A 12-Step Guide

How to Conduct an Ethics & Compliance Risk Assessment
INTRODUCTION

 Organizations of every shape and size are facing a growing range of ethics and compliance-related risks. More regulation, rapidly-changing business practices and new working realities are changing organizational risk profiles at an unprecedented pace. As a result, organizations must be able to identify ethics and compliance risks, and respond to them, in order to safeguard their long-term success.

 This guide offers a 12-step framework that will help you complete your own ethics and compliance risk assessment. Armed with your findings and action plan, you will be equipped to develop and implement an effective and ethics and compliance program.
What is an Ethics & Compliance (E&C) Risk Assessment?

An E&C risk assessment can help you understand where unethical or illegal conduct might occur within the organization. A risk assessment is key to developing your organization’s risk profile. It identifies:

- ethics, compliance and reputational risks your organization may face given its industry and geography
- risks related to your employee population
- your current and planned mitigation strategies to reduce risk to a level deemed acceptable by your organization

Defining Ethics & Compliance Risk

For the purposes of this guide, we have defined ethics and compliance risk as a threat posed to an organization’s operational, legal, financial, or reputational standing, resulting from:

- a failure to comply with applicable laws and regulations, and internal standards of ethical conduct, and/or
- unlawful or unethical behaviors of those working for or on its behalf, resulting in legal and reputational damage to the organization, themselves or others

The approach outlined in this guide can be applied to any form of compliance, ethics, and conduct risk. For instance, it would work equally well for data privacy, bribery and corruption, conflict of interest, financial integrity and fraud, modern slavery and other forms of economic crime.

The broader context

An E&C risk assessment is one element of a broader integrated risk management (IRM) process, and can be conducted concurrently with other risk assessments.

The classic definition of risk management considers risks in relation to their potential negative impact on an organization’s ability to achieve its strategic objectives. It could then be argued that offering a bribe to win a contract may support the strategic objective of generating revenue.

However, bribery can lead to severe fines, prosecution and reputational damage. An effective E&C risk assessment therefore looks beyond the immediate consequences to account for long-term financial and reputational impact.

A well-informed E&C risk assessment looks at:

- the organization’s business model
- the geographic location of its operations
- the industry sector and the competitiveness of the market
- the regulatory landscape
- clients and customers
- products and services
- supply chain and third parties
- transactions and projects
- the ways in which risks may manifest themselves

Risk assessment vs Due diligence

While the two terms are often used in relation to each other, there is a difference between risk assessment and due diligence. The latter is a detailed examination of a third party, and its financial records, conducted before becoming involved in a business arrangement with it. In that context, a risk assessment will generally inform the extent of the due diligence efforts at various points in a third-party relationship or transaction.

Don’t forget about third parties. NAVEX Global’s Definitive Guide to Third-Party Risk Management will help you navigate this increasingly important area of compliance risk.

---

*COSO Enterprise Risk Management – Integrated Framework, Executive Summary, p. 4
*Cambridge Online Dictionary
*US Department of the Treasury, A Framework for OFAC Compliance Commitments, 2019, p.4
Why are Ethics & Compliance Risk Assessments Important?

1 They help you understand your organization’s risk profile

Your risk profile is an evaluation that identifies the unique risks your organization may face given its industry, geography, and employee population. In many cases, organizations may be subject to regulations and vulnerable to risks about which they know little. It can be dangerous to assume you fully understand your organization’s risks. After conducting a thorough risk assessment, you are likely to discover risks that are either new or that have become more significant since the last time you completed an assessment.

According to the 2020 NAVEX Global Definitive Risk & Compliance Benchmark Report, risk assessment is a high priority ethics and compliance activity with 46% of respondent organizations planning to conduct a comprehensive organizational risk assessment in the next 12 months1.

2 They provide a strong foundation for your ethics and compliance program

A proactive, systematic risk assessment is an essential first step to creating and maintaining an effective ethics and compliance program. Without it, the program may lose credibility because you can’t be sure that you have adequate:

- policies, procedures, and controls
- training for the right audiences
- resources invested into the program
- scrutiny, time, and effort allocated to managing and policing risks

In other words, you won’t be able to explain why you have chosen to set up the ethics and compliance program in the way that you have, and why and how your program has evolved over time2.

A rigorous E&C risk assessment helps you:

- understand the organization’s exposure to potential criminal, reputational and ethical risks
- design an effective ethics and compliance program from scratch
- set the agenda or priorities for the compliance activities
- raise awareness of compliance risks with key stakeholders involved in the process
- perform a gap analysis
- enhance procedures and internal controls
- make informed risk management decisions
- measure progress or effectiveness of previous compliance initiatives

3 They help you meet regulatory expectations

While today’s ethics and compliance regulations are numerous, complex, and vary depending on industry and geography, the overarching message remains the same: organizations are expected to adopt a risk-based compliance program, based on a thoughtful and rigorous assessment of their own risk profile.

Therefore, if your organization is yet to implement a robust, recurring risk assessment process as part of its ethics and compliance program, it should become a top priority. Regulators have articulated their expectations for E&C risk assessments in various regulatory guidance. At the same time, they have made it clear that a risk-based approach does not necessarily demand that complex procedures be put in place. For example, a risk assessment for small and medium-sized organizations may comprise a management team brainstorming session that explores potential exposure to ethics and compliance risks.

The key objective of a risk assessment is to identify high-risk areas and focus on those. In other words, organizations are expected to devote a proportionate amount of time, effort and resource to each risk depending on its risk level.

