Ask Treliant

Best Practices for Conducting Risk & Control Self-Assessments (RCSAs)

During the Consumer Bankers Association (CBA) webinar "RCSAs: Putting it All Together", on March 22, 2018, there were a large number of questions asked. Please see the Q&A below.

1. **What are your thoughts on manual vs. automated risk and control self-assessments (RCSAs)? Do you have any recommendations on effective tools for automated risk assessments?**

   There is no one-size-fits-all methodology for conducting risk assessments. However, there are some key factors that institutions should consider when selecting risk assessment methodologies and tools:

   - **Size of the institution.** If the institution is large or systemically important, regulators may expect more robust RCSAs as part of expectations for rigorous risk management systems.
   - **Understand the basics.** What products or services does your institution offer, to whom are they marketed (through what channels), and in which geographic region(s)? All of these factors should be considered when thinking about how to plan and execute RCSAs.
   - **Complexity of the institution.** Institutions with more business units or more complicated business units may find using technology eases their execution of their RCSAs.
   - **How the institution conducts its RCSAs.** Depending on the methodology and frequency of updates, business units may need assistance in completing their RCSAs, including assistance in using any RCSA technology.
   - **Choose the right tool.** If an automated tool or third-party service is deemed necessary, reach out to multiple vendors for tool demonstrations and conduct a thorough analysis of each. Does it meet all of your needs? What type of reporting is available—is it comprehensive and is aggregation available and effective for executive and board review? Does it provide for a sign-off process and allow for review and challenge documentation? Can you sufficiently categorize and provide detail according to the financial institution's needs? Will the users be trained, and is the tool itself user friendly? Can you expand to multiple modules, ensuring that the product is scalable for your use as your institution grows? How well will the tool fit your risk management environment and capabilities?

2. **Please explain best practices for integrating (or not) operational and compliance RCSAs.**

   It is important that the institution conduct both operational and compliance RCSAs when evaluating and reporting on risks and controls. Whether or not the two activities are integrated is dependent on the risk reporting structure of the organization. Banks often report on operational and compliance risk categories separately, including inherent and residual risk, which allows for separate risk appetites per risk category. However, it is also important to coordinate the activities to ensure complete coverage without duplication of risk. In addition, coordination and aggregation is necessary in order to provide for a comprehensive risk profile.

(continued on next page)

3. Can you provide some guidance on how professional control groups (i.e., legal, finance) are supposed to design RCSAs and controls?

A front-line unit, or business unit, has been defined by regulators as an organizational unit that is accountable for the identified risk and that also engages in generating revenue, reducing expenses, providing operational support or service to any organizational unit, or delivering products or services. It also includes providing technology services. The Office of the Comptroller of the Currency (OCC) specifically indicates that front-line units do not necessarily include the legal or finance units. However, sometimes these units do carry risk. For example, the CFO's organizational unit may be responsible for setting goals and providing oversight to enterprise-wide expense reduction initiatives. Some of these support units may have regulatory reporting functions, which would require appropriate controls. These initiatives have the potential to create one or more risks, if actions taken to achieve cost saving goals inappropriately weaken risk management practices or internal controls. There may also be instances in which the general counsel is responsible for functions that extend beyond legal services. In addition, an organizational unit may own a risk when it is assigned responsibility for a risk, even if it did not create the risk, for example during a loan portfolio review. Finally, some second-line (risk management and/or compliance unit) and other support functions may have responsibility for control activities. Therefore, it is important to review the practices of these units, determine if there are activities, responsibilities, or functions that are accountable for a risk, and consider the specific risks without implicating the entire business (or professional control group) unit. A review of your specific regulator's practices, as well as your institution's policy requirements for RCSAs, is advisable.

When designing controls, it is first important to have a complete understanding of the unit's functions and risk(s), as well as their impact and likelihood. One or more controls should then be designed to effectively bring the risk within the parameters of the bank's risk appetite.

For example, assume your bank has a risk appetite of obtaining greater than 95 percent of all post-closing loan documentation within 30 days of closing, and you have to design a control. First you would need to assess where you are now (let's assume 90 percent) and then figure out how to get to greater than 95 percent. Second, take a look at the controls currently in place. Could they be enhanced to be more effective and bring your bank within tolerance? Assuming you have to create one or more entirely new controls, look at factors such as the type of technology available, the resources at your disposal, and existing processes. After taking all this into consideration, design your control and document it well. Lastly, test your control. Did it work and get you within your risk tolerance? If not, keep following the same steps until you get where you need to be.

