Exam Study Guide

2022

NCRM
CERTIFICATION

NCRM | NAFCU CERTIFIED RISK MANAGER

This comprehensive manual will provide you with the necessary information you'll need to earn the NAFCU Certified Risk Manager (NCRM) designation. 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 3

Regulators 3

Why This Matters, Risk Focused Exams 4

Risk Management Program 5

- Risk Impact 5
- Silo Approach 6

Risk Management Program Foundations 6

What are the Risk Factors? 6

NCUA Identifies Seven Risk Categories 7

2022 Risks 10

- Credit Risk Management 10
- Information Security (Cybersecurity) 11
- Payment Systems 12
- Bank Secrecy Act (BSA) Compliance and Anti-Money Laundering (AML)/Countering the Financing of Terrorism 12
- Capital Adequacy and Risk Based Capital Rule Implementation 12
- Loan Loss Reserving 13
- Consumer Financial Protection 14
- Loan Participations 14
- Fraud 14
- London Inter-Bank Offered Rate (LIBOR) Transition 15
- Interest Rate Risk 15
- NCUA Examination Manual 15

2022 Data Breaches 18

Enterprise Risk Management (ERM) 19

- What is ERM? 19
- ERM Defined 19

Benefits of an ERM Program 20

Risk Appetite 20

ERM Program Requirements 21

NCUA Examiner Expectations 24

Updated COSO Framework 25

Vendor Management Program 26

Third Party Risk(s) 27
Risk Measurement, Monitoring and Control 28
Emerging risk Issues 28
Climate-Related Financial Risk 28
Diversity, Equity and Inclusion 31
Final Thoughts 32
Exam Preparation Study Questions 33
Appendix A 36

NAFCU NCRM STUDY GUIDE

Welcome to the 2022 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 (38 out of 50 correct). 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 (BSA).
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. NCUA's risk based examination program has evolved to address new and emerging risks in the industry and to respond to the agency's supervisory focus.

NCUA uses the CAMELS rating system, which is based upon an evaluation of five critical elements of a credit union's operations: Capital Adequacy, Asset Quality, Management, Earnings, Liquidity and Sensitivity to Market Risk. 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, CAMELS 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 BSA.

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

Risk is an uncertain future outcome that will improve or worsen your position. 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.

RISK MANAGEMENT PROGRAM FOUNDATIONS

While there is no uniform risk management program, there are a number of common processes a credit union can employ to ensure risks are being accurately monitored. If one or more of these components is inadequate, the result can be an insufficient risk management program.

1. **Policies** are generally written and set the standards and courses of action to pursue, implement and enforce specific objectives. Policies reflect a credit union's underlying mission, values and principles as well as clarify its tolerance for risk.
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. 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.

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 CAMELS codes. The seven risk categories are **Credit**, **Interest Rate**, **Liquidity**, **Transaction**, Compliance, Strategic and **Reputation.** 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 tenets 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 a party'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.

2022 RISKS

NCUA issued its initial 2022 supervisory focus in January. With the ongoing impact of the pandemic, NCUA's Examiner's Guide was updated in 2020 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. Credit Risk Management
2. Information Security (Cybersecurity)
3. Payment Systems
4. Bank Secrecy Act (BSA) Compliance and Anti-Money Laundering (AML)/Countering the Financing of Terrorism
5. Capital Adequacy and Risk Based Capital Rule Implementation
6. Loan Loss Reserving
7. Consumer Financial Protection
8. Loan Paricipations
9. Fraud
10. London Inter-Bank Offered Rate (LIBOR) Transition
11. Interest Rate Risk

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

Credit Risk Management

Examinations will continue to review a credit union's credit risk-management and mitigation efforts. Risk management practices should be comparable with the level of complexity and

nature of all of a credit union's lending programs and activities. Safe and sound lending practices must be maintained in addition to compliance with consumer financial protections laws, including disclosures and regulatory reporting requirements.

NCUA examiners will focus on adjustments made to lending programs to address borrowers facing financial hardship. Examiners will review credit union policies and the use of loan workout strategies, risk management practices and new strategies made to lending programs to address borrowers impacted by the COVID-19 pandemic. A credit union's controls, reporting and tracking of new programs authorized through the CARES Act and extended in the Consolidated Appropriations Act, 2021 will be evaluated.

