OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JUN 16 2003

MEMORANDUM FOR DEPUTY DIRECTOR, DEVELOPMENTAL TEST AND EVALUATION, DEFENSE SYSTEMS, OUSD(AT&L)
DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH)
DIRECTOR, NAVY TEST AND EVALUATION AND TECHNOLOGY REQUIREMENTS
DIRECTOR, AIR FORCE TEST AND EVALUATION
COMMANDER, ARMY TEST AND EVALUATION COMMAND
COMMANDER, OPERATIONAL TEST AND EVALUATION FORCE
COMMANDER, AIR FORCE OPERATIONAL TEST AND EVALUATION CENTER
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND EVALUATION ACTIVITY
COMMANDER, JOINT INTEROPERABILITY TEST COMMAND

SUBJECT: Guidelines for Conducting Operational Test and Evaluation for Software-Intensive System Increments

Attached are the revised guidelines for conducting operational test and evaluation for software-intensive system increments. These guidelines support the Deputy Secretary of Defense's Management Initiative Decision 905 "Net-Centric Business Transformation and E-Government." Their implementation will help both streamline and simplify the commercial off-the-shelf software testing procedures and improve the test and evaluation process.

Thomas P. Christie
Director

Attachment:
As stated

GUIDELINES FOR CONDUCTING OPERATIONAL TEST AND EVALUATION (OT&E) FOR SOFTWARE-INTENSIVE SYSTEM INCREMENTS[1]

1. BACKGROUND

An increasing number of DoD software-intensive systems are being procured with incremental acquisition strategies. The systems are deployed in a series of program increments, where each successive increment builds upon the capabilities and functionality previously deployed.

Most DoD acquisitions have traditionally employed fairly rigid testing plans in which the test phases were extensive, distinct, and dependent upon the completion of one phase prior to starting the next. The increased use of commercial-off-the-shelf (COTS) products and non-developmental items (NDI), coupled with the initiative to streamline the acquisition process, requires a more flexible and responsive operational test and evaluation strategy.

2. PURPOSE AND SCOPE

This document presents a set of guidelines for tailoring pre-deployment test events to the operational risk[2] of a specific system increment acquired under OSD oversight. For insignificant to moderate risk increments, these guidelines streamline the OT&E process by potentially reducing the degree of testing. These guidelines also permit the delegation of testing and fielding decisions for a specific increment to the Component.

These guidelines apply to all increments of software-intensive systems except the "core increment,"[3] which undergoes full operational testing. The OT&E of the core increment will provide a performance baseline for testing subsequent increments. This revised operational testing strategy provides "affordable confidence" to the development and procurement process, while mitigating risks. Services and Agencies are encouraged to employ these guidelines for non-oversight programs as well.

---

[1] For the purposes of these guidelines, software-intensive systems are computer-based information systems executing one or more resident, separable application software programs. Examples include automated information systems (AIS) and command and control (C2) systems. Software systems embedded in weapon systems are excluded from these procedures pending further study. An increment of a software-intensive system is a militarily useful and supportable operational capability that can be effectively defined, developed, deployed, and sustained as an integrated entity or building block of the target system. An increment may be composed of one or more spirals or other developmental elements.

[2] Risk is a compound function of the likelihood and mission impact of an increment's failure to be operationally effective and suitable.

[3] The core increment of a system provides the basic infrastructure necessary to support the ensuing incremental functionality and/or the bulk of the planned capabilities. This increment usually delivers the initial operational capabilities and is a worthwhile stand-alone system even without additional increments. It normally consists of basic hardware, system software and tools, and fundamental applications.

3. GENERAL APPROACH

The objective of these guidelines is to provide a method for determining levels of operational testing appropriate to the risk posed by specific system increments. The first step is assessing risk. Risk assessments are made by the appropriate Operational Test Agency (OTA). Most are based upon two essentially independent evaluations: analysis of the factors that affect the likelihood of success of an increment, and an understanding of the mission impact of increment failure.

The next step is to define the amount of operational testing that will provide sufficient assurance that the risk will be mitigated to an acceptable level. The appendices to this document provide suggested techniques and recommendations for assessing risk and determining appropriate levels of testing.

The OTA then presents the proposed operational test strategy to the Director, Operational Test and Evaluation (DOT&E) during the normal test concept briefing; if it is approved, it is then implemented. If the increment poses insignificant to moderate risk, the OT&E and fielding decision may be delegated to the Component.

