11 COMMON SHORTFALLS OF RISK ASSESSMENTS ...and How to Overcome Them
INTRODUCTION

Risk assessments take on many forms; some are broad evaluations of compliance or operations risk, while others focus on a particular business unit, project or risk type, like fraud. Organizations’ reliance on risk assessments also varies greatly. For some organizations, risk assessments are a necessity, helping them design and implement initiatives in order to meet regulatory requirements and other obligations. For others, risk assessments have been initiated but not leveraged to their full potential. And then there are organizations for which risk assessments still fall in the “nice to have” category—the potential benefit is understood, but the assessment process is delayed due to a lack of resources.

Done right, risk assessments enable an organization to gauge the significance of identified risks and empower leaders to develop risk response plans focused on the organization’s most critical threats and opportunities. Too frequently, though, risk assessments fall short of achieving these goals. Here are 11 common risk assessment shortfalls and their remedies.

“A systematic process for identifying and evaluating events (i.e., possible risks and opportunities) that could affect the achievement of objectives, positively or negatively.”

—Committee of Sponsoring Organizations (COSO), on risk assessment
1 | **Unclear or Unrealistic Expectations**

Because the scope and purpose of risk assessments can vary widely, some risk and compliance teams set out to conduct a risk assessment without a clear directive or common understanding of the purpose or goals of the assessment. On top of this, your organization’s leaders may have unrealistic expectations for the assessment, believing it to be the silver bullet of risk management. A risk assessment will help organizations evaluate internal vulnerabilities and external threats, but it is not the only piece of an effective program, and it should not be treated as such. The risk assessment should form the foundation of your risk and compliance program, but be sure that everyone understands that it cannot single-handedly protect your organization from risk events.
Overcoming Unclear or Unrealistic Expectations

Define scope

When undertaking a risk assessment, ensure that the scope of the proposed assessment is explicitly understood. Make clear the objective and timeline—what does the organization hope to achieve, and how soon? Finally, ask whether that outcome is realistic; if not, the objective should be revised. Once a clear, achievable aim has been defined, confirm that all individuals involved in the risk assessment understand the purpose and process.

Don’t hide flaws

To ensure that expectations remain realistic after completion of the assessment, communicate to senior leadership any known flaws or gaps in the risk assessment—potential inconsistencies in information collection or methodology, omission of business units or risk areas and time or resource constraints that impacted the development of the assessment. This will help keep expectations reasonable as the organization begins to form its risk response plans.
2 | Time Constraints

If your company has a bare-bones compliance/risk team, you may already be spread thin with internal audits and policy revisions. Creation of a robust risk assessment requires a significant time investment, and due to time constraints of compliance staff, conducting a thorough, annual or biennial risk assessment may be an unattainable goal. It’s also possible that your organization may have the time to assess its risks, but not to implement new policies, procedures and controls to address risks once they’ve been identified.

Time constraints may also extend beyond the compliance team: Other leaders in the organization may be too overloaded to participate in the risk interviews, workshops or surveys necessary for completing the assessment.

23% of companies reported having just two or fewer full-time compliance staff.

—PwC State of Compliance Survey 2014
Overcoming Time Constraints

**Tone at the top**

If executive leadership regularly communicate the importance of compliance and ethics (to all employees), it is more likely to become an organization-wide priority that staff make time for.

**Leverage and incentivize middle managers**

Your front-line managers are the most visible representation of your organization to employees. As a result, they’re often the ones that set the ethical tone (good or bad) across the company. While additional training can help secure their buy-in, it’s also increasingly common for organizations to include completion rates for compliance training and surveys as part of manager performance and compensation reviews. The more information you have from these surveys and training, the more clearly you’ll understand the risks your organization faces and how effectively you’re addressing them.
3 | Resource Limitations

Your organization may be eager to conduct a risk assessment but lack the internal capability to follow through. For a risk assessment to be effective, those involved in conducting it must have strong facilitation and analytical skills, familiarity with the business and the industry and awareness of risk management best practices.

In addition to skill limitations, your organization may also lack the technological tools to design, implement and manage a strong risk assessment. Recent surveys show a majority of compliance teams still rely primarily on spreadsheets and email to manage their programs. This can be a good starting point, but large, complex and/or multinational organizations may require more sophisticated, integrated technology for managing and scaling risk assessment efforts and data.

“People aren’t enough. To be efficient, they must be supported by the right technology.”

—COSO
Overcoming Resource Limitations

Consider a consultant
For some organizations, the best solution may be to bring in outside help. Consultants with expertise in risk assessments can make up for any internal skill or knowledge deficiencies. It may also help ensure a wholly objective analysis of the risks your organization faces.