Key regulatory requirements for E&C risk assessments

<table>
<thead>
<tr>
<th>UK Bribery Act 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 3 requires that “the commercial organization assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it.” The assessment is periodic, informed and documented.3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OECD’s 13 Good Practices on Internal Controls, Ethics, and Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>According to the OECD guidance, “Effective internal controls, ethics, and compliance programs […] should be developed on the basis of a risk assessment addressing the individual circumstances of a company […] Such circumstances and risks should be regularly monitored, re-assessed, and adapted as necessary to ensure the continued effectiveness.”5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U.S. Department of Justice Evaluation of Corporate Compliance Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DOJ’s most important guidance document on corporate compliance states that: “The starting point for a prosecutor’s evaluation of whether a company has a well-designed compliance program is to understand the company’s business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.”6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sapin II</th>
</tr>
</thead>
<tbody>
<tr>
<td>The anti-corruption program must include “a risks mapping intended to identify risks according to the business lines and geographical areas where the company carries out business.”11</td>
</tr>
</tbody>
</table>

---

2 US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, p. 2
3 US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, p. 2
4 OECD Council, Good Practice Guidance on Internal Controls, Ethics, and Compliance, adopted 18 February 2010, Annex 4, p. 2
5 OECD Council, Good Practice Guidance on Internal Controls, Ethics, and Compliance, adopted 18 February 2010, Annex 4, p. 2
6 LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, Chapitre 3, art.17
A Closer Look at COVID-related Business Risks

The coronavirus (COVID-19) pandemic has brought unprecedented challenges, human suffering, major economic disruption and uncertainty on a global scale.

At the same time, its rapid escalation exposed an entire spectrum of ethics and compliance risks such as the vulnerability of supply chains, degradation of public procurement rules, and limitations of existing business continuity plans. These risks are not new, but the pandemic brought their potential magnitude into sharp and immediate focus. A state of urgency, like that seen during the pandemic’s onset, create situations and environments ripe for unethical conduct and compliance violations.

How has the pandemic changed the risk profile of organizations?

Third party risk
COVID-19 exposed the fragility of supply chains and underscored the crucial role of a robust third-party risk management program. Unprecedented strain has made it possible for criminals to exploit the situation to defraud companies and government agencies. As a result, the organizational benefits of identifying and managing supply chain risks have become apparent as never before.

Health and safety risks
Re-opening offices and transitioning workforces are likely to exacerbate health and safety concerns and continue to increase liability for organizations. As office workers in many parts of the world return to their workplaces, companies are confronted with a “new normal”: the need to ensure compliance with rules on social distancing and personal protective equipment (PPE) use. To ensure a safe return, organizations should conduct “hazard assessments” and implement changes accordingly. Addressing employees’ mental health issues including social anxiety and safety concerns is likely to require new support strategies too.

Data security risk
Cyber risks have intensified as more people have moved to work-from-home models. These tend to require the use of unsecured Wi-Fi connections, personal devices, and working environments with a range of listening systems such as smart TVs and speakers. Evidence suggests that the most common and destructive cyber risks occur because employees unknowingly fall prey to cyber threats - that's why changing behaviors through employee training is key.

Behavioral risks
Thanks to the rise in remote working, many of the “normal” workplace practices and daily routines are gone – and with them, the accompanying sense of security. This has increased the potential of behavioral risks among employees, including hot state decision-making, deviations from agreed procedures, and excessive risk-taking. Pressure to perform, increased physical and psychological distance, and less oversight have contributed to an increase in conduct risk.

The COVID-19 pandemic crisis has already forced organizations to revisit their business continuity plans, more thoroughly assess and mitigate supply chain risks and conduct ad-hoc ethics and compliance risk assessments in light of the new behavioral and corruption risks. The job of adapting programs and practices to meet the challenges will fall to ethics and compliance professionals, working together with risk management, HR, and other groups.

NAVEX Global’s Coronavirus Comeback Kit will help you identify key back-to-work risks and useful tools and strategies as you plan for the future.
A high-quality E&C risk assessment requires careful planning.

This section looks at steps 1-6 and explains how to get started with a risk assessment process – from leadership buy-in to stakeholder involvement and automation. No matter how robust your current ethics and compliance program is, these steps provide a strong foundation for your risk management practice.
Get Leadership Buy-in

Active and visible support from senior executives and the board of directors is a key component to secure. Without it, risk assessments can lose momentum, avoid or inadequately deal with certain issues, or have their quality impaired by other executives and managers choosing not to participate.

The board of directors, its equivalent (trustees or advisors), or a designated board committee (including Risk Management Committee or Audit Committee) should have overall responsibility for the risk assessment. They should understand the ethics and compliance risks facing the organization, drive the risk assessment process and monitor the implementation of risk mitigation activities.

Senior leadership buy-in is key for a successful implementation of a risk response plan. Without their support it may stagnate, as certain functions or individuals may not be willing to give it the importance and attention it deserves. By overseeing the process, the board will be equipped to challenge and energize their management teams.

Tactics to encourage leadership buy-in

**Tailor your approach**

- Become conversant in the company culture, business model, strategic goals and plans to achieve them.
- Gear the message around things that matter most to your audience, for example: revenue growth, cost control, staff retention, etc.
- Familiarize yourself with the audience’s knowledge, values, and preferred communication style.

**“Package” the issue**

- Provide strategic context to your argument and link it to “the big picture”.
- Provide supporting evidence from industry peers and/or similar companies.
- Anticipate questions and issues.
- Create a sense of urgency and focus on the benefits.
- Bundle with related ideas to give your proposal greater prominence and support.

**Establish the communication process**

- Choose the right timing and communication channel, and be mindful of known, relevant deadlines.
- Build a coalition of supporters and allies to accelerate buy-in.
- Secure sufficient agenda time and make the most of it.
- Manage emotions on both sides: be passionate and seek to inspire positive emotions in decision-makers.
- Always follow up afterwards.

Establish the Process

Ask yourself why you’re initiating your E&C risk assessment and what results you want to achieve from it (your objectives). Most commonly, this will be to better understand the risk exposure of your organization so that informed risk management decisions may be taken. Clarity on these points will inform the design of the risk assessment process and should therefore be considered at the planning stage.

The tactics you employ to meet your objectives will vary depending on your organization’s size, business model, its locations, industry and regulatory landscape. Larger organizations may consider centralizing or decentralizing their risk assessment efforts. Smaller organizations might look to avoid diverting employees away from their daily tasks to ensure there is no disruption to the business.

