ethics & compliance initiative™

ECI WORKING GROUP PAPER

RISK ASSESSMENT

This report is published by the Ethics & Compliance Initiative (ECI).

Ethics & Compliance Initiative™

ISBN 978-1-7923-2025-5

ECI
2650 Park Tower Drive, Suite 802
Vienna, VA 22180

Tel: 703.647.2185 | FAX: 703.647.2180
www.ethics.org | research@ethics.org

ABOUT ECI

The Ethics & Compliance Initiative (ECI) is a best practice community of organizations that are committed to creating and sustaining high-quality ethics & compliance programs. With a history dating back to 1922, ECI brings together ethics and compliance professionals and academics from all over the world to share techniques, research and, most of all, exciting new ideas.

ECI is the leading provider of independent research about workplace integrity, ethical standards, and compliance processes and practices in public and private institutions. Our research includes the long-standing National Business Ethics Survey® (NBES) of workplace conduct in the United States and the more recent Global Business Ethics Survey® (GBES) of workplaces in leading world economies.

ECI assists organizations in building strong cultures and developing High-Quality Ethics & Compliance Programs (HQPs) in line with the five pillars identified by an **ECI Blue Ribbon Panel**. Embracing these pillars as our own operational standard, ECI provides organizations with tools and benchmarking services that enable them to assess the relative strength of their culture and program, identify areas for attention and stay abreast of new developments and best practices.

ECI also supports E&C officers, individual practitioners, academics and thought leaders with a full calendar of educational programming, networking and idea exchange opportunities and professional certification services. Ours is a vibrant and active community of professionals that shares knowledge, encourages thoughtful innovation and explores new ideas to help organizations and individuals meet key objectives.

For more information about ECI or to download our research reports, please visit www.ethics.org.

ACKNOWLEDGEMENTS

We are grateful to the following members of our Working Group for their many hours of effort in compiling this report:

CO-CHAIRS

Katrina Campbell
Campbell Ethics Consulting

Todd Spillane
Morgan Stanley Investment Management

MEMBERS

Alice Cegielski
S&C Electric Company

Betsy Happe
Principal Financial Group

Simone Holliday
Deloitte Touché Tohmatsu Ltd

Jeff Kagan
Edison International

Patricia Kidwingira
UNICEF

Ketlin Kunrath
Laureate Education Inc.

Steve Luciw
ITC Holdings

Alex Sleightholme
EY

Jeff Simpson
CoreCivic

Sunela Thomas
AT&T

Nicole Wade
Fannie Mae

Wendy Wheeler
Koch Ag & Energy Solutions

Paul Zikmund
Baker Tilly

ABOUT ECI'S WORKING GROUPS

In an effort to encourage networking and collaboration among ethics & compliance (E&C) professionals, ECI regularly convenes small groups of our members to network, share ideas, and address issues that are of particular interest. Working groups of 20 to 25 individuals meet to identify, research, and develop new resources to help practitioners prepare for a new or emerging E&C issue. They also learn from best practice with regard to an existing E&C program area.

The views expressed in this publication are those of the authors and do not necessarily represent those of their employer.

ECI RISK ASSESSMENT

Since at least the late 1990s, companies have understood the need for a comprehensive ethics and compliance program. Scandals of the 1990s, and the ensuing ethics and compliance reform measures caused (and forced some) companies to assess and upgrade their programs. In particular, the Sarbanes Oxley Act of 2002 and the updated U.S. Federal Sentencing Guidelines for Organizations (1994) set forth strict requirements for accountability of companies and their senior management.

Among the reform measures that were set forth were the need for compliance risk assessments. Often included as part of an enterprise risk assessment, these initiatives are formal attempts that organizations use to anticipate the most likely and most important things that can go wrong in that organization. Properly done, such an assessment can help that organization avoid, mitigate, and address risks, thereby ensuring the overall health of the organization.

Smaller companies, non-profit organizations, and organizations outside the jurisdiction of the United States may have took longer to incorporate risk assessments as compared to accept the importance. Indeed, while the original impetus for risk assessments was a need to comply with corporate reform measures, organizations have found that, when executed well, risk assessments help any organization to achieve its mission and minimize problems along the way.

