Common Mistakes Organizations Make When Implementing Compliance Projects

AUSTIN STRATEGIC PARTNERS

Viewing compliance as a one-time project.

According to the Project Management Institute, a "project" must have a definite beginning and end. Compliance is a continual, on-going, daily, operational endeavor that needs constant vigilance, reinforcement and improvement, and must be practiced by every member of your organization. Be wary of companies who promise to "make you compliant."

Viewing compliance as a set of technical solutions or as a product you can buy.

You cannot purchase a product that will make you compliant, so beware of vendors who make these hollow claims. At best, a product may aid in facilitating one aspect of compliance. Even the best "technical solution" will fail to have any affect on compliance if not implemented correctly, not kept up-to-date, the staff is not trained on its use, and its function is not made part of the organizational culture (i.e., standard operation procedure). Just *purchasing* tools will not make you compliant.

Having well-documented (but weakly implemented) policies, processes and procedures.

Having documented policies, processes and procedures is just a *start*. These must be disseminated, staff must be indoctrinated in their use, and they must be made part of everyone's job description and performance evaluation. Don't believe anyone who tells you just *having* the documented policies and procedures makes you compliant!

Limiting efforts to the minimum possible requirement or trying to maneuver around the obstacles.

The auditor assessing your compliance efforts likely will not have the same interpretation of the regulation or compliance standard as you. No matter what the goal, aspects of the organization are apt to come up short on occasion. You're skating on thin ice if you already started out with watered-down expectations or minimal solutions. Worse yet, employing workarounds to maneuver around compliance obstacles will get you cited faster and more harshly by auditors, because it is evidence you *knew* what the right thing to do was and you *chose* to skirt it!

Doing what is easy (non-proportional responses); not using an appropriate risk-based approach.

In the face of so many requirements, it is tempting to address the "easy" ones first or more thoroughly. But is that where your biggest risks are? Beware of companies that offer a canned solution without doing an assessment of your *unique* environment to learn *where* your biggest risks are! The last thing you want to do is spend $50,000 on a $25 problem, or barely address your biggest source of risk because it was thought to be "too difficult."

Allowing too many exceptions to policies, procedures, or standards.

If many people or situations are treated as a "special case" or allowed exemptions from following policies, soon no one will follow or even know what the "real policy" is. You are only secure as your weakest link! With many exceptions, many weak links are created. Be firm in requiring compliance and in citing violations across the board.

Not collaborating with technical/operations staff in the creation of policies and procedures.

This is apt to result in policies and procedures that cannot be implemented. Worse yet, the compliance effort loses credibility and respect. If the compliance team writing the policies and procedures does not have the technical ability to effectively interface with network and systems staff, enlist professionals who can facilitate this needed collaboration, and craft workable, meaningful policies and procedures.