Defining who should own the risk assessment, and who needs to be involved, is key to the planning stage. A well-planned risk assessment has clearly delineated roles and responsibilities that are communicated and understood. Consider the following points:

The board has overall responsibility for establishing, overseeing, and monitoring the risk assessment process.

Management should be responsible for performing the risk assessment, reporting periodically to the board of directors on the status and results of the risk assessment and on the implementation of the risk mitigation action plans.

Functions that might have responsibility for leading the risk assessment include compliance, legal, ethics, or risk management.

Larger organizations may wish to decentralize risk assessment responsibilities among business units or regions. This may be advisable in situations where the complexity of risks requires specialist or local knowledge.

When should you risk assess?

It makes sense to conduct an E&C risk assessment when your organization is:

• preparing to implement an ethics and compliance program
• considering expansion to a new market, sector, country or region
• considering a project or transaction
• facing a regulatory development that might affect the organization
• contemplating a change in the organization’s business model or business developments like M&A, joint ventures, or greater use of agents or distributors
• evaluating the effectiveness of the existing ethics and compliance program, its elements and controls

Defining roles and responsibilities in a risk management process

The “Three Lines of Defense” is a risk management model for clarifying roles and responsibilities. It explains the relationship between the functions and serves as a guide to how responsibilities should be divided.

1st Line of Defense – The Doers

The first line of defense is represented by the doers – the people on the front lines. They’re managing risk, complying with regulations and standards, and carrying out the company’s defined risk management processes daily.

2nd Line of Defense – The Superintendents

The second line of defense is managerial and is responsible for oversight of the doers. They also develop and implement risk management processes, policies and procedures.

3rd Line of Defense – The Investigators

The third line of defense is the auditors, both internal and external, who independently assess and report on the work of the other two lines.

The IIA’s Three Lines Model

**Governing Body**

Accountability to stakeholders for organizational oversight

**Governing body roles**

Integrity, leadership and transparency

**Management**

Actions (including managing risk) to achieve organizational objectives

**Internal Audit**

Independent assurance

**First line roles**

Provision of products/services to clients; managing risk

**First line roles**

Expertise, support, monitoring and challenge on risk-related matters

**Third line roles**

Independent and objective assurance and advice on all matters related to the achievement of objectives.

**Key**

Accountability, reporting

Delegation, direction, resources, oversight

Alignment, communication, coordination, collaboration

When should you risk assess?

It makes sense to conduct an E&C risk assessment when your organization is:

• preparing to implement an ethics and compliance program
• considering expansion to a new market, sector, country or region
• considering a project or transaction
• facing a regulatory development that might affect the organization
• contemplating a change in the organization’s business model or business developments like M&A, joint ventures, or greater use of agents or distributors
• evaluating the effectiveness of the existing ethics and compliance program, its elements and controls


Source: The Institute of Internal Auditors, “The IIA’s Three Lines of Defense Model”, 2020, p. 4
A well-designed E&C risk assessment should include participation and input from many stakeholders - members of senior management, corporate functions personnel, as well as those involved in operations.

The function leading the risk assessment, whether it be compliance or another department, is unlikely to have expertise in every area, and would therefore require support from other functions. These may include legal, risk management, internal audit, sales and marketing, procurement, finance, HR, supply chain and corporate affairs.

For organizations with a one-person or part-time compliance function, it is advisable to have a committee of individuals/functions sharing the leadership responsibilities.

Stakeholders should discuss the implementation plan, timeframe, resources and any enhancements that would make the risk assessment more effective. Ensure that each stakeholder has a clearly defined role and a clear understanding of when and how they will be involved. If there is ambiguity about responsibilities, the process could break down or result in unproductive turf battles.

Source: PWC State of Compliance Survey 2015

### How do you conduct your compliance risk?

- Engage with senior stakeholders: 67%
- Analyze compliance-related violations: 58%
- Analyze business units’ compliance KPIs: 41%
- Undertake a staff survey: 29%
- Solicit input from the Board: 23%
- Conduct focus groups: 21%
- Don’t know: 13%
- Other: 9%

Source: PWC State of Compliance Survey 2015
# Build a Framework and Methodology

A rigorous E&C risk assessment includes both a comprehensive framework for evaluating and prioritizing risk and a methodology to identify, analyze, and address the particular risks it identifies.10

The purpose of the framework is to help you integrate risk assessment into the activities, functions, and business processes of your organization. It allows you to walk through the steps of the process including the identification, assessment, mitigation and ongoing monitoring and reporting of your risks. The main aim of a risk assessment methodology is to define rules on how the risk assessment should be performed. Rather than practically identifying or assessing risks, it states how risks should be identified and assessed, the methods that should be used, the people that should be involved and the documents and templates which are appropriate.

For example, it will state whether the assessment will be qualitative or quantitative. If you don’t define this upfront, you may end up with the data that can’t be compared (e.g. interview transcripts, historical data, numerical ratings), which may limit the value of your results.

A methodology will also enable you to outline and define specific terms relevant to the risk assessment, including:

- Risk scale
- Internal controls’ effectiveness scale
- Risk appetite
- Risk tolerance
- Inherent risk
- Residual risk

## Risk management frameworks

### ISO 31000: 2018 Risk Management – Guidelines

ISO’s framework bases the management of risks on principles, framework, and process. It works well for any type of organization. ISO 31000 is written for anyone interested in risk management and focuses almost exclusively on risk and incorporating it into the strategic planning process. Many organizations choose to rely on this framework because of familiarity with other ISO standards they are already using.

### COSO Enterprise Risk Management – Integrating with Strategy and Performance

Originally issued by COSO in 2004, the framework was revised in 2017 to strengthen the emphasis on the integration of ERM with strategy and performance. The framework is principles-based and focuses on general corporate governance, i.e. how the board should oversee the entire organization, not necessarily risk. Developed in partnership with one of the “big four” auditing firms, the framework is often considered to be targeted more toward people in the accounting and audit profession.

