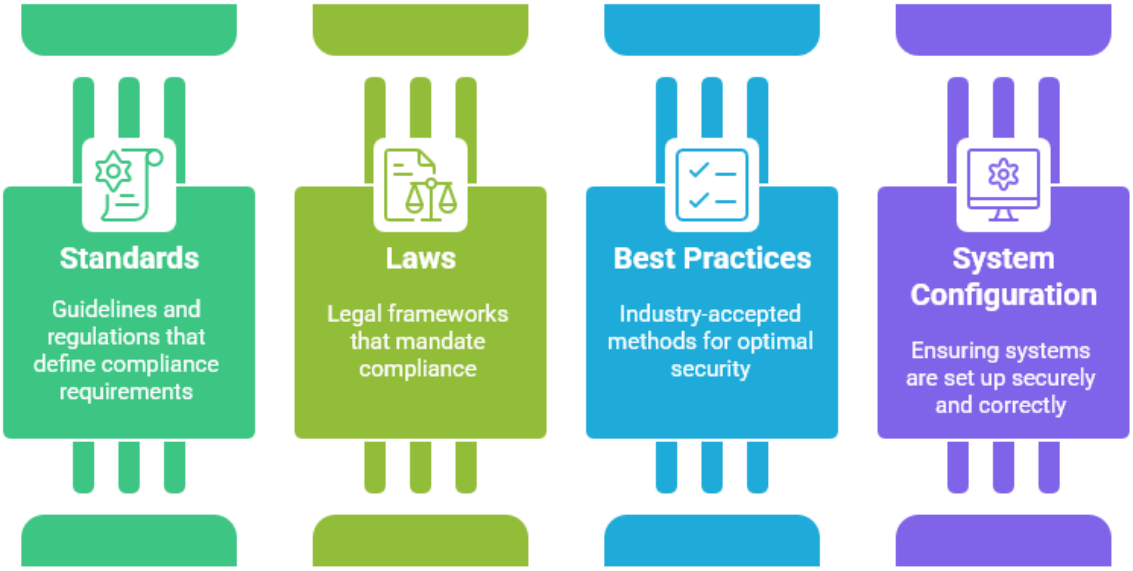
Policy Compliance Auditing:

Compliance:

In cybersecurity and IT, compliance means making sure that your computers, systems, and software are configured correctly and securely, according to certain standards, laws, or best practices.

If a rule says, "Passwords must be at least 12 characters long," then checking your systems to make sure this is true and fixing it if it's not is part of **being compliant**.



It is in Nessus is a process that evaluates whether your IT assets (servers, operating systems, databases, applications, network devices, etc.) are configured according to internal policies, industry benchmarks, or regulatory standards. Unlike traditional vulnerability scans that focus on missing patches or exploitable flaws, compliance auditing checks for secure configuration and adherence to best practices.

Rather than just looking for vulnerabilities, this feature checks system settings, configurations, and applied policies against a defined baseline to ensure proper hardening and compliance. Nessus uses audit files that contain predefined rules or custom checks to verify the system's configuration.