4. IMPLEMENTATION

a. Prepare risk assessment. The OTA, with inputs from the Program Management Office (PMO), the developmental tester, and the user, conducts a risk assessment that includes the evaluation of potential threats to success and the mission impact of failure. The post-deployment software support organization, if available, should also be consulted regarding the stability of the increments already deployed.

b. Determine appropriate level of OT&E. Based upon the assessed risk, the OTA proposes an appropriate level of OT&E for the new increment during the OT&E concept briefing to DOT&E. For insignificant to moderate risk increments, the operational testing, evaluation, and fielding decision may be delegated to the Component.

c. Develop OT&E plan appropriate for the validated level of test. The OTA develops an operational test and evaluation plan based upon the DOT&E-approved test concept.

d. Conduct test activities and prepare report. The OTA conducts the test and collects the data. The OTA then prepares an independent evaluation report (IER), consistent with the test concept and plan, and provides a copy to the appropriate offices of the Component and to DOT&E.

e. Provide operational effectiveness and suitability recommendations. The IER and any additional evaluation data are analyzed by DOT&E for test events conducted under OSD oversight. For non-delegated increments, DOT&E provides independent operational effectiveness and suitability recommendations to the Milestone Decision Authority (MDA). For delegated increments, the OTA provides operational effectiveness and suitability recommendations, consistent with the test concept and plan, to the Component Acquisition Executive (CAE), who makes the fielding decision for the increment.

5. EFFECTIVE DATE

June 16, 2003

APPENDIX A

ELEMENTS OF RISK ASSESSMENT FOR SYSTEM INCREMENTS

There are two primary factors in assessing the risk of a system element: the likelihood of failure and the impact on the mission of an increment's failure to be operationally effective and suitable. Fortunately, these two components need to be evaluated only to the degree required to decide among a few distinct levels of operational testing.

This appendix will discuss these two fundamental elements of risk assessment: the likelihood of failure, which will be evaluated via a surrogate method, and the mission impact of failure, which will be approached in a more direct fashion. The final step is the fusion of these two evaluations into an assessment of the overall risk of a system increment. This document was developed to present a general concept and suggestions for tailoring operational testing to risk. Users should recognize that the procedures needed to properly assess risk should be tailored to the characteristics of the specific increment. The procedures presented in this appendix are provided as examples to guide the OTA in the risk assessment process, rather than a checklist or hard set of rules.

1. Identification and Evaluation of Threats to Success for Increments

The data required to accurately define the true probability of failure of an increment are not likely to be available. As an alternative approach, the analysis can be based upon an evaluation of a comprehensive set of factors that have been shown as potential threats to the success of a software-intensive increment. These threats to success can be evaluated relative to the specific increment, and a general estimate of potential effects can be determined. The evaluation of the cumulative effect of the threats to an increment's success is analogous to determining the likelihood of failure for the increment. Of necessity, this aggregate assessment is usually a judgment call.

Most concerns associated with the deployment of a new, generic, software-intensive system increment may be grouped under a few general categories. As an example, this appendix identifies six primary categories of threats to success, although fewer or more categories may be appropriate for a specific increment. This set of categories is certainly not unique, and any set that comprehensively covers the issues of concern will give similar structure to the approach. Further, the categories may have significantly different relative sensitivities for any particular increment. The six categories of threats to success presented as an example in this appendix are:

- Development
- Implementation
- Technology
- Complexity
- Safety
- Security

The OTA should first assess the threat to an increment's success from each separate area, by examining the particular characteristics of the increment and its development. This evaluation is guided by the specific issues identified with each category, and based upon input from the user, the developer, the developmental tester, the post-deployment software support organization, available documentation, and any new data collected by the OTA. Clearly, not all issues within a category will have equal importance.

Then, based upon these assessments and the relative significance of each area, the OTA should make an overall evaluation of the likelihood of the increment's failure to be operationally effective and suitable. Not all categories need to be given equal importance. The evaluator should base this judgment upon the particulars of the increment, the development process, and the utility and reliability of available data. Note that the categories and issues presented are merely examples; the evaluator should always consider risk factors specific to the increment. In other words, use good judgment, based on detailed knowledge of the increment.

