Technology Readiness Assessment Guidebook

June 2023

Office of the Executive Director for Systems Engineering and Architecture

Office of the Under Secretary of Defense
for Research and Engineering

Washington, D.C.

Technology Readiness Assessment Guidebook

Office of the Executive Director for Systems Engineering and Architecture
Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301
osd-sea@mail.mil
https://www.cto.mil/sea/

Approved by
Principal Deputy Executive Director for Systems Engineering and Architecture
Office of the Under Secretary of Defense for Research and Engineering
June 2023

Technology Readiness Assessment Guidebook

Date	Change	Rationale

This page is intentionally blank.

Contents

Figures

Tables

Preface

A Technology Readiness Assessment (TRA) is an evaluation to determine whether a technology is mature enough to include in a larger system. A TRA examines program concepts, technology requirements, and demonstrated technology capabilities. This guide is intended to assist Department of Defense (DoD) acquisition programs to conduct high-quality TRAs and to identify the critical technology elements (CTEs) a program should assess through a TRA.

A TRA involves a fundamental metric, the Technology Readiness Level (TRL), first developed at the National Aeronautics and Space Administration (NASA) in the 1970s. In 1999, the Government Accountability Office (GAO) (then General Accounting Office) published an influential report, *Best Practices: Better Management of Technology Can Improve Weapon System Outcomes,* concluding that using immature technology increased program risk and recommending wider use of TRLs. The report illustrated that maturing new technologies before they were incorporated into a product was perhaps the most important determinant of the success of the eventual product. Incorporating immature technologies into products increased the likelihood of cost overruns and delays in product development.

DoD formally endorsed the use of TRLs in 2001. DoD produced a TRA Deskbook in 2003 and revised the guidance in 2005, 2009, and 2011. This guidebook incorporates and supersedes TRA 2009 and TRA 2011, and it incorporates recommendations from the January 2020 GAO *Technology Readiness Assessment Guide–Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects* (GAO 2020), which describes characteristics and best practices of high-quality TRAs. This TRA Guidebook also discusses TRAs from the perspective of the DoD Adaptive Acquisition Framework pathways introduced in 2020 and discusses additional measures, such as Manufacturing Readiness Levels and System Readiness Levels, that DoD programs use.

For DoD, the main purpose of the TRA is to provide the Program Manager with a comprehensive assessment of technical risks associated with technologies to be incorporated into a program. This assessment includes whether the technologies have been demonstrated in a relevant environment in order to satisfy certification requirements for Milestone B in accordance with 10 USC 4252, “Major Defense Acquisition Programs: Certification Required before Milestone B or Key Decision Point B Approval” (January 2021).

The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) prepared this guide in cooperation with defense subject matter experts (SMEs). OUSD(R&E) will provide periodic updates to incorporate comments and new information.

1 Introduction

This guidebook is intended to assist Department of Defense (DoD) programs to initiate, organize, and conduct high-quality Technology Readiness Assessments (TRAs) on acquisition programs. It supersedes DoD TRA guidance published in 2009 and 2011 and incorporates recommendations from the 2020 Government Accountability Office (GAO) *Technology Readiness Assessment Guide–Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects* (GAO 2020).

TRAs are not unique to DoD as other Government agencies and commercial developers conduct TRAs. This guide draws on relevant sources and focuses on guidance applicable to DoD acquisition programs. Whereas DoD policy is mandatory, this guidance is not mandatory but offers recommendations and best practices. The guidebook may refer to mandatory statute and policy for information.

The following introductory paragraphs provide background on the benefit of TRAs, the development of the GAO 2020 guide, and other sources of education, policy, and guidance. Section 2 discusses the concepts of CTEs and Technology Readiness Levels (TRLs) essential to TRAs. Sections 3 and 4 highlight detailed recommendations from GAO 2020. Section 5 discusses TRAs in relation to the DoD acquisition pathways and phases outlined in DoD Instruction (DoDI) 5000.02, “Operation of the Adaptive Acquisition Framework (AAF).” Section 6 discusses additional measures applicable to DoD Major Defense Acquisition Programs (MDAPs). The appendices include practices for identifying CTEs, a suggested TRA outline, and other supplementary information.

1.1 Benefit of Conducting TRAs

Experts agree that following an evidence-based and repeatable process that focuses on how the end user plans to employ the technology, leads to enhanced TRA outcomes for Program Managers (PMs) and leadership. TRAs help programs make decisions to safeguard technical development from undue risk. They provide PMs and program leadership with information for making decisions about whether technology is sufficiently mature and can move to the next acquisition phase or whether it needs additional maturation work or should be discontinued. The TRA report, resulting from the assessment, informs program management decisions regarding cost, schedule, and risk.

TRAs provide a standard framework for applying measures and methods that identify potential technical risks. The program can respond to these identified risks by preparing a Technology Maturation Plan (TMP), which outlines the steps and level of effort required to mature the identified risky (immature) technologies. TMPs are discussed in Section 4.5.

1.2 Statute and DoD Policy

The following statute and DoD policies state requirements for TRAs:

- 10 USC 4252[1] requires a TRA for MDAPs before a Milestone B decision; it states

  > *MDAPs may not receive Milestone B approval until the milestone decision authority. . . certifies that the technology in the program has been demonstrated in a relevant environment, as determined by the milestone decision authority on the basis of an independent review and technical risk assessment conducted under section 4272.*[2]

- DoDI 5000.88, "Engineering of Defense Systems," establishes policy and assigns responsibilities in accordance with DoD Directive (DoDD) 5000.01, "The Defense Acquisition System." Programs already conducting an Independent Technical Risk Assessment (ITRA) should follow TRA guidance to assess technologies but are not required to prepare the corresponding TRA report. DoDI 5000.88 states

  > *for programs for which an ITRA is conducted, a TRA report is not required. Programs will continue to assess and document the technology maturity of all critical technologies*[3] *consistent with the technology readiness assessment guidance. ITRA teams may leverage technology maturation activities and receive access to results in order to perform independent technical reviews and assessments.*

  DoDI 5000.88 requires MDAPs and Acquisition Category (ACAT) I and II programs to employ the DoD Systems Engineering Plan (SEP) Outline and the Defense Technical Risk Assessment Methodology (DTRAM) (OUSD(R&E)) to incorporate metrics into the SEP and collect objective, quantitative data for TRAs.

- DoDI 5000.86, "Acquisition Intelligence," establishes policy and assigns responsibilities in accordance with DoDD 5000.01. Pursuant to this issuance, the Under Secretary of Defense for Research and Engineering (USD(R&E)) "coordinates and provides acquisition intelligence considerations for use in DoD Component and USD(R&E) independent technology readiness assessments."

1.3 TRAs in the Commercial Sector

Commercial organizations also use TRAs to evaluate internal investments and research and development efforts that could be used on future government contracts. Examples of ways in

[1] 10 USC 4252 (certification before Milestone B) replaced 10 USC 2366b.
[2] 10 USC 4272 (Independent Technical Risk Assessments) replaced 10 USC 2448b.
[3] This guide uses the term "critical technology element (CTE)" in place of "critical technology (CT)." The term CT may appear in examples and related sources and is equivalent in meaning.

which commercial organizations have developed processes to follow DoD's TRA steps include the following:

- Identifying potential systems and programs as likely recipients of the technology.
- Using the research team to perform the TRA, supplemented when necessary by internal technology readiness experts.
- Having SMEs and business leaders review assessments for accuracy and to ensure the technology is progressing adequately.
- Relying on mechanisms to change the research plan to accelerate, slow down, or retire the development based upon the technical readiness assessment.
- Ensuring the assessment is objective, particularly with regard to demonstration environments, as system requirements evolve.

1.4 GAO 2020 Guide

GAO 2020 is a current, thoroughly researched and compiled guide for conducting a TRA. While the GAO 2020 recommendations are not specific to one type of organization or agency, the GAO 2020 development involved a rigorous process that considered a variety of practices by different types of organizations (including DoD) that were well-researched and vetted by specialists and experts. For this reason, DoD has used GAO 2020 as a resource for compiling recommendations in this TRA Guidebook.

To document generally accepted best practices, GAO worked with practitioners and technical experts from across the Federal Government including DoD, commercial industry, nonprofit organizations, and academia. Among other agencies, GAO studied DoD's TRA practices, case studies, and policies. From 2013 to 2019, GAO conducted meetings, focus groups, and interviews with more than 180 experts to collect information and elicit feedback on drafts of the guide. To reflect a range of expertise and viewpoints, GAO consulted with specialists from science and technology (S&T), systems engineering, nuclear engineering, software and computer sciences, risk management, acquisition policy, and program management.

GAO released a public draft (GAO-16-410G) in August 2016 for a 12-month comment period. From August 2017 to June 2019, representatives from several mission teams adjudicated more than 400 comments. The panel vetted each comment and placed it in one of two categories: (1) actionable, meaning the comment could be further adjudicated; or (2) not actionable because the comment did not align with the broader opinion of the specialist community, was outside the guide's scope, was factually erroneous, or had no basis for specific action. GAO documented the adjudication in the GAO 2020 guide.

2 Critical Technology Elements and Technology Readiness Levels

TRAs involve two essential concepts, critical technology elements (CTEs) and Technology Readiness Levels (TRLs).

2.1 Definition and Use of CTEs and TRLs

A CTE is a new or novel technology on which a program or platform depends to successfully develop a system or to meet an operational threshold. A CTE may be hardware, software, or a process critical to the performance of a larger system or to the fulfillment of a key objective, such as a cyber-related capability.

