5 Steps for Easing into ERM

By Michael Carpenter

Building out an enterprise risk management (ERM) program can be overwhelming for financial institutions and others in the financial services industry. Risk management is a broad umbrella covering a wide range of risks, including operational, cybersecurity, compliance, reputation, and financial risk, among others. With so many areas to cover, it's hard to know where to begin or how to get it all done.

One common mistake banks make when faced with an overwhelming task like building out a risk management program is to kick the can down the road. They decide they are too busy, and the job is too big, so they'll dig in once things quiet down.

This creates two problems:

Problem #1: A quieter time isn't coming

We all like to imagine that a simpler, quieter time is just down the road. We just need to reach a deadline or milestone and we'll have plenty of time to tackle our backlogged to-do lists.

The problem is that a quieter time isn't really coming. When Aristotle said, "nature abhors a vacuum," he probably wasn't talking about project management, but he may as well have been. New projects are always coming to take the place of those that are finished. It's rare to finish a project and then wonder "What should I do next?" The next thing has already been defined and mapped out. There is no pause.

Problem #2: Exposing the institution to unknown amounts of risk

The goal of risk management is to identify, assess, measure, mitigate, and monitor risk to ensure your financial institution isn't taking on too much or too little risk. Your institution's risk exposure needs to align with its risk tolerance.

The longer you wait to build out a risk management program, the longer your institution is exposed to unchecked risk.

5 tips for simplifying your ERM program buildout

Now that you know why you shouldn't put off building out your ERM program, let me show you the five things you need to know to get the job done.

1. You don't have to do it all at once.

Rome wasn't built in a day and your risk management program doesn't have to be either. Like any project, risk management should be broken down into phases. For example, you might decide that it will

take three years to completely fully build out your risk management program — but that doesn't mean you won't get any value from the program for at least three years.

Any time you manage risk, you're helping your institution. Whether its compliance risk, cybersecurity, or corporate governance, each building block of risk management will help make your institution stronger and more resilient.

Choose one approach to risk management and start.

2. Decide where to begin.

When building out a risk management program, there are two recommended approaches to choose from:

- **Start with a strategic goal or initiative.** When starting with the goal in mind, begin by identifying all the objectives and hurdles. What do you need to do? What might stand to prevent that from happening?
- **Start with the highest inherent risk** (i.e. the risk that exists naturally when there are no safeguards in place to avoid trouble).

Both approaches help you "right size" your risk management. Often it makes the most sense to start with a strategic goal or initiative and then define inherent risk.

Whichever route you choose, gather and update existing risk assessments to determine the highest inherent risks and identify the controls in place.

3. Leverage your data to assess risk.

Risk management empowers your institution to evaluate threats and opportunities to better understand how significant a risk is, how well it's being controlled, and what else, if anything, needs to be done to better manage it.

Starting with areas of high inherent risk not only makes risk management more manageable, but it also maximizes the value of your risk management investment by helping you remediate risks that could have a major impact on your institution.

Sure, you could start with something small and easy, but if it's not going to have a big impact on your risk profile, you're better off starting with something else.

Inherent risk is best understood with relevant, recent and quantifiable data, including test results, audits, and exams. Have you had feedback from examiners about your BSA (Bank Secrecy Act) program? Or maybe your institution has identified risks relating to data security, vendor management, regulatory compliance, UDAAP (Unfair, Deceptive or Abusive Acts or Practices) and fair lending, or attracting and retaining employees?

Use the available data to identify and prioritize areas with the greatest inherent risk. Then identify the controls that help mitigate the risks.

4. Dig into controls.

Once you identify inherent risk and the controls to mitigate them, it's time to identify key controls (controls that are automated or expected to prevent a risk).

Decide who will assess these controls and when, remembering that some controls are provided by vendors and may have already been reviewed by your vendor management program. Go through one cycle of control assessments to get a feel for how effective the process is and how well it works with other areas of risk management including business continuity and compliance.

It's also a good idea to create key performance indicators (KPIs) to help measure risk (and whether you are within your institution's risk tolerance) and progress towards strategic goals.

5. Work your way through areas of lower inherent risk.

Once you've knocked out your biggest areas of inherent risk, continue down the list. Knock out other high-risk areas working your way down to other, less critical areas of risk. By now you'll have learned what works best for your institution, so it should go quicker and more smoothly.

Since risk management touches every area of a financial institution, each new area added to the program will build on what was already created, making the program stronger and more effective.

Risk management is a cumulative activity. As you build out the program and expand into different areas, your institution will benefit from having a more well-rounded view of risk and the information the board and management need to make more informed strategic decisions.

Don't let analysis paralysis stop your financial institution from adopting enterprise risk management. Know that your ERM buildout is a journey — one that will take a while but will offer many rewards along the way. It's okay to ease into risk management.

Want to learn more? Read Creating Value with A Culture of Risk Management.

Michael Carpenter is vice president of risk management at Ncontracts, the leading provider of risk and compliance management solutions to the financial services industry. An indispensable risk management, compliance, and vendor management resource, he is an advocate of building stronger, more proactive and more resilient institutions. Prior to joining Ncontracts, Mr. Carpenter served as the vice president of risk management at several banks and credit unions. His broad base of industry knowledge is the result of building and running programs—including director training and reporting, compliance management, information security, BSA/AML, among others—at both small community financial institutions and larger institutions such as KeyBank and Chase Bank. He is the veteran of the U.S. Army.