Each category should be evaluated as accurately as possible, at least to the levels of resolution described below. Each of these levels is defined in terms of typical characteristics; actual assessments will be a mix of positive, neutral, and negative characteristics.

a. Insignificant Threat to Success (Insignificant Likelihood of Failure) – Increments posing this level of threat to success are typically small, simple modular increments that come from a highly reliable developer and an ideal development environment. Additional characteristics that support this assessment are a program's demonstrated success with all previous increments, employment of very mature technologies, excellent training programs or highly experienced users, no impact upon other system elements, and no safety or security issues.

b. Low Threat to Success (Low Likelihood of Failure) – Increments posing this level of threat to success may be small- to medium-sized, involving few complicated issues. Other characteristics justifying a low threat to success are a solid development environment with few shortcomings, employment of stable technologies, capable users, little interaction with basic system elements, and few safety or security issues.

c. Moderate Threat to Success (Moderate Likelihood of Failure) – This level of threat to success is typically assigned to medium- to large-sized increments having several complex elements and employing recent technological developments. Complicated interfaces, significant interaction with external system resources, or multiple safety and security concerns would suggest this level of assessment.

d. High Threat to Success (High Likelihood of Failure) – This highest level of threat to success typically involves large to very large, complex, multi-functional increments. Other characteristics include untested or unreliable development environments with poor performance histories, new technologies, many untested interfaces, new or untrained users, and multiple safety and security issues.

It is unlikely that all six categories of evaluation will be assigned the same level of threat to success. One simple scheme of evaluation would be to assign to the increment as a whole a level equal to or greater than the highest level of threat to success determined for any single category. For example, if the highest level category poses a moderate threat to success, then the overall level should be no lower than moderate. If two or more important categories are rated as moderate, then the overall level might be elevated to a high threat to success (or high likelihood of failure).

Example Issues for Evaluating Threats to Success

The following issues represent some potential threats to an increment's success. Detailed knowledge of a particular system increment will tailor the assessment.

a. Development

- Have mission needs been adequately described and user requirements clearly identified?
- Do the requirements address operational needs rather than specifying a technical solution?
- Are the capabilities included in the new increment traceable to requirements, as specified in the requirements traceability matrix?
- What is the developer's Capability Maturity Model rating as defined by the Software Engineering Institute? Is the rating justified by the developer's experience?
- How extensive was the developmental test program for this increment, i.e., did the developmental testing (DT) program explicitly address each requirement? Did the DT program also evaluate operational requirements?
- Does the developer employ a robust set of software management indicators?
- Are interfaces with existing systems fully documented and under configuration control?
- Does the developing contractor's test agent have sufficient experience and technical expertise to conduct a proper technical evaluation?
- Has the necessary integration and regression testing been conducted?

- Were any Priority l or Priority 2 problems[4] experienced with the last increment from this development team?
- How numerous and how significant are the deficiencies identified in previous tests of the new increment?
- What is the history of the developer regarding similar programs?
- What is the history of the developer with respect to previous increments?
- How effective is the established configuration management process for the program development and/or installed systems?
- How extensively have prototypes been used to evaluate acceptance by typical users?
- Have exit criteria been identified for developmental testing of this increment?
- Are there requirements/capabilities of this increment that will be unavailable for testing?

b. Implementation

1) User:

- Is the user committed to the successful implementation of the new increment?
- Have operational and user support procedures been developed and readied for implementation along with the new increment? Have user representatives developed appropriate concepts of operations, policies, procedures, training, support, and contingency plans for a full operational deployment?
- Do the operators possess the skill levels required to use the increment's capabilities effectively?
- Has an adequate training plan been developed or implemented to include reorientation and sustainment training?
- Has a point of contact been established to represent the views of users?

2) Organization:

- Is the receiving organization committed to the successful implementation of the new increment?
- Is the receiving organization prepared for the changes in business processes associated with the new increment?

