8 Steps to Build & Maintain a Compliance Program

Achieving and maintaining compliance doesn't have to feel like constantly putting out fires.

Here are some tips to help you stay compliant.

1 Identify Compliance Team

All employees are responsible for complying with regulations, but **the core team comprises individuals who develop policies and gather evidence to support them regularly.** Typically, the core team includes members from HR, Finance, and IT.

2 Leverage a Compliance Tool

Simplify compliance with automated tools that offer benefits such as updates and highlighted changes, clear evidence tasks, streamlined collection, and timely notifications to prevent last-minute scrambles and ensure program compliance.

3 Remediate Gaps

Choose a compliance framework, view requirements and provide current practices which will identify gaps. **Gaps should be addressed with new tools or quick updates.** Your IT Director should prioritize these gap based on importance and budget and communicate resolution plans.

4 Collect Baseline Evidence

The term "baseline" evidence refers to the initial collection of evidence that is **crucial to demonstrate where you stand at the beginning of your compliance program.** Typically, evidence consists of IT reports or screenshots that detail security measures such as patching or configurations (like the mandatory use of multi-factor authentication for all email accounts).

5 Collect Periodic Evidence

To ensure IT team compliance, collect evidence according to standard practice. A compliance platform can help. If your tool doesn't collect evidence automatically, do it manually. Review privileged accounts quarterly, taking screenshots and verifying account lists and group membership. Store evidence centrally in the compliance platform or shared folder.

6 Internally Audit Policies and Procedures

Develop an internal audit function for adherence to external audit and attestation programs. Work with each team to request evidence corresponding to the program set. **Conducting internal audits will ensure the program is on track and any remediation and alignment activities can occur.** Note that attestation may require 6-12 months of periodic evidence collection.

7 Gain Attestation from External Audit

After establishing your compliance program, you can opt for an attestation from an external auditor. **This attestation confirms your adherence to regulatory requirements and often includes a report or emblem for client presentation.** The frequency of external audits varies, usually every 1 or 3 years, depending on the framework you follow.

8 Maintain Your Compliance

To maintain the work you've done, it's important to continue with steps 5 and 6 on a regular basis, even if you decide not to obtain a formal attestation.

Occasionally, there may be changes to regulatory guidelines, which would require you to review steps 3 and 4 to ensure that you meet the updated requirements. Utilizing a compliance tool can simplify this process for you.

Take Charge of Compliance Excellence Today!

Don't wait for the fire to spread - act now and safeguard your business with a strong compliance program!

www.tenisitech.com (408) 217-1380 info@tenisitech.com

TENISI TECH