### NIST Risk Management Framework

Developed by the National Institute of Standards and Technology (NIST), which is now part of the US Department of Commerce, the framework outlines the activities related to managing information security risk—today’s top risk and compliance concern11. It allows companies to determine which systems or applications present the highest risk and implement, assess and monitor security controls. This framework can be combined with NIST Cybersecurity Framework (CSF) to ensure a holistic approach to a broader spectrum of IT-related risks.

## NAVEX Global Risk Assessment framework

Use this framework to walk through the steps of a risk assessment process including the identification, assessment, mitigation and ongoing monitoring and reporting of your risks.

<table>
<thead>
<tr>
<th>Step</th>
<th>Identification</th>
<th>Risk Identification</th>
<th>Review and assess organization-wide processes and efforts to mitigate risks</th>
<th>Create an inventory of the ethics, compliance, legal and reputational risks confronting your organization, industry and regions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Assessment</td>
<td>Risk Assessment</td>
<td>Risk rank</td>
<td>Assess the likelihood and magnitude of each category or risk and note where there are significant variations by business unit, region and country or employee segment</td>
</tr>
<tr>
<td>2</td>
<td>Mitigation</td>
<td>Risk Mitigation &amp; Action Steps</td>
<td>Assign responsible parties</td>
<td>Report assessment results to senior leadership and board</td>
</tr>
<tr>
<td>3</td>
<td>Monitoring</td>
<td>Ongoing Monitoring &amp; Process Repetition</td>
<td>Develop action steps and timelines</td>
<td>Share risk assessment with business units</td>
</tr>
<tr>
<td>4</td>
<td>Reporting</td>
<td>Reporting &amp; Escalation</td>
<td>Monitor risk mitigation</td>
<td>High level sharing more broadly within the organization</td>
</tr>
<tr>
<td>5</td>
<td>Escalation</td>
<td></td>
<td>Regularly repeat the process</td>
<td></td>
</tr>
</tbody>
</table>

---

Establish your Risk Appetite

Determine the organization’s risk appetite, and risk tolerances, early in the E&C risk assessment process to help streamline the evaluation of residual risk.

If risk appetite is not explicitly determined upfront, there is the potential that management will rationalize existing risk levels as acceptable, undermining the purpose and value of the risk assessment.

That said, setting a risk appetite is not the same as saying that, for example, a certain amount of bribery is acceptable. The management should always maintain a zero tolerance for corruption. However, it is not sustainable to spend infinite time and resources in managing a risk down to a zero likelihood of occurring, and regulators do not expect you to do so. Instead, you should strive to properly understand a risk and manage it down to a reasonable level.

Note that various documents use the terms ‘risk appetite’ and ‘risk tolerance’ interchangeably. However, although related, these are different concepts. Risk appetite is the amount of risk an organization is willing to pursue or retain and represents a broad view of risk. A risk tolerance is relative to specific risks and performance targets, and can be defined as the organization’s readiness to bear the risk after risk treatment in order to achieve its objectives.12

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent risk</td>
<td>The amount of risk that exists in the absence of controls</td>
</tr>
<tr>
<td>Residual risk</td>
<td>The risk remaining after risk treatment</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>The amount and type of risk that an organization is willing to pursue or retain</td>
</tr>
<tr>
<td>Risk tolerance</td>
<td>The organization’s readiness to bear the risk, after risk treatment, in order to achieve its objectives</td>
</tr>
</tbody>
</table>

Ethics and compliance risk: Risk tolerance vs Risk appetite

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Risk tolerance</th>
<th>Risk Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk 1</td>
<td>Immediately reduce exposure</td>
<td></td>
</tr>
<tr>
<td>Risk 2</td>
<td>Reduce exposure</td>
<td></td>
</tr>
<tr>
<td>Risk 3</td>
<td>Optimal</td>
<td></td>
</tr>
<tr>
<td>Risk 4</td>
<td>Optimal</td>
<td></td>
</tr>
</tbody>
</table>


If risk appetite is not explicitly determined upfront, there is the potential that management will rationalize existing risk levels as acceptable.
Successful organizations are increasingly adopting technology to automate elements of their compliance and risk management programs, helping them to reduce costs and increase efficiency. Following manual processes can increase risk by sustaining a silo-based approach, with individual groups or functions focused on specific risks. Automated governance, risk management and compliance (GRC) platforms, on the other hand, can facilitate a unified approach by:

- Integrating operational, compliance, third party and other risk assessments with appropriate ethics and compliance activities, offering a holistic view of all risk and compliance activities.
- Importing and combining relevant data from multiple sources.
- Enhancing process maturity by establishing standard, repeatable procedures.
- Increasing communication and collaboration between departments and business areas.
- Allowing for the development of a unified risk appetite and risk tolerance approach.

Common examples of compliance automation

**Policy and Procedure Management**
An effective system will provide centralized document storage, automatically trigger review or update reminders, and automate policy review and employee attestation tasks based on the rules you’ve set.

**Incident Management Report Routing**
Even the most rudimentary incident and case management systems will allow you to set up case workflows and escalation triggers, meaning reports can be automatically routed to the right teams quickly.

**Third Party Risk Monitoring and Screening**
These systems enable you to screen and continuously monitor your third parties (such as vendors and partners) against risk intelligence databases, and notify you of changes to risk status.

**Conflicts of Interest Disclosure Management**
Disclosure management tools can help you automate the distribution and notification process for identifying and capturing conflict of interest risks.

Discover how the NAVEX One platform can help you automate your program.

Looking for an Integrated Risk Management Solution?
The Lockpath platform brings visibility to risks frequently managed in disparate sources including ethics and compliance, business continuity, IT, health & safety and third-party risks.

