Defense Business Systems – Guidance

Summary

Reliability, maturity, and sustainment measures for business systems acquisitions rely heavily on configuration management, defect tracking, and automated regression testing. This section of the guidebook provides related examples of text from previously approved TEMPs for business systems that have successfully prepared for developmental and operational testing.

Processes for developing and managing information technology software are provided in IEEE Standard 12207.2, Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations, dated April 1998.

The TEMP should describe the acquisition program's configuration management and configuration control framework. Testers will need accurate configuration information to understand the system and to determine the system's adherence to effectiveness, suitability, and cybersecurity requirements.

Defect tracking should be conducted during all phases of test and evaluation, using a clearly-defined process that is explained in the TEMP. Generally, as a defect is discovered, the developer or tester will document it through a deficiency report (DR). A Deficiency Review Board (DRB) will assign a DR level as defined by IEEE 12207.2 Annex J, and track the status of each defect, over time, as to which are open, closed, or resolved. During regression testing or as part of another test event, testers will validate that identified deficiencies have been resolved. Additionally, software change requests (SCR) for capabilities that are needed but not inherent in the software baseline should be generated and assigned severity levels using the IEEE definitions based on impacts to mission accomplishment.

As a rule, test measures for business systems should be specified in terms of the types of data that can automatically be logged and reported by the system. Measures used for testing will typically be the same measures as those that operators and system managers will use over the course of a system's lifecycle to gauge acceptable performance or service degradation. Accordingly, automated logging and reporting of performance data should be included in the core system design. When possible, automated approaches to data collection should be used versus less accurate manual methods (e.g., relying on a stopwatch to measure system response times). Objective human performance measures, such as human error rates and the amount of time it takes the operator to complete a task, should be used to evaluate human factors, as appropriate for the system under test. Surveys should be used sparingly when human performance measures are not feasible or to supplement these measures. When used, surveys should comply with DOT&E's guidance on survey design and administration.

References

DoDI 8500.01, Cybersecurity, dated March 14, 2014 incorporates guidance from the now obsolete DoDI 8500.2, Procedures for the Operational Test and Evaluation of Information Assurance.

Defense Business Systems – Guidance

DoDI 8501.02, Risk Management Framework (RMF) for DoD Information Technology (IT), dated 12 March 2014, specifies the use of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). RMF replaced the now-defunct DoD Information Assurance Certification and Accreditation Process (DIACAP).

Guidance on the Use and Design of Surveys in Operational Test and Evaluation (OT&E), DOT&E, 22 December 2014

Discussion on the Use and Design of Surveys, DOT&E, 24 February 2015

Discussion on Including Neutral Responses on Survey Questions, DOT&E, 2 April 2015

Survey Pre-Testing and Administration in Operational Test and Evaluation, 6 January 2017

Defense Business Systems Examples