Credit unions are encouraged to work with their members who were affected by the COVID-19 pandemic. NCUA examiners will not criticize a credit union's efforts to provide prudent relief for borrowers when such efforts are conducted in a reasonable manner with proper controls and management oversight.

Agency resources on these requirements include:

- Joint Statement on Additional Loan Accommodations Related to COVID-19;
- NCUA Letter to Credit Unions, 20-CU-13, Working with Borrowers Affected by the COVID-19 Pandemic;
- and the Lending Programs section on NCUA's Frequently Asked Questions for Federally Insured Credit Unions.

Information Security (Cybersecurity)

Cybersecurity risks remain a significant threat to the financial sector, and the likelihood of these threats adversely affecting credit unions and consumers continues to rise. Ransomware threats, third-party/supply chain risks and business email compromises are of particular concern. As credit union information security practices continue to be a priority, NCUA is developing updated information security examination procedures tailored to an institution's size and complexity, to be finalized in 2022.

NCUA released the Automated Cybersecurity Examination Tool (ACET) in 2021, a self-assessment resource for credit unions to determine and measure their cybersecurity preparedness in alignment with the Federal Financial Institutions Examination Council (FFIEC)

Cybersecurity Assessment Tool. The ACET is entirely voluntary and does not introduce any new requirements or expectations on credit unions.

Information on cybersecurity is available on NCUA's Cybersecurity Resources webpage.

Payment Systems

Payment products, services and operations is a growing area of complexity and increasing corresponding risk for credit unions and consumers. As the retail payments landscape shifts and grows to meet consumer demand for easier and faster electronic access to and settlement of funds, the changes in payment systems increase the risk of fraud, illicit use and breaches of data security. NCUA will expand its focus in this area.

Bank Secrecy Act (BSA) Compliance and Anti-Money Laundering (AML)/Countering the Financing of Terrorism

Bank Secrecy Act (BSA) compliance and Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT) continue to be national priorities. The Anti-Money Laundering Act of 2020 and the Corporate Transparency Act amended the BSA for the first time since 2001. New requirements for credit unions to update their risk based BSA and AML/CFT policies, procedures and processes will be implemented incrementally throughout 2022. NCUA will communicate changes in BSA and AML/CFT requirements, and any impacts on examinations to credit unions. The FFIEC will continue to publish updates to the BSA/AML Examination Manual.

Additional resources are available on NCUA's Bank Secrecy Act Resources webpage.

Capital Adequacy and Risk Based Capital Rule Implementation

New in 2022 is the risk-based capital rule and NCUA's focus on capital adequacy and credit unions' implementation of the rules related to risk-based capital requirements. As of January 1, 2022, credit unions with total assets exceeding $500 million are subject to the risk-based capital rule. In support of this new framework, the agency made changes to the quarterly Call Report as of the March 31, 2022, reporting period. Examiners will assess a credit union's efforts to assist its members through some of the economic challenges related to the COVID-19 pandemic and how those efforts affect the credit union's "capital position and financial stability." Examiners

will also focus on whether complex credit unions are accurately reporting risk-based capital information in the Call Report.

Loan Loss Reserving

Credit unions are required to implement the Financial Accounting Standards Board's Accounting Standards Update No. 2016-13, Topic 326 by January 1, 2023, commonly referred to as the current expected credit losses methodology, or CECL. Examiners will also discuss a credit union's preparations to implement CECL

NCUA examiners will be evaluating the adequacy of credit unions' Allowance for Loan and Lease Losses (ALLL) accounts by reviewing: ALLL policies and procedures; documentation of an ALLL reserving methodology, including modeling assumptions and qualitative factor adjustments; adherence to generally accepted accounting principles; and independent reviews of credit union reserving methodology and documentation practices by the Supervisory Committee or by an internal or external auditor.

Federal credit unions with less than $10 million in assets are not required to implement CECL but will still need to follow a reasonable reserve methodology that adequately covers known and probable loan losses. Federally insured, state-chartered credit unions will want to check with state law for GAAP-related requirements.

Information and resources include:

› Interagency Statement on Loan Modifications and Reporting for Financial Institutions Working with Customers Affected by the Coronavirus (Revised).

› FASB's Accounting Standards Update 2016-13, Topic 326, Financial Instruments—Credit Losses.