OUSD(R&E) defines a technology element as "critical" if the system being acquired depends on this technology element to meet operational requirements and if the technology element or its application is either new or novel or in an area that poses major technological risk during detailed design or demonstration.

Programs should identify and document CTEs as early as possible, document the process for choosing the CTEs in the Acquisition Strategy, and, for MDAPs, assess the maturity before Milestone A and in the Analysis of Alternatives.

During a TRA, evaluators examine program concepts, technology requirements, and demonstrated technical capabilities to determine each CTE's maturity. They assign each CTE a TRL between 1 and 9, with 9 representing the most mature. TRLs are not a measure of design validity, but they indicate the specific CTE's level of maturity at the time it is measured and therefore the CTE's relative readiness to be incorporated into the larger system.

2.2 CTEs and Critical Program Information

CTEs may often overlap with critical program information (CPI). The emphasis of CTEs is to identify technologies essential to the system design that need to be matured, whereas the emphasis on CPI is to identify potential vulnerabilities and security needs in operations. TRA teams should review the Technology and Program Protection Guidebook to see if any technologies have been identified as CPI. Any CPI technologies would be strong candidates to also be CTEs whose maturity would need to be assessed.

2.3 TRL Concept for Hardware

Many TRAs evaluate hardware CTEs that are being developed for weapon systems, communications systems, soldier systems, and so forth. Table 2-1 shows the TRLs DoD uses to assess hardware. It also lists typical documentation that evaluators should extract or reference to support a TRL assignment.

Table 2-1. DoD Hardware TRL Definitions, Descriptions, and Supporting Information

TRL	Definition	Description	Supporting Information
1	Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development (R&D). Examples might include paper studies of a technology's basic properties.	Published research that identifies the principles that underlie this technology. References to who, where, when.
2	Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.	Publications or other references that outline the application being considered and that provide analysis to support the concept.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.	Results of laboratory tests performed to measure parameters of interest and comparison to analytical predictions for critical subsystems. References to who, where, and when these tests and comparisons were performed.
4	Component and/or breadboard validation in a laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared with the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.	System concepts that have been considered and the results of testing laboratory-scale breadboard(s). References to who performed this work and when. Provides an estimate of how breadboard hardware and test results differ from the expected system goals.
5	Component and/or breadboard validation in a relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include "high-fidelity"	Results from testing a laboratory breadboard system are integrated with other supporting elements in a simulated operational environment. How does the "relevant environment" differ from the expected operational environment? How do the test results compare with expectations? What problems, if any, were encountered? Was the breadboard system refined

TRL	Definition	Description	Supporting Information
		laboratory integration of components.	to more nearly match the expected system goals?
6	System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment.	Results from laboratory testing of a prototype system that is near the desired configuration in terms of performance, weight, and volume. How did the test environment differ from the operational environment? Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
7	System prototype demonstration in an operational environment.	Prototype near or at planned operational system. Represents a major step up from TRL 6 by requiring demonstration of an actual system prototype in an operational environment (e.g., in an aircraft, in a vehicle, or in space).	Results from testing a prototype system in an operational environment. Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
8	Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.	Results of testing the system in its final configuration under the expected range of environmental conditions in which it will be expected to operate. Assessment of whether it will meet its operational requirements. What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before finalizing the design?
9	Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation(OT&E). Examples include using the system under operational mission conditions.	OT&E reports.

2.4 TRL Concept for Software

If the program develops the software and the software is in itself a CTE, it should appear as a software CTE. The hardware technology classification may include software that executes on the hardware if (1) the software is not being developed or modified as part of the acquisition, or (2) the software is not the reason for placing the element on the CTE list.

Table 2-2 shows the TRLs DoD uses to assess software. Although the TRL definitions are similar to those for hardware, the examples and supporting information to support the assessment differ. During planning, assessment teams may add supporting information items that are appropriate for the technology under assessment.

Table 2-2. DoD Software TRL Definitions, Descriptions, and Supporting Information

TRL	Definition	Description	Supporting Information
1	Basic principles observed and reported.	Lowest level of software technology readiness. A new software domain is being investigated by the basic research community. This level extends to the development of basic use, basic properties of software architecture, mathematical formulations, and general algorithms.	Basic research activities, research articles, peer-reviewed white papers, point papers, early lab model of basic concept may be useful for substantiating the TRL.
2	Technology concept and/or application formulated.	Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies using synthetic data.	Applied research activities, analytic studies, small code units, and papers comparing competing technologies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. The level at which scientific feasibility is demonstrated through analytical and laboratory studies. This level extends to the development of limited functionality environments to validate critical properties including cybersecurity and analytical predictions using non-integrated software components and partially representative data.	Algorithms run on a surrogate processor in a laboratory environment, instrumented components operating in a laboratory environment, laboratory results showing validation of critical properties.

TRL	Definition	Description	Supporting Information
4	Module and/or subsystem validation in a laboratory environment (i.e., software prototype development environment).	Basic software components are integrated to establish that they will work together. They are relatively primitive with regard to efficiency and robustness compared with the eventual system. Architecture development initiated to include interoperability, reliability, maintainability, extensibility, scalability, and security issues. Emulation with current/legacy elements as appropriate. Prototypes developed to demonstrate different aspects of eventual system.	Advanced technology development, stand-alone prototype solving a synthetic full-scale problem, or stand-alone prototype processing fully representative data sets.
5	Module and/or subsystem validation in a relevant environment.	Level at which software technology is ready to start integration with existing systems. The prototype implementations conform to target environment/interfaces. Experiments with realistic problems. Simulated interfaces to existing systems. System software architecture established. Algorithms run on a processor(s) with characteristics expected in the operational environment.	System architecture diagram around technology element with critical performance requirements defined. Processor selection analysis, Simulation/Stimulation (Sim/Stim) Laboratory buildup plan. Software placed under configuration management. Commercial-of-the-shelf/ government-off-the-shelf (COTS/GOTS) components in the system software architecture are identified.
6	Module and/or subsystem validation in a relevant end-to-end environment.	Level at which the engineering feasibility of a software technology is demonstrated. This level extends to laboratory prototype implementations on full-scale realistic problems in which the software technology is partially integrated with existing hardware/software systems. Cybersecurity verification should be included in the testing.	Results from laboratory testing of a prototype package that is near the desired configuration in terms of performance, including physical, logical, data, and security interfaces. Comparisons between tested environment and operational environment analytically understood. Analysis and test measurements quantifying contribution to system-wide requirements such as throughput, scalability, and reliability. Analysis of human-computer (user environment) begun.

TRL	Definition	Description	Supporting Information
7	System prototype demonstration in an operational, high-fidelity environment.	Level at which the program feasibility of a software technology is demonstrated. This level extends to operational environment prototype implementations, where critical technical risk functionality is available for demonstration and a test in which the software technology is well integrated with operational hardware/software systems.	Critical technological properties, including cybersecurity, are measured against requirements in an operational environment.
8	Actual system completed and mission qualified through test and demonstration in an operational environment.	Level at which a software technology is fully integrated with operational hardware and software systems. Software development documentation is complete. All functionality and cybersecurity measures tested in simulated and operational scenarios.	Published documentation and product technology refresh build schedule. Software resource reserve measured and tracked. All severity 1 and severity 2 defects are resolved/confirmed, and a reasonably low level of severity 3 defects remain open.
9	Actual system proven through successful mission-proven operational capabilities.	Level at which a software technology is readily repeatable and reusable. The software based on the technology is fully integrated with operational hardware/software systems. All software documentation verified. Successful operational experience. Sustaining software engineering support in place. Actual system.	Production configuration management reports. Defect resolution system and process is in place for deployed software to address defects discovered in production.

2.5 Additional TRL Definitions

Table 2-3 provides additional TRL definitions.

Table 2-3. Additional Definitions of TRL Descriptive Terms

Term	Definition
Breadboard	Integrated components that provide a representation of a system/subsystem and that can be used to determine concept feasibility and to develop technical data. Typically configured for laboratory use to demonstrate the technical principles of immediate interest. May resemble final system/subsystem in function only.

Term	Definition
High Fidelity	Addresses form, fit, and function. A high-fidelity laboratory environment would involve testing with equipment that can simulate and validate all system specifications within a laboratory setting. High fidelity models are accredited to represent the system for their defined purpose.
Low Fidelity	A representative of the component or system that has limited ability to provide anything but first-order information about the end product. Low-fidelity assessments are used to provide trend analysis.
Model	A functional form of a system, generally reduced in scale, near or at operational specification. Models will be sufficiently hardened to allow demonstration of the technical and operational capabilities required of the final system.
Operational Environment	Environment that addresses user operational requirements and specifications required of the final system to include platform/packaging.
Prototype	A physical or virtual model used to evaluate the technical or manufacturing feasibility or military utility of a particular technology or process, concept, end item, or system.
Relevant Environment	Testing environment that simulates both the most important and most stressing aspects of the operational environment.
Simulated Operational Environment	Either (1) a real environment that can simulate all the operational requirements and specifications required of the final system or (2) a simulated environment that allows for testing of a virtual prototype. Used in either case to determine whether a developmental system meets the operational requirements and specifications of the final system.

2.6 Assessing Hardware CTEs

Applying the TRL definitions to assess the maturity of hardware technologies appears to be straightforward. For a particular technology, evaluators assign the level of technical readiness that best describes the accomplishments and evidence according to the TRL definitions. In practice, this approach is more difficult than it appears because the TRL definitions often fail to account for all situations.

