held-to-maturity and available-for-sale accounts) and the economic perspective (i.e., the effect on the market value of the credit union's loans and investments.) In some credit unions, the broader category of market risk captures interest rate risk.

To put it plainly, these are the risks posed by external interest rates that can affect a credit union's earnings and capital.

**Liquidity Risk**: The current and prospective risk to earnings or capital arising from a credit union's inability to meet its obligations when they come due, without incurring material costs or unacceptable losses. This includes the inability to manage funding sources, including unplanned decreases or changes. Liquidity risk also arises from the credit union's failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly and with minimal loss in value.

In other words, this is the risk that a credit union will not have the ability to meet financial obligations when they come due.

**Transaction Risk**: The risk to earnings or capital arising from fraud or error that results in an inability to deliver products or services, maintain a competitive position and manage information. This risk (also referred to as operating or fraud risk) is a function of internal controls, information systems, employee integrity and operating processes. This risk arises on a daily basis in all credit unions as they process transactions.

So, these are the risk(s) posed to a credit union's balance sheet by fraud, and its ability to launch products and services effectively. How vulnerable is the credit union to fraud losses, and could those losses effect its ability to deliver member service.

**Compliance Risk**: The current and prospective risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. Compliance risk may also arise in situations where ambiguous or untested laws or rules govern certain credit union products or activities of the members. Compliance risk exposes the credit union to fines, civil money penalties, payment of damages and the voiding of contracts. Compliance risk can lead to a diminished reputation, limited opportunities, reduced field of membership expansion potential and lack of contract enforceability.

Compliance risk goes beyond a failure to comply with consumer protection laws. It encompasses all laws as well as prudent ethical standards, contractual obligations and exposure to litigation. Compliance risk can blend into operational risk, transaction processing and even legal risk, increasing the difficulty of identifying this risk.

Another way to put it is, this is the risk posed to a credit union by not following the rules. Compliance risk has a number of moving parts. The CFPB and NCUA regulate this area heavily. In addition, the Department of Justice (DOJ) uses enforcement actions against bad actors in this area. The typical tolerance for compliance risk is near zero.

**Strategic Risk**: The current and prospective risk to earnings or capital arising from adverse business decisions, improper implementation of decisions or lack of responsiveness to industry changes. This risk is a function of the compatibility of a credit union's strategic goals, the business strategies developed to achieve those goals, the resources deployed to accomplish these goals and the quality of implementation.

The tangible and intangible resources needed to carry out business strategies include communication channels, operating systems, delivery networks, monitoring systems, and managerial capacities and capabilities. The foundation for strategic risk management is the three to five year strategic plan.

Simply put, these are the risks posed by a credit union's business decisions. Strategic risk can arise from both action (creating an action plan to launch a product) or inaction (choosing to ignore market factors and not launch a product or service).

**Reputation Risk**: The current and prospective risk to earnings or capital arising from negative public opinion or perception. Reputation risk affects the credit union's ability to establish new relationships or services, or to continue servicing existing relationships. This risk, which occurs in activities such as asset management decisions and transactions, can expose the credit union to litigation, financial loss or a decline in membership base. Reputation risk exposure appears throughout the credit union organization. The officials, management and staff must accept responsibility to exercise an abundance of caution in dealing with members and the community.

To put it another way, would a credit union survive being on the front page of the *New York Times* in a negative light? Reputation risk is often the by-product of other risks presented to the credit union. For example, if a credit union is the victim of fraud (transaction risk), its members' perception of the credit union's security program is the reputation risk component.

**Study Tip!** Risks can be made up of multiple risk categories. For example, a data breach could be tied to compliance risk, reputation risk and transaction risk. When looking at where a specific risk should be aligned, remember there is often more than one category that fits!

In addition to the seven categories of risk for credit union supervision purposes, credit unions also face concentration risk. This occurs when a concentration such as in a particular product or investment creates the potential for losses large enough to threaten the credit union's solvency. NCUA's Letter to Credit Unions 10-CU-03, Concentration Risk, offers additional guidance on concentration risk.