› FASB Staff Q&A, Topic 326, No. 1: Whether the Weighted-Average Remaining Maturity Method Is an Acceptable Method to Estimate Expected Credit Losses.

› FASB Staff Q&A, Topic 326, No. 2: Developing an Estimate of Expected Credit Losses on Financial Assets.

- NCUA Letter to Credit Unions 16-CU-13 – Frequently Asked Questions on the New Accounting Standard on Financial Instruments Credit Losses.
- NCUA Letter to Credit Unions 17-CU-05 – Frequently Asked Questions on the New Accounting Standard on Financial Instruments Credit Losses.

Consumer Financial Protection

NCUA will continue to examine for compliance with applicable consumer financial protection regulations. An examination's consumer compliance review scope is largely risk-focused, and based on the credit union's compliance record, products and services provided, and any new or emerging concerns.

In 2022, examiners will focus on areas related to: the COVID-19 pandemic, fair lending, the Servicemembers Civil Relief Act, the Fair Credit Reporting Act (FCRA), and overdraft programs. Reviews will include areas such as a credit union's policies and procedures concerning the temporary COVID-19 Mortgage Servicing Rule (Regulation X), mortgage forbearances and other loan accommodations made during the pandemic, and fair lending racial equity and appraisal fairness. Examiners will also request detailed information about a credit union's overdraft programs as the agency plans for a fuller review of credit unions' overdraft programs in 2023.

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

Loan Participations

Credit unions are encouraged to employ safe-and-sound practices in the management of loan participation portfolios. NCUA examiners will verify that loan participation transactions are risk evaluated and how that risk fits within the tolerance levels established by a credit union's board. The agency notes that each loan participation must have separate and distinct records and appropriate third-party due diligence practices are utilized when purchasing loan participations.

Fraud

The advent of remote or offsite work over the last two years has increased potential fraud risks. NCUA examinations will review efforts to deter and detect fraud, including internal controls and separation of duties. Transaction testing will also be part of examination procedures.

London Inter-Bank Offered Rate (LIBOR) Transition

With the end of LIBOR, NCUA examiners will focus on credit unions with significant LIBOR exposure. NCUA's Supervisory Letter, 21-01 provides the supervision framework examiners will continue to use to evaluate a credit union's risk management processes and planning for the transition away from LIBOR. The agency also recommends the inclusion of fallback language and a replacement rate(s) for all legacy LIBOR-based contracts.

Credit unions can continue using NCUA's LIBOR Assessment Workbook for assistance and refer to the July 2020 Interagency Statement and the October 2021 Interagency Statement for additional guidance. The CFPB has also issued resources addressing some of the regulatory challenges posed by shifting away from LIBOR for contracts with consumers.

Interest Rate Risk

NCUA indicates a credit union's interest rate risk could be affected by the high growth in shares during the pandemic and investment in longer-term assets. The agency advises credit unions to model and manage interest rate risk by using a variety of scenarios that include various prepayment speed and yield curve assumptions.

More information on the 2022 supervisory priorities including a summary of various resources can be found in this NAFCU *Compliance Monitor* article (member-only).

NCUA Examination Manual

The online Examiner's Guide is intended to provide a framework with respect to conclusions made about a credit union's financial and operational condition, and related CAMELS and risk ratings. It also provides a consistent approach for evaluating the adequacy of a credit union's relevant risk-management processes. It is important to note that the supervisory criteria in the guide are not strict requirements unless required by law or regulation. In 2020, NCUA began updating the guide on an ongoing basis.

The revised NCUA Examiner's Guide includes online sections within chapters on areas of specific concern that a robust credit union risk management program should address.

ALLL: Primary risks to a credit union's ALLL account include compliance, strategic and transaction. Credit unions manage the risks associated with the ALLL account through a combination of people, processes, and systems/technology.

Call Report: Compliance and reputation risks are associated with the misreporting or delay of reporting of the Call Report and Profile to NCUA. A credit union can manage such risks associated with the Call Report and Profile through its people and policies and processes.

Cash Operations: With its cash operations. a credit union is exposed to potential credit, compliance, transaction, strategic, liquidity and reputation risk. There are three essential components to a credit union managing its cash operations risk exposure. They are its people, processes, and data processing systems and technology.