This publication summarizes the basics of risk assessments, with a particular focus on compliance risk assessments. It will discuss risk assessment methodologies, tools, and reporting methods, as well as factors that can be used to measure the success of any such assessment. It will consider challenges to risk assessment processes, and suggest best practices. Of course, this will not be a comprehensive overview of the topic; ECI maintains a library of resources that cover risk assessments (and other aspects of an effective ethics and compliance program), which we encourage you to consult.

TABLE OF CONTENTS

SCOPE OF THE RISK ASSESSMENT

When considering the undertaking of an organization-wide risk assessment, clarifying the scope of the risk assessment is an important first step. The appropriate methodology and assessment activities will differ depending on the scope of the assessment. The type of risk assessment is closely linked, and often drives, the scope for the assessment. The scope and need for regulatory compliance assessments, for example, are often determined by risks specific to the industry in which the organization operates or the focus of specific regulators. For example, in the financial services industry, if an entity is regulated by the SEC, it must have a compliance program in place that identifies, prevents, detects and remedies any violations of securities laws. These requirements might, in turn, influence the geographic or business unit scope of the assessment.

There are a number of considerations when determining the scope of a risk assessment, including:

- risk areas;
- products and services offered;
- business/geographic areas; and
- inherent and residual risk.

RISK AREAS

Most risk assessments are restricted to either one or a small group of specific risk areas to make the assessment more manageable, unless the organization is engaged in a complete enterprise wide assessment. Even then, it is not possible to cover all risks in an organization. Thus, some culling of risk types will have to be done. It is common for an organization to base its risk types on one of a few established frameworks. For example:

Common types of risk assessments include:

- **Enterprise risk assessments** - Enterprise risk assessments are generally broader than compliance risk assessments and usually cover the top high-level risks across the organization. They include financial risks, operational risks, human resources risks strategic risks and business risks and are usually conducted by a risk management area of an organization. We considered enterprise risk assessments as a larger risk management activity that can include compliance risks as one component.
- Strategic
- Financial
- Legal
- Compliance and/or Ethics
- Operational
- Human Resources
- Market
- Reputational
- **Compliance** – this is often done by compliance professionals in the organization and involves looking at the various regulatory requirements and evaluating the associated controls to determine whether the compliance risk is appropriately mitigated. This assessment forms the basis of periodic compliance testing of controls that manage the regulatory risk.
- **Culture and Conduct risk assessment** – Conduct assessments look at risky environments and the underlying causes of those behaviors. These types of assessments are useful for comparing cultural norms in different areas. A vital component of any ethics and compliance program is an assessment of the ethical culture of the organization.

This paper will focus primarily on compliance and ethics risk assessments, whether conducted separately or as part of an enterprise risk assessment. Key points are generally applicable to enterprise and specific risk type assessments.

In order to understand the enterprise risk profile, some type of common risk classification is helpful so that lower risks can be categorized appropriately for enterprise purposes.[1]

Another area of consideration should be whether to limit the assessment to specific business units or locations/ geographical regions that may be affected more by certain compliance or ethics risks. Other risks might be enterprise-wide and therefore may justify a wider scope. The limitation to a specific or unique business operating model may be justified; for example, if business units operate autonomously, or operate in different commercial areas.

COORDINATION AND COLLABORATION WITH OTHER GROUPS

A compliance and ethics risk assessment is a collaborative effort. It is important that a diverse team contributes to this effort. Members of the risk assessment team should reflect the organization's divisions, various job functions, levels within the organization, and background experiences. Different eyes will spot different risks and controls.

For example, Human Resources will often be involved, as they should know about employee misconduct and cultural issues that should be considered. Management in operations should be included as they may have knowledge of previous risk events. Senior managers from each department should be sharing with the risk assessment team which specific risks that they see in their operations in order to get a complete picture of the day-to-day risks of the organization. From the other parts of the organization, inclusion of these stakeholders will also increase the likelihood that the entire organization will accept the results.

Culture assessments can also include a component which compares the ethics and compliance program elements against the Department of Justice guidelines. In this instance, the maturity of each element of a compliance program is assessed. Taken together, the compliance and culture assessments focus on the ethics and culture of an organization.[2]

[1] Risk classifications can be based on various risk frameworks, such as anti-corruption, NIST cybersecurity framework, compliance program requirements or the COSO framework. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established a model for evaluating internal controls, which includes control environment, risk assessment, control activities, information and communication and monitoring. The COSO framework is explained here: https://info.knowledgeleader.com/bid/161685/what-are-the-five-components-of-the-coso-framework.

