WolfPAC
INTEGRATED RISK MANAGEMENT

Preparing for FI Regulatory Exams: A Guide for Risk Management Pros

Discover insights from two veteran risk and compliance experts to help you avoid penalties and stay up to date.

This comprehensive guide offers a detailed checklist and best practices designed to help financial institutions (FIs) reduce risk and transition from outdated methods to more modern risk management methods. Keep reading to ensure thorough preparation for regulatory exams and start building a more mature, scalable risk management strategy.

Meet the Experts

You didn't download this guide for generic advice you could find anywhere else.

Of course not. You're reading this because you're serious about improving the risk management and compliance program at your FI.

Say hello to Lisa and Puja, who will guide you through the best practices you need to pass your next exam. Their combined expertise covers everything you need to know about proper compliance, IT and cybersecurity risk, vendor management, and more.

Lisa Spampinato

CRVPM

Lisa serves as Director of Implementations for WolfPAC Integrated Risk Management®. A specialist in client support, she oversees all WolfPAC module implementations and assists. Lisa is also the Vendor Manager for Wolf & Co.

Lisa offers robust project management experience in information technology, having spearheaded projects for healthcare, manufacturing, and financial services organizations. She has also spent time as an engineering leader and product manager, with a specialization in software development.

Puja P. Ghiya

Director of Product

Puja serves as Senior Manager for WolfPAC Integrated Risk Management®. She brings more than 12 years of experience supporting business solution software and optimizing business operations.

Puja's specialty ranges across business analysis, testing, reporting, support, software development, product implementation, delivery, and training. She's demonstrated in-depth experience in financial management, business administration, information technology applications, process modeling, and data modeling. Puja also brings hands-on management experience to the table, which she developed and established across several cross-functional team assignments.

What is WolfPAC?

WolfPAC provides a low-friction, easy-adoption risk management platform for financial institutions, healthcare organizations, and FinTech companies.

Backed by the expert guidance of Wolf & Company, WolfPAC Integrated Risk Management® is a fully integrated suite of software and advisory services that helps risk professionals automate and streamline risk assessment, tracking, and reporting processes.

With easy implementation and proactive customer support, WolfPAC customers can get started in weeks – not months — and continuously mitigate risk with help from the latest expertise and technologies.

Introduction

The risk landscape is becoming increasingly complex — which means many examiners and regulators are operating with a little extra scrutiny these days.

Financial institutions are juggling more software vendors than ever before — and each new partner brings its own complications related to data usage and privacy protections. Hacks, data breaches, ransomware, and widespread IT troubles such as the Crowdstrike outage are spotlighting the need for robust cybersecurity protections. Artificial intelligence (AI) and cryptocurrency bring new implications that hardly anyone can predict.

Risk management teams at regional FIs have a lot of ground to cover as they prepare for their next exam. Relying on manual methods such as spreadsheets can leave banks and credit unions in a difficult position as they prepare for exams. Risk management software is rarely a silver bullet; only the right maintenance and support can help turn a software platform into a crucial instrument of a larger risk management strategy.

This guide delves into the critical aspects of preparing for a regulatory exam and outlines best practices for establishing a robust risk management program. In these pages, we'll cover:

- Common risk red flags regulators are looking for
- Best practices for hot-button areas such as vendor management
- A 7-step checklist to help you prepare for your upcoming exams
- Insights and predictions for two emerging trends: AI and crypto

After reading, you'll be empowered with the tools and strategies to excel in your regulatory examinations and build a more sustainable risk management strategy for your FI.

Poor results from a regulatory exam can be a costly affair. If things go wrong, your FI could face hefty fines, reputational damage, and even operational restrictions. Proactive risk management approaches can help ensure regulatory compliance and foster a culture of risk awareness within your organization.

Common Risk Assessment Red Flags

Examiners tend to be on the lookout for some key risk assessment signals, including outdated manual processes, a lack of controls in place for consumer protection, and gaps in cybersecurity strategy. Let's discuss eight common focus areas that typically draw scrutiny from regulators and examiners.