Credit union service organizations (CUSOs): Defined in NCUA regulation section 712.1, a CUSO is an entity that may be wholly owned by a credit union or a group of credit unions and other investors. The types of risk a CUSO can pose to a credit union vary greatly from CUSO to CUSO, and are influenced by its operating structure and the services it offers. CUSOs can be a source of compliance, credit, interest rate, liquidity, reputation, strategic and transaction risk to a credit union. CUSOs are maintained as separate legal entities and often operate as third-party vendors. A credit union that invests in or loans to, or receives services from a CUSO is expected to conduct third-party due diligence reviews. NCUA Letter to Credit Unions 07-CU-13, Evaluating Third Party Relationships provides more information on the topic.

Earnings: This is a broad term, generally referring to the amount of money a credit union retains after deducting costs from gross income, earnings are necessary to adequately build capital commensurate with its current and prospective financial and operational risk exposure, economic climate and strategic plans. Each of the seven risk areas can affect a credit union's earnings. A credit union's ability to manage the risks that can affect earnings depends on its people, and policies and processes.

Electronic Payment Systems: There are many types of electronic payment systems (EPS) available to credit unions. Such services can generate earnings, satisfy member demand and attract new members to the credit union. In addition to the seven risk areas, EPS activity can expose a credit union to third-party risk. A credit union's people, policies and processes, and systems and technology impact its ability to effectively manage the risks posed by EPS.

Employee Benefits and Investments for Employee Benefits: Unsafe and unsound practices related to employee benefit programs in a credit union can vary, from establishing unreasonable benefit plans that can expose its net worth to excessive risk, to failing to perform adequate due diligence. Providing employee benefits can subject a credit union the seven risk areas. A credit union should accept a certain level of risk in providing employee benefits and investing to fund them, and need to manage the risk.

Fidelity Bond Coverage: Bond coverage (also known as blanket, surety, or discovery bonds) protects a credit union against some losses caused by fraud, dishonesty, theft, and related activities committed by credit union employees, directors, officers, supervisory committee members, and credit committee members. Primary risk areas impacting a credit union and bond coverage include compliance, reputation and transaction risks. Managing bond coverage risk depends on a credit union's people, and policies and processes.

Fraud: This can be conducted by insiders at a credit union or a credit union may be the victim of an external fraud. It has the potential to impact a credit union in all risk areas. A credit union's ability to effectively manage its exposure and deter fraud depends on its people, policies and processes, and systems/technology.

Internal Controls: A credit union's board and senior management staff design and implement internal controls to mitigate risk. If internal controls are inadequate, a credit union's exposure may increase in all seven risk areas. Creating an effective internal control system involves the people who design and implement the system, the policies and procedures that define and document how the internal controls are intended to be performed, and the systems and technology that facilitate the internal controls.

Interest Rate Risk: Interest rate risk is a potentially significant risk that arises from credit union activities, and it is inherent to some degree in all credit unions. NCUA evaluates a credit union's interest rate risk exposure because the level of exposure can represent a major potential threat to its earnings and capital and when extreme, can present undue risk to the National Credit Union Share Insurance Fund. The impact of interest rate risk can expose a credit union to credit, liquidity and strategic risks.

Liquidity: Various situations can increase a credit union's liquidity risks such as reputation, credit, interest rate, strategic and concentration. As previously noted, none of these are mutually exclusive. A credit union's ability to effectively manage the risks posed by liquidity depends on corporate governance and its policies, procedures, and limits.

2022 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 a few of the data breaches involving financial data, as tracked here, for 2022.

PracticeMax – A provider of healthcare support services, PracticeMax, advised 165,698 individuals of a security incident resulting in an unauthorized party gaining access to their sensitive information. While varying by consumer, compromised information may include the affected parties' names, addresses, Social Security numbers, dates of birth, treatment and diagnosis information, health insurance information, financial information, patient account numbers, employer and employee identification numbers, passport numbers, driver's license numbers, state identification numbers, prescription information and provider or employee login information.

Block - The company behind the mobile payment service Cash App, Block, acknowledged a Cash App data breach in which a former employee accessed reports that included U.S. customer information. About 8.2 million current and former customers will be notified about the breach. The reports included customer names and brokerage account numbers, and in some cases brokerage portfolio values, brokerage portfolio holdings and stock trading activity for one trading day.