## 2020 RISKS

NCUA issued its initial 2020 supervisory focus in January. However, with the advent of the COVID-19 pandemic, the agency released an update in July to reflect the resulting economic conditions, as well as various statutory and regulatory changes occurring since March 2020. Due to the ongoing impact of the pandemic, NCUA updated the Examiner's Guide to include additional guidance for examiners, including review procedures for assessing the safety and soundness of credit unions.

NCUA's primary supervisory focus includes:

1. Bank Secrecy Act (BSA) Compliance/Anti-Money Laundering (AML)
2. COVID-19 pandemic and Coronavirus Aid, Relief and Economic Security Act (CARES Act)
3. Consumer Financial Protection

4. Credit Risk Management and Allowance for Loan and Lease Losses (ALLL)
5. LIBOR Transition Planning
6. Liquidity Risk
7. Serving Hemp-Related Businesses
8. Information Systems and Assurance (Cybersecurity)

The agency outlined each objective and provided a baseline of examiner expectations.

### *Bank Secrecy Act Compliance*

NCUA remains vigilant in ensuring the credit union system is not used to launder money or finance criminal or terrorist activity. The agency will continue to conduct BSA/AML reviews and take appropriate action when necessary to ensure credit unions meet their regulatory obligations during every examination. Customer due diligence and beneficial ownership requirements that went into effect May 11, 2018, will still be ongoing areas of emphasis. NCUA's Letter to Credit Unions 18-CU-02, Examination Guidance for Bank Secrecy Act Customer Due Diligence and Beneficial Ownership Compliance provides more details. NCUA will also continue focusing on proper filing of suspicious activity (SAR) and currency transaction (CTR) reports, as well as reviews of bi-weekly 314(a) information requests from FinCEN. Additional resources are available on NCUA's Bank Secrecy Act Resources webpage.

### *Covid-19 and CARES Act*

NCUA states the COVID-19 pandemic may have a lasting impact on credit unions' financial and operational conditions. The agency indicates examiners should consider the extraordinary and potential long-term nature of the COVID-19 economic issues confronting credit unions, understand it is a unique circumstance, and be flexible in their supervisory approach. Credit unions and examiners should also reference NCUA's Coronavirus (COVID-19): Information for Federally Insured Credit Unions and Members webpage for frequently asked questions that are updated periodically.

NCUA added the CARES Act as a supervisory priority to reflect the importance of the provisions outlined in the Act, which was signed into law on March 27, 2020. Examiners will review credit unions' good faith efforts to comply with the CARES Act and take appropriate action, when necessary, to ensure credit unions meet their obligations under the new law.

Multiple provisions of the act directly affect credit unions. NAFCU has a summary of these provisions available here. More information is also available from NCUA in its Letter to Credit Unions, 20-CU-07, Summary of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

### *Consumer Financial Protection*

As the COVID-19 pandemic continues to effect consumers and could result in increased consumer compliance risk in certain areas, NCUA will continue to examine for compliance with applicable consumer financial protection regulations during every examination. The scope of each examination's consumer compliance review is largely risk-focused; based on a credit union's compliance records, products and services provided, regulatory changes and other emerging concerns. Examinations for compliance with applicable consumer financial protection regulations include:

