**Company Name:** AeroSync Technologies

**Industry:** Aerospace Engineering & Avionics Software Development

**Description:**AeroSync Technologies designs and develops mission-critical software and avionics systems for the aerospace industry, including major airlines, space exploration companies, and defense contractors. Their products include flight navigation systems, safety monitoring software, and data analysis platforms for aircraft and spacecraft. AeroSync is known for its high standards in software reliability and safety, as their systems are often used in high-stakes environments.

### **Scenario: AeroSync Technologies’ Change Management Audit and Improvements**

**Overview of Audit Findings:**AeroSync recently underwent an internal audit, which identified gaps in their change management processes for engineering and software development teams. The findings highlighted areas where change controls were not adequately enforced, particularly around documentation, testing, and authorization. Following the audit, AeroSync hired a consultancy (you) to assess their processes against the NIST 800-53 Revision 5 framework and recommend improvements.

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

1. AeroSync has a formal change management policy that requires engineers to document changes, with high-level information on what changes were made and why. This documentation, though basic, ensures there is some accountability and record for each change made.
2. For major updates or changes that affect critical systems, AeroSync mandates rigorous testing protocols. This includes simulated stress tests, performance validation, and compatibility checks. These tests, while lengthy, help prevent significant failures in critical systems and are essential for maintaining safety standards in avionics.
3. AeroSync has a structured review and approval process for high-risk changes. Engineers must submit high-risk changes to a panel that includes a lead engineer, a project manager, and a quality assurance specialist for review and approval. This process has been effective in minimizing the risks of changes to critical systems, but is limited in scope to only high-risk modifications.
4. Although major changes are well-documented and approved, AeroSync lacks robust controls for minor and medium-risk changes. These changes are often implemented with minimal documentation and oversight, leading to inconsistencies and potential system instabilities.
5. AeroSync does not have a consistent rollback procedure for unsuccessful changes, meaning that if a new change fails, engineers may lack a clear path to revert to the previous stable version. This gap can lead to extended system downtimes or rushed solutions that might not fully restore functionality.
6. The audit found that multiple team members had permission to implement changes, even those outside their designated projects. This loose access control has led to situations where changes were deployed without proper coordination.
7. AeroSync lacks an automated system to track and audit changes in real-time, relying instead on manual documentation. This limits visibility into the timing, impact, and specifics of each change.
8. AeroSync does not conduct periodic audits of its change management processes to evaluate compliance and identify potential vulnerabilities. Such audits could help identify recurring issues and drive improvements.
9. AeroSync currently skips a detailed impact analysis for changes, assuming that minor and medium-risk changes will not significantly affect other systems. This assumption has, at times, led to unforeseen conflicts or disruptions in other modules.

**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.