

Why and How to Conduct an Effective Legal Risk Assessment

Compliance and Ethics



Request reuse permissions

Cheat Sheet

- **One tool, many outcomes.** A legal risk assessment can help the legal department implement a strategic plan, corporate compliance program, and crisis management plan.
- **The effective checklist.** An effective assessment considers the risk management process, risk-tailored resource allocation, updates and revisions, and lessons learned.
- **Controls and residuals.** Once legal risks are identified and prioritized, controls can be created to limit risk and expose residual risks.
- **Essential to the company.** An effective legal risk assessment is essential to the integrity of the entire company, preserving shareholder value and promoting good corporate governance.

A successful legal department has as its cornerstone a legal risk assessment.

Accurate gauging of the legal department's competency to address legal risks can only be determined once legal risks are identified and prioritized. With this knowledge, in-house counsel can explain to businesspeople what resources are needed to limit the risks so that controls can be created and residual risks determined.

The legal risk assessment is a vital tool for the legal department to implement and execute a legal department strategic plan, corporate compliance program, and crisis management plan (which not only addresses legal risks but also force majeure and operational risks).

This process enables the company to develop overall short-term and long-term strategic plans because it can use the knowledge embedded in the legal department's strategic plan.

For example, the company strategic plan may require mergers and acquisitions as well as new product launches in the next year to five years. Because the legal department has a current legal risk assessment and has incorporated it into the legal department's strategic plan, the company will have assurance that the legal department has built the capacity to support the business objectives of the company. The company's mission statement and strategic plan drives the short-term and long-term strategic plan of the legal department.

The role of legal risk assessments in compliance programs

Moreover, the legal risk assessment conducted by the legal department is the foundation of the compliance program. Indeed, a corporate compliance program cannot be effective unless the legal risk assessment is effective.

In fact, in June 2020 the US Department of Justice (DOJ) stated:

> 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.
>
> - Evaluation of Corporation Compliance Programs, US Dept. of Justice, Criminal Division

Furthermore, the DOJ memorandum emphasizes that to properly evaluate the effectiveness of a legal risk assessment, one must determine whether the "program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether the corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct."

The bottom-line is that an effective legal risk assessment is not only the "starting point" for an effective compliance program but the foundation of an effective compliance program. Similarly, an effective risk assessment is the foundation of a well-executed strategic plan and an indispensable crisis management plan.

Effectiveness checklist

The DOJ provides the following checklist to determine if your legal risk assessment is effective:

Risk management process

- What methodology has the company used to identify, analyze, and address the particular risks it faces?
- What information or metrics has the company collected and used to help detect the type of misconduct in question?
- How have the information or metrics informed the company's compliance program?

Risk-tailored resource allocation

- Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors?
- Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?

Updates and revisions

- Is the risk assessment current and subject to periodic review?
- Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions?
- Has the periodic review led to updates in policies, procedures, and controls?
- Do these updates account for risks discovered through misconduct or other problems with the compliance program?

Lessons learned

- Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?

These DOJ recommendations are useful in strategic planning and in crisis management planning.

The role of legal risk assessments in crisis management

Crisis management is a critical area for in-house counsel to understand in relation to the legal risk assessment. As previously stated, the crisis management program considers not only legal risks but force majeure and operational risks. In fact, the crisis risk assessment includes but is not limited to the legal risk assessment.

In today's 24-7 news and social media world, handling a crisis requires dealing with public relations while important strategic decisions are made. Therefore, in-house counsel have a vital role in helping the corporation deal with a crisis, deal with public relations, and minimize legal liability. While the goal of limiting legal liability is critical, it should not be achieved at the expense the company's reputation

among consumers and shareholders as a “good citizen corporation” that acts with integrity.

The legal risk assessment combined with all other risks, including force majeure and operational risks, should be evaluated by an enterprise risk manager as well as the in-house counsel. However, if there is not an enterprise risk manager or a corporate leader responsible to lead the crisis, in-house counsel may have to function as the crisis leader.

In this case, in-house counsel should pre-plan with a crisis management program and use the legal risk assessment already developed for the strategic planning and the corporate compliance program to create the crisis risk assessment with available assistance to identify additional force majeures and operational risks.

A possible framework for conducting an effective legal risk assessment is provided below.

Conducting a legal risk assessment

A legal risk assessment requires the following steps:

1. Create an inventory of documents
2. Draft interview questions
3. Interview key stakeholders
4. Determine inherent risks and create a heat map of inherent risks
5. Establish controls for inherent risks and determine residual risks, and
6. Create an executive summary, including heat maps.

