Operational Testing of Software-Intensive Systems - Guidance

Summary

This guidance applies to software-intensive systems that are covered by the DoDI 5000.02, January 7, 2015, under Incrementally Deployed Software Intensive (Model 3), software-intensive Accelerated Acquisition (Model 4), and Hybrids Acquisition programs. The DOT&E policy, Guidelines for Operational Test and Evaluation of Information and Business Systems, 14 September 2010, especially applies to Model 3 systems. Model 3 systems are distinguished by the rapid delivery of capability through multiple acquisition increments, each of which provides part of the overall required program capability. Each increment may have several limited deployments; each deployment will result from a specific build and provide the user with a mature and tested sub-element of the overall incremental capability. Several builds and deployments will typically be necessary to satisfy approved requirements for an increment of capability. Software systems must also address cybersecurity testing, as required by DOT&E Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, 01 August 2014 and further described in Appendix E, Cybersecurity.

OT&E for software acquisitions will be guided by the assessment of operational risks of mission failure. The DOT&E Guidelines should be used by the OTA to help determine the level of risk and the corresponding adequate level of OT&E for all capabilities that are to be deployed. There will be at least one full OT&E for every formal acquisition increment of a software intensive system unless waived by DOT&E. For software intensive systems on DOT&E oversight, DOT&E approval of the level of risk and adequate level of OT&E is also required. The degree of independent operational testing appropriate for each software increment or capability can be tailored by using the risk analysis described in the DOT&E Guidelines. The Guidelines also permit delegation of test plan approval using the same criteria.

Overall sustainment approaches should be adequately described in the Life Cycle Management Plan or similar document. A weak integrated logistics and sustainment approach can be a huge risk even if the system effectiveness and suitability are otherwise acceptable. There should be a documented, repeatable process whereby problems are documented at the help desk and problems that are fixed by any tier of help desk support are tracked to completion; those problems that the help desk system cannot resolve should be escalated through a well-defined process and IEEE 12207.2 priorities assigned as discrepancy reports (DRs). Then, each DR should go through a Configuration Control Board (CCB) process to verify operational impact and priority with the result being a plan to fix the problem. After fixes are implemented in projected releases, there needs to be a regression test procedure within the organization that provides the fix and a further CCB process to release into production the new version, with rollback procedures in case the new version fails. This aspect of risk directly relates to the operational impact if the problem were to be missed during testing and subsequently found during operational use, since it helps determine the fix process and appropriate regression testing.

The entire risk assessment and design/conduct of testing process should be a significant focus area for continuous improvement. Whenever significant risks are encountered after completion of testing, it must be assumed that the risk assessment process, operational test adequacy, and/or the test/fix/test process require significant improvement. A simple metric showing the cumulative number of Category I problems encountered, and cumulative Category I problems fixed, after completion of operational testing of the previous software release, should be shown as part of the risk assessment level of test package when submitted to DOT&E for approval.

References

DoDI 5000.02, 7 January 2015

DOT&E Guidelines for Operational Test and Evaluation of Information and Business Systems, 14 September 2010

DOT&E Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, 01 August 2014

Directive-Type Memorandum (DTM) 11-009, Acquisition Policy for Defense Business Systems (DBS), 23 June 2011 with 9 Dec 2011 change, AT&L Directive

Software Maturity Criteria for Dedicated Operational Test and Evaluation of Software-Intensive Systems, DOT&E Memo, 31 May 1994

IEEE 12207.2

Examples

Operational Testing of Software Intensive Systems Example