# **Framework Implementation Best Practice Guide**

The instructions below provide a detailed, step-by-step guide for implementing the CD/CS framework that integrates Agile methodologies with ISO/SAE 21434 standard’s implementation of the V-model practices in automotive cybersecurity projects. This guide is a byproduct of the research study to ensure a systematic, efficient, and repeatable process to be followed for an automotive cybersecurity development project.

**Step 1: Initial Preparations**

1. Determine Project Compliance
   * Assess whether the project aligns with ISO/SAE 21434 requirements.
   * Confirm that the organization performs regular Threat and Risk Assessments (TARAs) and adheres to cybersecurity best practices.
2. Define Project Scope
   * Clearly outline the project’s objectives, deliverables, and cybersecurity considerations.
   * Collaborate with stakeholders to set initial cybersecurity goals (CG0).
3. Assemble the Team
   * Form an interdisciplinary team that includes developers, engineers, project managers, and cybersecurity specialists.
   * Assign roles and responsibilities for framework implementation, sprint planning, and TARA execution.
4. Set Up Tools
   * Use an in-house or a third-party threat assessment tool for conducting and documenting TARAs.
   * Set up project management tools to track tasks that follow and allow the Agile sprints methodology. This study suggests configuring a widely used project management tool, JIRA, for workflows and ticket management.

**Step 2: Initial Cybersecurity Sprint (CGS1)**

1. Establish Initial Cybersecurity Goals (CG1)
   * Using project requirements, define the cybersecurity goals for the first sprint (e.g., encryption standards, authentication protocols).
   * Document these goals in the project’s requirements repository.
2. Perform Initial TARA (T1)
   * Utilize TARA tools to conduct the first Threat and Risk Assessment.
   * Identify potential threats, vulnerabilities, and risks.
   * Prioritize risks based on severity and likelihood.
3. Create Initial JIRA Tickets (ID1)
   * Translate TARA findings into actionable tasks and create corresponding JIRA tickets.
   * Label tickets clearly (e.g., “ID1: Encryption Threat Mitigation”).
4. Update Cybersecurity Goals (CGi)
   * Based on the TARA results, refine or add new cybersecurity goals (e.g., CG1.1, CG1.2, etc.).
   * Ensure these updated goals are traceable to specific JIRA tickets.
5. Sprint Execution
   * Assign tickets to team members and begin the sprint cycle.
   * Hold daily stand-up meetings to track progress and address roadblocks.
6. Sprint Review
   * At the end of the sprint, review completed tasks and evaluate whether CGi goals were met.
   * Document any gaps or unresolved issues.

**Step 3: Iterative Process for Subsequent Sprints**

1. Repeat TARA and Updates
   * Perform subsequent TARAs (e.g., T2, T3) at the start of a new sprint.
   * Refine and expand cybersecurity goals based on new findings (e.g., CG2, CG3).
   * Formula for tracking the sprints: ***CGi = CGi + CGSi***
2. Create and Manage JIRA Tickets
   * Update the JIRA board with new tasks derived from TARAs (e.g., ID2).
   * Ensure each ticket is traceable to specific cybersecurity goals.
3. Monitor Progress
   * Track progress through JIRA and ensure all tasks are completed by the end of each sprint.
   * Use JIRA reports to analyze team performance and identify bottlenecks.
4. Sprint Reviews and Retrospectives
   * Conduct sprint reviews to evaluate deliverables.
   * Hold sprint retrospectives to identify process improvements for the next sprint.
5. Update Project Documentation
   * Continuously document TARA results, resolved issues, and achieved cybersecurity goals.
   * Maintain traceability between TARAs, tickets, and cybersecurity goals.

**Step 4: Project Completion**

1. Final TARA and Validation
   * Conduct a final Threat and Risk Assessment to ensure all risks have been mitigated.
   * Validate that all cybersecurity goals (CG\_Final) have been achieved.
2. Documentation and Reporting
   * Compile a comprehensive report also known as a Cybersecurity Case, documenting the entire framework implementation and the ways in which the risks were addressed and mitigated.
   * Include all the TARA results, resolved tickets (as necessary), and achieved goals achieved.
   * Highlight lessons learned and best practices for future projects.
3. Stakeholder Presentation
   * Present the project outcomes to stakeholders.
   * Demonstrate how the framework enhanced cybersecurity resilience and project agility.

**Key Considerations**

* Iterative Nature: The process is iterative, with each sprint building on the results of the previous one. Adapt goals and tasks dynamically as new information emerges.
* Collaboration: Maintain open communication among team members to ensure alignment and efficient problem-solving.
* Traceability: Ensure all TARAs, tickets, and cybersecurity goals are traceable to streamline audits and compliance checks.
* Flexibility: Tailor the framework to suit the project’s specific needs and constraints while adhering to ISO/SAE 21434.

By following these guidelines, teams can efficiently implement the CD/CS framework in their projects, ensuring robust cybersecurity practices and improved agility.