Ask the Expert: How to Draft Risk Assessments

Creating the most effective risk assessments involves a combination of research, analysis, experience, and collaboration. Monica Bolin, CERP, NCRM, is a risk management expert with Ncontracts and former chief risk officer with over three decades of experience in the banking industry.

As a banker, Monica built her bank's entire risk management program from the ground up by request of the bank president. She developed every risk assessment, figuring it out as she went.

Today, Monica creates model risk assessments. We spoke with Monica about her method for crafting risk assessments, the elements of a good risk assessment, and strategies for drafting a risk assessment when unfamiliar with the area being assessed.

Q: How can you determine if a risk assessment is needed?

A: This decision is primarily based on your enterprise risk management program plan. Begin by creating a list of areas within your institution that require risk assessments, including those mandated by regulators. Examine your entire ERM program and organizational structure to identify areas of exposure. Break down the institution's various areas to establish a comprehensive strategy.

Additionally, ensure that whenever you introduce a new product, service, process, or procedure, a risk assessment is conducted or an existing one is updated as needed.

Q: How do you start to build a risk assessment?

A: Once you've outlined your plan for all necessary risk assessments, it's time to gather your resources. Collect relevant regulations and guidance for your regulatory risks.

Examination handbooks are invaluable, particularly for operational risks without specific regulations. These handbooks provide insight into what regulators expect when assessing your institution, helping you identify risks and controls.

Then you can start identifying pertinent risks. Assess each risk to determine its inherent risk level, which is the likelihood and potential impact of the risk occurring.

Next, pinpoint existing controls by asking, "What are we currently doing to mitigate this risk?" Evaluate the effectiveness of each control. For example, if someone not responsible for payroll reviews payroll records daily to ensure accuracy, an audit may be conducted to gauge the control's efficacy.

If a control involves a policy or procedure, an independent party should review it for comprehensiveness and risk mitigation effectiveness.

If the control is a policy or procedure, somebody else is going to look at that policy and ask: Is it comprehensive? Does it mitigate risk?

Q: How long should a risk assessment be?

A: It depends on a lot of factors, including the type of risks, products, and service involved.
For instance, a BSA risk assessment tends to be lengthy due to the extensive regulations. On the other hand, risk assessments for smaller regulations, like the Military Lending Act, may only encompass 5 to 10 risks.

Ultimately, the length depends on the scope of the process, the size of the financial institution, and the extent of its involvement in the project.

Q: Where do you begin when drafting risk assessments on subjects outside your area of expertise?

A: As risk practitioners, it's impossible for us to be experts in every department. Working at the bank, I found the most effective approach was conducting thorough research, developing my assessment, and then collaborating with the business process owner.
For example, I had never worked in human resources before. When I tackled the HR risk assessment, I drafted it first and then approached the business owner to fill in any gaps. I explained that they, as the ones immersed in their work daily, would be familiar with all the risks and controls in place to mitigate those risks. They could either sit with me to review the assessment or do it independently and provide feedback via email later.

I initiated the process to ease their workload since risk assessments are not part of their regular duties. Even though it takes time from their daily tasks, and they might be hesitant to participate, their input is invaluable for a successful risk assessment.

Q: How can you be sure your risk assessment is comprehensive?

A: A comprehensive risk assessment will be the product of thorough research and utilizing all available resources. You'll have collaborated with the business owner to identify any additional risks and controls. Another team member will assess control effectiveness, and your internal audit will review the process to ensure the controls are functioning properly. Moreover, you'll continuously update risk assessments as new guidance, regulations, products, and processes emerge.

When regulators review your risk assessments, they'll inform you if anything is missing or incorrect, providing valuable feedback for improvement.

Q: When should the risk assessment process for a new product or service begin?

A: When introducing a new product, service, program, or process, it's essential to involve the risk management function from the get-go. Its expertise is crucial in identifying potential risks and ensuring a thorough risk assessment is carried out before any contracts are signed or implementation begins.

Your bank needs to know if the risk associated with a new product or service aligns with your risk appetite. If the board expresses concerns about excessive risk, you'll need to explore alternative

controls or approaches to reduce the risk to an acceptable level before proceeding with the new product.

Q: Any final risk assessment wisdom to share?

In the past, we saw risk assessments as an annual task, completed and then shelved until the following year, for an update. The field has matured, and we realize now that risk assessments are actually an ongoing process.

With constant changes in regulations, processes, the economy, and the banking system, it's crucial to continually evaluate the adequacy of your risks and controls. Risk assessments should be a routine part of daily operations, not just a once-a-year activity.