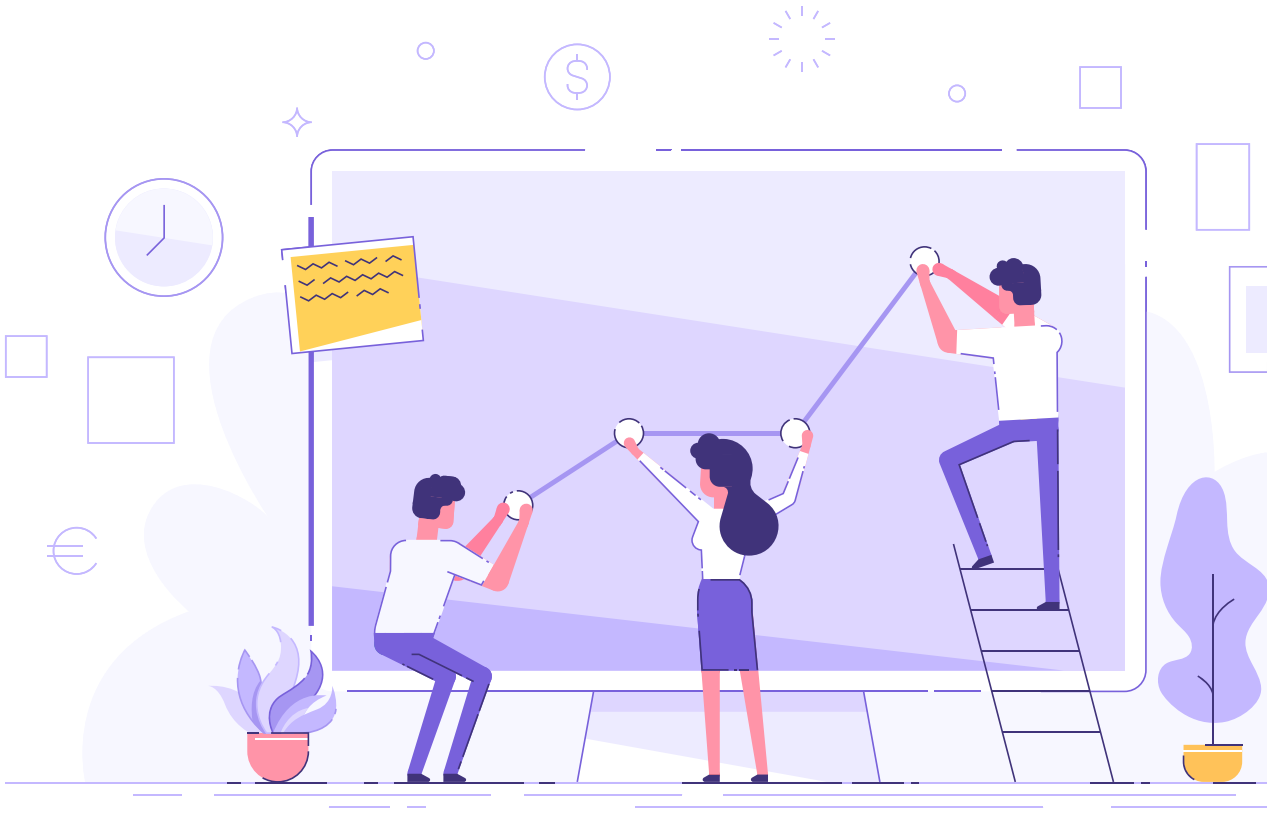
OLIVER WYMAN

HOW TO GET THE **COMPLIANCE RISK ASSESSMENT** TO WORK FOR YOU

Elena Belov, Tammi Ling, Allen Meyer, Yesle Kang

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES



Introduction

Each year, most financial institutions spend significant time and resources on the compliance risk assessment process. However, many executives still feel that they repeat the same labor-intensive process for marginal benefit. As a Compliance lead, does the risk assessment help you meaningfully prioritize activities across businesses and corporate functions? As a senior executive, does the assessment help you formulate a view on the organization's top areas of regulatory concern?