Manual Risk Assessment

When a regulator notices an FI using manual methods to track its risk assessments, it's usually a flashing red light. Some spreadsheets used for operational purposes are acceptable. However, manual risk assessments are **inherently riskier** than leveraging integrated risk management software. You can point to a variety of drawbacks related to over reliance on spreadsheets: human error, data accuracy, poor visibility, and a lack of version control.

Examiners might question these outdated processes, especially given the prevalence of risk management software options in the market.

Out-of-date risk management software

Simply having risk management software isn't enough to satisfy the requirements of an exam. Regulators will want to see that your team constantly updates risk assessments within your software program. Risk management software typically makes it easy to stay on top of your updates, but that also means regulators will be able to easily identify any outdated assessments.

WolfPAC's Integrated Risk Management® solution automatically displays the dates associated with your risk assessments and suggests when they should be updated.

A perceived lack of controls to mitigate risk in high-leverage areas

It's one thing for an examiner to spot a high-risk area within your institution. It's another to identify a lack of controls to remedy that risk. Risk managers should be sure to show proof that they have corrective action plans in place to address and mitigate the risk.

Unreasonable or inconsistent risk assessments

Examiners can usually tell if you're underestimating the risk level of your processes and controls. A regulator might assess hundreds of FIs throughout their career. Most of these institutions use similar software and vendors, so examiners usually know which systems bring inherent risk.

If your risk management practices show strong, but the actual logs have issues, there's a good chance it will get flagged.

Poor quality of loan underwriting or credit risk management

Inadequate credit risk management practices can lead to significant losses. Examiners will assess your loan underwriting procedures, credit monitoring processes, and collection strategies. Any inadequate practices – failing to verify income, neglecting debts, or poor collection controls – could bring you under regulator scrutiny.

Deficient consumer protection measures

Compliance with data privacy regulations is crucial. It's especially important to have a grasp on the regulations in the geographic areas you do business. This includes measures such as GDPR (if you're operating in Europe) and the California Consumer Privacy Act (CCPA).

Examiners will tend to look for gaps in your data security protocols, consumer notification procedures in case of data breaches, and compliance with fair lending practices.

Insufficient cybersecurity infrastructure

Regulators will often place scrutiny on your **cybersecurity and IT practices**, including ransomware preparedness. They'll want to ensure that you've downloaded all recent application updates and cybersecurity patches. In some cases, they'll check to see if you're complying with multi-factor authentication (MFA) for applicable technologies. Resources such as the **InfoSec handbook** can help risk management teams stay compliant.

And if you did get breached since your last exam, they'll assess the speed and compliance of your institution's response as it relates to protecting customer data.

Inadequate monitoring and reporting of suspicious activities

Effective Anti-Money Laundering (AML) and Know Your Customer (KYC) programs are essential for detecting fraud and preventing financial wrongdoing. Failing to monitor and report suspicious activity could cost your institution when it's time for your next exam.

For example: you should ensure each deposit over $10,000 in cash is accompanied by a suspicious activities report.

Extra Credit: Best Practices for Vendor Risk Management

There are many areas to address when it comes to exam prep, but risk professionals can add value by ensuring that their vendors remain an asset — not a liability — to their financial institution.

Before any exam, FIs should ask themselves: how well do I know my vendors? Given the proliferation of cloud software and outsourced IT, many FIs are dealing with more vendors than ever before. Vendor risk management, especially related to data and consumer protection practices, is an increasingly important component of many risk examinations.

Maintain visibility over high-leverage vendors.

Not all third-party vendors need to be monitored every year. It's important to keep a list of all vendors in a central place; this will help you identify the moderate and high-risk vendors that deserve your constant attention.

Third parties that deal with sensitive information such as customer data and social security numbers should be monitored more closely. The same goes for any software system that helps move money, such as wire transfers.

Research your vendor's data practices

We always recommend that risk teams at FIs understand how vendors collect, store, and use data. Consider your third-party providers' data privacy policies, security measures, and incident response plans.

