Network Device Interpretation # 201727rev2

Redundant assurance activities associated with FAU_GEN.1

Status: ☒ *Active* ☐ *Inactive*

Date: *6-Mar-2019*

End of proposed Transition Period (to be updated after TR2TD process): *6-Apr-2019*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *ND SD V1.0, ND SD V2.0e, ND SD V2.1*

Affected Section(s): *FAU_GEN.1*

Superseded Interpretation(s): *Rfl#201727(rev1)*

Issue:

FAU_GEN.1 Audit data generation has two fully redundant assurance activities (AA):

Guidance Documentation

"The evaluator shall check the guidance documentation and ensure that it lists all of the auditable events and provides a format for audit records."

Tests

"The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above."

First, it is of questionable value to administrators to have a list "all of the auditable events". It is sufficient to describe the audit record format and how to access the logs. In practical terms, having a lengthy and exhaustive list of all audit events makes the guidance much less readable and consequently far less useful.

Second, as an evaluation activity, ensuring that all auditable events are listed is fully redundant given that the evaluator is already generating all of them during testing. Either of these activities would ensure that all of the mandatory audit events are generated by the TOE.

We suggest modifying the guidance requirement to state:

"The evaluator shall check the guidance documentation and ensure that it contains an example of an auditable event and describes the TOE's format for audit records in sufficient detail to allow an administrator to interpret the audit trail."

Resolution:

The NIT acknowledges the issue described in the 'Issue' section. The following changes shall be applied.

The first paragraph of the requirements on Guidance Documentation for FAU_GEN.1

<old>" The evaluator shall check the guidance documentation and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the cPP is described and that the description of the fields contains the information required in FAU_GEN1.2, and the additional information specified in the table of audit events." </old>

shall be replaced by

<new>"The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e. at least one instance of each auditable event – comprising the mandatory, optional and selection-based SFR sections as applicable – shall be provided from the actual audit record)."</new>

Rationale:

See "Issue" section

Further Action:

None.

Action by Network iTC:

None.