Lakeview Loan Servicing – Mortgage servicer Lakeview Loan Servicing disclosed a data breach that went undetected for over a month. The company said the breach impacted 2,537,261 borrowers. An unauthorized person external to the company obtained access to the firm's servers and information including names, addresses, loan information and 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) indicates the purpose of effective ERM is to help boards and management optimize outcomes as "Risk is the possibilty that events will occur and affect the achievement of strategy and business objectives."

ERM:

- Is not a function or department.
- Is more than a risk listing or inventory. It is broader and includes management practices to actively manage risk.
- It addresses more than internal control. Its principles apply at all of the organization and across all functions.
- It is not a checklist. It is a set of principles on which processes can be developed and integrated as a system of monitoring, learning and improving performance.
- It can be used by organizations of any size.

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 "the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with the purpose of managing risk in creating, preserving, and realizing value."

The Risk & Insurance 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.

BENEFITS OF AN ERM PROGRAM

1. It increases the range of opportunities for an organization with the consideration of all possibilities, both the positive and negative aspects of risk.
2. Management can identify and manage entity-wide risks.
3. It allows an organization to improve its ability to identify risks, increasing positive outcomes and advantage while reducing negative surprises.
4. It allows organizations to anticipate risks to reduce performance variability.
5. It improves the allocation of resources.
6. It enhances enterprise resilience as the pace of change accelerates and business complexity increases.

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. Updated guidance focuses on linking risk appetite with an organization's strategies and objectives. Risk appetite must be flexible enough to adapt to changing conditions and is a critical link between forming strategy and realizing performance.

The COSO guidance lists six things to remember about risk appetite:

1. It not a separate framework. Risk appetite should be integral to managing risk and to organizational communication and action.
2. Risk appetite and risk tolerance differ. Though related, they are different ideas.

3. It applies to more than the financial services industry. Risk appetite can help all organizations understand and manage performance more effectively.
4. It is at the heart of decision-making. Risk appetite also is important in determining that a decision is even necessary.
5. It is much more than a metric. Although often treated as part of an approach where each metric is assigned a target appetite, a better, forward-looking application ties appetite and strategy together for future action.
6. It helps increase transparency. Risk appetite can raise awareness of the risks the organization is willing to assume as well as the risks it aims to limit.

A clear risk appetite is invaluable for strong compliance or risk management programs.

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 2004 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.

ERM Component	Description	Positive Examples
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. st
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 reports performance versus established risk limits.

ERM Component	Description	Positive Examples
	management and makes modifications as necessary.	

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 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.

UPDATED COSO FRAMEWORK

COSO has updated its ERM framework since 2004 to provide stronger guidance and greater emphasis on the importance of integrating risk considerations throughout the organization when developing and implementing strategic objectives.

Source: COSO

As the figure illustrates, the new ERM framework now includes five interrelated components or categories which COSO defines as:

1. **Governance and Culture –** This sets the organization's tone by providing guidance on board oversight responsibilities, operating structures and leadership's tone in addition to attracting, developing, and retaining the right individuals.

2. **Strategy & Objective-Setting –** This focuses on strategic planning and how the organization can understand the effect of internal and external factors on risk.

3. **Performance –** After an organization develops its strategy, it then moves on to identify and assess risks that could affect its ability to achieve these goals. This section not only helps guide the organization's risk identification and assessment, but also how to prioritize and respond to risks.

4. **Review and Revision –** At some point after risks have been prioritized and a course of action been chosen, the organization moves into the review and revision phase where it assesses any changes that have taken place. This is also the opportunity to understand how the ERM process in the organization can be improved upon.

5. **Information, Communication, and Reporting –** This last component involves sharing information from internal and external sources throughout the organization. Systems are used to capture, process, manage, and report on the organization's risk, culture, and performance.

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.

This past NAFCU *Compliance Monitor* article (member-only) has an in-depth discussion of federal regulators' expectations for vendor management programs.

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.