[4] As defined in IEEE/EIA Standard 12207.2-1997, Annex J

- Have new standard operating policies and procedures been developed or implemented to use the capabilities of the new increment?
- Has the receiving organization developed plans for continuity of operations during the installation of the new increment?

c. Technology

- How dependent is the new increment upon new technologies (hardware and software)?
- What is the commercial tempo of change in the technology areas represented in the increment?
- How mature are the new technologies incorporated into the increment?
- Does the new increment introduce any new standards or protocols?
- Does the integration of the entire system (e.g., hardware, software, communications, facilities, management, operations, sustainment, personnel) present unusual challenges?
- Does the system include the necessary system administration capabilities?
- If the increment is primarily COTS, NDI, or GOTS (government-off-the-shelf), what is the past performance and reliability?
- For new technologies, what is the performance record in other applications?

d. Complexity

- How complex is the new increment (e.g., industry standard complexity metrics, or as compared to other fielded increments)?
- How many agents (government, contractors, sub-contractors) participated in the development of this increment?
- How stable are the system requirements?
- What is the proportional change to system hardware and software introduced by the new increment?
- What is the cumulative change to system hardware and software since the last full operational test?
- Is the new system (including the increment of interest) to be integrated with other systems during development or deployment?
- How complex are the external system interface changes (hardware, software, data) in the new increment?

- How complex are the user interactions with the new increment?
- How complex are the interactions of the new increment with the fielded databases?
- To what extent does the new increment introduce changes that place in jeopardy or modify the system data structures?
- Does the new increment implement a change in executive software (operating system or database management system)?

e. Safety

- Does the system present any safety hazards to the operators or operational environment?

f. Security

- Does this system require multi-level security?
- Can the new increment affect the security or vulnerability (to information warfare) of the installed system (e.g., have external interfaces been added)?
- Does the new increment modify or possibly interfere with information assurance protective measures?
- If it has external interfaces, has the system been tested for unauthorized access?

In addition to the above general matters, there may be other overriding concerns – conditions that are potentially so important that, if they are present, a thorough and comprehensive operational testing effort is mandatory.

2. Identification and Evaluation of Mission Impact of Increment Failure

The mission impact assessment should consider the impact of the possible failure of the new increment on the mission of the whole system. This assessment should also consider increment-related changes in concept of operations, maintenance concept, training concept, and the roles of the increment in a possible "system of systems" configuration. Table A-l provides a typical set of potential mission impact assessments, related to resolution of system critical operational issues (COIs).

Table A-1. Degree of Mission Impact

Effect on Mission	Definition
Minor Impact	Increment failure would cause noticeable problems, but no major interference with mission accomplishment. System COIs can be satisfactorily resolved, even without increment success.
Moderate Impact	Increment failure could cause substantial degradation of mission-related capabilities. System COIs are moderately dependent upon increment performance.
Major Impact	Element is required for mission success. System COIs are critically dependent upon increment performance.
Catastrophic Impact	The element is required for mission success, and its malfunction could cause significant damage to the installed system, to other interconnected systems, or to personnel.

The evaluator must make a mission impact assessment for each of the mission areas affected by the new increment. The total impact to the mission is then assessed as the highest impact noted for any area of concern, or at a level above the highest level noted if many lower potential impacts are evident.

3. Assessing the Risk of a System Increment

When the mission impact and likelihood of failure of an increment have been determined, the risk assessment may be made as the product of these two basic elements. However, in assessing risk, the mission impact should be weighted more heavily than the likelihood of failure. The methodology in Appendix B presents a direct method for determining the proper level of OT from the levels of mission impact and likelihood of failure obtained from the analysis in Appendix A.

APPENDIX B

DETERMINING APPROPRIATE OT&E FOR SYSTEM INCREMENTS

The specific evaluation procedures presented in this appendix are provided as examples, rather than requirements.

1. Multiple Levels of OT&E for System Increments

The tester must determine the level of operational testing that most effectively provides "affordable confidence" that an increment will meet mission needs. A range of test activities should be considered and matched to the risk of the specific system increment. The range of operational testing for increments other than the core increment extends through four levels, from an abbreviated assessment to a full, conventional operational test and evaluation.

For each of these four levels of OT&E, it is presumed that the exit criteria from DT have been satisfied and that all previously deployed increments are functioning properly prior to the fielding of any new increment. It is further presumed that user representatives have developed appropriate concepts of operations, policies, procedures, training, support, and contingency plans for a full operational deployment. Where these are lacking, the OTA must consider associated risk factors as high, increasing the level of OT required. It is also presumed that the exit criteria from developmental testing have been satisfied and that all previously deployed increments are functioning properly prior to the fielding of any new increment. Regardless of the level of testing actually executed, the OTA is obligated to implement applicable OSD policies in the course of testing such as the DOT&E policy regarding information assurance.