We believe that at many banks the answer to these questions is "no". In this paper, we discuss recent progress made by the industry as well as key remaining challenges facing many institutions. We provide recommendations for how to address these common hurdles and unlock greater benefits from the compliance risk assessment process. Specifically, we provide ideas for how firms can further leverage data to increase automation, foster stronger engagement from senior leadership, gain a better understanding of emerging risks and control strength, and ensure the assessment process drives action.

Why isn't your compliance risk assessment as effective as you would like?

Since the financial crisis, significant investment has been made into improving the compliance risk assessment process. One of the most encouraging developments has been greater ownership of the assessment by the first line, with process execution now being owned by the business and corporate functions in many organizations. Workflow tools are increasingly being leveraged to encourage consistency, timeliness of responses, clarity of roles and responsibilities, and simplify aggregation of results. Most have a systematic methodology to help assess inherent risk, control strength and residual risk for various regulatory risk themes that face the organization – with the granularity and accuracy of these gradually becoming better each year (with some institutions adopting a numerical scoring system that helps rank order their risks). We are also starting to see a reduction in overlap and duplication with other risk assessments (e.g., Risk Control Self Assessment (RCSA) in operational risk) – please see our paper on this topic for more details.[1]

Despite the recent progress, at most financial institutions numerous pain-points remain related to the data used to support the assessment, senior leadership engagement, the assessment methodology around emerging risks and controls, and how the results are reported and used. The following is a list of the most commonly faced problems that we observe through our work. These issues often slow down the process and lead to less accurate results.

DISCONNECTED DATA

Although many banks have automated the assessment completion process to some degree, very few have invested in injecting the relevant data into the workflow tool to help the assessor make decisions about the level of risk. Relevant data can include control testing results, control details, regulatory and internal audit issues, incidents, as well as trends of these indicators over time. Since they are often not readily available in the workflow tool, the assessor must manually collect this information from other sources; thus, slowing down the process, increasing the administrative burden and leading to potential gaps in the assessment if the information is not collected in time.

1 Non-Financial Risk Convergence And Integration: Breaking Down the Silos.

THE BOSS'S BOSS ISN'T INTERESTED

Because risk assessments can be labor intensive, they are often delegated down the organization. The person who fills out the questionnaire is not the same person who is accountable for compliance risk in the department which leads to insufficient senior attention. If the results are in line with expectations, there is little narrative and discussion around *how* you got there and *why* you are seeing certain outcomes. And if the results are *not* in line with expectations, they are too quickly overridden instead of prompting real debate around the level of risk.

NOT ENOUGH FOCUS ON EMERGING RISKS

Despite the industry's efforts to draw attention to emerging risks, most compliance risk assessment processes remain backward-looking, focusing on issues from the past not potential issues in the future. The assessors often place insufficient emphasis on the evolving regulatory environment, evolving business mix, changes in technology and operations, or regulatory events that have occurred in other areas or at peer institutions.

CONTROLS ARE OFTEN OVERRATED

Control strength is often one of the more imprecise measures in the assessment given the latitude around what is considered adequate. We have come across control strength assessments that are too generous. For instance, many institutions give substantial credit to highly manual, error-prone controls or high-level policies or procedures that are difficult to ensure are being followed. In such cases, control effectiveness on paper may not be aligned with what the day-to-day users of the controls in the business experience, and the residual risk may be understated.

RESULTS ARE REPORTED BUT NOT USED THROUGHOUT THE YEAR

Although there has been some progress in this area, many institutions continue to treat the risk assessment as a tick-the-box exercise to be collated and reported to senior management and the board once – and then forgotten until the next year. Not enough institutions are using the results to drive decisions around control mitigation and investment, business strategy and regulatory compliance risk appetite.

How do you get it right?

No risk assessment is perfect and can fully predict compliance issues, and there will always be unwelcome surprises. However, with some practical adjustments, we believe that most compliance risk assessments can be made more robust and shed more light on where to focus time and attention. It should also improve the chances of preventing incidents, or at least detecting them earlier.