- **Electronic Fund Transfer Act (Regulation E)**. An evaluation of electronic fund transfer policies and procedures and review initial account disclosures as well as Regulation E's error resolution procedures for when consumers assert an error. In addition, examiners will evaluate credit union practices concerning the Regulation E, Remittance Transfer Rule changes enacted since the start of the pandemic to the safe harbor threshold and disclosures of rates and costs associated with remittance transfers.
- **Fair Credit Reporting Act**. A review of credit reporting policies and procedures and the accuracy of reporting to credit bureaus, particularly the date of first delinquency.
- **Gramm-Leach-Bliley (Privacy Act)**. An evaluation of credit union protection of non-public personal information about consumers.
- **Small dollar lending (including payday alternative loans)**. Testing for compliance with the NCUA Payday Alternative Lending rules and interest rate cap. Examiners will determine whether a credit union's short-term, small-dollar loan programs that are not NCUA Payday Alternative Lending comply with regulatory requirements.
- **Truth in Lending Act (Regulation Z)**. An evaluation of credit union practices concerning annual percentage rates and late charges. This includes evaluating whether finance charges and annual percentage rates are accurately disclosed, and late fees are levied appropriately. Examiners will also evaluate credit union practices concerning the changes made in response to COVID-19 to the Truth in Lending-Real Estate Settlement Procedures Act (TRID) rule and Regulation Z Rescission rules that permit members to waive the waiting periods under both rules.

- **Military Lending Act (MLA) and Servicemembers Civil Relief Act (SCRA)**. These have been supervisory priorities for NCUA since 2017. For credit unions that have not received a recent review, examiners will review credit union compliance with the MLA and SCRA.

For additional consumer compliance tools and resources, visit NCUA's Consumer Compliance Regulatory Resources webpage.

### *Credit Risk Management and Allowance for Loan and Lease Losses*

NCUA is shifting its emphasis to reviewing actions taken by credit unions to assist borrowers facing financial hardship. The agency will also review the adequacy of loan and lease losses (ALLL) accounts to address the pro-cyclical effects of economic downturns.

Examiners will review credit union policies and the use of loan workout strategies, risk management practices, and new strategies implemented to assist borrowers impacted by the COVID-19 pandemic. A credit union's controls, reporting and tracking of new programs authorized through the CARES Act will be evaluated. Examiners will also ensure credit unions have evaluated the impact of pandemic decisions on their capital position and financial stability.

Credit unions must still maintain an ALLL account in accordance with FASB Accounting Standards Codification (ASC) Subtopic 450-20 (loss contingencies) and/or ASC 310-10 (loan impairment). NCUA examiners will be evaluating the adequacy of credit unions' ALLL accounts.

Agency resources concerning these requirements include:

- Examiner's Guide Chapter on Allowance for Loan and Lease Losses
- Interagency Statement on Loan Modifications and Reporting for Financial Institutions Working with Customers Affected by the Coronavirus (revised).
- Letter to Credit Unions, 20-CU-13, Working with Borrowers Affected by the COVID-19 Pandemic.
- The Credit Union Operations section on NCUA's Frequently Asked Questions for Federally Insured Credit Unions.
- Letter to Credit Unions, 02-CU-09, Allowance for Loan and Lease Losses.
- Accounting Bulletin, 06-01, Interagency Advisory Addressing the ALLL Key Concepts and Requirements.

### *LIBOR (London Interbank Offered Rate) Transition Planning*

The United Kingdom's Financial Conduct Authority has announced that it can no longer guarantee the reliability of LIBOR beyond 2021. Currently, LIBOR is used an indicative measure of the average interest rate at which major global banks could borrow from one another and often tied to consumer loan rates. Although not all credit unions rely on LIBOR as an index for variable rate loans, some do. Addressing the risks posed by this change is a 2020 supervisory priority. Planning for the LIBOR transition is an important operational and safety and soundness consideration for credit unions with material exposures. Examiners will continue to assess credit unions for exposure to LIBOR, conducting reviews using the agency's LIBOR Assessment Workbook, located in the Interest Rate Risk Exam Procedures section of the online Examiner's Guide. The CFPB has also issued resources addressing some of the regulatory challenges posed by shifting away from LIBOR for contracts with consumers.

