**Company Name:** TerraBloom Solutions

**Industry:** Environmental Monitoring & Agricultural Technology

**Description:**TerraBloom Solutions develops advanced environmental monitoring systems and smart agriculture solutions for farmers, environmental agencies, and research institutions. Their product line includes sensors, data analytics platforms, and software that track soil health, water usage, weather patterns, and crop conditions in real-time. TerraBloom’s mission is to help optimize sustainable agriculture practices, improve crop yields, and promote eco-friendly land management.

### **Scenario: TerraBloom Solutions’ Configuration Management Audit and Improvements**

**Overview of Audit Findings:**TerraBloom recently underwent an internal audit that highlighted deficiencies in their configuration management controls, particularly in the consistency and security of configurations across their engineering and product deployment teams. The audit revealed gaps in version control, standardized configurations, and documentation for various systems and devices. TerraBloom hired a consultancy (you) to evaluate their configuration management processes according to the NIST 800-53 Revision 5 framework and to provide recommendations.

Here is what you learned from your review of TerraBloom’s change management processes:

1. TerraBloom has established baseline configurations for its core systems, including their primary environmental monitoring platforms. These baselines ensure that critical configurations are consistent, providing stability for their most essential software. The baseline configurations are reviewed bi-annually, which helps maintain consistency in critical areas of their operations.
2. TerraBloom keeps detailed logs for major configuration changes, particularly when it involves high-priority client systems or critical components of their agricultural technology platforms. This logging practice allows TerraBloom to trace changes back to the responsible engineer and has helped them troubleshoot quickly when issues arise with major configurations.
3. TerraBloom utilizes configuration templates for new device deployments, ensuring that new hardware and software installations align with the company’s operational standards. These templates are well-documented and provide engineers with a structured starting point for device configurations, reducing errors and variability in initial setups.
4. While TerraBloom’s software team uses version control tools to track and manage code, their hardware engineering team does not consistently use version control for device configurations. This inconsistency leads to scenarios where configurations differ between devices or get lost entirely after changes are made.
5. Although major configurations are documented, TerraBloom lacks a formal review process to validate these configurations regularly. Without periodic checks, undocumented deviations and misconfigurations are more likely to occur, particularly on client-deployed systems.
6. TerraBloom’s logging practices focus heavily on major configuration changes, but minor modifications often go undocumented. This oversight means that TerraBloom sometimes struggles to trace issues arising from small tweaks made by individual engineers.
7. TerraBloom does not use automated configuration monitoring tools to detect unauthorized or unintended changes across systems. This lack of automation limits their ability to identify changes in real time and increases their reliance on manual reviews.
8. Although TerraBloom has some configuration management practices in place, they lack a comprehensive, formal configuration management policy. Without clear guidelines, configuration management practices can be inconsistent and vulnerable to errors. Developing a formal policy based on the NIST 800-53 framework would ensure that all teams adhere to consistent standards and provide a foundation for best practices across the organization.
9. TerraBloom currently has no defined procedures for rolling back configurations when issues arise. If a problematic configuration is identified, engineers must attempt to manually revert the system, which can lead to prolonged downtime or further errors.

**Group Activity**:

Manual assessment:

* Based on the above information, determine which controls from the NIST 800-53 r5 framework the company complies with today, and which controls it does not. For the non-compliant controls, provide recommendations to bring them into compliance, including process, technology, services, and/or configurations they should implement.

AI assessment:

* Run the AI “agent” to assess the above scenario against the NIST 800-53 r5 framework, to identify the controls that are compliant, non-compliant, and recommendations to remediate the control gaps.