Below are our perspectives on what can be done to tackle the common challenges that slow down and dilute the accuracy and effectiveness of the risk assessment process.

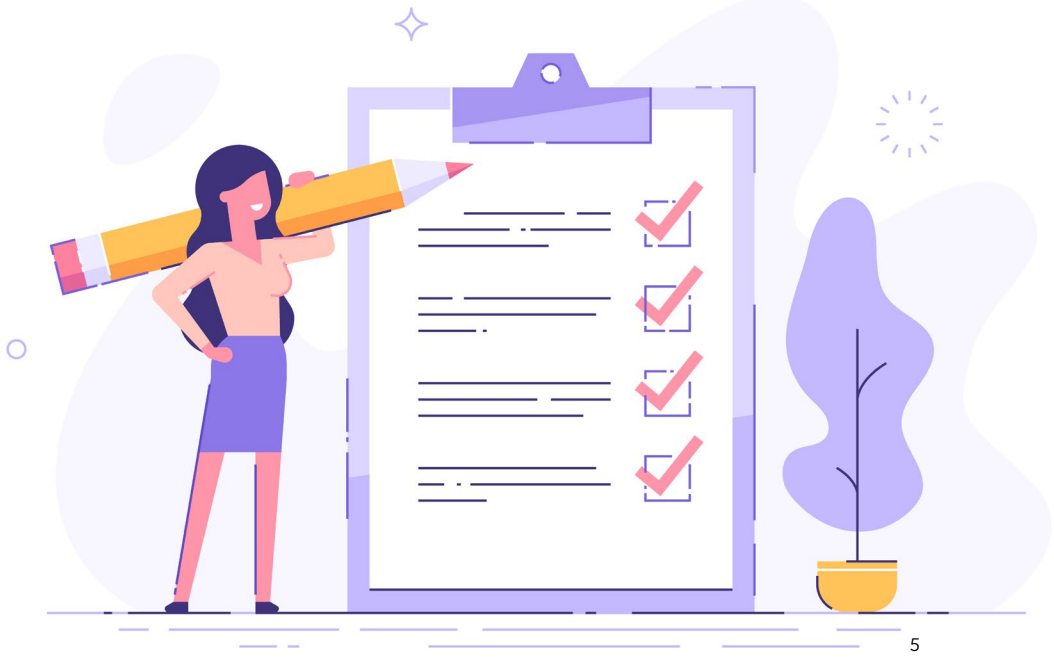
SUPPORT THE WORKFLOW WITH DATA

As discussed above, most organizations use some type of tool or smart-form to house the risk assessment questions, enable the workflow and associated audit trail, calculate residual risk and aggregate the results across different levels of the organization. We recommend that relevant data such as the results of control testing, audit results, internal and external loss events are pooled into an interface that is considered by the risk assessor. We recommend starting small and focusing on the data that can be easily extracted from control systems (e.g., control testing results), but then expanding this information to include indicators that are more difficult to gather (e.g., external loss events). The information should also be presented to the user in an easily digestible format leveraging data visualization techniques as much as possible to draw attention to the biggest drivers of potential risk.

ELEVATE THE CONVERSATION

For the results to be meaningful, compliance risk assessments should be completed at a sufficient level of seniority in the organization. At most institutions there are procedures that specify the required level of seniority for assessors. There is also often a process that requires senior business leads to review and sign off on the results for submission. We recommend that senior business leads become actively involved in the assessment through the review and challenge process and be expected to attend the meetings and engage in thoughtful discussion.

In our experience, senior management engagement is highest when leaders' performance assessments are based on a balanced scorecard that includes a measure



or assessment of the quality of compliance (and other risk) processes in the relevant business area. Such mechanisms add rigor to the process and ensure that this is more than an academic exercise.

PERFORM "WAR-GAMING" AS PART OF THE REVIEW AND CHALLENGE PROCESS

Even with efforts to elevate the conversation, not all assessors will have thought through different scenarios and potential issues they haven't experienced before. Therefore, we recommend taking the review and challenge process to the next level by including "war-gaming" – either in existing review-and-challenge sessions or as separate workshops designed to dig deeper into a theme of interest (e.g., data privacy or sales practices).