### *Liquidity Risk*

Assessments of liquidity risk management is an agency supervisory priority, as on average, credit union balance sheets generally exhibit lower levels of on-balance sheet liquidity due to strong loan growth. The economic impact of the pandemic may result in additional stress on credit union balance sheets, potentially requiring robust liquidity management over the course of 2020 and into 2021. Examiners will continue to review liquidity risk management and planning in all credit unions and will place emphasis on:

- The effects of loan payment forbearance, loan delinquencies, projected credit losses and loan modifications on liquidity and cash flow forecasting.
- Scenario analysis for changes in cash flow projections for an appropriate range of relevant factors (for example, changing prepayment speeds).
- Scenario analysis for liquidity risk modeling, including changes in share compositions and volumes.
- The potential effects of low interest rates and the decline of credit quality on the market value of assets, funding costs and borrowing capacity.
- The adequacy of contingency funding plans to address any potential liquidity shortfalls.

More information, along with additional resources and guidance on liquidity risk, is available in the NCUA Examiner's Guide. The agency also added a subsection on liquidity in its COVID-19 chapter.

### *Serving Hemp-Related Businesses*

In June 2020, NCUA issued Letter to Credit Unions, 20-CU-19, Additional Guidance Regarding Servicing Hemp-Related Businesses, for institutions that are serving, or considering serving, legal hemp-related businesses and may be affected by the COVID-19 pandemic. The letter outlines responses and guidance relating to some frequently asked questions. FinCEN also issued guidance on June 29, 2020, to address questions related to BSA/AML regulatory requirements for hemp-related business customers. NCUA examiners will continue to collect data concerning the types of services credit unions provide to hemp-related businesses through the examination process.

### *Information Systems and Assurance (Cybersecurity)*

Emerging cyber-attacks have become a persistent threat to the financial sector, and the likelihood of these threats adversely affecting credit unions and consumers has increased due to advances in financial technology; an increase in a remote workforce; and the increased use of mobile technology for financial transactions.

NCUA has transitioned its priority from performing Automated Cybersecurity Examination Tool (ACET) cybersecurity maturity assessments, to evaluating critical security controls. The agency is also piloting an Information Technology Risk Examination solution for Credit Unions (InTREx-CU). The InTREx-CU will be deployed to identify gaps in security safeguards, allowing examiners and credit unions to identify and remediate potential high-risk areas through the identification of critical information security program deficiencies as represented by an array of critical security controls and practices.

Information on the increased cybersecurity threats resulting from COVID-19 and additional resources for protecting members is available on NCUA's Cybersecurity Resources webpage and the Cybersecurity, Frauds, and Scams section of NCUA's Frequently Asked Questions for Federally Insured Credit Unions.

## 2020 DATA BREACHES

It does not take long to realize why cybersecurity continues to be an issue as well as a focus of NCUA. Here are just a few of the data breaches, as tracked here, for 2020:

1. **Landry's** – Restaurant conglomerate Landry's announced on January 2, 2020, that a point-of-sale malware attack targeted customers' payment card data – the company's second data breach since 2015. The collected Personally Identifiable Information (PII) included credit and debit card numbers, expiration dates, verification codes, and cardholder names.
2. **Fifth Third Bank** – On February 11, 2020, Fifth Third Bank, a financial institution with 1,150 branches in 10 states, claims a former employee is responsible for a data breach, which exposed customers' name, Social Security number, driver's license information, mother's maiden name, address, phone number, date of birth and account numbers. The total number of affected employees and banking clients remains undisclosed.
3. **MGM Resorts** – February 20, 2020, over 10.6 million hotel guests who have stayed at the MGM Resorts had their personal information posted on a hacking forum. The data dump exposed includes names, home addresses, phone numbers, emails and dates of birth of former hotel guests. Updated July, 15 2020, researchers found 142 million personal records from former guests at the MGM Resorts hotels for sale on the Dark Web, hinting that the original breach was larger than previously announced.
4. **T-Mobile** – March 5, 2020, an unknown number of customers' sensitive information was accessed through a T-Mobile employee email accounts after a malicious attack of a third-party email vendor. The personal information of T-Mobile customers accessed includes names and addresses, Social Security numbers, financial account information and government identification numbers, as well as phone numbers, billing and account information, and rate plans and features.
5. **Twitter** – On June 23, 2020, a security lapse at Twitter caused the account information of the social media company's business users to be left exposed. The number of impacted business accounts has not been disclosed but its business users' email addresses, phone numbers and the last four digits of their credit card number were impacted.
6. **Dave Mobile Banking App** – On July 26, 2020, a third-party breach leaked the account details of over 7.5 million users of the digital banking app, Dave. Although no financial information was disclosed, the breach exposed names, phone numbers, emails, birth dates, home addresses and encrypted Social Security numbers.