4. How do you determine the risk appetite level in order to determine that the residual risk is within the risk appetite?

The risk appetite should be set by the board of directors as part of its role in setting strategy and providing oversight. The risk appetite aggregates the levels and types of risk the board of directors and management are willing to assume to achieve the bank's strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements. The risk appetite should be well documented and communicated to stakeholders throughout the organization as necessary.

(continued on next page)

5. **Can you explain what an effective review and challenge looks like? Can you define an effective challenge process?**

   The second line of defense should conduct a review of the first line's RCSA activities.

   At a minimum, an effective review and challenge would include:

   - Setting standards for RCSAs;
   - Reviewing risk identification to ensure the capture of relevant risks;
   - Reviewing the inherent risk likelihood and impact rationale determinations;
   - Reviewing control ratings and comparing them to the results of control testing;
   - Reviewing any overrides of residual risk ratings for appropriateness; and
   - Ensuring that any rating and/or rationale differences and unmitigated risks that are outside of the institution's risk appetite have been appropriately escalated.

6. **How specific do you recommend making the "why" part of the risk description?**

   The "why" portion of the risk description should demonstrate an understanding of the potential consequences should the risk event occur. It should be detailed enough to ensure that business units understand the consequences of the risk, but short enough to enable ready comprehension.

7. **How many RCSAs would be ideal for good representation/inventory? How detailed and comprehensive should you get?**

   The ideal number of RCSAs will depend on the size, number, and complexity of business units within an institution. Risk statements should be granular enough to represent a single risk, or a small group of closely related risks. Control descriptions and assessments should be specific enough to clearly identify the type of control (preventive vs. detective and automated vs. manual), the frequency with which the control process is executed, the maturity of the control, and the strength of the control.

8. **Should risk ownership be tied to an individual or a business unit?**

   Whether risks are owned by an individual or a business unit will depend on the institution's structure. If risks are owned by an individual, however, it becomes more important to update ownership when staffing, roles, or responsibilities change.

9. **Can you elaborate on the inherent likelihood concept?**

   Inherent risk is the risk that occurs in the absence of any actions that management might take to alter the risk's likelihood or impact. It is the risk before management implements controls. Likelihood is the possibility or probability that a given event or threat (risk) will occur. Impact is the result or effect associated with the occurrence of a specific event or threat. Often, likelihood and impact ratings are assigned to determine the inherent risk rating.

(continued on next page)

When reviewing possibility or probability criteria to determine likelihood, several factors may come into play, and likelihood justifications should be documented. These criteria could include, for example, product volumes, numbers of customers or transactions, often-conducted repeatable processes, dollar values, or number of reportable fields. These are only examples, and the criteria should be identified by the bank and applied consistently throughout the process as applicable.

10. Is it a best practice to have risks owned by front-line business units, and the associated controls owned by others (e.g. back office)?

In a three-lines-of-defense structure (including the business, compliance, and audit functions), the business units are responsible for owning and managing their risks. As a result, it is appropriate for business units to own controls that are specific to their business units. However, controls with broader impact may be owned by second-line functions. For example, policies, procedures, and training are often controls that affect multiple business units and therefore are managed centrally.

11. Should control ratings be proportional to the size of the risk?

The minimum acceptable strength of a control should be determined by the severity of the inherent risk, which is a function of both likelihood and impact. Remember the control rating should be proportional in order to bring the risk to an acceptable level. A high-risk item therefore would likely need a strong control to bring it to an acceptable level of risk as defined by the bank's risk appetite.

Janet M. Hale

Janet Hale, Senior Director, is a seasoned executive with regulatory compliance experience in both the public and private sectors. Janet advises on the consumer-focused areas of risk, including mortgage origination and servicing, fair lending, Unfair, Deceptive, or Abusive Acts or Practices (UDAAP), the Servicemember Civil Relief Act (SCRA), and Flood Disaster Protection Act (FDPA). jhale@treliant.com

Lynn Woosley

Lynn Woosley, Engagement Director, is a seasoned executive with extensive risk management experience in regulatory compliance, consumer and commercial credit risk, credit and compliance risk modeling, model governance, regulatory change management, acquisition due diligence, and operational risk in both financial services and regulatory environments. lwoosley@treliant.com

Timothy J. Stokes

Tim Stokes, Director, with 20 years of experience in the financial services industry. He specializes in building and optimizing comprehensive compliance management programs for financial institutions of varying sizes. tstokes@treliant.com

Treliant