---


---

Automated governance, risk management and compliance (GRC) platforms can facilitate a unified approach.
IMPLEMENTATION

With clearly defined roles and a strong framework in place, you are ready to begin your risk assessment.

This section covers steps 7-12 and provides tools and templates to identify, assess, and mitigate risks facing your organization. You will begin by collecting the data to determine risk factors triggering risks.
How to Conduct an Ethics & Compliance Risk Assessment

Step 1: Collect the Data

There are different ways to collect data on how ethics and compliance risks may manifest themselves. Be sure to consider both internal and external resources to create a rounded picture.

Desktop research

- Familiarize yourself with the history and current practices of your organization, employee histories, and organizational culture.
- Review relevant documents and reports, involve knowledgeable stakeholders and conduct interviews with employees. You may even try to benchmark your operations against similar companies to determine how well you are performing from a regulatory perspective. Internal resources that will give you a head start with your research may include:
  - your organization’s criminal records
  - past cases of non-compliance and misconduct
  - whistleblower hotline reports
  - employee background check logs
  - internal audit reports on compliance risks
  - conflict of interest disclosure forms
  - annual HR surveys
  - M&A due diligence reports

To determine the industry-specific risks facing your organization, seek out examples of ethical and regulatory lapses that have been in the news. Take a particular interest in your competitors and peers in this regard and look at the fines and penalties levied against others in the industry.

Reviewing your competitors’ Codes of Conduct for hints as to their own perceived risk areas may also give you some perspective. The same approach can be used to identify country-specific and region-specific risks. Alternatively, consider attending industry webinars and conferences to discuss best practices with fellow compliance professionals.

Interviews

Interviewing key stakeholders can be an effective way to capture an overview of the ethics and compliance risks facing the organization. Corporate units may offer valuable insights at a high level, while line management (country, regional, or local) may provide additional insights arising from geographic and operational experience. Process owners may be able to identify process-specific issues.

Interviews provide an opportunity to explore specific topics and risks in more detail, although be cautious of confidentiality concerns among interview subjects. Hiring an outside consultant to conduct the interviews is advisable for smaller organizations where anonymity is difficult or impossible to guarantee. If interviewees fear exposure and retaliation for speaking up about risks or wrongdoing of others, they may be reluctant to share the information you’re looking for. Consider interviewing the following stakeholders:

- Members of the board of directors
- Suppliers
- Clerks
- External auditors
- Investigators
- Local authorities
- Shareholders
- Institutional investors
- Journalists

Surveys

Surveys are an efficient way to collect views from both employees and external parties. They can be easy and inexpensive to set up, give respondents the ability to remain anonymous, and enable you to streamline the measurement and interpretation of results through standardized questions. Careful planning and thoughtful structuring is critical to ensure your survey generates meaningful data, rather than new questions or issues.

Organizational culture, and the associated dynamics, can be a risk indicator in itself. An ethical culture assessment survey can help you identify the areas that may be problematic. Evaluating your culture survey results against your whistleblowing hotline data may provide additional insights into the underlying ethical and behavioral risks faced by the organization.

Self-assessment

A self-assessment is a particularly valuable tool for organizations with different locations and operating units. This is a bottom-up approach where the risk identification is largely driven by the local business’ operating environment (rather than developed at corporate level and pushed down to the operating units). However, the data quality may vary. For example, in multinational organizations it’s possible that some country managers may think questions on compliance risks from the headquarters will lead to additional controls and reporting lines. This perception may impact their responses.

Workshops and interactive sessions

Using workshops and interactive sessions is another way to collect feedback from different stakeholders. A team of experts may look at individual business processes, map each of them in detail, and then interrogate them to find weak spots. This method may enable participants to not only identify risk indicators, but also propose internal controls to mitigate them.

*Prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners.*

14 The US DOJ Criminal Division, ‘Evaluation of Corporate Compliance Programs’, 2020, p. 3

Benchmarking reports can help you identify the ethics and compliance risks faced by other organizations, and how they are addressing those risks through their own programs. NAVEX Global’s annual risk and compliance benchmark report includes survey responses from over 1,400 professionals globally.

Drive Measurable Value with Your Culture Assessment. Studio Etica’s White Paper on Measuring Ethical Culture provides more insight into measuring the key drivers of ethical behavior.
Identify Risk Factors and Risks

Now that you have collected all the relevant data, you should be able to identify ethics and compliance risk factors specific to the nature of your organization’s operations and geographies.

Risk factors are the reasons why risks may occur at the organization, based on its environment. The analysis of risk factors should be holistic and focus on the entire organization, including all units, locations, and major accounts.

Once you have a good understanding of risk factors, you can begin to determine what type of underlying risks may exist and how they might manifest themselves, given those risk factors. You should break the risks down to a reasonable level of detail, keeping in mind that one risk factor can result in multiple risks.

The primary objective of the risk identification is to create a comprehensive inventory of ethics and compliance risks confronting your organization, industry, and regions. It is a critical step to understand what needs to be assessed and what needs to be folded into the overall risk response strategy.

Each risk can take many forms. Take a structured and methodical approach and aim to document all of them in your risk register (see Step 12: Develop your action plan).

Example: How a risk factor can exhibit as multiple risks

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Business Climate in Country A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improper payments to government officials to secure tenders</td>
<td>Customs authority requesting a bribe for clearance procedures</td>
</tr>
</tbody>
</table>

Definitions

- Risk factors: The reasons why risks may occur at the organization, based on its environment.
- Risk register: A record of information about identified risks.
- Residual risk: The risk remaining after risk treatment.
Step 9

Rate Inherent Risk

Having identified your ethics and compliance risks, it’s time to rate the likelihood that each risk might occur, and the corresponding potential impact of that occurrence. The aim is to prioritize the responses to the identified risks in a logical format.