While NCUA and other regulators continue to stress and enforce cybersecurity standards, such risks have been around since credit unions have been using core processors. Core processors have been vulnerable to attacks and subjected credit unions to transaction risk(s) since the 20th century. However, problems do not always come from outside and inside attacks. Sometimes service providers stop supporting systems currently being used. For example, on July 15, 2015, Windows Server 2003 became obsolete. Before that, a number of credit unions dealt with vulnerabilities due to Windows XP being sunset. NCUA expects credit unions to maintain vigilance on the cybersecurity front. The risks posed are numerous and cleanup efforts are typically calculated in the millions of dollars.

As cyber security continues as an ever-evolving threat to every credit union, NAFCU also has a webpage dedicated to cybersecurity compliance. It contains a number of different resources to assist credit unions in complying with the numerous data standards.

## ENTERPRISE RISK MANAGEMENT (ERM)

### *What is ERM?*

Widely recognized throughout the financial services industry as acceptable guidance, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) states in its *Enterprise Risk Management — Integrated Framework* that ERM is a process that is:

- Ongoing and applied throughout an organization,
- Effected by people at every level of an organization,
- Applied in strategy setting,
- Takes an organization-level portfolio view of risk,
- Designed to identify potential events that could affect the organization and to manage risk within the organization's risk appetite,
- Able to provide reasonable assurance to an organization's management and board of directors,
- Geared to achieve objectives in one or more separate but overlapping categories.

### *ERM Defined*

Multiple groups have defined ERM, including NCUA. These definitions address different angles but there are overlapping concepts and themes. Here are several key examples.

NCUA: In Supervisory Letter No.: 13-12, the agency defines ERM as a comprehensive risk-optimization process that integrates risk management across an organization. An organization's board of directors ultimately makes the decision to develop and implement an ERM framework, often with the goal of aligning risk with strategic objectives.

ERM is not a process to eliminate risk or to enforce risk limits, but rather to encourage organizations to take a broad look at all risk factors, understand the interrelationships among those factors, define an acceptable level of risk and continuously monitor functional areas to ensure that the defined risk threshold is maintained.

**COSO:** ERM is defined by COSO as a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

**The Risk Management Society (RIMS):** ERM, as defined by RIMS, is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.

**The Risk Management Association (RMA):** The RMA defines ERM as an organization's enterprise risk competence—the ability to understand, control, and articulate the nature and level of risks taken in pursuit of business strategies—coupled with accountability for risks taken and activities engaged in, which contributes to increased confidence shown by stakeholders.

## BENEFITS OF AN ERM PROGRAM

1. Provides the ability to define the risks, apply controls and effectively obtain the necessary information from these to maximize the credit union's strategic plan.
2. Develops a unique, relevant and specific program that gives a credit union the proper tools necessary to enhance the business decision-making processes.
3. ERM assists with creating a baseline for assessing the value of a risk analysis and reactions to risks that are measured by the levels defined by the credit union's risk strategy.

4. A robust ERM program provides a baseline for assessing the effectiveness of internal controls and compares how those controls relate to a credit union's overall risk strategies.
5. Helps bolster the confidence in management and provide evidence to regulators related to the ability to proactively respond to risks within the credit union.

## RISK APPETITE

COSO states that risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. Risk appetite guides resource allocation. Risk appetite assists in aligning the organization, people and processes and designing the infrastructure necessary to effectively respond to and monitor risks.