TRL definitions describe characteristics such as the *scale of application* or the *environment*. The scale of application ranges from device to component, subsystem, and system. Environment includes the laboratory, mathematical models, physical simulations, field tests, and operational use. A TRA should present increasingly representative tests to demonstrate the technologies in relation to the characteristics in the definition.

Some TRL definitions mention characteristics directly; others do not. When a technology fails to match the literal definition during the assessment, the evaluator should make a judgment about the relevance of what the technology has accomplished and decide whether the accomplishment equates with the TRL definition.

Environment is perhaps the most difficult characteristic to interpret. Both TRL 5 and TRL 6 depend on performing in a *relevant environment*. Although the details of a relevant environment depend on the intended use of a technology, the TRL criteria are as follows:

- A relevant environment is a set of stressing conditions, representative of the full spectrum of intended operational employments, which are applied to a CTE as part of a component (TRL 5) or system/subsystem (TRL 6) to identify whether any design changes to support the required (threshold) functionality are needed.

To assess whether a technology can perform in the full range of required operational employments, it is not enough to conduct only one or a few demonstrations under only the most favorable conditions, or in a few useful environments. An effective assessment requires a body of data or accepted theory to support, with confidence, that the technology will be effective in the full spectrum of employments.

Demonstration of a CTE as part of a component or system /subsystem in a relevant environment requires successful trial testing that either:

- Validates that the CTE satisfies the required functionality across the full spectrum of intended operational employments

  or

- Validates that the CTE satisfies the functional need for important, intended operational employment(s) and then uses accepted/approved analytical techniques to extend confidence in supporting the required functionality across the required, intended operational employments.

As an example of a demonstration in a relevant environment, a CTE as part of a system or subsystem model or prototype might be tested in a high-fidelity laboratory environment or in a simulated operational environment.

The progression from TRL 6 to TRL 7 involves a shift in the scale of the demonstration of the technology. TRL 6 requires the CTE to be embedded or installed in a representative model or prototype. TRL 7 requires the CTE to be embedded or installed in a prototype of the planned operational system in the operational environment. At Milestone C, hardware (and software) CTEs should be able to achieve TRL 7.

While the details of an operational environment depend on the intended use of a CTE, following is a general description of an operational environment, and what it demonstrates:

- An operational environment is a set of conditions, representative of the full spectrum of employments, which are applied to a CTE, prototype (TRL 7) or actual system (TRL 8) to identify whether any previously unknown or undiscovered design problems might impact required functionality.

Demonstration of a CTE in an operational environment requires successful testing that either:

1. Validates that the CTE satisfies the required functionality across the full spectrum of operational employments

   or

2. Validates that the CTE satisfies the functional need for important, operational employment(s) and then uses accepted analytical techniques to extend confidence in supporting the required functionality over all the required operational employments.

As an example of a demonstration in an operational environment, a CTE as part of a system might be installed in an aircraft or vehicle, which is then tested in the operational conditions of a test bed or at a test range facility.

2.6.1 Aircraft

Aircraft are likely to have CTEs in aerodynamic configuration and controls, airframe structure and aeroelasticity, flight control systems, and propulsion. In addition, rotary-wing aircraft have CTEs in power transfer, rotor hub, and blades. CTEs could also be factors in mission equipment, secondary power, environmental control, and other systems, depending on the aircraft's missions. A variety of methods and facilities are used to demonstrate these different technologies.

TRAs for aerodynamic configuration and controls typically use demonstrations such as analysis, computational fluid dynamics (CFD) investigations, wind tunnel tests, and flight tests.[4] When aerodynamic configurations are significantly different from those of existing aircraft, TRAs may use free-flight models (manned or unmanned). Similarly, TRA evaluators may use a variety of methods and facilities for airframe, flight control, and other aeronautical disciplines.

---

[4] Programs may test a variety of scale models in different wind tunnels to obtain data for different flight conditions and mission phases.

2.6.2 Ground Vehicles

Most new military ground vehicle concepts and systems involve CTEs. Combat and tactical vehicles must meet requirements to address new threats and new or extended performance needs of operational forces. Utility and general-purpose vehicles—many of which are adapted versions of commercial vehicles—also may be required to provide special performance characteristics that exploit new technologies or novel application of existing technologies.

The automotive features of any class of military vehicles are likely to exploit CTEs in propulsive power, drive trains, platform stability, suspension systems, and endurance. Demonstrating the efficacy of CTEs requires various means of test, analysis, and verification. In most cases, these tests and analyses are unique to the military environment.

The protection requirements of combat and tactical vehicles are unique for combat environments. CTEs should be anticipated in vehicle-integrated passive protection against diverse weapon and munitions threats. Similarly, as threats increase and become more sophisticated, CTEs may provide reactive (e.g., explosive armor) or active (e.g., detection and attack of threat munitions) features. Evaluators often judge the maturity of these technologies by building on existing analysis and test capabilities.

2.6.3 Missiles and Guided Weapons

The development program for a missile or other guided weapon differs from that of a "platform" vehicle, and the program for a solid propellant rocket differs from that of a liquid propellant rocket. Most military missiles involve structure, propulsion, guidance, flight control, and payload. Each of these systems comprises numerous elements that must function together to meet the objectives of the system, and any of these elements may depend upon CTEs. Although each of the technologies will be discussed independently with associated TRLs/technology, the development of the system and associated TRL must be done from a system perspective because of interdependencies.

To assess the maturity of these CTEs, issues that should be considered in performance demonstrations include how the test environments compare with the real environments and how the performance exposes what is required. Each of the missile components can be tested to high TRLs. The integrated ordnance payload is often evaluated with a sled test (penetration testing) or arena testing (fragmentation testing); both tests are often required to achieve TRL 5-6. The fuze system can only achieve TRL 6 via flight test demonstration due to the required inclusion of the safe and arm function.

Missile structural integrity and flight control are highly interdependent. Structural bending modes, placement of accelerometers, control system time constants, aerodynamic loads and control moments, and reaction controls must work together to achieve stable, controlled flight.

Structural rigidity and inertial properties can first be computed during computer-aided design (CAD) and then confirmed by ground tests. Engineers determine aerodynamic characteristics by analysis and wind tunnel tests. High-fidelity, 6-degree-of-freedom (DOF) simulations can represent the complete missile in its intended flight environment. Components tested in hardware-in-the-loop (HWIL) simulations can reasonably be considered TRL 4.

Assuming flight accelerations and vibrations are important to the functioning of a component, testing that component while on a surrogate missile could support the component to achieve TRL 5. After the components have been integrated into a dynamically correct prototype missile and flown with preprogrammed maneuvers, the components are considered TRL 6 if the environment is relevant for those components.

Missile guidance systems can include a variety of sensor types. Several types of test environments are useful for particular types of sensors. These include anechoic chambers for radars and other radio frequency (RF) systems, terrain tables for visual and infrared (IR) detectors, towers overlooking tactical targets, captive carry on aircraft and missiles, and free flight. The maturity associated with these sensors depends on the fidelity of the relevant features of the environment and the fidelity of the test article when compared with the final product. If a tower can provide the correct viewpoint and range to a target and if motion is not important, perhaps a tower test of a prototype sensor can be adequate to assess TRL 5.

If motion is important, a captive carry test might be necessary to achieve TRL 5. As motion is almost always important to missile guidance systems, captive carry for TRL 5 and demonstration on a prototype or surrogate missile for TRL 6 are the norms.

For liquid fuel rockets, factors to consider include movement and metering of fuel and oxidizer, throttling or multiple starts, and cooling of the nozzle with fuel. Relevant conditions may include very low ambient pressures and longitudinal and lateral accelerations that can be achieved only in flight.

Air-breathing rockets must establish inlet performance and flammability limits over a wide range of Mach numbers and ambient pressures. Demonstrations are to include connected tests (inlet connected to an air source) to merit TRL 4 and free-flow tests including inlet, captive carry, and free-flight tests to merit TRLs 5 and 6, respectively, if the test articles of the free-flight tests are functionally representative prototypes.

2.6.4 Ships and Ship Systems

Ships are likely to have CTEs in hydrodynamic hull form, materials and structures, propulsion, drag reduction, and motion controls. Ship systems, such as sensors (radar/sonar), weapons (torpedoes/missiles), hotel (waste disposal/desalination/material movement), and aircraft interfaces (elevators), will require some additional CTEs. Ships also have CTEs related to survivability, such as signatures, countermeasures, and intact and damaged stability. A variety of methods and facilities are used to demonstrate these different technologies.

Ships are usually large and complex; therefore, prototyping of a complete system, such as a new hull form, is expensive and time consuming. The types of demonstrations used normally for ship hull-form technologies include analysis, CFD investigations, towing tank model scale tests, and land-based subsystem tests. For ship configurations that represent large departures from the existing base of knowledge, full-scale prototypes are usually needed.

Similarly, a variety of methods and facilities are used for structures and materials, motion control, and other ship-related disciplines. Torpedo development would follow an approach similar to that of a missile system. The technologies of active drag reduction are treated similarly to those of a propulsion subsystem, such as a new propeller, and would follow the propulsion approach. Passive drag reduction systems, such as hull shaping, are treated similarly to the hull form development approach.

2.6.5 Hardware for IT Applications

As an example of hardware for IT, Microelectromechanical Systems (MEMS) technology delivers computer displays in creative designs, such as a high-tech monocle or a helmet-mounted display (HMD) for operational environments that would not be suitable for laptops or other conventional displays.[5] Infantry soldiers are expected to carry the equivalent of a laptop computer with them. They require an ergonomic fit and form for their environment, which may include active combat, harsh weather, and traveling long distances on foot.