Assessing likelihood and potential impact can be a subjective process, but the results of your benchmarks, interviews, and other reviews should help you make well-informed decisions. When rating the likelihood, you should disregard the controls already in place. The evaluation of a risk’s magnitude should account for financial, operational and reputational damage to the organization, as well as any negative impacts on employees and other stakeholders. Use a simple three or five-point scoring matrix. On a qualitative scale your classification of likelihood and impact might look like one of the following:

(i) “very high”, “high”, “medium”, “low”, and “very low”.

Alternatively, you could use a quantitative scale with the potential impact and likelihood of a violation weighed from minor to major.

Steps:

1. Minor
2. Moderate
3. Major

<table>
<thead>
<tr>
<th>Potential Impact</th>
<th>Reputational</th>
<th>Financial</th>
<th>Legal</th>
<th>Employees</th>
<th>Health &amp; Safety</th>
<th>Privacy Infringement</th>
<th>Customers</th>
<th>IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Minor</td>
<td>Local market impact, short-term recoverability</td>
<td>&lt;10% of net income</td>
<td>Routine litigations subject to minimal fines and penalties</td>
<td>Isolated instances of employee dissatisfaction and/or above average turnover</td>
<td>Low degree of injury or discomfort to an individual or several people</td>
<td>Isolated individual personal detail compromised/revealed</td>
<td>Minor decline in customer relationships, minimal recovery costs</td>
<td>Loss of key systems for less than 1 hour</td>
</tr>
<tr>
<td>2 Moderate</td>
<td>Sustained local media attention with escalating implications</td>
<td>10-20% of net income</td>
<td>Routine litigations subject to substantial fines and penalties, regulatory proceedings</td>
<td>Turnover is generally higher than normal, pockets of low morale</td>
<td>Major injury to an individual or several people</td>
<td>Some individual personal details compromised/revealed</td>
<td>Decline in customer relationships, moderate recovery costs</td>
<td>Loss of key systems for 1-5 days</td>
</tr>
<tr>
<td>3 Major</td>
<td>National, regional and/or global media coverage, long-term damage to the brand and public image</td>
<td>&gt;20% of net income</td>
<td>Significant governing body scrutiny, investigations subject to substantial fines and penalties, criminal charges and proceedings</td>
<td>Loss of leadership team members, decline in employee morale</td>
<td>Death of an individual or several people</td>
<td>All personal details compromised/revealed</td>
<td>Loss of key customers, threat to future growth</td>
<td>Loss of key systems for 5 days or more</td>
</tr>
</tbody>
</table>

Sample rating criteria for rating risk impact (3-point matrix)

How can a risk impact an organization?

- **Operational impact:** Adverse events, such as embargos or plant shutdowns, that could significantly disrupt the organization’s ability to operate.
- **Financial impact:** Negative impact on the organization’s bottom line, share price, potential future earnings, or loss of investor confidence.
- **Reputational impact:** Damage to the organization’s reputation or brand – for example, bad press or social media discussion.
- **Stakeholder impact:** Negative impacts including loss of customer trust, key personnel leaving the organization, elevated turnover or decreased employee morale.

Source: Deloitte, Compliance risk assessments: The third ingredient in a world-class ethics and compliance program, 2015
Once you have determined the inherent risk, you can begin mapping risks against the internal controls and other risk mitigating activities already in place (for examples, see Step 12: Develop Your Action Plan).

This is likely to be a cross-functional, multi-stakeholder effort because many of the controls may be embedded into business processes owned by individual functions.

Start with a review of the process documentation (flowcharts, procedures, written standards and related forms), then supplement this with interviews with relevant stakeholders. Make sure that the controls you catalog in your risk assessment have been actually implemented (as opposed to only existing “on paper”). When identifying the existing controls, you should also rate their effectiveness in mitigating the risks. To achieve greater accuracy and objectivity:

- base your ratings on the results of independent control testing procedures
- use multiple sources of information
- involve only knowledgeable stakeholders (such as process owners)

A control can be deemed effective when you have confidence, evidence and certainty in its efficacy and can identify the “line of defense” it is covered by.

Internal controls and how to classify them

Internal controls can be classified in many different ways. For the purposes of the E&C risk assessment, it may be helpful to understand that they can be:

**General (organization-level) vs Risk-specific**

General controls are high level and may not be directly related to the risks that you have identified. Nevertheless, they still have a positive impact on risk reduction. Having an ethics and compliance program, written standards, policies and procedures, and a whistleblower hotline are all good examples of organizational lead controls.

On the contrary, risk-specific controls will be tightly mapped to the identified risks and will vary from one risk to another.

**Preventative vs Detective**

Preventative controls are designed to prevent the potential wrongdoing. Examples include a strong ethical culture, written policies, training and communication, and segregation of duties.

The purpose of detective controls is to help detect the misconduct that already took place by performing continuous monitoring, periodic audits, and culture assessments.

**Use a simple three-point qualitative scale to classify the controls as:**

- **Effective**
- **Partially Effective**
- **Ineffective**
Calculate Residual Risk

Residual risk is the extent of risk remaining after considering the risk-reducing impact of existing controls. The level of residual risk is used to determine whether a risk response is required, and, if so, the right elements of your action plan.

A high residual risk would mean that a high-rated inherent risk is not mitigated by the existing controls in an effective manner, which makes it an area of primary concern for management.

At this point you should also account for your organization’s risk appetite, as no further risk mitigation will be required for a residual risk already within accepted levels.

Residual risk: an illustration

Adapted from Jason Chorlins and Kaufman Rossin, “Bridging the Gap Between Risk Assessment and Transaction Monitoring”, ACAMS Today Magazine, September-November 2017
Once the E&C risk assessment is complete, it’s time to draft the action plan that will prioritize your action items. This is a critical step to make sure that necessary enhancements are implemented.

It is important to keep your action plan selective and realistic. Regulators and prosecutors expect organizations to focus on high-risk areas and apply greater scrutiny to them specifically. For example, the DOJ Evaluation of Corporate Compliance Programs guidance states that your ethics and compliance program is unlikely to qualify as effective if you spend a disproportionate amount of time and resources on policing low-risk areas.17

Instead, take a structured, practical approach. Evaluate the need for a response based on the established risk appetite level, and resource constraints, of your organization. Seek input from functions and individuals who will be responsible for (or impacted by) the action items. Use their input to help you target your efforts to reduce residual risks in an effective and efficient way.

