Global Platform®

SESIP for Procurement

Turning Supplier Cybersecurity into Reusable Evidence

May 2026

Jorge Wallace Ruiz, GP Chair of SESIP Auto WG

Agenda

- Why Procurement should care
- What SESIP Provides
- RFQs Requirements
- SESIP Levels
- Where to Start
- Common procurement pitfalls
- Business Value

Why Procurement Should Care

- Automotive cybersecurity evidence is now supply-chain critical.
- OEMs keep responsibility under UN R155/R156 and ISO/SAE 21434 / 24089.
- Repeating bespoke security assessments for each supplier/component is costly and inconsistent.
- SESIP provides reusable, independently verified component evidence.

The Procurement problem

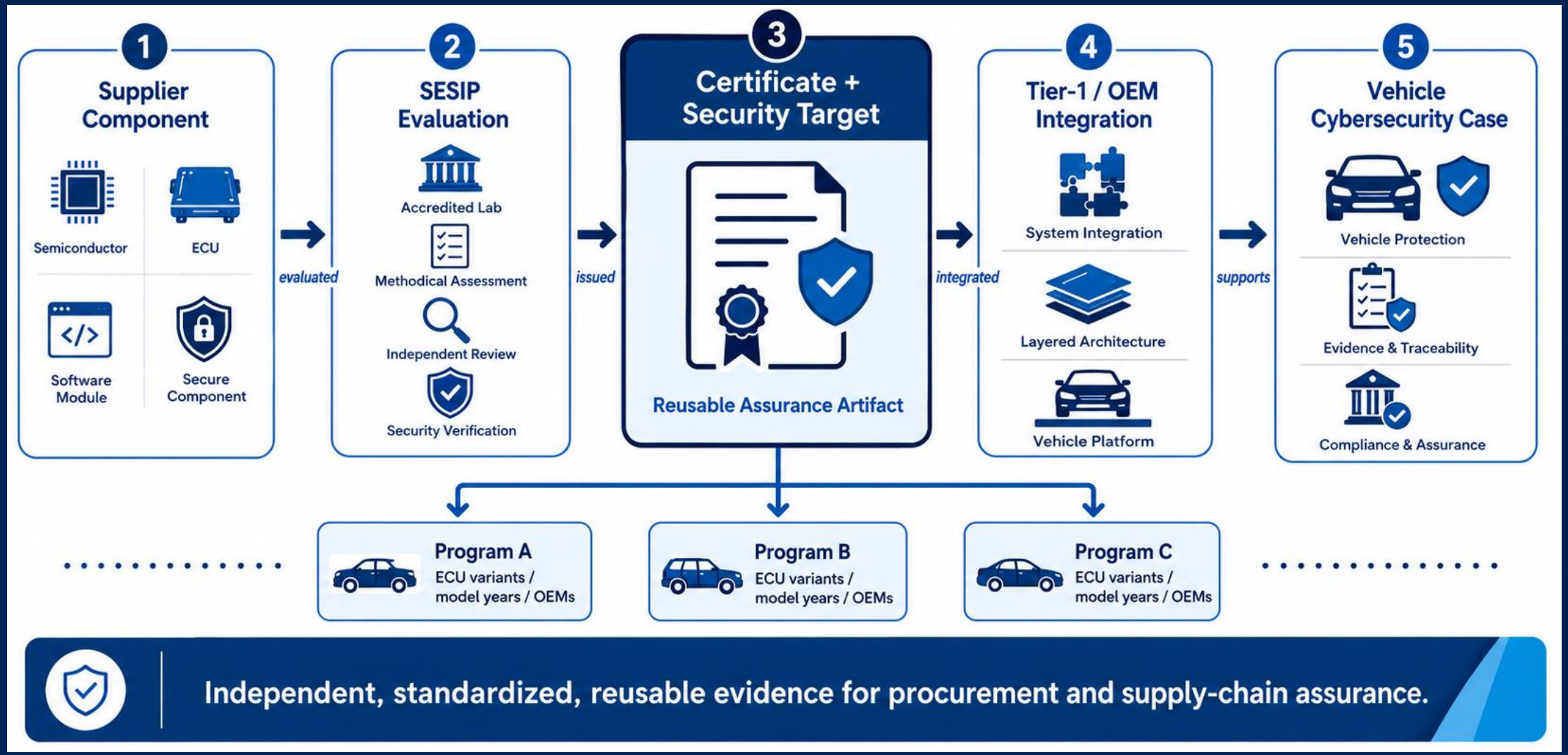
- **Without SESIP**
  - Supplier self-declarations.
  - Different evidence formats.
  - Repeated evaluations by each OEM/Tier-1.
  - Hard-to-compare supplier claims.
  - Late discovery of cybersecurity gaps.

Procurement needs comparable, auditable supplier evidence.

What SESIP provides

- Standardized security evaluation methodology.
- Certificate for a defined platform/component scope.
- Security Target describing:
  - what is evaluated,
  - what security functions are claimed,
  - what assumptions must be satisfied.
- Assurance levels SESIP1–SESIP5.

SESIP in One Picture



What Procurement can require in RFQs

- Applicable SESIP Profile, if available.
- Required SESIP assurance level.
- Valid certificate and scope.
- Security Target availability.
- Certificate maintenance obligations.
- Notification of security-relevant changes.
- Evidence of vulnerability handling process.

Selecting the right SESIP Level

- SESIP level should be driven by TARA/CAL, not by generic purchasing rules.
- Higher level is not always better: it may increase cost unnecessarily.
- Too low a level creates assurance gaps.
- Example:
  - Secure update mechanism: SESIP2/3 may be enough depending on threat.
  - Hypervisors / HW components: SESIP4/5 may be justified.

Profiles vs Security Targets

- **SESIP Profile** = generic baseline for a component type.
- **Security Target** = specific evaluated product/version.

- Procurement should not only ask:
  - “Do you have SESIP?”
    - but also:
  - “What profile, what scope, what version, what assurance level, and what assumptions?”

Composition: Why it Matters

- SESIP supports component reuse through composition.
- Lower-level component assumptions become obligations for the integrator.
- The OEM/Tier-1 must verify that inherited environment objectives are satisfied.
- Weakest assurance level can limit the composed system unless justified.

Common Procurement Pitfalls

- Asking for “SESIP certification” without defining level or scope.
- Accepting expired or version-mismatched certificates.
- Ignoring Security Target assumptions.
- Assuming a certified component secures the whole ECU.
- Not contractually requiring certificate maintenance.

Practical Procurement Checklist

- Is there an applicable SESIP Profile?
- Which SESIP level matches the TARA/CAL?
- Is the certified version the delivered version?
- Are assumptions/environment objectives clear?
- Who is responsible for satisfying them?
- What happens if the certificate expires or the component changes?

Business Value

- Reduced duplicated assessments.
- Faster supplier onboarding.
- More comparable supplier claims.
- Stronger evidence for CSMS/type approval.
- Earlier detection of security gaps.
- Better scalability for software-defined vehicles.

Global Platform®

SESIP is not only a technical certification

For procurement is a tool to make cybersecurity requirements contractual, comparable, reusable and auditable

Global Platform®

Questions ?