In these sessions, difficult what-if questions should be asked of the assessors. The what-if questions typically cover a set of adverse scenarios defined by the Compliance team. The scenarios can be based on events that have occurred at peer institutions, drawn from parallels in other industries or completely hypothetical. The number of these can range anywhere between 2-5 scenarios for each area, enough to instill discipline and sense check the assessments, but not so many that they become a time drain on the institution. For example, how would your risk level change if your regulator starts to focus on new topics that weren't relevant in the past, such as use of artificial intelligence in credit decisions, or chat-bots for customer interaction? Were these considered when the assessor rated his/her activities as inherently low risk? Such scenario-based reviews can help make the assessors think outside the box with the goal of inserting greater consideration of emerging risks into the process.

BE THOROUGH WHEN ASSESSING CONTROL ADEQUACY

A robust rules and controls inventory can greatly improve the assessment. Many organizations have started to document the regulatory rules relevant to their institution, the businesses to which these rules apply, and the description of controls that are in place to mitigate the risk of non-compliance.

Analysis of this data set can then support the compliance assessment ratings and narrative. For example, for each regulatory compliance risk category (e.g., market abuse, conflicts of interest, consumer protection) one could mine the portion of material rules covered by controls, average control design adequacy, average control operating effectiveness and other characteristics such as whether controls are largely manual and require oversight vs. automated, or predictive vs. detective.

This information is then critical to form a view on typical control strength criteria, for example:

- Do the controls exist and cover the applicable laws and regulations?
- Are the controls formally codified and documented?
- Have the controls been designed effectively with the regulation in mind?
- Have the controls been implemented effectively in the relevant area?

All these questions should be considered when assessing the adequacy of controls and simply saying, "We have a policy related to this risk theme" is unfortunately not going to cut it.

MAKE SURE RESULTS DRIVE ACTION BASED ON RISK APPETITE

Based on the rating results and supporting narratives, reporting should include clear, action-oriented implications for the business. At most organizations, when the residual risk or control adequacy is worse than what is considered acceptable by the bank, it is brought to the attention of management. We recommend supporting the reporting with remediation plans created by the business to either lower the risk by enhancing the controls, limiting certain business activities or adopting a risk transfer mechanism such as insurance. The exact action should be based on the organization's risk appetite and the two should be discussed at senior levels (see our second recommendation).

It is then the responsibility of the executives, via frequent check-ins and reassessment, to ensure that the residual risk level or control adequacy are improved over time. Overall, this approach helps avoid the compliance risk assessment turning into a check-the-box exercise and keeps the business leaders engaged.

Next steps

Whether it's greater use of available data, fostering stronger engagement from senior leadership, introducing war-gaming, better control assessment or ensuring the assessment drives action – there are simple no regret moves you can implement this year to get the assessment to work for you. And if the thought of making changes to this gigantic process is intimidating, we highly recommend road-testing some of these suggestions in a focused pilot so that you can see what methods work best for your organization.

In our experience with financial institutions of various size, business profile, organizational structure, and geographical footprint, the most effective compliance risk assessments are those optimized to work within the institution's unique set-up and circumstances, not necessarily ones with the most advanced features. We hence believe that with the right construct and role, the compliance risk assessment can act as the spotlight that guides you to focus on the highest areas of compliance risk.

ABOUT THE AUTHORS

ELENA BELOV

Partner in the Risk & Compliance and Organizational Effectiveness practices
elena.belov@oliverwyman.com

TAMMI LING

Partner in the Finance, Risk & Compliance practices
tammi.ling@oliverwyman.com

ALLEN MEYER

Partner in Financial Services, Head of the Compliance practice in North America
allen.meyer@oliverwyman.com

YESLE KANG

Engagement Manager in the Risk & Public Policy Practice
yesle.kang@oliverwyman.com

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS,
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

www.oliverwyman.com

OLIVER WYMAN