EMERGING RISK ISSUES

Climate-Related Financial Risk

On May 20, 2021, the White House issued an Executive Order on Climate-Related Financial Risk. Section 1 notes the intensifying impacts of climate change present physical risk to U.S. economic assets and investments. It states, "The failure of financial institutions to appropriately and adequately account for and measure these physical and transition risks threatens the competitiveness of U.S. companies and markets, the life savings and pensions of U.S. workers and families, and the ability of U.S. financial institutions to serve communities." The Executive Order sets forth a policy of advancing "clear, intelligible, comparable and accurate disclosure of climate-related financial risk." Member financial regulators of the Financial Stability Oversight Council (FSOC) are tasked with: assessing climate related financial risk to the stability of the federal government and the U.S. financial system; facilitating the sharing of climate-related financial risk data among FSOC member agencies; and issuing a report to the President by November 16, 2021, on any efforts by FSOC members to integrate climate-related financial risk into their policies and programs. FSOC voting members include the chairperson or director of

the various banking regulators, NCUA, the CFPB, Federal Housing Finance Agency (FHFA), the Federal Reserve Board, and the securities and futures/derivatives markets regulators.

A Congressional Research Service report noted that as of 2019, Fannie Mae and Freddie Mac guaranteed $6.88 trillion in home mortgage debt without pricing flood risk into their guarantee fees. Almost all insured U.S. flood risk is backstopped by the U.S. government through the National Flood Insurance Program. The same report stated the municipal bond market already shows signs of pricing to account better for climate change risk. This is an indicator of potential risks in the market that are not perhaps addressed today and could lead to losses and price shifts.

Some of federal financial regulators have already been addressing climate related risk in public comments or reports. As an example, the Office of the Comptroller of the Currency (OCC) named a climate change risk officer back in July 2021, indicating that "prudently managing climate change risk is a safety and soundness issue." The OCC is planning a two-prong approach – learning and engaging from others and supporting the adoption of climate risk management at banks. Back in January 2021, the Federal Reserve Board also created an internal Supervision Climate Committee to identify and assess potential financial risks from climate change. NCUA Chairman Todd Harper discussed climate financial risk in August 2021 testimony before Congress and in separate remarks to fellow federal regulators. According to Harper, NCUA can fulfil its safety and soundness obligations in part by measuring, monitoring and mitigating these kinds of risks.

The NCUA Board noted the need for consideration of climate-related financial risks in the agency's 2022-2026 Strategic Plan. However, while the plan speaks to risks from climate change, NCUA is not mandating any related actions by credit unions.

Although members of Congress have introduced legislation on the issue, this kind of legislation does not have current bipartisan support. Some states have also begun issuing guidance relating to climate change.

In early July 2021, the Washington Department of Financial Institutions issued an alert on the systemic risk of climate change. The alert gives some background on the risks and aims to "begin discussions with stakeholders" on how entities it regulates can address these risks and integrate them into their governance, risk management and strategic plans. Potential risk categories were highlighted.

Physical Risk – A credit union's branches and offices can be damaged by a weather event, wildfire, or similar. However, credit unions also have significant amounts of loans that are secured by physical premises. Floods and fires can lead buildings to be deemed a total loss as an example.

Transition Risk – The economy seems poised to transition to a low or net-zero carbon economy. Consumer and investment sentiment is changing in this regard, and discussions around infrastructure spending, advancing technology, and policy/regulatory changes are factors for this transition. This in turn represents a shift in the economy and market forces, so assets that have a high carbon footprint or that are linked to carbon-heavy industries could be "stranded." In other words, the value of some assets used to secure loans could end up lower in value than today rather than appreciating. Financing to industries that rely on fossil fuels is subject to this risk, like manufacturing, construction and transportation.

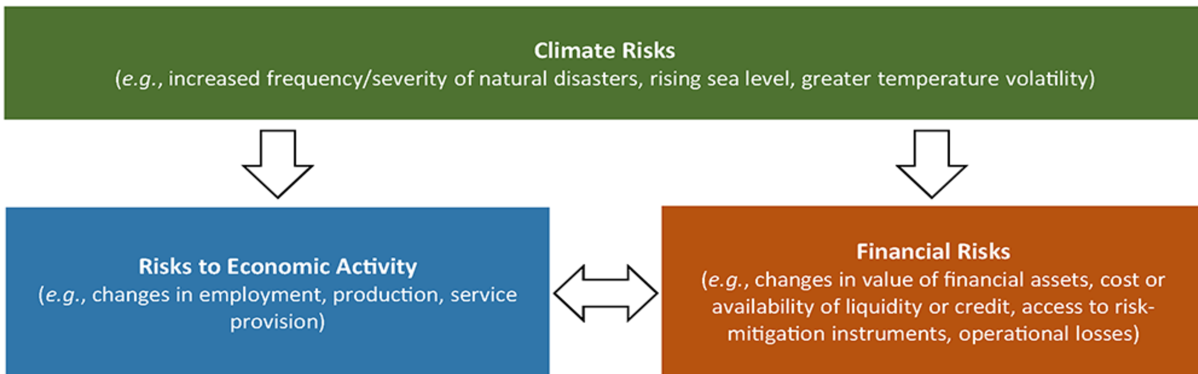
Impact to Vulnerable and Disenfranchised Communities – The alert briefly mentions that climate change will have a disproportionate impact on economically vulnerable populations, including people of color given histories of redlining.