A good action plan should feature the following:

- Identified risk/risk factor
- Description of each action item
- Action owner(s)
- Proposed timeline
- Estimate of resources required to address each action item (e.g. individuals, hours, budget)
- Monitoring and review process: steps required and parties responsible
- Implementation status
- Review date

### BEST PRACTICE

<table>
<thead>
<tr>
<th>Risk response strategies: COSO Methodology18</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reduce</strong></td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
</tr>
<tr>
<td><strong>Impact</strong></td>
</tr>
</tbody>
</table>

#### Risk avoidance
- Risk reduction is a response where action is taken to mitigate the risk by enhancing internal controls and/or changing business processes.

#### Risk sharing (or risk transfer)
- A response that aims to reduce the risk by transferring it/them to a third party through contract terms.

#### Risk acceptance
- A response where no action is taken because the risk is within the organization’s risk appetite level.

### Sample risk register

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Business climate in Country A</th>
<th>Homogenous workforce in Location B</th>
<th>COVID-19 outbreak</th>
<th>Increase in home working</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Improper payments to government officials to secure tenders</td>
<td>Sexual harassment and improper conduct</td>
<td>Onboarding third parties without proper due diligence to meet crisis-mode tight deadlines</td>
<td>Employee unethical conduct due to uncertainty, stress, anxiety and increased financial pressure</td>
</tr>
<tr>
<td>Likelihood</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Potential impact</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Inherent risk</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Key mitigating controls</td>
<td>Code of conduct</td>
<td>Code of conduct</td>
<td>Standard third-party due diligence process</td>
<td>Code of conduct training programs on code of conduct topics</td>
</tr>
<tr>
<td>Control rating/ gaps in controls</td>
<td>Effective</td>
<td>Partially effective</td>
<td>Partially effective</td>
<td>Ineffective</td>
</tr>
<tr>
<td>Current residual risk rating</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Target residual risk rating/risk appetite</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Management action/ risk response</td>
<td>No action</td>
<td>Develop and roll out anti-discrimination training program</td>
<td>Implement centralized software system to automate third party screening and monitoring and track any exceptions</td>
<td>Reinforce the organization’s commitment to ethical conduct through awareness materials, manager training, and microlearning courses</td>
</tr>
<tr>
<td>Action owner</td>
<td>CCO</td>
<td>HR business partners, CCO, line managers</td>
<td>Head of Procurement, CCO</td>
<td>CCO, HR business partners, line managers</td>
</tr>
<tr>
<td>Status</td>
<td>Completed</td>
<td>Open</td>
<td>In progress</td>
<td>Open</td>
</tr>
</tbody>
</table>

---

17 US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, p. 3  
An effective E&C risk assessment is dynamic and should evolve alongside your ethics and compliance program and your organization.

You should continually evaluate whether your risk assessment efforts are in alignment with the organization’s internal developments and external environment. Monitor your progress and be sure to repeat and update your risk assessment at least annually.
Monitor, Measure and Improve

The importance of implementing the action plan cannot be overstated. Regulators and prosecutors expect you to update your policies, procedures, and controls in light of lessons learned from your periodic risk assessments. These updates should account for the risks you’ve identified.

Although you will have many stakeholders from various functions responsible for the implementation of action items, it is important to nominate one individual who will coordinate the efforts and provide progress reports to the board and senior management. The monitoring of risk mitigation should be performed on a continuous basis, with any necessary amendments made and approved by the board in a timely manner.

To drive discipline in the implementation process, consider linking the successful delivery of action items with individuals’ and functions’ goals and performance evaluations.

**Definitions**

**Inherent risk**

The amount of risk that exists in the absence of controls

**Control risk**

The chance that an ethics and compliance risk would materialize because of a failure in an organization’s system of internal controls.

---

**Simple risk assessment matrix or ‘heat map’**

- **Likelihood**
  - Very high
  - High
  - Medium
  - Low
  - Very low

- **Impact**
  - Very low
  - Low
  - Medium
  - High
  - Very high

The organization conducts...[...] a risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks. 19

OFAC Guidance

---

**Report and escalate**

Compile all of your findings, recommendations, and action items in a comprehensive report. This report can be shared with business units and those functions/individuals who will need to see this level of detail. The board and senior management are likely to benefit from a concise summary of the key risks identified, key control gaps, and the action items planned to address the risks in order of priority.

A risk “heat map” is an impactful way to present the results of your risk assessment to the board. Simple heat maps typically have sections that are red (high risk), yellow (medium risk) or green (low risk). A more detailed heat map would have inherent risk ratings on one axis and control risk ratings on the other. This approach visualizes the interplay between inherent risk and control risk, giving a clear picture of the effectiveness of risk mitigating controls against the identified risks. It also helps to overcome the bias of focusing only on high-impact, high-likelihood risks. As we have learned from the COVID pandemic, high-impact and low-likelihood risks require treatment, too.

Your summary report should include:

- Statement of objectives
- Assessment scope
- Locations and business units covered
- Established risk appetite and risk tolerance levels
- Key procedures/work steps
- Key stakeholders
- Key risk areas
- Key controls
- Key action items from the response plan
- Key statistics
- Data visualization (e.g. graphs and charts)

**Done? Now repeat**

It is best practice to complete an E&C risk assessment regularly (at least annually), not just when developing or refreshing your ethics and compliance program.

This is likely to be an optimal timeframe because enforcement trends, such as those involving anti-corruption, trade, antitrust, data privacy and anti-money laundering laws, evolve rapidly. At the same time, organizations (particularly large or multinational companies) tend to go through numerous significant changes within a given fiscal year.

You should also be open to completing a new risk assessment on an “as needed” basis, such as when marketing a new product, or entering into a new business venture.