[2] https://www.justice.gov/criminal-fraud/page/file/937501/download or Chapter 8B of the Federal Sentencing Guidelines. https://www.ussc.gov/guidelines/2018-guidelines-manual.

IDENTIFICATION OF RISKS

The next step in conducting a compliance risk assessment is to identify the universe of the risks. This can be done at a high level for the top ethics risks across an organization, or at a very detailed level to consider specific compliance risks a division might face. Generally, it will involve the following steps:

- Identify potential risks;
- Assess the inherent risk based on severity and likelihood, assuming that no controls are in place to manage the risk;
- Identify controls and other mitigating factors;
- Assess effectiveness and importance of controls;
- Determine residual risk using the same criteria for severity and likelihood, assuming the controls are in place

If risks are varied across the organization and there are different types of businesses being conducted, development of a common risk classification is recommended. Another area to consider is the **inherent versus residual** risks. Inherent risks are those risks that are present without any mitigating controls. Residual risks are the perceived risks that remain after the consideration of the mitigating controls. Measuring inherent risk is helpful to determining the amount of effort that should be expended to mitigate the risk; but the residual risk, taking into account controls and other mitigation, is the key output of many risk assessments.

Compliance and ethics-focused risk assessments often include a survey of employees throughout the organization to gain insight into how they approach ethics and compliance decisions. Such surveys can be short and, repeated over time, give insight into trends. There are a number of other ways beyond the survey to get information as part of this type of assessment including:

- Hotline call data;
- Feedback from training sessions; and
- Face to face interviews.

“If risks are varied across the organization and there are different types of businesses being conducted, development of a common risk classification is recommended.”

IDENTIFICATION OF CONTROLS

A **control** is a measure that, if implemented, reduces either the severity or likelihood of the risk event occurring. In order to identify whether a control is relevant to a risk area, it is important to understand the business activity and processes that give rise to the risk. Controls are normally thought either to be preventive, in that they prevent the risk from occurring or detective, in that they detect a risk event after it has occurred. Both preventive and detective controls are good to have in place. For example, to avoid bribery and conflicts of interest, an entity will generally have a gift and entertainment policy in place, with reporting requirements, limits, approvals and oversight. This policy is a preventive control. On the other hand, an ethics hotline for reporting misconduct and conflicts of interest is a detective control.

Many controls such as segregation of duties or targeted training will target a particular risk. Yet, it is also important to look at controls that are not specifically targeted at a particular risk that might nonetheless help to mitigate that risk. For example, many finance controls help to control behavior relevant to bribery and corruption risk. Human Resources background checks may mitigate compliance, strategic and other risks by detecting problems in candidates background.

TESTING CONTROL EFFECTIVENESS

An ineffective control is not a control. Thus, a successful risk assessment must include a phase in which identified controls are tested to ensure that they are real and effective. There are two elements of control effectiveness that can be tested:

Importance – how well does the control address the specific risk?

Effectiveness – how well does the control operate?

A three or five-point scale is commonly used for this assessment.

Controls cost time, money and effort. Thus, not all controls should be maintained. For controls that have lower ratings (e.g., not important and ineffective), the risk assessment team, in consultation with the business line, should evaluate whether the control should be continued. Similarly, if a control is important but ineffective, it either needs attention to improve it, or it should be re-evaluated.

As an example, employee training is often cited as a control measure. Training serves the dual purposes of educating employees and putting them on notice that there are consequences to ethics and compliance violations. Thus, training is seen to mitigate the risk of employees violating organizational standards. However, what if the training is not repeated often enough, or isn't in the right language? In that case, while the control might be important, it will not be effective.