The New York Department of Financial Services issued a guidance circular with a similar introductory discussion about climate risk – hurricanes, floods, wildfires, disruption to agriculture. Properties securing mortgages and commercial mortgage-backed securities are at risk of damage such as to flood. Transition risk was also flagged, again as society moves away from carbon-based energy to low-carbon options.

The agency lists its expectations for all regulated organizations. This includes incorporating financial risks of climate change into governance, management and business strategies. A board member or a committee of the board and a senior management function are expected to be designated to assess enterprise-wide risk, and the potential for climate change to impact credit, market, liquidity, operational, reputational and strategy risks. Financial institutions are also expected to develop climate-related risk disclosures.

In March 2021, Federal Reserve Board staff released an article with an economic analysis on climate change and financial stability. The analysis offers a way to "assess the financial stability impact of risks resulting from climate change as information on the nature, extent, and timing of those risks improves." The following two charts illustrate the potential risks and outcome of climate change to the U.S. financial system.

Stylized Relationships between Climate, Economic, and Financial Risks



Illustrative Examples of Transmission Channel Framework

	Climate Risks	Economic Risks	Financial Risks	Financial Stability Risks
Real Estate	Rising sea levels, frequency of storm surges	Increased inundation of coastal parcels	Decreased value of coastal real estate	Abrupt repricing of mortgage lending markets
Insurance	More frequent and severe hurricanes, wildfires, etc.	Greater disruption to local economic activity	Pressure for higher rates, lower supply of insurance and reinsurance	Greater uninsured losses, spillover effects

Source: Federal Reserve Board

Diversity, Equity and Inclusion

The issues of diversity, equity and inclusion (DEI) have taken center stage in the workplace. Among the risks that credit unions may face by not having a strategy focus on DEI are failing to attract and retain talent, losing member customers and missing out on emerging opportunities and areas for innovation. Reputation risk is also a factor and can surface in a variety of ways. This RIMS article discusses how reputation risk can be avoided by embracing DEI.

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?

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

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

4. What is enterprise risk management?

5. How is enterprise risk management beneficial?

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

NCUA Expectations under Risk Management: The 7 Categories of Risk

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

2. What has NCUA identified as risk factors?

3. Explain/define the risk categories.

4. What are NCUA's supervisory priorities for 2022?

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

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?	2-4 Questions
NCUA Identifies Seven Risk Categories	10-12 Questions
2022 Risks	5-7 Questions
Enterprise Risk Management (ERM)	4-6 Questions
Benefits of an ERM Program	1-3 Questions
Risk Appetite	1-3 Questions
ERM Program Requirements	2-4 Questions
NCUA Examiner Expectations	1-2 Questions
Vendor Management Program	3-5 Questions
Third Party Risk(s)	1-2 Questions

APPENDIX A

NCUA Examiners Guide Risk-Focused Examination Program Section

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

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

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

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

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).

NCUA Letter to Credit Unions 21-CU-16 (Relationships with Third Parties that Provide Services Related to Digital Assets)

NCUA Letter to Credit Unions 22-CU-08 (Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence)

NCUA Letter to Credit Unions 22-RISK-01 (Heightened Risk of Social Engineering and Phishing Attacks)

FFIEC Guidance Authentication and Access to Financial Institution Services and Systems

FFIEC Guidance Security in a Cloud Computing Environment

In re Trustmark National Bank, Case 2:21-cv-02664 (October 22,2021)

In re American Express Centurion Bank and American Express Bank, FSB, 2017-CFPB-0016 (Aug. 23, 2017).

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 2016-02 (Oct. 31, 2016) (Service Providers)

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

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