1. Create an inventory of documents

An inventory of relevant documents includes the following:

- Organizational charts reflecting company partnerships or affiliations and management responsibilities
- Existing compliance structure or program and any previous internal or external reviews or assessments of the compliance program
- Corporate audit document checklist
- Crisis management policies and/or manuals
- Interview checklist or evaluation forms
- Insider trading guides
- Advertising materials

- Business plans, annual reports, and other materials describing business operations and strategic business initiatives
- Business partner inventory lists, including any government officials or entities with whom the company interacts
- Previous internal or external reviews and investigations of reports received through a whistleblower hotline or other misconduct reporting mechanisms

- Environmental policies and reports
- Performance evaluation form

- Handbooks and any other policies or procedures reflecting company standards or operational protocols
- Training curriculum and related materials (diversity, sexual harassment, etc.,)
- Litigation lists and settled cases for the past five years
- Data retention policies and/or manuals
- Employee application forms
- Human resources annual reports
- Exit/termination checklists
- Community right-to-know reports

2. Draft interview questions

Based on the inventory of documents, you should create a preliminary list of risks and interview questions based on them. The interview questions should include questions concerning the culture of the company, the interviewee's role in the company, the risk the interviewee sees in his or her role, the risks the interviewee perceives for the company, and the significance of each risk. The interviewer should sort out the risks to determine legal risks and then ask additional questions on these legal risks.