The military has tested some early prototypes of MEMS. Stryker vehicle commanders have the option to view the onboard battlefield computer with an HMD. Helicopter pilots have a prototype system with a digital display of the battlespace to increase situational awareness. These tests provided a technical readiness of TRL 6. Achieving a TRL 7 or higher would require the military to test the display in the infantry soldier’s operational environment.

2.6.6 Hardware for Space Systems

Environmental qualification testing (e.g., vacuum, temperature extremes, solar radiation, micrometeorite impact, etc.) for space system hardware is not the same as a "demonstration in a relevant environment" needed to substantiate TRL 6.

---

[5] MEMS projects images directly onto the retina. Essentially all light generated enters the eye, so the MEMS device is energy efficient and reduces demand on the local power supply. A system using MEMS is expected to be more rugged than a conventional system; for example, the display is readable in daylight and provides higher resolution.

2.7 Assessing Software CTEs

Software and process technologies have grown increasingly critical to defense systems, and it is important to distinguish them from hardware. In recent years, Services, such as the Navy, have made extra efforts to decouple hardware from software within traditional combat systems. Doing this helps to separate the hardware and software development processes so that software is not tied to slower developing hardware processes (Eckstein 2023). This move is an important nod to the importance of distinguishing hardware and software CTEs as well as the process for assessing them.

The definitions of TRLs applied to software involve several facets. At the application level are values of device, component, subsystem, and system for hardware and algorithms, software components, software programs, and software packages. Another facet includes the environment (or application)—integration issues, laboratory user environment issues, logical relationship issues, data environment issues, security environment issues, and possibly interface issues. Other system-wide facets include obsolescence, scalability, and throughput and are usually expressed in terms of system-wide requirements, but the hardware components often contribute to meeting these requirements.

The combination of these facets determines any TRL. When the accomplishment and the definition do not match, the assessor must use judgment regarding the relevance of what has been accomplished and ask whether the accomplishment is equivalent to the TRL definition.

In assessing software's technical readiness, the terms *relevant environment* and *operational environment* indicate a significant progression in accomplishing the demonstration and include cyber-congested and cyber-contested environments. Claiming technical readiness in a relevant environment (TRL 5 or higher) requires a detailed architecture that exposes all components and elements affecting the operation of the critical software element. Claiming technical readiness in an end-to-end relevant environment (TRL 6 or higher) requires evidence of performance on full-scale, realistic problems. Claiming technical readiness in an operational environment (TRL 7 or higher) requires evidence of the acceptable performance of the software element under operational factors such as system loading, user interaction, security, and realistic communications environment (e.g., bandwidth, latency, jitter).

3 Characteristics of a High-Quality TRA

This section outlines the characteristics that GAO 2020 offered as indicative of a high-quality TRA and the best practices associated with those characteristics. This section also discusses a TRA's limitations. References to "critical technology element (CTE)" and "critical technology (CT)" are equivalent.

3.1 Four Characteristics of a High-Quality TRA

In its research and discussions with experts from government, industry, non-profits, and academia, the GAO found that high-quality TRAs have four common characteristics: credibility, objectivity, reliability, and usefulness. Table 3-1 (adapted from GAO 2020) summarizes these characteristics and the best practices that support them.

Table 3-1. Characteristics of a High-Quality TRA

Characteristic	Description	GAO's Identified Best Practices to Achieve the Characteristic
Credible	Conducted with an understanding of the requirements that guide development of the critical technology elements (CTEs) and system, the relevant or operational environment in which it will function, and its integration or interaction with other technologies	• Is comprehensive and includes all of the key information identified in the Technology Readiness Assessment (TRA) plan • Identifies and has the expertise needed to conduct the assessment • Considers the newness or novelty of technologies and how they plan to be used as basis or selecting CTEs • Considers the operational performance environment and potential cost and schedule rivers as a basis for selecting CTEs • Considers the relevant environment as a basis for selecting CTEs • Considers the potential adverse interaction with other systems as basis for selecting CTEs • Selects CTEs during early development • Selects CTEs at a testable level
Objective	Based on objective, relevant, and trustworthy data, analysis, and information; and the judgements, decisions, and actions for planning and executing the assessment are free from internal and	• Is conducted by an independent and objective TRA team • Is based on a level of detail consistent with the detail (evidence) available • Includes all of the key information (evidence) obtained by the TRA team to conduct the assessment • Is based on quantitative and qualitative analysis to determine the number of CTEs

Characteristic	Description	GAO's Identified Best Practices to Achieve the Characteristic
	external bias or influence"	• Confirms the CTEs based on specific questions and requirements • Is based on test articles and results that have been verified by the TRA team • Assigns TRL ratings based on credible and verified evidence • Is verified by management with respect to the factual accuracy of the TRA report
Reliable	Follow a disciplined process that facilitates repeatability, consistency, and regularity in planning, executing, and reporting the assessment"	• Follows a reliable, disciplined, and repeatable process to select CTEs • Is reviewed by the TRA team to ensure the initial TRA plan has all the essential information • Has adequate time and resources to conduct the assessment • Documents the rationale used to select CTEs, including technologies not selected • Confirms the TRL definitions are still appropriate, and agreement is reached between the TRA team and the PM on the kinds of evidence needed to demonstrate that a goal or objective has been met • Has a documented TRA policy or guidance for preparing a report • Includes all the key information in the TRA report • Includes management's written response to the TRL rating in the TRA report including dissenting views • Documents lessons learned in the TRA report
Useful	Provide information that has sufficient detail and is timely and can be acted upon.	• Identifies the recipient or recipients of the TRA report • Is used for its stated purpose, such as to inform decision makers about whether a prescribed TRL goal has been met, or identify potential areas of concern or risk, among other purposes. • Identifies the actions to take for CTEs assessed as immature, such as considering an alternate or backup technology, developing a TMP, updating the program risk management plan, or updating the cost and schedule risk assessments • Is submitted in advance of a decision point or Stage Gate Review for leadership reviews

3.2 Understanding TRA's Limitations

3.2.1 Organizational Experience, Culture, and Bias Can Affect TRAs

Each organization that develops, manages, and integrates technology has its own set of goals and objectives. Organizations have different perspectives and experiences as they conduct TRAs, and their terms and definitions may vary across organizations. GAO 2020 cites "simulated environment," "relevant environment," and "operational environment" as terms that are easily deployed with different meanings in different organizations and programs. (See Section 2 for the DoD definitions of "relevant environment" and "operational environment.") Therefore, the quality of a TRA depends on communication among all the stakeholders and the assessment team that performs the evaluation.

Optimism can also influence TRA results. In today's competitive acquisition environment, and especially before contract award, contractor PMs can be overly optimistic about the maturity of certain technologies in an effort to secure funding and buy-in from stakeholders.

3.2.2 TRAs Depend on the Quality and Availability of Credible Data

TRAs establish technical maturity from a technology performance perspective. TRAs may not address design considerations such as reliability, system safety, producibility, manufacturing, human systems integration, or operational suitability; however, each of these design areas may affect the outcome of a TRA.

As with any report, the quality of a TRA depends on the accuracy and relevance of the report's inputs. In a TRA's case this is the artifacts, test data, analytical reports, documents, and information used to conduct the TRA assessment. These inputs may depend on and interact with other program elements that are outside the assessment scope or unavailable to the team conducting the TRA. It is important to account for components and systems that are out of scope because these could have an impact on the report's conclusions.

3.3 Human Systems Integration Considerations in TRA

TRA teams may use the following tools to assess human systems integration (HSI) readiness in conjunction with the TRA:

- The Comprehensive Human Integration Evaluation Framework (CHIEF) promotes understanding and assessment of HSI throughout the acquisition process. The framework includes an HSI Activity Model to conceptualize HSI activity in military acquisition. It establishes human factors and human computer interaction to develop a concise view of HSI in action. The core activity of HSI is the balancing of human capabilities and limitations with the affordances and constraints presented by system technology, to accomplish system objectives. A CHIEF provides a tool for assessing HSI during acquisition. A measurement approach, rating scales criteria, and a consolidated scoring matrix are created from lessons gathered on current system assessment measures, and refinement with HSI practitioners. The HSI Activity Model and CHIEF offer the potential to increase HSI understanding and awareness, leading to improved system outcomes across system acquisition.

- The Human Factors Risk Manager (formerly the Human Factors Workbench (HFW)) software suite is an integrated set of eight human factors tools designed to support a wide range of analyses that are typically carried out in safety-critical systems. These eight tools can be used independently or together.

- The Risk Identification: Integration and 'Ilities (RI3) is an Excel tool to identify technical risks that have hindered previous programs. It is intended to assist program managers and systems engineers in the development and transition of new technologies. If used as part of a coherent systems engineering strategy, this assessment will enable sound decisions and avoid cost overruns and schedule delays.

See also the DAU HSI Community of Practice website.

4 Initiating and Conducting High-Quality TRAs

This chapter discusses TRA roles and responsibilities and presents the GAO 2020 recommended five-step "best practices" process to conduct a high-quality TRA. It also describes the relationship between the TRA and an ITRA and provides the purpose and a checklist for a Technology Maturation Plan (TMP). References to "critical technology element (CTE)" and "critical technology (CT)" are equivalent.

