

Compliance Risk Assessments – An Introduction

Chapter 3. Step One: Defining Your Compliance Risk Universe

Chapter Goals:

- Identify what counts as risk for your organization.
- Identify resources to establish the scope of the compliance risk universe.

Step one—the basics. When you decide to do some baking today, is your goal to bake a wedding cake or a vanilla sheet cake, or is the extent of your skills limiting you to a store-bought, ready-mix brownie delight? It is the same kind of question that you would ask regarding a compliance initiative.

What will be the scope of your compliance initiative? Will it be limited to only federal laws and regulations? Will it cover compliance with your organization’s policies and procedures? Will you incorporate regional and local laws?

Those are all good questions with no right or wrong answer. The answer depends on the scope of your initiative and what is reasonable to accomplish. It is only after you decide what you want to accomplish that you can seek out and identify your compliance risk universe.

The USSG states that an organization should promote a culture that encourages ethical conduct and a commitment to compliance with the law.^[1] So, a broader compliance risk assessment could include risks for unethical behavior as well. The Anti-Bribery Convention, an international standard created by the Organisation for Economic Cooperation and Development (OECD) and ratified by 44 countries,^[2] provides similar guidance in its “Good Practice Guidance on Internal Controls, Ethics, and Compliance.”^[3] Within these broad mandates, your compliance effort can be customized to fit the needs of your entity.

Whatever your decision, start with a reasonable and achievable goal. Going from no assessment to a full-blown identification and analysis of every federal, regional, and local law that touches your entity may be unrealistic. Adopting that broad of a scope may even be more unrealistic if your business has a decentralized mindset, an entrepreneurial spirit, or maybe even a laissez-faire philosophy regarding compliance. A more gradual and expandable version of a compliance risk assessment might be a better option at the onset.

Start your compliance effort with clear and attainable goals that can be achieved within a reasonable time period identified in your plan. If your compliance effort is not well thought-out and does not have clear follow-through with visible, actionable results communicated to the CEO, board, employees, shareholders, and other key stakeholders, the effort will fail. Restarting the effort after an initial failure will be difficult.

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)

}