Evaluate your existing tools
Scrutinize the tools you use for managing your risk assessment process and findings, along with your compliance program data. Do these tools integrate with one another or require time-consuming manual data entry and analysis? Is your organization exposed to more risk due to human error or oversight that may result from gaps in your data?

Define bottom-line benefits
If your compliance budget is keeping you from acquiring the technology you need, take another look at how you can communicate the bottom-line benefits of your compliance program and bolster your case for a bigger slice of funding.
4 | Failure to Assign Ownership

If no one is tapped to shepherd the risk assessment along to completion, an organization’s risk management attempts will quickly fall flat. Deadlines can be missed, gaps in data may not be filled and relevant business leaders may be left out of risk assessment discussions. A successful risk assessment needs an owner.
Overcoming Failure to Assign Ownership

Don’t select a leader, select the RIGHT leader

Assign ownership of the risk assessment to someone in the organization with the necessary knowledge, skills and authority to complete the task, such as the Chief Risk Officer or Chief Compliance Officer. This owner must be capable of:

- Engaging the appropriate parties in evaluation of risks;
- Facilitating workshops and group discussions;
- Compiling and organizing risk assessment data; and
- Assuming responsibility for the final product.

Have an executive sponsor

After you’ve selected an appropriate risk assessment owner, clearly establish who is acting in an oversight capacity. This will often be the board or a sub-committee of the board. Executive or director-level sponsorship of the process provides the added bonus of increased senior leadership knowledge about and oversight of your program, a key provision of regulatory guidance. It also allows them to see where resources may be needed to effectively address your risks—which may be instrumental in helping you secure additional program funding and resources.
5 | Insufficient Planning & Coordination

Effective, efficient risk assessments require forethought. Unless you put together a plan before beginning, your assessment may fall victim to incomplete information, haphazard analysis, inconsistency or missed deadlines. The planning process should take into account all the issues we’ve discussed up to this point—and should occur before the assessment is initiated, not when you’re staring down an impossible deadline and canyons of missing data.

Just as important as a plan is coordinating the process from start to finish. Your risk assessment efforts can quickly unravel unless the owner can exercise strong project management skills to keep the project on track amidst distractions and unforeseen challenges.
Overcoming Insufficient Planning & Coordination

Define the procedure

Establish a clearly defined, complete risk assessment procedure:

- Identify relevant stakeholders to engage;
- Select methods for collecting and analyzing information (e.g., surveys, interviews, group workshops, etc.); and
- Plan for any necessary training for staff involved in the assessment.

Commit to a timeline

Create a timeline with set dates for gathering information and completing milestones.
Overcoming Insufficient Planning & Coordination

**But be flexible**

Pieces of your timeline may change during the course of the assessment. Allow room for flexibility in the event that new or unexpected information comes to light and additional interviews or data collection must be completed.

**Communicate, communicate, communicate**

It’s important that key members of the risk assessment process are aware of the procedure you plan to follow and the initial timeline you create. It’s equally important that they’re aware the timeline may be adjusted as the assessment gets underway. If any changes to the process or timeframe do occur, be sure to quickly communicate these updates to the pertinent parties.
6 | Unavailable Data

It’s not uncommon to lack quantitative data for your risk assessment. However, without data, developing realistic assessments of the likelihood or impact of risk events may be a struggle. For example, the risk and compliance team may identify excessive overtime use as a key concern to employee health and safety, but without data showing overtime hours worked, a risk assessment pinpointing this as a high risk will be unconvincing.

Similarly, you may not have reports from your hotline, investigations, training efforts, policy rollouts or culture surveys at your fingertips. If your organization does not have a central platform for collecting and managing this documentation, it can be difficult to pull together the information necessary for a risk assessment.
Overcoming Unavailable Data

**Involve other units**

Seek out relevant data from other areas of the organization—another department or manager may already be collecting some of the information you need.

**Enlist help**

If pertinent data truly does not exist, partner with other leaders in the organization to start collecting it.

**Centralize**

Mounds of spreadsheets and disjointed solutions are things of the past. Implement a single platform to pull together all relevant risk-related data.
7 | Subjectivity vs. Credibility

If your risk assessment lacks a defined methodology, subjectivity may severely skew the results. Two employees with different risk tolerances, roles, world views and training may give the same risk wildly different ratings for likelihood, impact and velocity. Here, too, lack of quantitative data can be dangerous: If the assessment is entirely qualitative, subjectivity will loom large in the process.

Too much subjectivity in the risk assessment process can weaken the credibility of the assessment results and inhibit the success of the broader risk and compliance management program. If leaders in your organization don’t trust the findings of the risk assessment, you will be off to a rocky start in developing an effective risk-based compliance program.