4.1 Key Players and Roles and Responsibilities

Key players in the TRA process are as follows:

- The Milestone Decision Authority or Defense Acquisition Executive (DAE)
- The Component Acquisition Executive (CAE) or Program Executive Officer (PEO) and Science and Technology (S&T) Executive
- The Program Manager (PM)
    - Lead Systems Engineer (LSE) or Chief Architect if delegated by the PM
    - Responsible for tasking the independent entity to conduct the TRA
- The Under Secretary of Defense for Research and Engineering (USD(R&E))
- The team of independent SMEs

Key player roles and responsibilities are as follows:

- The Milestone Decision Authority or DAE:
    - Determines whether to approve the milestone decision or to defer until technology matures.
    - Determines whether or not the technologies of the program are under 10 USC 4252 based on independent review and assessment by USD(R&E), whose review and assessment are informed, in part, by the program TRA.
    - In case of technologies not demonstrated in a relevant environment, determines whether the PM's proposed risk-mitigation plans are adequate and, in turn, determines whether to issue a waiver under 10 USC 4252.
    - Determines whether risk can be reduced to an acceptable level by relaxing program requirements.

- The CAE or PEO and S&T Executive:
  - Approve the PM's TRA plan and assign additional participants as desired.
  - Review and approve the list of CTEs that pose potential risk to program success.
  - Review and approve the TRA final report and cover memorandum and include any additional material desired.
  - Transmit the completed TRA to USD(R&E). Raise unresolved issues with USD(R&E) to the Milestone Decision Authority.

The CAE may choose to make the Service S&T Executive a key participant in the TRA process. For example, the CAE may direct the S&T Executive to take responsibility for TRA management and execution. The CAE may assign the S&T Executive as a reviewer or signatory on MDAP Technology Development Strategies to support identification and management of CTEs leading up to Milestone B.

- The USD(R&E):
  - Receives the TRA plan.
  - Reviews the TRA plan provided by the PM and provides comments regarding TRA execution strategy as appropriate.
  - In conjunction with the PM and SME team, reviews the PM-provided list of CTEs and recommends additions or deletions.
  - Based on the TRA final report, provides the Milestone Decision Authority with an independent assessment and review concerning whether the technology in the program has been demonstrated in a relevant environment.
  - If a 10 USC 4252 waiver has been requested, provides a recommendation to the Milestone Decision Authority, with supporting rationale, as to whether a waiver should be granted.
  - Recommends technology maturity language for an Acquisition Decision Memorandum (ADM), noting conditions under which new technology can be inserted into the program.

- The PM, LSE, and Chief Architect:
  - Assess the technological risk in the program.
  - Plan funding of the program's risk-reduction activities so technologies reach the appropriate maturity levels before being incorporated into the program's Preliminary Design Review (PDR) and before Milestone B or another certification decision event. The TRA will be updated based on the PDR and source selection

results to ensure that knowledge obtained at PDR and in the proposals is available to inform the USD(R&E).

- In consultation with USD(R&E) and with PEO and CAE approval, identify the subject matter expertise needed to perform the TRA. Assign members of the SME team and inform the CAE, PEO, USD(R&E), and S&T Executive of the final membership.
- Familiarize the SME team with the program, the performance and technical requirements, and the designs under consideration.
- Identify possible CTEs for consideration by the SME team. Provide evidence of technology demonstration in relevant environments to the SME team for assessment, including contractor data as needed.
- Provide proposed risk-mitigation plans to address remaining technological risk with CTEs to the SME team, independent of levels of demonstration.
- Provide technical expertise to the SME team as needed. Prepare the TRA report that will include findings, conclusions, and other pertinent material prepared by the SMEs.
- Prepare the TRA report cover memorandum, which may include additional technical information deemed appropriate to support or disagree with SME team findings.
- Send the completed TRA through the PEO to the CAE for review and transmittal to USD(R&E), together with any additional information the CAE chooses to provide.
- Determine whether a waiver to the 10 USC 4252 certification requirement may be appropriate, and if so, request PEO and CAE approval to request the waiver.

- The SME team:
  - Works closely with the PM and LSE throughout the TRA process.
  - Reviews the performance, technical requirements, and designs being considered for inclusion in the program.
  - In conjunction with the PM and USD(R&E), reviews the PM-provided list of CTEs and recommends additions or deletions.
    - The SME team should make recommendations to the PM (with associated rationale) on the candidate technologies that are assessed in the TRA.
  - Assesses whether adequate risk reduction has been accomplished to enter Engineering and Manufacturing Development (EMD) (or other contemplated

acquisition phase) for all technologies, including demonstration in a relevant environment.

- The assessment is based on objective evidence gathered during events, such as tests, demonstrations, pilots, or physics-based simulations. Based on the requirements, identified capabilities, system architecture, software architecture, concept of operations (CONOPS), and/or the concept of employment, the SME team will evaluate whether performance in relevant environments and technology maturity have been demonstrated by the objective evidence.
- If demonstration in a relevant environment is not achieved, the SMEs will review the risk-mitigation steps identified by the PM and make a determination as to their sufficiency to reduce risk to an acceptable level.
- TRLs are a knowledge-based standard or benchmark but should not substitute for professional judgment tailored to the specific circumstances of the program.

o Prepares the SME comments in the TRA report including (1) the SME team credentials and (2) SME team findings, conclusions, and supporting evidence.

4.2 Five-Step Process for Conducting a High-Quality TRA

GAO 2020 proposed a five-step process for planning, assessing, and reporting a TRA (Figure 4-1). The process provides a consistent methodology based on government and industry best practices and can be used across programs to assess the maturity of CTEs. Using the steps, programs should be able to produce high-quality TRA reports that can be traced, replicated, and updated to inform decision makers at different stages. Each of the five steps is important for ensuring TRAs provide decision makers with high-quality information. The following subsections elaborate on the five steps.

Source: GAO 2020

Figure 4-1. Five Steps for Conducting a High-Quality TRA

4.2.1 Step 1: Establish a TRA Plan and Select a TRA Team

The TRA plan should define the purpose and scope, goal of the assessment, resources to be provided to support the assessment (i.e., funding and time to conduct the assessment), how dissenting views will be handled, and for whom the TRA is being conducted. In addition, the TRA plan should describe the system, specify the CTE definition and TRL definitions to use, identify potential CTEs to evaluate, and identify the expertise needed to select the TRA team members, along with any agreements, such as statements of independence.

The initial TRA plan includes the program master schedule that aligns with the Acquisition Strategy and is incorporated into the program's Integrated Master Schedule (IMS) budget documents, test plans, and a technical baseline description of the program's purpose, system, performance characteristics, and system configuration.

Once a TRA schedule has been established, the PM, Chief Systems Engineer, and other key stakeholders identify SMEs to serve on the TRA team. Subject matter expertise and independence from the program are the two principal qualifications for SME team membership. Members should be experts who have demonstrated current experience in the relevant fields and with assessing technology maturity. SME team members might be required to sign non-disclosure agreements and declare that they have no conflicts of interest. Section 4.2.1.2 discusses the TRA team in more detail.

The PM guides SME team members on their role in the TRA process, as outlined in the TRA plan. The PM should include an overview of the system, an overview of the TRA process, criteria for identifying CTEs, and examples and instructions for determining whether technologies have been demonstrated in a relevant environment. The PM should exploit planned demonstration events and tests to provide the data needed by the SME team. The TRA team and the PM may discuss and revise the plan (e.g., scope, schedule, funding, personnel) to ensure the approach is sound and understood. The level of detail in the TRA plan needs to comport with the level of detail (evidence) available about the program.

4.2.1.1 Purpose and Scope of a TRA Plan

DoD views the fundamental purposes of the TRA as (1) providing the PM with a comprehensive assessment of technical risk, and (2) supporting the USD(R&E)'s independent assessment of the risk associated with the technologies incorporated in the program—including whether the technologies of the program have been demonstrated in a relevant environment—so that the MDA is informed as to whether certification under 10 USC 4252 can be accomplished, whether a waiver is appropriate, and whether risk-mitigation plans are adequate. Thus, it is important to identify all appropriate technologies that bear on that determination. These technologies should be identified in the context of the program's systems engineering process, based on a comprehensive review of the most current system design and performance requirements, technology maturation tasks identified in the Integrated Master Plan, and the availability of alternative technologies for critical functions.

As the TRA team or SME team (also referred to as the "team") develops the plan, they should ensure that the assessment documents a level of detail (evidence) that is consistent with and available for the expected maturity level of the CTE. As an example, the amount of information available for technologies that are in the early stages of development would be less than for more mature technology.

GAO 2020 developed two categories of TRA assessments. These categories are useful for understanding why TRAs are conducted:

1. A "comprehensive assessment" of CTEs is conducted to inform leadership before a decision point or Stage Gate Review. The TRA compiles the evidence of a prescribed maturity or criteria to justify a decision such as whether to commit resources and approve a program's move to the next phase of development.
2. A "knowledge-building TRA" is used to evaluate the maturity of a CTE(s) to assess their progress during development.

According to GAO 2020, TRAs conducted as "comprehensive assessments" should apply the GAO's full range of best practices outlined in the GAO 2020; but for "knowledge-building TRAs" conducted for a narrower audience, the purpose can vary. For example, the purpose could be to learn about specific aspects of a technology's development, to identify risks, or to determine whether a more comprehensive TRA needs to be conducted before an upcoming decision point.

GAO 2020 outlines some helpful best practices for planning the TRA:

- Scope: Start by identifying the TRA's customer and the need for the TRA assessment.
  - Include measures that will quantify the TRA's results (e.g., the CTE definitions, TRL definitions, evidence sufficiency standards, etc.)
  - Tailor the TRA plan to suit the type of technology being evaluated.