Which countries does the vendor operate within – and which data laws are applicable? Does the fine print show the vendor's plan to sell customer data? Will they use customer data to train AI models? Even if intentions aren't nefarious, it's important to understand what's happening to your member data beyond the walls of your institution.

WolfPAC provides guidance on the frequency of monitoring and the recommended tasks to monitor vendors based on their inherent risk ratings.

Don’t forget “fourth-party” connections

Another aspect of third-party visibility is understanding your vendor’s vendors. How would a potential breach or disruption within their supply chain impact your FI?

In 2023, a ransomware gang hacked the file transfer tool MOVEit. The ripple effects were felt across nearly every industry, with organizations ranging from financial services firms to British Airways to the New York City public school system. MOVEit took the brunt of the scrutiny, but there was also a class action lawsuit against IBM, which ran many of the servers that MOVEit used.

Long story short: it’s not just your vendors that present risk.

Review vendor’s SOC reports

If you’re overwhelmed with the idea of maintaining visibility over a slew of vendors, have no fear! Security Organization Controls (SOC) reports provide independent assessments of a service organization’s security and processes. These SOC reports can provide an efficient path to assessing risk across your spectrum of third-party relationships.

Document your vendor onboarding process

We recommend establishing a robust vendor onboarding process — one that includes risk assessments, contract negotiations, and continuous monitoring. But it’s not enough to simply follow this process; risk management teams should also document the onboarding process to show regulators that they’re following through on their promises.

WolfPAC’s platform offers a variety of tools to help you develop a comprehensive Third-Party Risk Management program to enhance your visibility, increase efficiency, and reduce vendor risk.

Checklist: 7 Risk Assessment Steps to Prepare For Your Next Regulatory Exam

Prioritize employee training

What's the most important ingredient in a sound risk management strategy? Typically, it's your employees. Risk management teams are responsible for driving a culture that naturally helps their staff avoid risk and stay compliant on a daily basis.

This checkbox includes staying up to date on exam procedures, business continuity training, promoting compliance with mandatory phishing training, and more. We encourage particular emphasis on best practices for data security, customer protection, and fraud prevention.

Is your next examination rapidly approaching? Want to make sure you're fully prepared? Follow these seven steps to help showcase the strength of your risk management program.

Stay up-to-date on the latest regulations

If we could condense this guide into four words, they would probably be: "Stay up to date!" Educating yourself and your team on the latest policies, procedures, regulatory mandates and compliance initiatives will leave you in a much better position as you put together your risk assessments.

One common strategy used by best-in-class risk organizations is proactively engaging with regulatory agencies. It's important to remember that examiners aren't out to get you. Asking for advice or clarification can show initiative and help you mold your risk program to better adhere to the latest guidance.

WolfPAC's Regulatory Compliance Risk Management solution automatically generates reports, develops monitoring and audit plans, and tracks federal and state regulatory obligations to help you analyze risks and remediate gaps.

Update your risk assessments

This tip may seem fairly obvious, but it's crucial to avoid findings on your next regulatory exam. Work with your team to continuously update your risk assessments so you can stay exam-ready. You'll be better equipped to showcase the quality of your risk management program if you're not scrambling.

Double check inventories of third-party applications and vendors

As we mentioned in the previous section, it's important to create a comprehensive list of third-party vendors in a central location. Set up a recurring time on your calendar to update this list, as well as the accompanying onboarding documentation for each third party. Simply knowing who all of your vendors are will give you a leg up.

Build plans to address areas with inadequate controls

It's possible you've run a risk assessment and identified a high-risk area with a lack of strong controls. That doesn't mean you're doomed. Regulators will just want to see evidence that you have a strategy in place to improve this area. Show, in good faith, that you're going to mitigate that risk with a concrete action plan.

Upgrade cybersecurity practices per the latest guidance

Hackers and threat actors are constantly finding new ways to attack critical systems. That means that cybersecurity regulations and best practices are continuously evolving, as well. For example: organizations such as the Federal Financial Institutions Examination Council (FFIEC) now require multi-factor authentication for any applications that handle sensitive data.

