

---

# I-0434: Treatment Of TSF Components Provided By A Third-Party

---

TYPE: Guidance  
NUMBER: I-0434  
STATUS: Ready for External Repost after Interpretations Board Rework/Review

TITLE: Treatment Of TSF Components Provided By A Third-Party

FIRST POST: [\[cc-cmt 00558\]](#)  
MOST RECENT REPOST: [\[cc-cmt 00713\]](#)  
COMMENTS DUE BY: Friday, February 6, 2004 to [cc-cmt@nist.gov](mailto:cc-cmt@nist.gov)

RELATED TO: <None>  
CCIMB ENTRY: CCIMB-INTERP-0240

## ISSUE:

How are components provided by a 3rd party to be addressed with respect to the assurance requirements? Consider requirements such as ACM or ALC. There are aspects of these requirements that are not visible to a vendor incorporating a 3rd party item (for example, the configuration management mechanisms used by the 3rd party vendor, or the development site security or compiler options)?

## STATEMENT

Third-party components included in the TSF are treated no differently from components provided directly by the developer unless the PP or ST includes explicitly stated assurance components or refinements to assurance components that indicate otherwise.

## SUPPORT:

The TOE is the TOE. The definitions of TOE and TSF make no distinction based on who is providing a component of the TOE, nor do flaws go away simply because the component is developed by someone other than the direct developer of the TOE.

If assurance cannot be provided for a 3rd-party component, that component should be relegated to the IT environment, with the SFRs being adjusted accordingly. Note that movement of a component may have an impact on the ability to comply with a PP, if the 3rd party component is required to address an element allocated to the TSF. In such cases, a business decision must be made about the value of PP compliance vs. the cost of evaluation of the 3rd-party component.

Note that the PP/ST author has the ability to do the following to treat third-party components differently from other components:

- Include explicitly specified assurance components; however, such components would not be covered by the CCRA.
- Apply operations to the applicable assurance components. The assurance components would have to meet the applicable rules for the operations applied. For refinement operations, the evaluator would have to ensure that the third-party component that meets the refined requirement also meets the unrefined requirement and meets the applicable CEM work units. For assignment operations, the evaluator would have to ensure that the sum of all scopes covers the entire TOE, per CCIMB-INTERP-0138.

Note that in both cases (explicitly specified assurance components or operations on assurance components), the PP/ST author would also have to justify that the approach taken is appropriate given the assumptions, threats, and organizational security policies of the system.