ASSESSING RISK IMPACT AND LIKELIHOOD

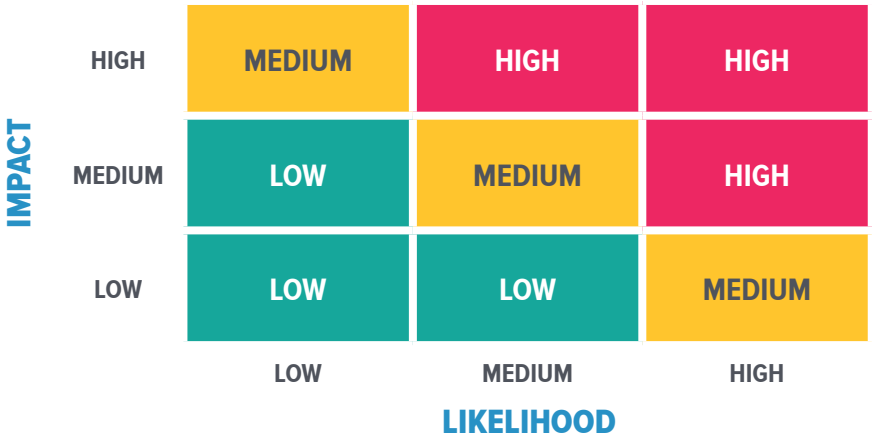
Impact assessment might consider:

- Financial impact;
- Reputational impact;
- Operational impact; and
- Regulatory action impact.

Likelihood assessment might consider:

- Historical performance/failures;
- Industry trends;
- Enforcement trends; and
- Potential frequency of failure.

A common approach is to assess risk with impact on one axis and likelihood on the other, generally scored from high-medium-low. The risk, based on a three-point scale of High/Medium/Low might look like this and can be done on both an inherent and a residual risk basis:



Once the universe of risks is assessed, a "heat map" of greatest risks might be created to demonstrate or highlight the significant risks of the organization.

FREQUENCY OF RISK ASSESSMENT

There is no required or standard frequency of risk assessments. Organizational type, size, resources, and perhaps most importantly, amount of commitment from senior management, will affect how often they are done. That being said, risk assessment exercises every 1-2 years are common. The first one, will likely be the most difficult and use the most resources. Additional assessments should be planned when changes occur to the business operating model, new business lines are created, or regulatory requirements or regulatory focus changes. Another important time to reassess risks is when an organization in the same industry has a significant compliance risk event.

Some organizations alternate internal assessments with assessments from a third party and some have a set frequency. Internal auditors can be helpful to determining appropriate frequency for the organization. Best practices suggest that the more frequent the assessment, the more useful the product is seen as useful as it is more of a current snap shot and can be easily compared with previous assessments. However, one must be careful not to conduct assessments so often that they become burdensome to business operations. This can lead to risk assessment fatigue, which itself may be a type of risk!

RISK ASSESSMENT TOOLS

Risk assessment tools are used throughout the assessment process, and later help an organization's leaders to maintain a state of ongoing risk awareness. These tools can better assist compliance professionals by identifying inherent risks (risks with no controls) and then through a consistent standard capture of current state by reducing the inherent risk with the current control structure, resulting in a clear understanding of residual risks. This awareness assists the organization to manage its risk appetite, monitor its controls, and continuously improve the control process.

Many technologies or tools promise to make the risk assessment easier. There are many options available to document the outcome of analysis. Understanding the needs of the stakeholders, selecting a system that an organization can flexibly deploy versus a system that is rigid and manages the process can make the process smoother and clearer for your management team. It is important to define the requirements of the outcome of the risk assessment in advance and minimizing "bolt-on" systems are keys to successful risk assessment execution and should be considered in evaluating the capabilities of any technology. Yet one must remember that any tool should not drive how the organization manages compliance; rather, the organization's compliance stance should drive the choice of the risk assessment tool.

CHALLENGES TO SELECTING AND USING RISK ASSESSMENT TOOLS

As with any attempt to apply a new tool to a process, risk assessment tools present challenges, starting even with the selection of the tool itself. Perhaps because there are so many risk assessment tools (also known as GRC tools) in the market, selecting the right product or tool is a challenge for many businesses.

Managing compliance will vary depending on the type of industry and organization. Further, future changes in the business of the organization may require different approaches to risk assessments. Yet, risk assessment tools are often "stand-alone" or "bolt-on"; they may not be able to operate using existing platforms used for other business activity that connect business data with compliance data to present a more full picture. Commercially available tools may not have an industry specific focus (except for certain industries, like healthcare and financial services).

Before selecting a tool to aid in the risk assessment, ensure that there is clear understanding of the various stakeholders and their differing needs. A common mistake some ethics and compliance teams make is to pursue risk assessment tools that work well for the benefit of the ethics and compliance department, without considering how/what all the other stakeholders may want to view or understand. Starting with everyone's perspective on what they want/need also increases the likelihood of acceptance of the selected tool. Any features that don't meet the needs of all stakeholders prior to the decision to move forward will require Risk Management to manage expectations of the other stakeholders.