Work with tools like the InfoSec handbook to gain a better grasp of the latest procedures so you can stay compliant.

WolfPAC's IT Risk Management solution provides a dashboard view of your entire IT infrastructure, including current technologies, inherent gaps, and outdated regulatory standards—allowing you to comprehensively analyze your framework to identify, manage, and reduce risk.

Run the correct reports

Another potentially obvious – but equally crucial — item on the checklist. If you've spent all of this time and effort making sure you're compliant, you must also run the correct reports that display the right data for examiners. Risk management software helps you automatically run these reports promptly so you can focus on addressing other key areas before your exam.

Emerging Trends That Could Affect Your Next Exam

There's a lot of chatter about AI and crypto in the financial space. But what do these emerging trends actually mean for risk management — and how do they affect your exam preparation? The answers aren't concrete, but staying ahead of the curve will help you ensure proper compliance.

Artificial intelligence can generate up to $1 trillion in additional value annually for the global banking industry.

Source: McKinsey

Artificial intelligence

> The rise of AI represents both an exciting opportunity and an increase in complexity for the risk management field.

On one hand, leveraging AI-led software can help risk management teams analyze customer behavior, predict market trends, and evaluate investment options using relevant data and advanced techniques. FIs such as Danske Bank are combining robotic process automation with AI to enhance its KYC and loan processing capabilities – increasing fraud detection by 50%. Leveraging AI tools to help you prepare for your next exam can be a massive efficiency booster.

However, we must also consider that the rest of the world is using AI, too. Many of your third-party vendors likely use and train their own AI models. How secure are those models from cyber-attacks? Is your customer data being used to train other AI models? These are important questions to understand as you identify high-risk areas before your next exam.

Cryptocurrency brings new regulatory considerations.

> Regional banks and credit unions have stood the test of time because they understand – and respond to – the needs of their customers. Some might dismiss cryptocurrency as a short-lived fad. But the truth is that nearly half of American adults have embraced the crypto movement. All of that's to say: your FI is likely to invest in some crypto infrastructure over the coming years to stay competitive — if it hasn't already.

40% of American adults now own crypto, up from 30% in 2023.

Source: Security.org

Just like with AI, embracing crypto brings both massive business potential and its own set of risks. Regulations and consumer protections are constantly shifting meaning risk managers must stay up-to-date and not be afraid to engage with regulatory agencies for advice.

Crypto products also bring their own set of software and third-party vendors for money transfers. Risk teams should pay close attention to these new vendors and the controls they have in place. The landscape will continue changing as we transition from the early "Wild West" days of crypto to a more structured, regulated crypto economy.

How to streamline your risk management with WolfPAC

Are you looking for an integrated risk management system to help streamline your preparation for regulatory examinations? WolfPAC is here to help.

You don't have to navigate your next exam alone. 6,000+ users trust WolfPAC Integrated Risk Management software to protect their organization and keep their FI exam-ready.

Partnering with WolfPAC will help you:

Onboard and derive value quickly

If you're reading this guide, there's a good chance you've got a regulatory exam on the horizon. You don't have time to wait, and WolfPAC makes getting started easy. Our industry professionals handle the heavy lifting to help you get onboarded fast – so you can start seeing value from our software immediately.

Leverage expert guidance to prepare for your exam

Partnering with WolfPAC means gaining access to the expertise of 300+ Wolf & Co. consultants, auditors, and experts in the field. These experts bring guidance on the latest regulations and trends to keep your risk assessments up to date.

Access helpful automations to keep you exam-ready

We mentioned that the major theme of this guide is, "Stay up to date!" WolfPAC elevates your team from the traditional spreadsheet by providing automated alerts to keep you educated and on track. Work smarter, not harder, with WolfPAC and our team of experts. Discover the ERM you'll actually use at www.wolfpacsolutions.com

This guide provides you with a baseline to update your risk management program ahead of your next exam. You got this – happy risk managing!