The Risk Assessment Process — One Size Doesn't Fit All

BY JASON CORDER

I am constantly searching for that one item that does everything – whether it's a single pair of shoes or the perfect pair of pants that can go from the office to the gym to the hiking trail to dinner, all while performing each task with excellence. Or, even better, I'd love to find an automobile that is an engaging sports car, a capable off-road vehicle, and a comfortable touring vehicle for my whole family.

The problem is that those things don't truly exist – there are always compromises. Those shoes that supposedly "do everything" don't quite look polished enough for the office, even if they offer solid support for gym activities. Or they lack the structure needed for hiking, yet they still only look somewhat appropriate for office wear.

Bankers are constantly trying to achieve this same "one size fits all" approach with their governance documentation – particularly their IT-related risk assessments. Risk assessments have several important purposes, including identifying, estimating, and prioritizing risks for an organization. However, an often-overlooked purpose of a risk assessment is to provide **awareness.** This means that the risk assessment should **clearly** and **effectively communicate** the level of risk for the area that is being assessed. There are risk assessments that are required by law, such as the information security risk assessment, required as part of the Information Security Standards implemented to comply with section 501(b) of the Gramm-Leach-Bliley Act (GLBA). Others are expected by regulatory guidance, such as business continuity, digital services, or cybersecurity risk assessments. Some are explicitly required; others are implied or suggested – and expected by examiners.

Many bankers, frustrated with the need to complete multiple risk assessments, try to combine them into a single enormous, "do everything" assessment. It may sound good in theory, but in practice it often becomes a spreadsheet that has 40 columns and more than 1,000 rows. Trying to incorporate threats related to information security, cybersecurity, business continuity, digital banking, remote deposit capture, and vendor management into one document results in something so overwhelming that it fails to communicate anything useful.

Another challenge with this approach is that responsibility for different risk areas is often distributed across different managers or departments. Extracting the relevant information for each group is overly complicated or even impossible. The "comprehensive" risk assessment may contain a lot of relevant information, but the "one risk assessment to rule them all" approach almost always fails to clearly and effectively communicate the bank's risk.

There is a better way. Just as my closet contains different types of shoes for different activities, a bank's governance documentation should include separate risk assessments – each purpose-built and bank-specific to provide awareness for a specific area or type of risk. The advantages of having separate risk assessments – greater stakeholder awareness, more actionable information for management, and cleaner alignment with examiner expectations – far outweigh the potential challenges of managing multiple risk assessments. Having relevant, customized risk assessments that reflect your bank's unique environment ultimately make your bank stronger.

If this is a challenge for your bank, Sawyers & Jacobs LLC can help by providing useful, examiner-approved risk assessments. Sawyers & Jacobs LLC asks the right questions and identifies the threats that help your bank reduce risk.

We may even be wearing the right shoes.

Jason Corder is Senior Vice President with Sawyers & Jacobs LLC, a consulting firm focused on serving financial institutions. Sawyers & Jacobs is an ACB Associate Member. Jason may be reached at 901-828-1942 or jcorder@sawyersjacobs.com.

ACB

SAWYERS & JACOBS