COSMOS
Navigate the Compliance Universe

# The Complete Compliance and Ethics Manual 2024
# How to Protect Compliance Risk Assessments from Unwanted Disclosure

By[1] Russ Berland[2]

A compliance risk assessment is a basic tool of compliance professionals. It is used to determine where risks and vulnerabilities exist in a company's compliance with laws. The Federal Sentencing Guidelines, [3] the Resource Guide to the U.S. Foreign Corrupt Practices Act[4] and the OECD Good Practice Guidance,[5] as well as numerous other guidance documents and best practices, mandate that a risk assessment is a necessary first step to have an effective compliance program. Typically a compliance risk assessment (1) catalogues the legal and compliance requirements facing the company; (2) uses information gathering tools such as interviews, surveys, benchmarking, and document and financial transaction review to determine the company's risks of failing to comply with legal and regulatory requirements; and (3) analyzes those risks to prioritize them according to likelihood, impact, and velocity. But how the risk assessment is conducted can determine whether it stays safely within the company's confidential information or must be given to prosecutors and plaintiffs' attorneys.

A risk assessment is a potentially risky undertaking in itself. Suppose, despite all expectations to the contrary, that some significant improper conduct were to come to light in the assessment. The company could be deemed to be on notice of the bad condition. Suppose that the assessment showed control weaknesses that the company had not previously been aware existed. While the results of the assessment are critical, at the end of the process, no one wants to be forced unwillingly to give that report to prosecutors or plaintiffs' attorneys. Because of the "dirt" that a risk assessment might uncover, it could end up being prosecutor's exhibit number 1 or plaintiff's exhibit A in court as they prosecute or sue your company. But unless the document is protected by some form of privilege, it may be disclosed outside the company in the event of criminal investigations or private litigation. Critical steps should be taken during the risk assessment to protect it from disclosure.

## What Is Privilege and Why Does It Matter?

Privilege protects certain kinds of information from forced disclosure in legal proceedings and investigations. Suppose the Securities and Exchange Commission (SEC) were to say to the company (through a subpoena), "Give us all your documents and other records that assessed your risks of violation of the Foreign Corrupt Practices Act in the last five years." When you look through your documents, you find one called "FCPA Risk Assessment" at your company. After reviewing the risk assessment, you think, "Some of this may be misunderstood, and it does not look like we acted very quickly when we learned about our risks," even though you know that compared to most initiatives in your company, the remedial FCPA measures happened quite rapidly. In other words, it is a potentially damaging document. So unless a privilege applies, the SEC probably gets to see the risk assessment report. But, if it is privileged and you do not do unwise things with the document, your company should be able to protect it from disclosure.

## Options

Here are the choices on how to conduct a risk assessment:

- Do not do one at all. If there were no risk assessment, there would be no report to disclose. But, the

resulting compliance program would not be risk-based, so it would be significantly less likely to be designed effectively. And, it would be difficult to argue that a compliance program meets the requirements of the Federal Sentencing Guidelines or similar standards if this crucial first step is skipped. This does not seem to be an acceptable outcome.

- Have a non-legal internal group or an outside consultant conduct the risk assessment. At the end of the process, the company would have its risk assessment, which could be used to design an effective compliance program. But, the risk assessment report would not be protected from disclosure through legal or administrative discovery processes later on. In other words, the company could be forced to hand it over to people who would want to hurt the company with it.
- Have in-house counsel direct the preparation of the risk assessment. The company might have an argument for attorney-client privilege or attorney-work product. If these succeeded, they would protect the report. But, there are circumstances where these privileges would not apply and the company could be forced to hand over the document.
- Have outside counsel direct the preparation of the risk assessment. If done right, the company should have protection under attorney-client privilege and might even have protection as attorney-work product.