A credibility gap can also emerge in the absence of tone at the top. Compliance officers who lack the backing of senior leadership may find it difficult to persuade others in the organization to participate in risk interviews or workshops, or otherwise aid in risk management efforts.
Overcoming Subjectivity

Create a consistent scale
To minimize subjectivity, establish a uniform rating scale and scoring methodology. For example, develop a 1 to 5 rating scale for measuring risk characteristics like impact, likelihood and velocity, and create specific definitions for each rating level. COSO has developed illustrative scales—including impact, likelihood, vulnerability and speed of onset—for organizations to use as a starting point in crafting their own assessment scoring system. While this will not eliminate subjectivity, it will increase rating consistency across individuals so long as those involved in the assessment understand the rating scale.

Rely on fresh eyes
Bring in a facilitator from outside the organization, or rotate facilitators, to help ensure that one individual’s perspective does not dominate the assessment process.

Garner support
Although there is no true replacement for tone at the top, engaging senior leaders can help build organizational support for risk management efforts and lend credibility to the risk assessment process.
8 | Narrow Focus

Although your risk assessment may purposely focus on a specific section of the business, beware of tunnel vision. Unless the assessment considers all aspects of the business within the scope of the assessment and interactions between these areas, your risk assessment could overlook a very real, very serious threat to the organization.
Overcoming Narrow Focus

**Break down silos**

If the scope of the assessment extends beyond a single business unit or geographic location, initiate communication and coordination across the different lines of business, segments or geographic areas as appropriate for achieving the risk assessment objectives. Engage this cross-functional group in workshops, scenario planning or other group discussions to break down silos and better understand the true extent of—and correlation between—risks.

**Visualize**

Identify risk interactions by creating risk interaction maps or event trees. This exercise can help you pinpoint and better understand how events in one part of the company can impact other areas (e.g., how a compliance violation could trigger a work stoppage, which in turn impacts other business operations). COSO has developed examples of risk interaction maps and event trees to use as a model in building your own.
9 | Failure to Prioritize

You may have assessed a hundred different organizational risks, but this list will be difficult to manage unless you prioritize those risks. Ranking risks can help you sort out the most pressing threats from those that will likely result in little harm to the organization.
Overcoming Failure to Prioritize

Identify your prioritization process

A variety of methods can be used to rank risks, but many organizations use a multi-step prioritization process. First, the organization will calculate an initial significance level based on one or more criteria (e.g., you may multiply impact by likelihood to calculate the risk’s overall importance). The company may then rank risks by score or plot them on a heat map to group into high, medium and low risk categories. Next, a company may use qualitative analysis to refine the risk prioritization, or adjust rankings based upon specific factors of concern, such as health and safety, social impact or reputational damage.

Consider context

Make sure that you have a clear understanding of the firm’s strategic goals; this can help you further hone in on risks that are high-priority for your unique organization.
10 | Failure to Follow Through

Risk assessments are virtually useless if nothing is done with the results. Unfortunately, organizations often fail to take the critical next steps:

(1) Using the assessment to inform organizational decision-making and develop internal controls and mitigation plans; and

(2) Assessing the effectiveness of those controls in addressing and mitigating the organization’s risks.

“If participants don’t see that their contributions and hard work during risk assessment lead to concrete actions that make a real difference, they will become cynical and withdraw from the process in future years.”

—COSO
Overcoming Failure to Follow Through

**Delineate what comes next**

- Who will be charged with developing and implementing controls and mitigation strategies;
- Who will take ownership of each risk;
- How risk owners will monitor risks;
- How the success of mitigation plans will be gauged; and
- How the assessment will be used to inform decision-making.
11 | One & Done

Given the time and effort involved in a risk assessment, organizations may complete one, and then let a few years pass before conducting another. This is a mistake. Given the increasingly complex and constantly evolving nature of government guidance, market environments, industry best practices and business structure and personnel, risk assessment results have a relatively short shelf life. Regulatory guidance and industry best practices call for risk assessments to occur at least every other year, with recent surveys showing more than half of organizations conducting annual risk assessments.
Overcoming “One & Done”

**Set a schedule**

Build risk assessments into your annual plan. Outline a systematic assessment process to streamline the procedure and make it repeatable and consistent over time.

**Assign an owner**

Scheduling regular risk assessments is a good first step, but without a recurring owner, it is easy to simply let the date for the next assessment pass by unnoticed. Assigning an owner creates accountability and makes it easier to adhere to the schedule.
ABOUT CONVERCENT

Convercent’s solution operationalizes and integrates compliance functions across key compliance risk areas, enabling a cohesive approach to managing, mitigating and monitoring compliance risks. Pairing a refreshingly intuitive user interface with natively integrated reporting and analytics, Convercent’s compliance program management solution ultimately facilitates the efficient, good-faith application of an effective and defensible corporate compliance program that safeguards the financial and reputational health of your company.

See Convercent in action