Pretty much every industry and organization you can think of has some sort of compliance they have to follow. Whether it be Sarbanes-Oxley for financial controls (SOX) or the North American Electric Reliability Corporation (NERC) that serves as a governing body for power production and distribution standards. There is a lot of things that require some sort of compliance in order to be in business. These standards are the bare minimum and are generally in place because some company failed to uphold some sort of standard truthfully. There are a few types of compliance such as Manual, Pipeline and Composition to name a few.

The first type of compliance is called Manual Compliance. Manual Compliance is a rudimentary and is simplified through checklists. It is the most simple of all the processes of compliance. (Nygard, n.d.) Essentially a team sets and defines all the requirements in a measurable form. (Nygard, n.d.) this would include simple survey questions such as a completion checkbox. It would even require teams to write a list of the open ports or URLS. (Nygard, n.d.) Also they would need to describe and rules for security or recovery procedures. This type of compliance does need a lot of resources to create and is generally used by smaller organizations. (Nygard, n.d.)

The next type of compliance is the Pipeline Compliance. The Pipeline Compliance is typically embedded in the CI/CD deployment pipeline and checks for requirements automatically. (Nygard, n.d.) It is executed as part of the pipeline build and gathers data and it then checks against preset values. (Nygard, n.d.) These values are created by a development team whose in charge of creating these standards set forth from their regulatory or standards team. Automating of these tests is a huge cost saving and time saving benefit. But it typically requires a larger organization that can accommodate these requirements.

Lastly a type of compliance is Composition. The Composition compliance “is based on the premise that compliance is distributive” (Nygard, n.d.) Thus creating systems that are already compliant and basing it off that system. This system is supposed to be reusable in every facet of the organization and that in practice everything would be in compliance.

Take a look at each compliance, they all seem reasonable. Except in our dev ops hand book it does distress the “overreliance” could result in certain vulnerabilities. Not every option is a fool proof method and requires the due diligence of its employees. From the creation of such policies to following policies. Or in the case of the deployment pipeline compliance, automating the correct system for checking on such compliance.

Which when reviewing the compliance of governing bodies could be a cumbersome task, like in the case of Sox compliance or even North American Electric Reliability Corporation and their requirements for organizations to follow to be in compliance with the law. Where North American Reliability Corporation serves as the governing body and enforcement of the electric grid. This would also include reliability and availability of power, as well as the security requirements of both physical security but also security against hackers who would want to shut down the electric grid.

References:

*Legal and regulatory*. (n.d.). North American Reliability Corporation (NERC). Retrieved July 17, 2023, from https://www.nerc.com/AboutNERC/legal/Pages/default.aspx

Kim, G., Debois, P., Willis, J. O., & Humble, J. (2016). *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. https://dl.acm.org/citation.cfm?id=3044729

Nygard, C. (n.d.). *Compliance in a DevOps culture*. martinfowler.com. Retrieved July 17, 2023, from https://martinfowler.com/articles/devops-compliance.html