ARTICLE

Author Ken Tays, *Practice Leader, Broadridge Consulting*

August 2018

Risk assessment methodologies creating consistency through a common process

Regardless of a financial institution's size, complexity or business model, they all have one common denominator: they are all in the risk business. As such, they all have a significant need for risk assessment. In fact, FDIC regulation 12 CFR 364 and OCC regulation 12 CFR 30 require federally insured financial institutions to have processes in place in order to effectively "identify, measure, monitor and control" their risks. Without an effective risk assessment process, financial institutions could not meet this, or any, regulatory requirement.

It would be wrong to think that a risk assessment process would be different depending on the size, complexity and business model of each institution. The basic tenants of any risk assessment process are the same for any financial institution. Those tenants include a risk appetite statement, risk assessment methodology, risk mapping, inherent risk evaluation and residual risk evaluation.

RISK APPETITE

An effective risk assessment process generally starts with a risk appetite statement (RAS), which is a communication from the board to management defining the level of risk they are allowed to engage. In larger institutions, this includes an evaluation of its risk capacity and risk tolerance. Smaller, less complex institutions may not have this level of documentation or analysis. Nonetheless, the board must communicate operational parameters to management. The risk appetite will continuously drive the risk assessment process in order to ensure management has effective control of the business.

RISK ASSESSMENT METHODOLOGY

A well-defined risk assessment methodology is imperative to an effective process. The methodology will establish:

- Timing of completion
- Levels of approval

Ken has over 30 years of work experience comprised of military and financial services. Ken began his career in the US Army serving in Europe, Korea, and the Unites States. Ken is a two-time combat veteran serving in the first Gulf War and in Bosnia. Ken began his financial services career with the Office of Thrift Supervision where he spent 12 years and was a Senior Bank Regulator. Ken left OTS to join PricewaterhouseCoopers to work on Dodd-Frank implementation and regulatory issues around third-party oversight. Ken then accepted a position at Citi Bank in Operational Risk in which he led the audit management, records management, supplier due diligence, data governance, and process and quality teams. Ken currently leads the Governance, Risk and Control and Internal Audit Practices at Broadridge Consulting, a division of Broadridge Financial Solutions, offering internal audit and GRC solutions to financial institutions.

- Types of risk assessments
- Risk ratings and definitions
- Remediation and escalation process should a risk assessment violate the risk appetite statement

RISK MAPPING

Risk mapping is how the institution identifies current risk. This begins with mapping business process to business units and evaluating the risk. In this evaluation, management should define risk as any event that could prevent them from achieving their business objectives. For institutions with the capabilities, it is recommended they create a risk library, which can be leveraged by each line of defense. For example, the business can leverage the library to conduct control self-assessments; the Chief Risk Officer can leverage it as a second line of defense for maintaining risk assessments; internal audit can use it in the execution of its audits. Over time, businesses and risks change. It is important that organizations don't view the risk library as a one and done exercise. As these evolutions occur, the risk library should be updated and validated at least annually.

INHERENT RISK EVALUATION

Once risk is identified, the institution can apply the methodology and evaluate risk on an inherent risk basis resulting in an inherent risk score, which should be defined in the risk assessment methodology. Inherent risk is generally most useful in the development of an audit plan for internal audit. This will drive how often a business and/or process is to be audited. It can be useful to management to identify processes that might pose more risk than expected. As an example, management would most likely view commercial real estate lending as an inherently high risk activity. Understanding the level of inherent risk of a process allows management to develop an appropriate control to ensure the risk is managed within the RAS and that they are using the most economical control.

RESIDUAL RISK EVALUATION

Once the inherent risk level has been established, management can evaluate the residual risk of the process which is the remaining risk once the controls are in place. Getting back to our commercial real estate lending example; we said it was inherently risky, but if we put proper underwriting techniques (controls) in place, we can reduce that risk to a moderate level. As long as the board has accepted that level of risk, management would be okay with this level. The goal of evaluating residual risk is to ensure the level of risk in the process is reduced to meet the RAS.

Historically, risk assessments have been focused on frequency and severity of a risk event. As this process has matured in the market, risk managers are now starting to evaluate velocity and duration. Velocity is defined as how fast a risk event can occur. A good example is the risk fintech poses to the banking industry. It takes a long time to develop software, gain traction and take market share. On the other hand, a cyber event can happen very quickly. One employee clicking on a phishing link can set into motion a series of events that can create chaos in the institution in a matter of hours. Duration refers to how long an event can last. While it may take a long time for the event to occur, the event can have significant staying power with continual negative effects. On the other hand, the cyber event can be dealt with quickly. The cleanup may be extensive, but we can stop and limit the effects of the event.

As businesses mature and risk evolves, so must the risk assessment process. An institution's success relies heavily on its ability to identify, measure, monitor and control risk. Those that have a well-established risk assessment process can ensure they meet regulatory standards and strategic objectives.