- Schedule: Create a detailed schedule that includes decision points and leaves time for inevitable delays.
  - Ensure the schedule reflects realistic resources and level-of-effort estimates.

- Additional Planning Documents: Include a list of the SME/TRA team members and their bios and credentials (experience, qualifications, certifications, training).
  - This should speak to the independence of each team member and the reason for their inclusion. (See "Forming the TRA Team" below for additional context.)

4.2.1.2 Forming the TRA Team

An independent TRA team consists of SMEs who have demonstrated, current experience in the relevant fields and independence from the program. These SMEs identify or affirm the selection of CTEs, evaluate the maturity of those CTEs, and assign the TRL rating for each. The TRA team, usually assembled and guided by the PM, is responsible for planning, documenting, and completing the TRA. The TRA team should have access to program and contractor personnel and the data and information necessary to conduct and complete the assessment. The PM should guide SME team members on their role in the TRA process and should provide an overview of the system, the TRA process, and criteria for identifying CTEs. The PM also should provide examples and instructions for determining whether technologies have been demonstrated in a relevant environment.

A typical TRA team is composed of three to five SMEs with expertise in the fields of the technologies being assessed. Each SME should also have experience and training in evaluating technological maturity. The number of SMEs on the team can vary depending on the purpose or requirements of the TRA and the complexity of the knowledge and expertise needed to conduct the TRA.

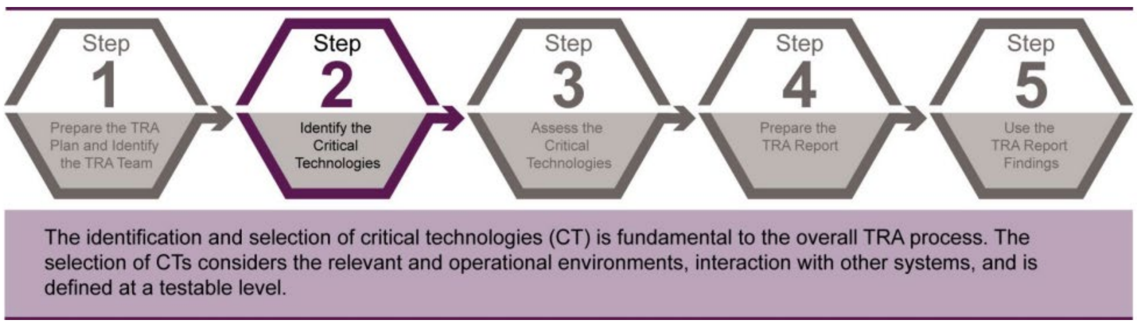
Following are a summary of the considerations and best practices for selecting the TRA team:

- Ensure that SMEs have demonstrated, current and relevant experience.
- Select SMEs that are independent from the program for which they are conducting the TRA. To ensure a successful independent assessment, the SME/TRA team is convened and bases its CTE evaluation on documentation provided by the PM. These experts may be selected from laboratories or other research entities that are independent of the program or other Federal research and development centers or from SMEs who are within the but not the specific program.
    - Sometimes it is not possible to appoint SMEs who are entirely independent of the program due to resource constraints. In this case, it may be necessary to create a "review board" that can independently review the team's approach, findings and conclusions and mediate disagreements between the PM and TRA team etc.
- Ensure that SMEs have the appropriate knowledge and training to perform the role.
- Select enough SMEs to account for the technologies being assessed. For example, if a technology involves operations on a ship, a team member with relevant experience in testing such technologies would be needed.
- Assemble a team that comports with the complexity and number of technologies being assessed. The number of SMEs will depend on the number of technologies needing to

be evaluated. For example, a TRA involving a large number of CTEs from multiple technological fields will be larger than a TRA involving few CTEs from related fields.

- Maintain access to additional SMEs. Teams commonly discover that they have limited knowledge or experience in certain areas once the review is under way. The TRA team should plan accordingly for this possibility.

4.2.2 Step 2: Identify Critical Technology Elements



Source: GAO 2020

Figure 4-2. Identifying Critical Technology Elements

Establishing a process to identify and select CTEs is a fundamental part of conducting a high-quality TRA (Figure 4-2). Technology risk identification should start well before the formal TRA process. In fact, identifying potential CTEs begins during the Materiel Solution Analysis (MSA) phase, which precedes MS A. An early evaluation of technology maturity, conducted shortly after MS A, may be helpful to refine further the potential CTEs to be assessed. It may be appropriate to include high-leverage and/or high-impact manufacturing technologies and life-cycle-related technologies if there are questions of maturity and risk associated with those technologies.

The PM should prepare an initial list of potential technologies to be assessed. When competing designs exist, the PM should identify possible technologies separately for each design. The PM should make key technical people available to the SME team to clarify information about the program. The determination of technologies as "critical" is fluid and may change as program or mission-related changes to objectives occur, system requirements are revised, or if technologies do not mature as planned.

The SME team should recommend changes to the list of potential CTEs to assess. Inputs to this process include the list developed by the PM and technical planning performed by existing or previous contractors or government agencies. The SME team should be given full access to these data.

4.2.2.1 Examples of Critical Technology Elements

Technologies are the enabling means for system capabilities. They should not be confused with subsystems or components; the technologies are defined by *how* these subsystems or components function. Some examples of CTEs from past U.S. systems include:

- A novel material that selectively transmits only certain radio frequencies
- A novel sensor fusion algorithm for resolving data from multiple radars
- A new additive manufacturing process for certain metal parts
- An aircraft overall configuration concept that minimizes radar cross-section
- A new propellant for 155mm howitzer shells
- Autonomous sense-and-avoid algorithms for an unmanned aircraft
- Neural network-based identification of unexploded ordinance
- A process for ensuring that manned space mission food is contaminant-free
- Laser-based LPD/LPI satellite-to-satellite communications
- Use of commercial speech recognition software in a combat system
- A novel key-distribution process for cybersecurity of distributed and networked devices
- A novel electromagnetic catapult design for aircraft carriers
- Cyber-related technical capabilities (survivability and resilience)

As is shown by these examples, CTEs can be material, electromagnetic, algorithmic, chemical, or process-based. They can arise not only in system design, but also in necessary manufacturing processes or logistics. They can also be mature technologies that are being considered for use in a significantly different environment or operational context.

Software technologies are increasingly important to U.S. national security capabilities. These include technologies used in sensor fusion, cloud computing infrastructure, autonomous navigation, natural language and speech processing, distributed network management, and many other mission applications. Algorithmic technologies, and especially artificial intelligence and machine learning, are a rich source of novel (and often critical) enabling technologies for planned defense systems.

PMs familiar with technologies that have been successful in the past may consider it unnecessary to identify those technologies as CTEs; however, this assumption could lead to disastrous cost increases, schedule delays, or technical performance problems. Technology reapplied in a new way or in a new environment could lead to differences in form, fit, or function that cause unexpected results.

The TRA team should strive to identify and select CTEs accurately to prevent wasting valuable resources (funds and schedule) later in the acquisition program. There should not be a limit on the number of CTEs, but over-identifying CTEs may divert resources from technologies requiring a more intense maturation effort, but under-identifying CTEs, because of a real or perceived limitation on the number of CTEs allowed, may result in system or requirements failure. For example, under-identifying CTEs could result in an underrepresentation of the integration needs which is a significant cause of system failure.

4.2.2.2 Selecting Critical Technology Elements

The SME team relies on its knowledge, experience, and professional judgment to determine what constitutes a CTE. For example, the team makes professional judgments about what a technology is, what makes it critical and at what level (e.g., subcomponent, component, system, element). When the key functions for a technology are identified, potential failure modes also should be identified and eliminated or mitigated as the technology matures.

DoD developed a list of questions to help PMs identify CTEs for applications, such as:

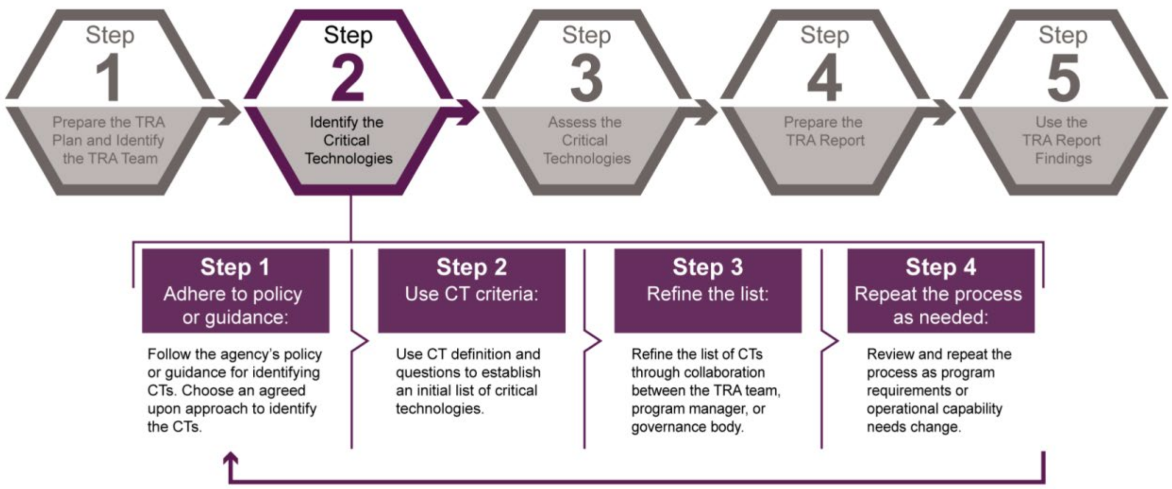
- Aircraft
- Ground vehicles
- Missiles
- Ships, submarines, and naval weapon systems
- Space Systems
- Information systems, networked communications systems
- Business systems
- Mission planning systems
- Embedded IT in tactical systems
- Manufacturing

Programs should build similar strategies to help identify CTEs.