The selection of the right tool for an organization requires that the tools that allow for the ability to compare risks across the enterprise, but processes and components that also allow for more granular, specific documentation to drive local actions, i.e., meet the needs of reporting to management and/or overall prioritization as well as local action. A key in the selection process for any tool is to have the capacity to collect and display information at different levels of detail, different breadths, etc., in order to meet core stakeholder needs. In order to optimize risk assessment activity, the more flexibility around level of detail will eliminate the use of multiple additional systems and keep all relevant information housed in a central repository.

Ensure that the tool clarifies inherent versus residual risks, with a focus on differentiating probability versus consequence in the risk ranking. A sophisticated risk assessment tool will allow for emphasis to be placed on the highest consequence risks, not just those that are most common. In most cases, senior leadership is most interested in the highest consequence risks, which are smaller in volume but critical to effectively manage. A risk analysis that doesn't provide both components does not provide the level of information necessary to prioritize and govern.

In assessing the tools as part of the selection process, tools that can integrate with other business software to best leverage business data, which may help identify changing risks. As an example, tools that can easily utilize with visualization tools will reduce the need for the risk assessment tool to meet all stakeholders' visual and reporting needs. Integration with other systems also provides the ability to get more relevant data into the tool without duplication of data. This builds a richer risk assessment database over time. Additionally, one of the essentials for any tool is that it must have a robust set of reports that can easily be exported for reports to management.

Risk assessment tools assist organizations in clarifying and managing the risk assessment process. Companies that make risk assessment tools and technology often market them to save time and improve consistency and outcomes, but little data exists to support the use of one methodology, tool, or technology over another.

“A key in the selection process for any tool is to have the capacity to collect and display information at different levels of detail, different breadths, etc., in order to meet core stakeholder needs.”

REPORTING ON COMPLIANCE RISKS AS PART OF AN OVERALL RISK MANAGEMENT PROGRAM

Once the risks have been identified and assessed based on the mitigating factors, senior management (along with guidance from the legal, ethics and compliance teams), will need to:

- Decide whether to accept, reduce or transfer (via insurance, for example) the residual risk. If the decision is to further reduce the risk, then a risk mitigation action plan should be put in place.

Risk reports, whether compliance-specific or as part of a larger effort, provide stakeholders three primary pieces of information:

- key risk areas identified by the process;
- opportunity to define risk appetites and tolerances for identified risks; and
- areas of focus to mitigate residual risk exposures.

REPORTING COMMON PRACTICES

Common practices in risk reporting include the following features:

- **Visual Format** – Most reports transform raw data sets into heat maps (see above), swim-lane charts, dashboards, or other types of infographics. The goal of these summary visualizations is to guide the viewer to essential pieces of information in an easily digestible form. Regardless of the selected visual design, formatting should be aligned with other risk reports in circulation at the organization. Additionally, the reports must convey the current state of risk mitigation in an easy to understand format.
- **Audience Appropriate** – Quality risk reports understand their audiences, which often include the board, audit committee and senior management levels. The reports should consider addressing the depth of risk knowledge, key areas of concern, and details around risk appetite.
    - Senior management materials should be aimed to clearly and fully explain any areas of very high risk for which a strong mitigation plan is not well defined or resourced. While charts and dashboards give an overall picture, explaining high risk areas through specific examples/case studies can supplement the information depicted in the charts.

- Middle management materials and approaches should be much more detailed, conversational, to build a partnership with those that know their businesses and are responsible for managing the risks. These reports should drive specific local action, including awareness training and risk mitigation efforts designed to reduce residual risk to an acceptable level. Combining risk assessment results with an assessment of maturity provides a combination of information a middle manager can use to align around an annual plan.
- **Frequency** – Best practices in this areas indicate that reports are refreshed and circulated on a quarterly or bi-annual basis to keep stakeholders apprised of major developments and to identify progress or areas of concern on risk mitigation efforts.

- **Assigning Risk Ownership** – Compliance reporting is aided when stakeholders clearly understand who is responsible for identified risk areas. Although many risk areas may require multi-departmental efforts, identifying a risk "owner" or "champion" ensures a single point of contact throughout the risk management process.

Implementing these practices will assist in delivering essential risk information to the target audience.