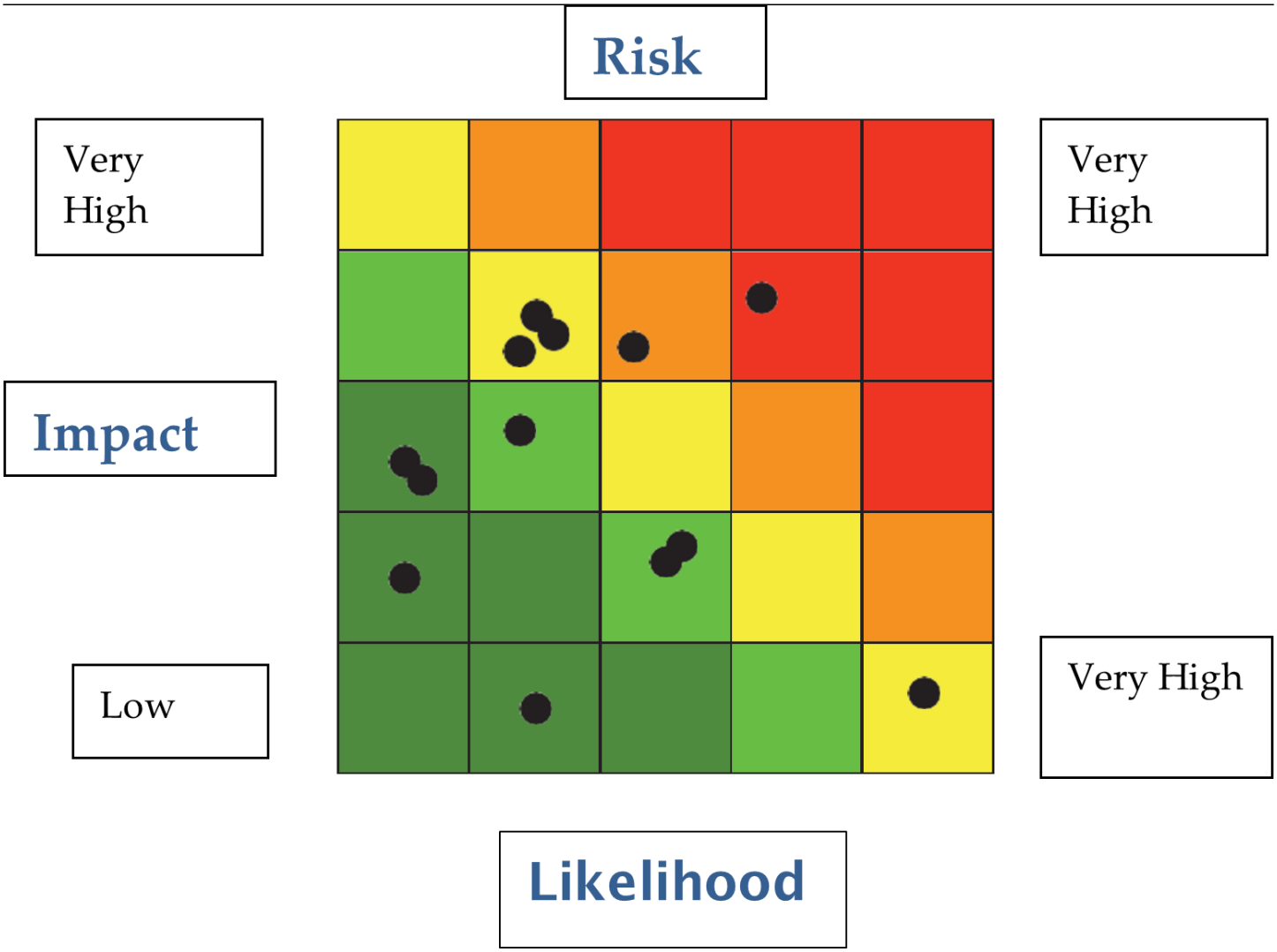
3. Interview key stakeholders

Based on the inventory of documents and the interview questions drafted, the interviewer should interview key stakeholders on legal risks. Key stakeholders include:

- The chief executive officer and C-suite officers
- Employees
- Outside counsel and legal service providers
- Insurance brokers, accountants, and law firms

4. Determine inherent risks and create a heat map of inherent risks

Illustrate the inherent legal risks considering likelihood of occurrence and its impact on the company.



Heat Risk Map

5. Establish controls for inherent risks and determine residual risks

Create a heat map of the residual risks by developing controls for each inherent risk. Once the controls are developed, subtract the control from the inherent risk, which equals the residual risk (Inherent risk – control = residual risk).

An example of an internal control is to have the internal audit department review gift and entertainment expenses for foreign officials to determine if these are reasonable and bona fide expenses.

Another example of an internal control is to have a second signature on any expenses over US$1,000.

6. Create an executive summary of the legal risk assessment including heat maps of the inherent and residual risks

Make a presentation to the C-suite officers and the board of directors, including an executive summary and heatmaps for inherent and residual risks. If you distribute any documents, make sure to identify the documents as attorney-client privilege, if applicable, confidential, and internal use only.

Conclusion

Do not think of a legal risk assessment as time waster but as a time saver. It is essential to the integrity of not only the legal department but the entire company. It preserves shareholder value, promotes corporate governance, and creates a good citizen corporation with an ethical tone at the top. Equipped with an effective legal risk assessment, in-house counsel can merit a seat at the table when strategic decisions are made by the company.

James Merklinger



Chief Advisor

ACC Credentialing Institute

James A. Merklinger oversees the institute In-house Counsel Certification Program and its Data Steward Program, assessing law firm data security practices. Having served ACC for over 20 years in a variety of key roles, Merklinger was named to the position of president of the ACC Credentialing Institute in 2017. In this role,

he is responsible for establishing standards and advancing ACC's ability to establish an in-house counsel credentialing program. Merklinger is also responsible for leading the ACC Data Steward Program to evaluate the security profile of law firms.

Previous to his role as the Institute's president, Merklinger served as ACC's vice president and chief legal officer. He represented ACC on all legal issues affecting the association, including mergers with the Australian Corporate Lawyers Association , the Hong Kong In-house Counsel Association and the Corporate Counsel Middle East. Merklinger advised the organization on meeting the needs of the in-house counsel community. He had also served as ACC deputy general counsel and vice president - legal resources, overseeing the development of ACC's array of resources to help in-house counsel do their jobs. In this position, he worked with 18 volunteer leadership committees, organized by practice areas, which contribute to the strategic development of the association's resources and education programs. Merklinger spearheaded ACC's regular benchmarking studies to provide members and the legal industry at large with key trends related to the in-house counsel practice and outside counsel management.

In addition to his non-profit legal experience, Merklinger served on the board of directors for the Tourette's Syndrome Association of Greater Washington, DC, the board of directors of the ACC Foundation, and President of the Washington Irish. Prior to joining ACC, he served as in-house counsel for DIAD, Inc. in Reston, Virginia. While at DIAD, he provided counsel in a variety of substantive areas, including commercial law, software licensing, disability law and issues affecting entrepreneurial development. Merklinger has served as faculty for CLE programs throughout the United States, Canada , Europe and the Middle East on a variety of in-house topics. Merklinger graduated from Wofford College and the University of South Carolina School of Law.

Carole Basri



Chief Advisor to the ACC Certification Program

ACC Credentialing Institute

Carole Basri is the chief advisor to the ACC Certification Program, president of the Corporate Lawyering Group, LLC, founder of the LLM in Corporate Compliance at Fordham University Law School, visiting professor at Peking University School of Transnational Law, and visiting professor, at Pericles Law School in Moscow, Israel.

Basri has authored the following treatises:
Corporate Legal Departments published by Practising Law Institute (PLI)
International Corporate Practice published by Practising Law Institute (PLI)
eDicovery for Corporate Counsel by ThomsonReutersWest
Corporate Compliance Practice Guide by Lexis