4.2.2.3 Four Steps for Selecting Critical Technology Elements

The TRA team should identify and document CTEs to ensure the TRA meets the four criteria discussed above: credibility, objectivity, reliability, and usefulness. GAO 2020 says, "The approach should be open and transparent to everyone in the process, including but not limited to representatives from the research and development program office, the test community, and the science, engineering, and user communities." Source: GAO 2020

Figure 4-3 illustrates four steps to guide programs in identifying and selecting CTEs for projects of any size.



Source: GAO 2020

Figure 4-3. Four Steps for Identifying Critical Technology Elements

Step 1

The program's respective policy or guidance codifies the approach for identifying CTEs and should be followed. The DoD's policies on TRAs are described in Sections 1, 2, and 3 herein.

Step 2

A program's policy or guidance defines the criteria for identifying or classifying a technology as a CTE; typically, the PM develops the initial list of CTEs. Early identification of CTEs leaves time for the PM to see whether the TRA team requires additional technical experts.

GAO 2020 developed a list of questions for a PM to use as a starting point for determining whether a technology should be included in the initial CTE list (Table 4-1). A "yes" answer to at least one question in each list signals a need for inclusion. A best practice is for the PM and SME team to refine this list of questions for their own TRA process.

Table 4-1. Questions for Determining Initial CTEs

Technical Questions	Programmatic Questions
• Is this technology new (for example: next generation)? • Is the technology used in a novel way? • Has the technology been modified? • Is the technology expected to perform beyond its original design intention or demonstrated capability? • Is the technology being used in a particular or different system architecture or operational environment than the one for which it was originally intended or designed? • Could the technology have potential adverse interactions with systems with which it will interface?	• Do requirements definitions for this technology contain uncertainties? • Does the technology directly affect a functional requirement? • Does this technology require development of new skills by stakeholders to include developers, manufacturers, users, or leadership? • Could limitations in understanding this technology significantly affect cost (for example, overruns) or affordability? • Could limitations in understanding this technology significantly affect schedule (for example, not ready for insertion when required)? • Could limitations in understanding this technology significantly affect performance?

Source: GAO 2020

Step 3

After the PM compiles the initial list of CTEs, the TRA team either affirms or refines the PM's findings. The TRA team should document any disagreements about the determinations and the rationale for each conclusion. The TRA team should consider the technology's operational environment in this part of the process.

Step 4

The PM, TRA team, and leadership repeat the CTE identification and determination process as needed. These parties should determine how they will handle any changes to the list of CTEs, as developing systems and technology can impact which technologies are still considered "critical" over time. Also, alternative technologies can be implemented or selected as new advancements are made or other technologies fail, which can also affect the list of CTEs. In other words, CTEs may be added or omitted as time passes and programs evolve. This should all be documented and reviewed.

4.2.3 Step 3: Assess Critical Technology Elements

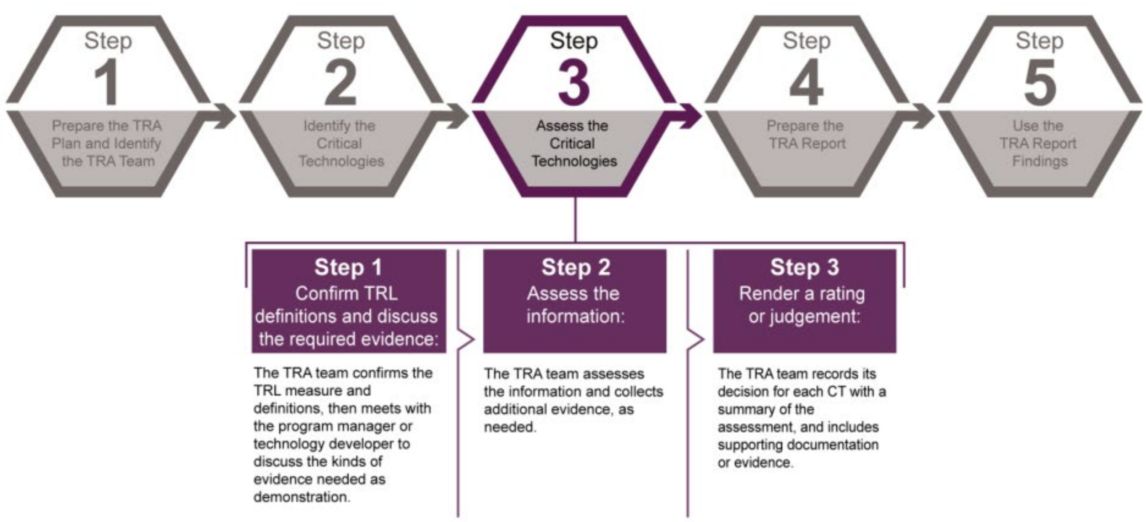
To determine each CTE's maturity, the SME team assesses each CTE and determines its TRL. The TRA team decides the TRLs by evaluating information (discussed below) against the criteria in the TRL descriptions.

Information relevant to assessing the CTEs, upon which the SME team relies, may include schematics, test data, analytical reports, digital engineering (DE), and potential functional failure modes, etc. Unexpected failures that occur after TRL 6 may incur cost and schedule delays, resulting in the inability to meet the key functions of the technology.

The PM and TRA lead should know why the assessment is being conducted and within what operational environment the technology is expected to operate; the purpose and operating environment determine what constitutes sufficient evidence that a TRL has been achieved.

4.2.3.1 Three Steps for Evaluating Critical Technology Elements

Evaluating and assessing CTEs is one of the TRA's primary objectives. Appropriate data and information are needed to assess whether the technologies of the program have been demonstrated in a relevant environment; this determination is a key factor in assigning a TRL to the CTE. The process of collecting and organizing the material for each technology should begin as early as possible. The PM should compile component or subsystem test descriptions, environments, and results in the context of the system's functional needs, and the SME team should conduct their own assessment of technology maturity. Any other analyses and information necessary to assess and rationalize the maturity of the technologies should also be included. Figure 4-4 depicts three steps that GAO 2020 determined can be repeated to help guide programs in conducting an evaluation that is objective and reliable.



Source: GAO 2020

Figure 4-4. Assessing Critical Technology Elements

Step 1

The TRA team confirms the TRL measures and definitions selected during the development of the TRA plan are still suitable. The TRA team and PM meet and consider input from the systems engineering community to determine the evidence that is sufficient to establish that a CTE has achieved a specific TRL.

Step 2

Before the assessment process begins, the SME team must ensure a sufficient understanding of the requirements, identified capabilities, system and software architectures, CONOPS, and/or the concept of employment to define the relevant environments. The SME team must also ensure that its understanding of design details is sufficient to evaluate how the technologies will function and interface.

The TRA team conducts the CTE assessment and reviews the information (evidence) and collects any needed additional information (evidence). To support this step, the PM must make key data, test results, and technical people available to the SME team to clarify information about the program. As part of this assessment, the SME team determines whether these technologies have been demonstrated in a relevant environment and whether risk has been reduced or can be reduced to an acceptable level for inclusion in an EMD program.

Once the TRA team considers the information, it generally makes one of the following three determinations:

> **Option 1 –** The TRA team reaches agreement because the fidelity of the test article (or digital model or constructive simulation) and test or simulation environment are appropriate, data are sufficient, and the results are acceptable such that no further evidence or assessment is needed.
>
> **Option 2 –** If the TRA team determines that information is insufficient to render a credible, objective, and reliable decision, the team asks the PM for more information to make a TRL rating determination for each CTE. The interaction between the TRA team and PM is often an iterative process as discussions can highlight the need for more information or raise additional questions.
>
> **Option 3 –** The TRA team may determine that a TRL rating cannot be assigned because the fidelity of the test article or test environment is insufficient and information and test results are inconclusive. Such cases are unusual but can occur. When they do, the TRA team identifies the inadequacies and works with the program manager to determine what should be done to conduct a TRA.

Step 3

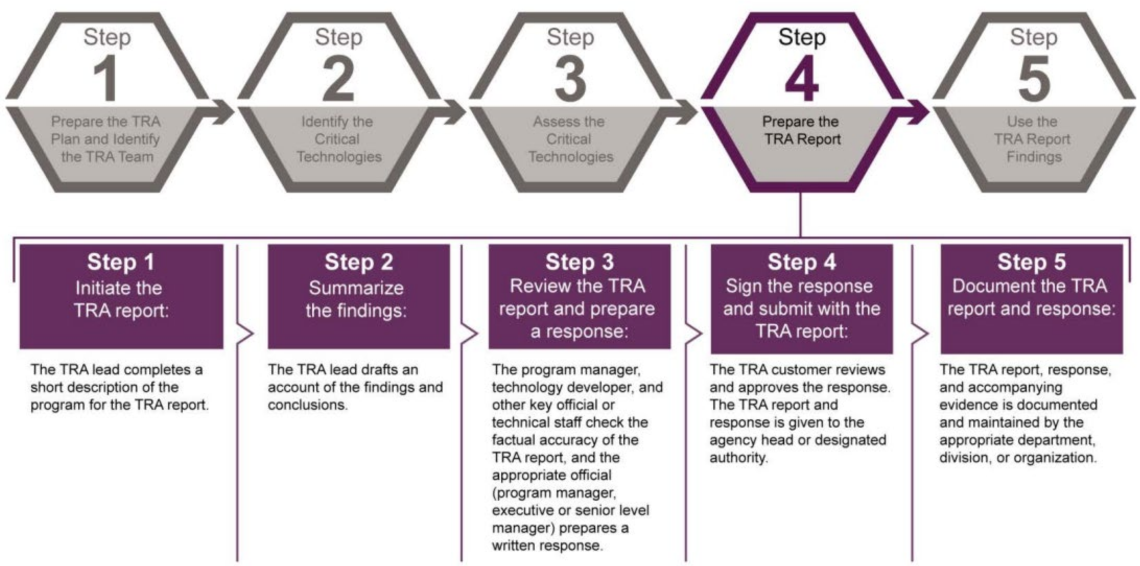
The TRA team documents the assigned TRL rating of each CTE and summarizes the underlying decision process and cites the supporting documentation, to rationalize the assigned TRL.