CHALLENGES IN REPORTING

Periodic risk reporting provides a number of distinct challenges. While specific reporting challenges will vary across industries and enterprises, common issues include:

- Integrating ethics and compliance risks with other business risks into the report;
- Discussing highly technical regulatory and compliance risks with a non-expert audience;
- Connecting hyper-technical risks to high-level strategic discussions;
- Reporting risks across the enterprise to different audiences – defining which information and how risks should be best communicated/reported to management, the board of directors, regulators and auditors and avoiding unnecessary risk allocations or other perceptions of "accusatory" language;
- Presenting a clear analysis of the nature and impact of uncertainties that affect business results and strategic plans;
- Communicating key points of critical knowledge that can be diluted in any attempt to "roll up" or summarize various forms of risk assessment across potentially diverse business lines.

These challenges, when addressed, force the risk management team to clarify exactly how the identified risks affect the organization. Utilizing the additional best practices below will help address these challenges, obtain stakeholder engagement, and ensure alignment with other ongoing efforts:

- **Advisory Committee**: Assemble an inter-departmental or multi-business line advisory committee for input during "work stages" of the process (especially if focused solely on ethics/regulatory risks). This body can act as a sounding board for presentation materials. Fielding questions and incorporating the committee's viewpoints will prepare you for stakeholder participation in the final risk report. This approach also has the added benefit of building rapport with key risk mitigation participants and provides added weight to your conclusions and work product.

- **Consistent Language**: Risk reports generally roll up metrics and related data into pre-defined categories. Defining key report elements (e.g., numeric risk rankings, impact/likelihood, and tolerance) and associated nomenclature (e.g., inherent risk vs. residual risk) allows a single format to be used across all reporting areas. Consistent usage and reinforcement of "risk language" allows all risk areas to be addressed consistently. Additionally, utilizing consistent language allows unrelated risk areas to be introduced and discussed efficiently within given time constraints.
- **Risk Packages** – Establish risk packages for different audiences. Consider the differing needs of senior versus middle management described above, and customize reporting packages for various stakeholders as needed.
- **Frequency Re-Visited** – While quarterly reporting to senior management is a common approach, differentiating the frequency of reporting based on the recipient adds appropriate detail and cadence where needed. Examples of how reporting frequency can differ include:
    - Monthly reports to risk owners and senior leadership
    - Quarterly reports to audit committee and external auditors
    - Annual reports to board of directors
    - More frequent reporting for high risk areas where residual risk remains beyond acceptable levels.
- **Data Fatigue** – Avoid reporting on lists and metrics, and instead focus the analysis on the nature and impact of uncertainties that affect business results and strategic plans.
- **Link Risk to Strategy** – Frame risks based on their potential effects on the enterprise's strategic goals and objectives. Providing case studies or scenarios involving technical compliance issues that raise outcomes affecting strategic goals help bridge this gap.
- **Material Matters** – Build in time to discuss material risks in more detail. This discussion should include contemplated mitigations strategies and the range of potential outcomes and responses. These discussions should include black swan events, business impact analysis and worst case scenario discussions.
- **Board of Directors** – Annual board reporting regarding top risks and remediation efforts provides added opportunity for incorporating key stakeholder points of view into your presentation materials. The board must assume overall responsibility for risk management governance, which is dependent upon their knowledge of risk management and mitigation programs and controls.

"Consistent usage and reinforcement of "risk language" allows all risk areas to be addressed consistently."

MEASUREMENT OF SUCCESS

A risk assessment exercise identifies and measures an organization's risk, then informs management of those outcomes. A final step to any risk management program is to ensure that the assessment itself was an effective exercise. This is normally done by cataloging the most significant risks that remain and requiring the respective business owners to put in place additional controls (e.g., additional policies and procedures, additional training, monitoring, or testing) to ultimately reduce the risks. The real evidence of success is revealed when the organization has, over time, reduced its most significant risks.

Organizations may choose to implement a risk assessment program that is static in nature and designed to measure risk at a single point in time. Or the program may be designed to function dynamically, allowing the organization to continuously assess risk over time. Regardless of the program's design, organizations should identify relevant indicators to measure its success. When measuring the success of the risk assessment program, management should consider:

- The evidence to document the performance of the risk assessment program.
    - An organization may need to provide evidence of its risk assessment activities for internal/external audits or regulatory oversight exams. A successful program should produce clear evidence of the inputs to and outputs from, the assessment process.
- The risk assessment program's ability to produce actionable results.
    - Successful programs should provide management with insight for deploying resources to riskier activities. Non-responsiveness may indicate weaknesses in the risk assessment program's design, or a lack of management understanding to address issues identified from the process.

