Running Head: ITSEC VS. TCSEC

Security Evaluation Criteria: ITSEC vs. TCSEC

Jered McClure

Walden University

Security Evaluation Criteria: ITSEC vs. TCSEC

When a software company develops a software application, whether this is a system or a product, certain security functionalities are expected by any customer of that organization. These expectations have been codified in the evaluation criteria standards TCSEC and ITSEC. Meeting each of the seven levels of these two standards gives an ever increasing sense of security viability of any application. This, in turn, provides confidence and assurances that the product’s security policy is being met.

The Trusted Computer System Evaluation Criteria (TCSEC) is a method of verifying and appraising a computer system based on the Bell La Padula model of system access and control. Built by the US Government, the TCSEC is modeled after the US. Department of Defense’s internal security policy and is primarily used for organizations with a hierarchy culture (Commission of the European Communities, 1991) (Dhillon, 2007). That is, it is strictly built around security and access restrictions to data, with less focus given to data integrity.

On the other hand, ITSEC (Information Technology Security Evaluation Criteria) was built in Europe with a greater focus on integrity, but also ensuring confidentiality and availability. Its primary purpose is to provide assurance as to a product or system’s ability to deter potential security threats. Unlike TCSEC, ITSEC is more generalized in its application, e.g. no specific security structures are required for compliance (Commission of the European Communities, 1991).

Given the situation of an unnamed software organization delivering a new chat program, security assurances can be provided using both ITSEC and TCSEC. At ITSEC level E0 and TCSEC D, no security is present, or whatever security is available does not meet any higher security requirements. This is a basic application without any thought behind security.

At level E1 of the ITSEC, the software organization would have to build a product security policy which defines the required security enforcing functions of the chat application. This meets the ITSEC requirement of having a security target and informal architecture defined. TCSEC requires that, at level C1, initial discretionary access controls (DAC) are applied, as well as, a product environment which promotes mutual data protection by all users of the program. This can be done by having user authentication mechanisms which only allow authorized users to access specific security functions, within the chat product.

Meeting level C2 of TCSEC requires the DAC previously mentioned to be drilled down for minute security control. User’s must also be required to log into the program and only able to access those objects within their security rights. ITSEC requires testing documentation, formal security architecture documentation, penetration testing evidence, and user/application audit trail documentation for level E2. The software company can comply with this mandate through developing testing documentation which shows evidence of penetration testing, and applying logs to the chat program for auditing user’s access to product functions.

At ITSEC E4 and TCSEC B2, clearly defined documented evidence for customer perusal is the key. That is, both criteria require the software company to provide a formal statement giving evidence for customers to decide if the product meets required security needs. That being said, TCSEC explicitly requires that the documentation show evidence in line with the specific security requirements of C1 to B2. ITSEC is more lenient in that it only wants proofs which customers can decide upon.

TSCEC B3 requires that any user services which access the chat program must pass through a reference monitor for mediation (Commission of the European Communities, 1991). Additionally, all source code must be cleaned to ensure only what is required for product operation and security constraints remain. ITSEC E5 compliance requires the organization to provide documented evidence explaining how and why the chat program’s security functionality counters threats, and the suitability of those counters.

Finally, level E6 of ITSEC brings the software company to a point where they must provide formal, mathematical, evidence which proves the underlying security model. The proof must also show rationale of the given product’s security enforcing functions. At level A1 of TCSEC, all of the previous level (B3) is still relevant. However, a formal, mathematical, proof must also be supplied as evidence that the product security policy functions as designed. This is another overlapping area, similar to E4/B2 where TCSEC requires applications specific examples over ITSECs general examples.

Having the chat program move up the levels of criteria for ITSEC and TCSEC ensures to users and customers that the security of the application in question is sound. Additionally, ITSEC assures data integrity and availability while TCSEC assures confidentiality and access control. Meeting both standards means meeting nearly any security requirement a user or customer could demand of a system. Standardization for ITSEC provides a means to outline best practice security guidelines, while for TCSEC this means specific and unmitigated choices which must be adhered to in order to fall within compliance standards.

Reference

Commission of the European Communities. (1991). *Information technology Security Evaluation Criteria (ITSEC).* Luxembourg: Office for Official Publications of the European Communities.

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases.* John Wiley & Sons, Inc.

Chat Program Requirements Comparing ITSEC and TCSEC

