

# Defense Business Systems – Guidance

---

## Summary

Reliability, maturity, and sustainment metrics 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 12207.2, Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations](#)

The TEMP should describe the acquisition program's configuration management 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 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.

As a rule, test metrics for business systems should be specified in terms of the types of data that can automatically be logged and reported by the system. Metrics used for testing will typically be the same metrics as those that the operators 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). User surveys should be used sparingly, and, if used, should comply with guidance in [DOT&E's memo on Surveys](#). The System Usability Scale (SUS) is recommended in DOT&E guidance and should be considered for evaluation of business system usability.

[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.

[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).

## [Examples](#)