CHALLENGES TO MEASURING THE SUCCESS OF A RISK ASSESSMENT

Organizations may encounter difficulty when measuring the success of the risk assessment program, particularly if the Organization is establishing a new program or the existing program is nascent in its implementation. Management may encounter challenges measuring the risk assessment program's success:

- If there is a lack of clear, reasonable expectations of the risk assessment program outcomes
    - It is difficult to measure success when management has disparate expectations of program outcomes. Unexpected results, particularly in areas previously deemed "low-risk" could result in management incorrectly concluding that the risk assessment program is deficient as opposed to highlighting the risk assessment program's success at identifying risk.

- As the organization responds to change in its strategic priorities, regulatory landscape, leadership structure, and other factors, management may find changes in its strategic priorities or leadership structure leads to a different outcome in the risk assessment. This may be further compounded by external changes to the legal/regulatory environment.

- The lack of established thresholds/baselines and defined KPIs (key performance indicators)
  - Management may find it challenging to measure the risk assessment program's success without a defined risk tolerance or appetite. And, while KPIs may vary by business unit, product/service type, or other factors, Management may encounter challenges measuring success if the KPIs do not accurately reflect the current risk relative to the organization's overall risk appetite.

WHAT ARE SOME OF THE COMMON/BEST PRACTICES TO ENSURE RISK ASSESSMENT SUCCESS?

Some of the best practices in the area of creating effective risk assessments will assist organizations in creating a successful risk assessment Program.

- The risk assessment process should employ a user friendly, repeatable framework that can be leveraged across the various business areas
  - Management should have a shared understanding of the risk assessment program at the outset of the process and establish clear, reasonable expectations of Program outcomes.
  - Make it easy for the users to complete. To ensure adoption, the tool needs to be easy to use so users are not easily frustrated and give up on the project.
- Risk assessment activities should produce a comprehensive list of internal controls mapped to the Organization's risk areas. While this may be challenging the first time, once it becomes part of the regular business cycle, it will become easier and faster to complete.
- The risk assessment program design is periodically validated to ensure data inputs/outputs are analyzed and accurate
  - Management should ensure that the end-to-end process incorporates the correct inputs and produces appropriate output
- The outcomes of the risk assessment program should drive actionable and measureable management response rather than vague or unmeasurable management responses
  - Management should agree on acceptable risk tolerances and expected changes in KPIs as it measures success.
- Prohibit risk responses that only address the symptoms; management responses should address the core issue/behaviors identified in the assessment.
- The risk assessment process can lead to a more fulsome review of the firm's policies and procedures, the more effective use of training and educational sessions and ultimately areas for management to address and deploy resources both strategically and tactically.

TOOLS

ADDITIONAL RESOURCES:

Gartner Report on **Competitive Landscape: Integrated Risk Management Solutions** can be found **here**.

APPENDIX A

SCOPE SECTION NOTES

[1] Risk classifications can be based on various risk frameworks, such as anti-corruption, NIST cybersecurity framework, compliance program requirements or the COSO framework. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established a model for evaluating internal controls, which includes control environment, risk assessment, control activities, information and communication and monitoring. The COSO framework is explained here: https://info.knowledgeleader.com/bid/161685/what-are-the-five-components-of-the-coso-framework.

[2] Culture assessments can also include a component which compares the ethics and compliance program elements against the DOJ guidelines https://www.justice.gov/criminal-fraud/page/file/937501/download or Chapter 8B of the Federal Sentencing Guidelines. https://www.ussc.gov/guidelines/2018-guidelines-manual. In this instance, each element of a compliance program is assessed for maturity. Levels could be Developing, Baseline, Managed and Mature. Taken together, these two assessments focus on the ethics and culture of an organization.

CONCLUSION

An effective risk assessment can drive better results, mitigate harm and assure an organization's leaders. In addition, it will show external stakeholders and oversight entities that the organization is prepared for what may come.

ETHICS & COMPLIANCE INITIATIVE™
2650 Park Tower Drive, Suite 802
Vienna, VA 22180
703.647.2185 | ethics@ethics.org

Support our research by making a donation at **www.ethics.org**.