## ERM PROGRAM REQUIREMENTS

There is no "off-the-shelf solution" for organizations seeking to launch an effective enterprise-wide approach to risk management. Rather, an organization can meet its specific needs with various tailored approaches that take into account its complexity, resources and expertise. Credit unions that incorporate ERM into their risk management infrastructure may resource the program internally, through paid consultants or through a combination of outsourced and internal resources. NCUA does not view any approach as preferable, provided core principles, controls and due diligence are properly established within the organization. That said, there are several basic components of an ERM program that likely will be evident at any financial institution that pursues an ERM approach to managing risk. Because examiners are likely to encounter one or more of these components in their analysis of a credit union's operations, they should be familiar with them.

The following table outlines these components (as identified in the COSO framework), describes each, and provides positive examples of how each component might manifest in a credit union's operations.

| ERM Component | Description | Positive Examples |
|---|---|---|
| Established "Risk Culture" | This is the "tone at the top" that sets the basis for how risk is viewed and addressed by an organization's stakeholders at all levels. The organization should define an enterprise wide philosophy for risk management and risk appetite that is grounded in integrity, ethical values and a good grasp of how various stakeholders are affected by the organization's decisions. | Consistent support for the ERM framework throughout the organization, from the chairman's office to staff members on the front lines. |
| Clear Objectives | An ERM program encourages management to set clear strategic, operations, reporting and compliance objectives that support and align with the organization's mission and are consistent with its risk appetite. | Future objectives are reasonably achieved without exceeding a pre-determined, stated risk tolerance. |
| Event Identification | The organization has identified internal and external events affecting achievement of objectives and has distinguished its risks from its opportunities. | For each uncertainty or potential event, a "leading indicator" is created along with parameters that would trigger a risk management response. |
| Risk Assessment | The organization continuously analyzes risk, considering the likelihood and impact of various scenarios, and uses the results of the analysis as a basis for determining how to manage those risks. | A risk "heat map" evolves from manager surveys to determine priority of risks. |
| Risk Response | Management evaluates possible responses to risks, selects a response (avoid, accept, reduce or share risk), and develops a set of actions that aligns risks with the organization's risk tolerances and risk appetite. | Management identifies the costs and benefits for accepting each type of risk. The most relevant risk information is centralized and reported timely, in the right form, and to the right people in order to make timely and effective decisions about risk. |

| | | |
|---|---|---|
| Control Activities | A set of policies and procedures that is established and implemented to help ensure that an organization effectively responds to risks. | Staff understand the differences between risk avoidance, risk reduction, risk sharing and risk acceptance. The senior manager responsible for ERM oversight reports directly to the board of directors or to a board-established committee that will assure proper oversight and independence. The ERM program is independent of the risk-taking and operational functions. |
| Information and Communication | Relevant information is identified, captured and communicated in a form and timeframe that enable stakeholders to carry out their responsibilities. Key information about strategy and decisions is communicated clearly and broadly throughout an organization. | All personnel receive a clear message from top management that ERM responsibilities are taken seriously. A robust and reliable reporting regimen is evident. |
| Monitoring | The organization monitors – through ongoing management activities and/or separate evaluations – the entirety of risk management and makes modifications as necessary. | Management reports performance versus established risk limits. |

## NCUA EXAMINER EXPECTATIONS

While not required for credit unions, other than corporate credit unions, ERM programs are becoming more common in credit unions. NCUA provided full commentary on ERM and the expectations for credit unions in its Supervisory Letter No. 13-12. It is also important to note that ERM is a still evolving target for credit unions and examiners alike.

1. NCUA understands there is no "off the shelf solution" for effective risk management and that organizations need to take a tailored approach that takes into account the individual organization's complexity, resources and expertise.

