Creating a Compliance Rich Culture

Checklist

Creating a Compliance Rich Culture - Checklist

This guide is intended to point you down the right path when it comes to bringing your company into any compliance standard, whether it's HIPAA, GDPR, or simply getting people to reset their network password every 90 days. It won't go into legislation specifically. That would make it 700 pages long. Instead, we'll focus on the key principles needed to create a culture of compliance.

Procedures: You can't hold people accountable unless procedures are clearly documented in an understandable way.

☑ Create a standardized format for all of your procedures. One department shouldn't be relying on vague bullet points, while another is documenting everything with intense screen shots and step-by-step instructions. Use a single template throughout the company.

☑ The entire team involved in the process should be included in the writing of that process. Documentation should never fall to one person.

☑ Create a clear indexing structure with search functionality. People will not use processes if they're difficult to navigate.

☑ Provide everyone access to the standard operating procedures, and send regular reminders about their existence. People fall into old habits very quickly and that's when processes become outdated.

☑ If a 15-year-old can come in and utilize the process effectively, it's a good process.

☑ Instill the mentality that employees should always be using, writing, or updating a process no matter they're doing. Information cannot be stored in one person's head.

Creating a Compliance Rich Culture - Checklist

Regular Reviews: Compliance is not a one and done gig. It requires ongoing engagement to adjust to legislative changes, as well as stay on top of internal operations.

☑ Revisit your processes every three to six months for appropriate updates and changes.

☑ Set a Google News alert for any legislative changes regarding things like HIPAA or PCI, so that you're always ahead of the curve.

☑ Visit departments regularly to see how they're doing implementing your processes and if something needs clarification.

☑ Meet with your IT team on a quarterly basis to discuss any necessary updates.

☑ Meet with your legal team as necessary for their input.

☑ Conduct a full annual review of your compliance plan.

Employee Training: Compliance is not typically top of mind for every employee on a daily basis. They're just worried about getting their job done. That's where training comes in.

☑ Create a standard onboarding training. Ensure that you cover data security, password standards, information sharing, and anything else that will impact their job in terms of compliance. This training should be as ingrained in your company as new hire paperwork.

☑ Conduct quarterly all staff refreshers. You can do this online, with your IT team, or in an all-company meeting. Lead with compliance, focusing especially on how each team member can best protect their department and the company.

Creating a Compliance Rich Culture - Checklist

☑ Implement testing where applicable. Concerned that your team may too often fall victim to a phishing attack, opening up your company to breach? Have your IT team do a test phishing campaign. Then, educate about the results and how they affect adherence to company policies as well as larger compliance principles.

☑ Embrace individual deep dives. Some employees maybe more heavily involved in compliance, or may be more challenged when it comes to a culture of compliance. Don't be afraid to conduct individual trainings as necessary. Compliance is everyone's responsibility.

☑ Visit departments regularly to see how they're doing implementing your processes and if something needs clarification.

☑ Meet with your IT team on a quarterly basis to discuss any necessary updates.

Reporting: This gives life to your compliance initiatives. You no longer are staring at a bunch of manuals. Instead, you've created something that you can truly measure.

☑ **Develop 3-5 metrics that measure your compliance.** Pull these metrics on a weekly to monthly basis. Make these items that are easy to pull from your existing dataG bases. If they're too complex, you will never end up tracking them effectively long term.

☑ **Develop a monthly compliance report to deliver to leaders.** This should summarize the metrics you've set forth above, as well as any actions that you're taking toward greater compliance.