According to the 2020 NAVEX Global Definitive Risk & Compliance Benchmark Report, 66% of organizations perform a periodic risk profile assessment, and this percentage increases with program maturity level (95% in organizations with “Advanced” risk and compliance programs). 21

Build the annual risk assessment into your ethics and compliance program and try to complete it at the same time each year. It will be helpful to demonstrate to regulators, shareholders and other key external stakeholders that your risk assessment is a formal corporate process rather than an occasional, ad-hoc exercise.

**Update and improve**

Your risk assessment should not be a “snapshot” in time. Prosecutors expect you to have a process for tracking and incorporating lessons learned into periodic risk assessments. Your updates and revisions should therefore reflect the following risk indicators:

- Cases of misconduct and other issues/problems linked to the ethics and compliance program encountered by your organization
- Compliance/regulatory issues encountered by other organizations in your industry/ geographical region

These, along with audit findings, internal controls testing results, and root cause analysis of any apparent violations or identified systemic deficiencies, should inform your risk assessment. In turn, this should result in appropriate updates to policies, procedures and controls, keeping your ethics and compliance program risk-tailored and up to date.

---

19 Adapted from UNGC, A Guide for Anti-Corruption Risk Assessment, 2013, p.5. 20 US Department of the Treasury, A Framework for OFAC Compliance Commitments, 2019, p.4

21 NAVEX Global, The Definitive Risk & Compliance Benchmark Report, 2020, p.42

22 US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, p.4

---
About the Author

Vera Cherepanova
Ethics Advocate, Consultant, Author
Studio Etica, Milan (Italy)

Vera Cherepanova is a former Regional Compliance Officer and author of "Compliance Program of an Organization." Vera has worked on the ground in Eastern Europe, CIS and Russia. Taking her experience in addressing the cross-cultural challenges of ethics and compliance, Vera currently consults with international corporations, non-profits, wholesale and retail establishments, and small to large businesses, advising them on ethics and compliance programs. Vera speaks Russian, English, French, and Italian.

About NAVEX Global® Solutions

NAVEX Global is the worldwide leader in integrated risk and compliance management software and services.

Our solutions are trusted by thousands of customers around the globe to help them manage risk, address complex regulatory requirements, build corporate ESG programs and foster ethical workplace cultures. For more information, visit www.navexglobal.com

NAVEX One® Ethics and Compliance Platform

The integrated NAVEX One® platform offers risk, compliance, legal and HR professionals a unified view and streamlined workflows across multiple applications, making it easier to manage and administer ethics and compliance programs.

Give your employees access via single sign-on to a unified view into their compliance tasks related to policies, training and disclosures, and ease the compliance burden on both administrators and employees to improve your organization’s compliance with corporate, legal and regulatory requirements.

Consolidate your entire ethics and compliance program onto a scalable cloud-based platform, enabling you to confidently anticipate and navigate global regulatory compliance.

Watch the video

An Integrated Platform to help you effectively manage your Ethics and Compliance Program.

NAVEX One® Ethics & Compliance Platform
### Key Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>Measure that is modifying risk</td>
</tr>
<tr>
<td>Inherent risk</td>
<td>The amount of risk that exists in the absence of controls</td>
</tr>
<tr>
<td>Residual risk</td>
<td>Risk remaining after risk treatment</td>
</tr>
<tr>
<td>Risk</td>
<td>Effect of uncertainty on objectives</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>Amount and type of risk that an organization is willing to pursue or retain</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Overall process of risk identification, risk analysis and risk evaluation</td>
</tr>
<tr>
<td>Risk criteria</td>
<td>Terms of reference against which the significance of a risk is evaluated</td>
</tr>
<tr>
<td>Risk impact (or consequence)</td>
<td>The cost of a risk if it does occur</td>
</tr>
<tr>
<td>Risk likelihood (or magnitude)</td>
<td>The probability that a risk will materialize</td>
</tr>
</tbody>
</table>

**Risk management**
Coordinated activities to direct and control an organization with regard to risk.

**Risk management framework**
Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

**Risk management process**
Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

**Risk matrix**
Tool for ranking and displaying risks by defining ranges for likelihood and impact.

**Risk tolerance**
Organization’s readiness to bear the risk after risk treatment in order to achieve its objectives.

**Risk register**
Record of information about identified risks.

**Risk treatment**
Process to modify risk.

### Additional Resources

#### Risk Assessment Frameworks

- COSO Enterprise Risk Management – Integrated Framework
- COSO “Risk Appetite – Critical to Success. Using risk appetite to thrive in a changing world”
- ISO GUIDE 73:2009 Risk management – Vocabulary
- NIST Risk Management Framework
- The IIA’s Three Lines of Defense Model 2020
- UNGC, A Guide for Anti-Corruption Risk Assessment

#### NAVEX Global® Resources

- Coronavirus Comeback Kit
- Corruption Risk Country Profiles
- Definitive Guide to Compliance Program Assessment
- Definitive Guide to Ethics & Compliance Training
- Definitive Guide to Policy and Procedure Management
- Definitive Guide to Third-Party Risk Management
- Definitive Guide to Whistleblowing Hotlines
- Definitive Guide to Your Code of Conduct
- Risk Assessment Framework
- Sample Risk Prioritization Framework
- Sapin II Legal Brief
- Seven Crucial Data Privacy Red Flags
- The Definitive Corporate Compliance Benchmark Report 2019
- The Definitive Risk & Compliance Benchmark 2020
- White Paper: Anti-Bribery and Corruption Risk Assessment Checklist

#### Studio Etica Resources

- White Paper: Measuring Ethical Culture

#### International Guidance on E&C risk assessments

- A Framework for OFAC Compliance Commitments
- OECD Good Practice Guidance on Internal Controls, Ethics, and Compliance
- UK Anti-Bribery Act Guidance from Transparency International
- U.S. Department of Justice Evaluation of Corporate Compliance Programs