2. A credit union may use internal resources, paid consultants or a combination of both in its efforts to manage risk.
3. It is expected that a credit union follow the basic components as previously outlined and that core ERM principles be integrated into the overall strategic planning and organizational risk-management infrastructure of credit unions of all sizes and risks levels.
4. There is no guidance that directs one approach over another as long as core principles are followed.
5. At this time, there is no NCUA expectation of a natural person credit union to implement a formal ERM program, only corporate credit unions are currently required to do so.
6. Examiners are expected to take a risk-based approach in gauging the effectiveness of a credit union's risk management program against identified, as well as the perceived risk posture of the credit union. Included in this review would be the capability and commitment of management toward a culture of risk management and financial strength of the credit union in relation to individual and collective risk exposures.
    - Risk posture, appetite and mitigation strategies;
    - Depth and breadth of potential exposures;
    - Strategic objectives, policies and controls;
    - Concentrations of risk;
    - Risk mitigating factors (controls);
    - Capabilities and resources of management;
    - Current and historical performance management; and
    - Financial strength of the credit union in relation to assets and activities.

## VENDOR MANAGEMENT PROGRAM

NCUA requires credit unions to have a vendor management program. A successful vendor management program contains several prescribed requirements. Those requirements include:

**Due diligence program.** This has been an NCUA requirement for years and numerous credit unions run a successful vendor due diligence program. The key review areas for the due diligence programs are:

- Reviewing financial records
- SSAE 18 and or SOC 2 audit reports for critical vendors
- Background and qualification checks
- Business continuity plans
- Review of any pending lawsuits against the vendor
- Obtain vendor references

**Risk assessments.** Provide a detailed risk assessment based on the information uncovered during the due diligence review. Remember that liability cannot be contracted away via a vendor relationship. If utilizing a vendor that has a cybersecurity or data breach, the credit union is liable. It is important to review all risks and weigh those against a credit union's risk appetite.

- Include assessments of cloud security risks if the vendor operates via the cloud.
- Review assessments annually as part of the due diligence review.
- Conduct assessments of all vendors, not just critical or high risk, in order to justify risk ratings.

**Contract review.** Have a qualified legal expert review the contractual agreement to ensure all terms are covered. Ensure that all expectations are met within the language of the agreement and there is a way to get out of the agreement in the event that such a need arises.

**Ongoing monitoring.** The credit union is expected to assign a vendor owner to each vendor relationship. These owners are responsible for the ongoing monitoring of the vendor management process.

**Study Tip!** Critical vendors pose heightened levels of risk given the nature of the relationship. This necessitates heightened due diligence and additional documentation. These vendors typically require an SSAE18 or SOC2 review. Information required from these vendors should be updated annually.

## THIRD PARTY RISK(S)

**Planning** – Third party arrangements should be synchronized with strategic plans, business plans and a credit union's philosophies.

**Risk Assessment** – A dynamic process that should consider the seven areas of risk as well as expectations of the arrangement, staff expertise, criticality of function, cost-benefit, insurance requirements, member impact and exit strategy.

**Financial Projections** – A return on investment should be estimated considering revenue, direct costs, indirect costs, fees and likely cash flow stream. Return should be considered relative to the credit union's strategic plans and asset-liability frameworks.

### *Risk Measurement, Monitoring and Control*

**Staff Oversight and Quality Control** – The credit union should have qualified staff designated to oversee and control the quality of the third party relationships.

**Policies and Procedures** – Policy guidance must be in place and sufficient to control the risks of the third party relationship. Policy guidance should address responsibilities, oversight, program and portfolio limitations, and content and frequency of reporting.

**Monitoring and Reporting** – Adequate infrastructure is required to support monitoring and reporting outlined in policy guidance. Credit unions should be able to measure and verify the performance of third parties and third party programs.

The common themes are to review and thoroughly vet the vendor. Once the initial assessment is completed an ongoing monitoring program must be set up to ensure all the risks are continuously addressed and mitigated. A vendor must be reviewed from a level of criticality, financial stability and benefit(s) offered to the credit union. In all instances, the credit union cannot contract away its own liability to a third party. What makes matters worse is that errors performed by the third party vendor can create spill-over liability to the credit union.