The detailed design of testing activities at each level of testing must be based upon the fundamental objective of evaluating the ability of the tested system to accomplish its mission goals when deployed. The increment's mission goals are expressed in the measures of effectiveness and suitability and the COIs stated in the Test and Evaluation Master Plan (TEMP).

Level I Test – After complete and successful developmental testing, permit limited fielding and assess feedback from the field (by the OTA) prior to full fielding. Contractor presence is permitted during the Level I test. Plans for recovery from failures, prepared by the Program Management Office (PMO) and validated by the OTA, must be in place prior to limited fielding.

Level I testing is appropriate for maintenance upgrades and increments that provide only minor system enhancements, pose an insignificant risk, and can be easily and quickly removed. Increments judged to be of sufficiently low risk for Level I testing will usually be delegated to the Component for testing, evaluation, and fielding decisions. The OTA prepares an assessment to support any fielding decision. A copy of the assessment is to be provided to the DOT&E. Key features of Level I testing are:

- It is essentially a DT effort.
- The OTA monitors selected developmental/technical testing activities.

- Limited fielding is permitted prior to the OTA evaluation.
- The OTA prepares an assessment for the CAE to support a fielding decision by the Milestone Decision Authority.

Level II Test – Assessment performed by an OTA primarily using DT data and independent "over-the-shoulder" observations. The OTA may prescribe and observe operationally realistic test scenarios in conjunction with DT activities. Contractor presence is permitted during the Level II test. DOT&E may observe any OT activity.

Level II testing should be applied to increments that provide only minor system improvements and present a minor risk. Such lower risk increments have only minimal potential to impact other system applications, and cannot disrupt the basic system's ability to support the mission. After thorough Level II testing, an increment may be deployed to selected operational sites for additional feedback (collected by the OTA) if needed prior to full fielding. Features of the Level II test are:

- It is essentially a combined DT/OT testing effort.
- The assessment is based primarily upon close monitoring of selected developmental/technical activities, and upon DT results.
- Prior to the limited fielding, plans must be in place for recovery from failures.
- The OTA evaluates the limited fielding results and reports on the operational effectiveness and suitability to the CAE to support a fielding decision by the MDA.
- A copy of the evaluation report is provided to DOT&E.
- For non-delegated increments, DOT&E will prepare an independent evaluation of the operational effectiveness and suitability for the OSD MDA regarding the fielding decision.

Level III Test – OTA personnel coordinate the Level III test (which is carried out by user personnel in an operational environment) and evaluate the operational effectiveness and suitability using primarily independently collected OT data. The Level III Test is conducted at one or more operational sites. In addition to normal user operations, the OTA may prescribe that scripted test events be executed and observed. Level III testing may be conducted in two phases. The Program Management Office controls Phase I, allowing contractors to fine-tune the system, but the OTA supervises Phase II, which defines an operational period without PMO or contractor participation. OT evaluators are allowed during both phases.

The Level III Test is suitable for increments supporting modest, self-contained, system improvements that present a moderate level of risk, but are limited in the potential disruption to an installed system. Features of Level III testing are:

- Actual operators are at the operational site(s) performing real tasks.

- The emphasis is on assessment and evaluation.
- It is less formal than a full operational test.
- Prior to fielding, plans are in place for recovery in the event of failure.
- The OTA prepares an evaluation of operational effectiveness and suitability for the CAE. For non-delegated increments, DOT&E will prepare an independent evaluation of the operational effectiveness and suitability for the OSD MDA regarding the fielding decision.
- A copy of the evaluation report is provided to DOT&E.

Level IV Test – Determine the operational effectiveness and suitability of a new increment by evaluating affected COIs under full OT constraints. This is the highest level of operational test and the most comprehensive. The OTA carries out test events in an operational environment. The OTA evaluates and reports on the operational effectiveness and suitability of a new system increment based upon all available data, especially independently collected OT data. Representatives of DOT&E monitor the test events for the OSD oversight programs. In special cases, the verification of minor capabilities and secondary issues may be relegated to lower levels of testing. Level IV testing must comply with all provisions of the DoD 5000 series regulations.

2. Matching OT&E to Risk Assessment

The OT&E Action Determination Matrix shown in Table B-1 forms the basis for relating the assessed failure potential (threat to success) and mission impact to an appropriate level of OT&E. The matrix provides for the four levels of OT&E described in the last section.

