Compliance Report — TuneSpace-FE

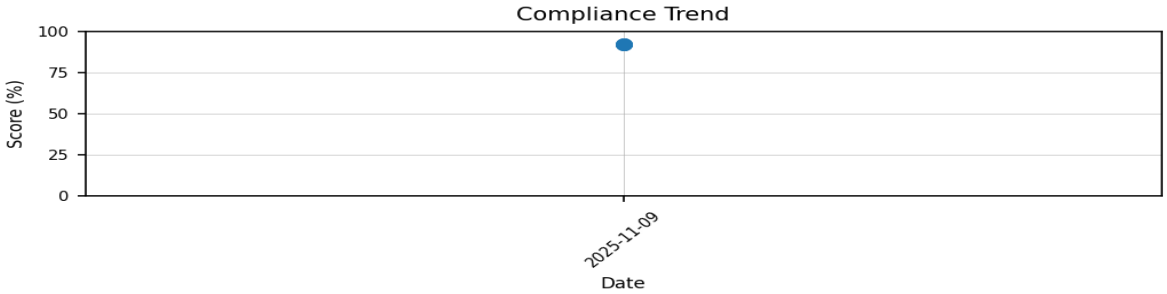
Compliance Score: 92.0%

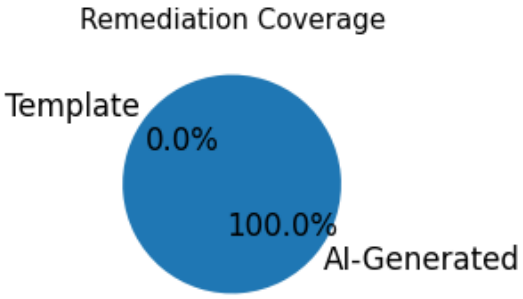
Standards Compliance:

ISO_27001	Compliant
NIST_SP_800_53	Compliant
OWASP	Compliant

Vulnerabilities Summary:

Severity	Count
Moderate	1





Detailed Control Scores

A.8.9 — Configuration management *(Technological)* — **90.0%**

Summary Poor configuration management can lead to system vulnerabilities, unauthorized access, and increased exposure to cyber threats, ultimately compromising the integrity and availability of sensitive data. Remediation Steps <ol> Establish a Configuration Management Policy
Develop a clear policy that defines standards for system configurations, ensuring consistent application across all systems.   Utilize Configuration Management Tools
Implement automated tools like Ansible or Puppet to manage and monitor configurations across environments.
Example Command:
<code>bash ansible-playbook configure.yml</code>   Regularly Audit Configurations
Schedule regular configuration audits to detect deviations from established baselines, using tools like CIS-CAT or Nessus for compliance checking.
Config Guidance:
Perform checks against industry benchmarks (e.g., CIS Benchmarks) to ensure configurations are compliant with best practices.