## FINAL THOUGHTS

Credit unions face a wide variety of ever-changing risks. There is no one size fits all risk management program that is perfect for every credit union. It is the job of everyone at the credit union to help manage risk. The programs and concepts laid out in this study guide are a starting point to help benchmark an existing program or to begin a risk management program.

## EXAM PREPARATION STUDY QUESTIONS

*The Foundations of Risk Management: A Basic Understanding*

1. Not having a risk management program could impact a credit union how?

   Type your answer here...

2. How does one design a risk management program for a credit union?

   Type your answer here...

3. What are some common elements of a risk management program?

   Type your answer here...

4. What is enterprise risk management?

   Type your answer here...

5. How is enterprise risk management beneficial?

   Type your answer here...

6. What are some of the requirements of an enterprise risk management program?

   Type your answer here...

*NCUA Expectations under Risk Management: The 7 Categories of Risk*

1. What is NCUA's overall focus when examining a credit union?

   Type your answer here...

2. What has NCUA identified as risk factors?

   Type your answer here...

3. Explain/define the risk categories.

   Type your answer here...

4. What are NCUA's supervisory priorities for 2020?

   Type your answer here...

5. What are some of the risks involved with vendor management and/or third party relationships?

   Type your answer here...

To help focus your studying, here is a breakdown of the exam questions per topic:

NCRM EXAM – 50 Questions

| NCRM Topic | Number of Questions |
|---|---|
| Why This Matters, Risk Focused Exams | 2-4 Questions |
| Risk Management Program | 3-5 Questions |
| NCUA Risk Management Program Foundations | 4-6 Questions |
| What are the Risk Factors? | 1-3 Questions |
| NCUA Identifies Seven Risk Categories | 10-12 Questions |
| 2020 Risks | 5-7 Questions |
| Enterprise Risk Management (ERM) | 4-6 Questions |
| Benefits of an ERM Program | 1-3 Questions |
| Risk Appetite | 1-2 Questions |
| ERM Program Requirements | 4-6 Questions |
| NCUA Examiner Expectations | 1-2 Questions |
| Vendor Management Program | 4-5 Questions |
| Third Party Risk(s) | 1-2 Questions |

## APPENDIX A

NCUA Examiners Guide Chapter 1 (Risk-Focused Program).

Supervisory Letter No.: 07-01 (Third Party Vendors).

Supervisory Letter No.: 14-05 (MSBs).

Supervisory Letter No.: 13-12 (Enterprise Risk Management).

Supervisory Letter No.: 13-05 (Investing in Securities).

Supervisory Letter No.: 14-04 (Taxi Medallion Lending).

NCUA regulations governing third-party servicing of auto loans (12 C.F.R. § 701.21(h)).

NCUA Letter to Credit Unions 08-CU-09 (AIRES Exam Questionnaire).

NCUA Letter to Credit Unions 08-CU-19 (Mortgage Brokers & Correspondents).

NCUA Letter to Credit Unions 10-CU-15 (Indirect Lending).

NCUA Letter to Credit Unions 10-CU-18 (Investment Due Diligence).

NCUA Letter to Credit Unions 10-CU-26 (Third Party Payment Processors).

In re Toyota Motor Credit Corporation, *2016*-CFPB-0002 (Feb. 2, 2016).

In re American Honda Finance Corporation, 2015-CFPB-0014 (July 14, 2015).

In re Ally Financial Inc., 2013-CFPB-0010 (Dec. 20, 2013).

In re Capital One Bank, N.A., 2012-CFPB-0001 (July 18, 2012).

CFPB Bulletin 2015-05 (Oct. 8, 2015) (Marketing Services Agreements and RESPA).

CFPB Bulletin 2013-07 (July 10, 2013 (Debt Collection).

CFPB Bulletin 2013-02 (March 21, 2013) (Indirect Auto Lending).