Table B-1. OT&E Action Determination Matrix

	Effect on Mission			
Failure Potential	**Minor Impact**	**Moderate Impact**	**Major Impact**	**Catastrophic Impact**
Insignificant	I	I-II	II-III	III-IV
Low	I-II	II-III	III-IV	IV
Moderate	II-III	III-IV	III-IV	IV
High	III-IV	III-IV	IV	IV

APPENDIX C

RESPONSIBILITIES FOR AND SCHEDULE OF OT&E ACTIONS

1. Responsibilities

a. Operational Test Agency – With regard to the OT&E for a follow-on system increment, the OTA is responsible for:

- Determining the type of data and level of detail required for assessing the threats to increment success.
- Collecting and analyzing information concerning potential threats to the success of the system increment, and determining the likelihood of failure based upon those threats.
- Determining the type of data and level of detail required for assessing the potential mission impact of the failure of a system increment.
- Collecting, analyzing, and determining the potential mission impacts associated with the system increment.
- Determining an appropriate level of OT&E according to the risk assessment.
- Developing and presenting a test concept briefing to the DOT&E.
- Developing and coordinating the applicable level of operational test plans.
- Validating recovery plans prior to deployment of an increment to any operational test sites.
- Conducting the approved level of OT&E.
- Developing the applicable independent evaluation report and providing it to the appropriate organizations.
- Making operational effectiveness and suitability recommendations.

b. Program Management Office – The PMO is responsible for:

- Providing the programmatic data required to evaluate threats to the success of the new increment to the OTA action officer and user representative.
- Providing the technical information requested to support the evaluation of each significant threat to the increment's success.
- Developing recovery plans prior to fielding of an increment to any operational test sites.
- Certifying the increment's readiness for OT&E.

c. User – The user (or user representative) is responsible for:

- Participating in the planning and execution of the OT&E.
- Providing the OTA with information regarding mission impacts of increment failure.
- Assisting the PMO in developing recovery plans, including workarounds for possible increment malfunctions.

d. Director, Operational Test and Evaluation (DOT&E) – In addition to the statutory and regulatory OT responsibilities of DOT&E,[1] the office is responsible for:

- Providing guidance as needed in the preparation of risk assessments and determining the appropriate level of OT.
- Evaluating and responding to the operational test concept and approving if appropriate.
- Evaluating and responding to the operational test plan and approving if appropriate.

2. SCHEDULE OF ACTIVITIES

Table C-1 shows key OT activities, schedules, and responsibilities.

[1] As described in USC Title X, DoDD 5141.2, DoDD 5000.1, DoDI 5000.2, and other applicable documents.

Table C-1. Operational Testing Actions, Schedules, and Responsibilities

Action	When	Responsible Agency	Approval Agent	Comments
Prepare Program Risk Assessment	As soon as data becomes available	OTA	Component	OTA and PM conduct assessments with information provided by PM and with participation of user and other appropriate Component agencies.
Determine Level of Operational Test	Upon completion of risk assessment	OTA	Component	Based on risk assessments.
Develop Test Concept and Outline Operational Test Plan	Upon decision regarding level of OT	OTA	Component	Brief elements within Component, as required.
Present Test Concept Briefing to DOT&E	At least 120 days prior to start of OT	OTA	DOT&E	If approved by DOT&E, proceed to next step. Otherwise, revise test concept and brief again.
Complete Operational Test Plan[2]	Submit to DOT&E at least 60 days prior to start of OT	OTA	Component, DOT&E	Brief elements within Component, as required.
Conduct Operational Test		OTA	Component	DOT&E may observe. Data supplied to DOT&E for non-delegated increments.
Analyze Test Results and Prepare Report	Complete within 90 days of test completion	OTA	Component	OTA briefs DOT&E and PM, plus other Component elements as required, on test results. DOT&E prepares independent evaluation for non-delegated increments.
Prepare and Present Deployment Recommendations to MDA		OTA DOT&E	MDA	OTA provides recommendations to the (Component) MDA for delegated increments. DOT&E provides recommendations to the OSD MDA for non-delegated increments.

[2] Following this stage, the PM or Program Executive Officer will need to certify that the increment is ready for operational testers to begin evaluation at the appropriate level.