



ISO/IEC JTC 1/SC 27/WG 3 "Security evaluation, testing and specification"

Convenorship: UNE

Convenor: Bañón Miguel Mr



PWI_25543_Progress_Report_Draft_20260916_V3

Document type	Related content	Document date	Expected action
Project / Other	Meeting: VIRTUAL 14 Sep 2026 Project: ISO/IEC PWI 25543	2026-09-17	INFO

ISO/IEC JTC 1/SC 27/WG 3
PWI 25543 – Progress Report

Consideration of the Target of Evaluation Concept for Emerging and Existing Technologies

Virtual meeting, September 2026

Kwangwoo Lee*, Elzbieta Andrukiewicz#, David Martin#, Jade Stewart#

1. Purpose and current status

PWI 25543 was initiated to examine whether the Target of Evaluation (TOE) concept defined in the ISO/IEC 15408 series and ISO/IEC 18045 remains adequate for evolving technologies, architectures, and deployment models. The study is intended either to provide guidance for applying the existing framework or to provide input for future revisions of ISO/IEC 15408 and ISO/IEC 18045.

The project has progressed through several calls for contributions and related WG 3 discussions. The September 2026 virtual session reviewed the contributions received to date, including the third call for contributions, and considered whether the accumulated material is sufficient to form a final recommendation. The discussion confirmed that useful findings have been collected, but also identified issues that require consolidation before the PWI can be concluded.

2. Inputs considered to date

The progress review considered the following main inputs and related material:

- The first Call for Contributions and its Statement of Contributions (WG3 N2797), including discussion of system concepts from ISO/IEC/IEEE 15288:2023 and their potential relevance to describing TOE boundaries, operational environments, and complex systems.
- CC in the Cloud guidance and the earlier contribution reflected in the SoC on PWI 25543 (WG 3 N2941), addressing cloud deployment models, TOE identification, TOE platform and trusted platform concepts, and the separation between the TOE and its operational environment.
- The late expert contribution on a non-tangible TOE (WG 3 N2812), using a Verilog RTL description as a case study and considering how the existing evaluation framework applies when the evaluation object is not a conventional deployable product.
- The third Call for Contributions (WG 3 N3095) and its SoC (WG 3 N3141), together with the previous progress report (WG 3 N3094).
- The DIN late contribution (WG 3 N3145), which introduced site-based and development-process-based evaluation objects and proposed that the TOE concept may need to support broader types of identifiable and evaluable security-relevant objects.
- Related WG 3 work on AI functionality, generative AI security testing, and AI agents/orchestration, used as additional examples for testing the applicability of the current TOE concept and TOE boundary model.

3. Main discussion and observations

3.1 Cloud and dynamically deployed TOEs

The cloud contribution generally supports the view that many cloud-hosted products can be handled within the current TOE framework when the TOE boundary, platform, trusted platform, and operational environment are clearly described. The contributor confirmed that the existing guidance is intended to adapt existing Protection Profiles to products hosted in cloud environments rather than to evaluate the cloud environment itself.

However, the discussion also showed that this conclusion should not be generalized too quickly. Practical experience from cloud evaluations highlighted issues including applications that cross cloud service-provider boundaries, dependencies on underlying platform services, and uncertainty over how the evaluated software version is traced when the platform is updated. The discussion also raised the example of load balancing, where multiple instances of an application may be created dynamically and may access distributed storage. These examples indicate that some cloud scenarios may require further analysis of TOE identity, configuration, boundary, and evaluation continuity rather than only a static separation between TOE and operational environment.

3.2 Non-tangible evaluation objects

The non-tangible TOE contribution remains relevant, particularly for pre-silicon evaluation and other design-level objects. The contribution emphasized that such evaluations are becoming more common, including in the context of hardware implementation of cryptographic functions. The discussion suggested that the issue is not necessarily a need to replace the current TOE concept, but that additional flexibility or evaluation treatment may be required to ensure that the TOE specification is complete and internally consistent, its integration with other elements is clearly defined, and relevant threats and environmental conditions are adequately considered.

3.3 Site TOE and Process TOE

The DIN contribution generated the most significant new discussion. The contribution explained the potential value of recognizing a site as an evaluation object and of evaluating security-relevant development processes independently so that the resulting assurance evidence can later be reused in product evaluations. This approach would be similar in intent to established site certification practices and to process-oriented evaluation approaches used in other standards.

DIN/BSI experts explained that the site evaluation concept is already supported by substantial practical experience and that related material has progressed through European technical work. She stressed that accommodating a Site TOE or Process TOE would require more than a terminology change: corresponding assurance elements in ISO/IEC 15408-3 and evaluation work units in ISO/IEC 18045 may also be needed. The discussion therefore moved from the narrow question of whether the TOE definition should be widened to the broader question of how site- and process-oriented evaluations could be integrated consistently into the CC/CEM framework.

The discussion also highlighted the need to define the scope of such concepts precisely, for example whether a site or process is evaluated specifically in support of later CC product evaluations. It was further observed that process-oriented evaluation may become increasingly important when lifecycle, vulnerability handling, patch management, and security update processes are considered.

3.4 Emerging AI-related cases

The comparison with current AI-related work suggests that many AI use cases can still be described using the existing TOE concept. AI models, AI functionality, generative AI models, and some single-agent systems can in principle be bounded as identifiable evaluation targets. Nevertheless, complex orchestration, external tools, memory, RAG, APIs, delegated actions, continuous adaptation, and multi-agent interaction may create difficult boundary and evaluability questions. These cases should therefore be retained as test cases when consolidating the PWI findings.

4. Current assessment

The work to date does not support a single broad conclusion that the existing TOE concept is either fully sufficient or fundamentally inadequate. Rather, the accumulated inputs appear to fall into three broad groups:

- Cases that can generally be accommodated by the existing TOE concept, subject to clear identification of the TOE and its operational environment.
- Cases that primarily raise TOE boundary, configuration, identity, or evaluation-continuity questions, particularly in dynamic cloud and complex AI deployments.
- Cases that may require extension of the evaluation framework itself, notably site-based and process-based evaluations, including the corresponding assurance requirements and CEM work units.

Accordingly, the September discussion should be treated as progress in refining the problem statement rather than as the final conclusion of PWI 25543.

5. Proposed next step

At this stage, the discussion did not identify a strong need for a further broad Call for Contributions. Instead, it may be beneficial for the editors to consolidate the existing contributions and the outcomes of the September discussion into a structured analysis. Such consolidation could help clarify which cases are already supported by the current framework, which cases may require additional interpretation or guidance, and which cases may indicate a need for future work.

The editors also intend to continue discussions with the contributor of the Site TOE and Process TOE proposal to further refine the analysis and its implications for the ISO/IEC 15408 and ISO/IEC 18045 framework.

The consolidated findings could then be presented to WG 3 at the next meeting, together with any recommendations regarding possible follow-on activities. Subject to the outcome of this work, a Final Report could be prepared for consideration by WG 3, irrespective of the administrative status of PWI 25543 at that time.