For additional detail on these three steps, see GAO 2020.

4.2.4 Step 4: Prepare the TRA Report (including USD(R&E) Review and Evaluation)

TRA reports document information about the maturity of CTEs, their state of development, and the potential areas of risk. The TRA report arms decision makers with information to identify maturity gaps, make plans for maturing technologies as needed, address potential concerns, and determine whether programs that will integrate CTEs have achieved TRLs at a certain decision point and are ready to move to the next acquisition phase.

Figure 4-5 and Table 4-2 show the GAO 2020 summary of general steps for preparing and submitting the TRA report:



Source: GAO 2020

Figure 4-5. Preparing and Submitting a TRA Report

Table 4-2. Steps in Preparing and Submitting a TRA Report

Step in Preparing TRA Report	Description
Step 1: TRA Team Lead Initiates the TRA Report	The TRA team lead initiates the report draft by documenting the introduction and other descriptive information. The TRA report summary explains the function of each CTE at the component, system, and subsystem levels.
Step 2: TRA Team Lead Summarizes the Findings	The TRA team lead summarizes the findings along with references to supporting evidence and explains how the evidence was used in the assessment to determine each TRL. The TRA report should present the evidence and rationale for the final assessment. Evidence could include records of tests or applications of the technology, technical papers, reports, presentations, test results or applications of technology and so forth. It should explain how the material was used or interpreted to make the assessment. The report should reference the sources and the pages in these sources for the evidence presented in the report to determine whether a technology has been demonstrated in a relevant environment. The material should explain the function of each technology at the component, subsystem, and system levels. The report should also contain an explicit description of the program increments or spirals covered if appropriate and relevant to the Milestone decision.
Step 3: Program Manager (or other) Reviews the TRA Report and prepare a response	The PM and other key officials or technical staff check the factual accuracy of the TRA report, and the appropriate official (program manager, executive or senior level manager) prepares a written response to document the coordination among the stakeholders. This response may be a cover letter, memorandum, or other type of document that is appropriate for the program. For this step, the S&T executive reviews the report and prepares the response, which may include additional technical information appropriately indicating concurrence or non-concurrence with the TRA team's rating of the CTEs. The purpose of the written response is to document the coordination among the various stakeholders and programs, and agreement or dissenting viewpoints with the TRA team's findings, along with supporting analyses for any disagreements. The S&T executive should certify that he or she stands behind the results or should provide rationale for any dissenting views or differences of opinion. The acquisition executive or appropriate official approves the response and forwards it to the organizational or agency head. If factual accuracies have been compromised as a result of new information, misinterpretation of data, etc., the TRA team lead should revise the TRA report with concurrence of the TRA team to correct any inaccuracies. The team lead should keep a log of how each issue was addressed and

Step in Preparing TRA Report	Description
	resolved. For TRA reports that are prepared for PMs, programs should modify this step as necessary to exclude governing bodies; however, there should be necessary reviews at the appropriate levels to ensure the information is factually correct.
Step 4: Sign the response and submit with the TRA Report and Step 5: Document the TRA Report and response	USD(R&E) evaluates the TRA in consultation with the CAE and the PM. USD(R&E) provides the MDA with an independent assessment of technology maturity based on this process. USD(R&E) will prepare a memorandum that contains the evaluation results of the TRA. The memo will summarize USD(R&E)'s determination as to whether the technologies of the program have been demonstrated in a relevant environment; if not, whether or not a waiver is acceptable; and a recommendation on the adequacy of risk mitigation plans and the readiness of the program to proceed to the next stage of the acquisition process. The memorandum is sent to the MDA, with copies to the Overarching Integrated Product Team, the CAE, and the PM. A TRA report prepared for decision makers for a decision point or Stage Gate Review review—such as a Milestone B decision for DoD defense programs—should be prepared well in advance of the scheduled time to allow decision makers sufficient time for their review. The time required to prepare the TRA report will depend on the size of the effort, complexity of technology, amount of available technical data to review, and purpose and scope of the review. Reports prepared for simpler technologies take less time, especially if no critical decisions will be based on the rating discussion of the TRA. When setting timelines, programs should consider their internal review processes, time and resources required, and any policy requirements.

Source: GAO 2020

For more information on these recommended steps, please see GAO 2020.

GAO 2020 noted that agencies should codify policy or guidance on how its TRA reports should be prepared. These policies should include "the processes and steps to create the report; reporting elements; process for submittal, review, and approval; how the results are communicated; and who is involved in the process."

GAO 2020 also noted that content in a TRA report can vary based on the report's purpose. To illustrate this point, GAO 2020 discussed TRA reports for governance purposes and TRA reports for knowledge building. It said, "TRA reports for governance purposes are developed to certify whether CTEs have met an expected TRL rating, and governing authorities use them to determine whether a program is ready to move to the next acquisition phase.” On the other hand,

> *knowledge-building TRA reports prepared for PMs are conducted with a focus on maturing technologies, not as a pass/fail assessment. Therefore, the information collected is to be used as a source for managing those efforts. Knowledge-building TRA reports may be used to learn about specific aspects of technology or prototype development, for example, to identify gaps in maturity or areas that may be challenging; to gather evidence to continue development efforts or initiate steps toward using an alternative or backup technology; or to determine whether CTEs are ready for a TRA for leadership at an upcoming decision point.*

See GAO 2020 for additional information on:

- Final Processing of the TRA Report
- Dissenting Views
- Next Steps

4.2.4.1 DoD: Preparing, Coordinating, and Submitting the TRA Report

In DoD, the CAE submits a draft TRA report to USD(R&E) 30 days prior to the Pre-Milestone B Defense Acquisition Board program review. An update will be submitted after PDR and source selection and before formal Milestone B or other certification decision event.

Generally, the TRA report should consist of (1) a short description of the program; (2) a list of CTEs that pose a potential risk of program execution success, with the PM’s assessment of the maturity of those technologies as demonstrated in a relevant environment and a description of any risk-mitigation plans; (3) the SME team membership and credentials; (4) SME team findings, conclusions, supporting evidence, and major dissenting opinions; and (5) a cover letter signed by the CAE approving the report, forwarding any requests for waivers of 10 USC 4252 certification requirement with supporting rationale, and providing other technical information deemed pertinent by the CAE and PM. The CAE and PM can provide any supplemental material as desired.

4.2.5 Step 5: Use the TRA Report Findings

The TRA report is used to inform leadership about the readiness of CTEs to guide in decision making and resource planning. These decisions can be determining whether programs that rely on CTEs are ready to move forward or deciding to mature technologies or to consider trade-offs because of cost, schedule, or program priority changes. In addition, systems engineers may use TRA reports to understand transition risks when maturing technologies or to determine whether technologies are ready to transition to new or existing acquisition programs.

Programs should be aware that each program or team involved in the development and maturation of CTEs has its own culture, perspective, or bias that can influence how a TRA report is interpreted or acted upon. Programs need to maintain professional judgment when using TRA reports.

GAO 2020 provides the following examples of ways in which the TRA report can be used or how it can support decisions:

- Informing the Integrated Project Team's TMP process for prior to a decision point or Stage Gate Review.
- Providing a basis for modifying requirements if technological risks are too high.
- Refining the TDS or similar planning document that is used in the systems engineering process.
- Informing the test and evaluation community about technology maturity needs.
- Establishing technology transition arrangements.

TRAs are snapshots of how a CTE has been assessed at a certain point in time or in its development. There is not standard guidance on the shelf life of a TRA rating, but experts generally agree that it can range from 1 to 6 months, depending on the type of technology and how rapidly it evolves.

See GAO 2020 for additional information on:

- TRAs for Governance Decisions
- Knowledge-Building TRA Reports for Project Management
- TRAs and Risk Reduction Efforts
- Options for Addressing Immature CTEs
- Relationship between TRA Reports and Other Project Management Tools

4.3 Options for Addressing Immature Critical Technology Elements

For CTEs assessed as immature or as "not progressing as planned," GAO 2020 suggests the TRA report may be used to:

- Consider or identify an alternate technology.
- Plan how technology development efforts should proceed.
- Initiate the development of a TMP to address immature CTEs (TMPs are covered in Section 4.5). It is unacceptable to discover immaturity and assume that the CTE will mature with no intervention.
- Update the program's risk management plan.
- Update or revise cost and schedule risk assessments, as appropriate.

Maturing a CTE from one TRL to the next may require varying amounts of effort. The time, effort, and activities needed to advance technology to a higher TRL may differ among TRLs and may not increase linearly between progressively higher TRLs. For example, moving a technology from TRL 3 to TRL 4 may not require the same amount of effort as moving the same technology from TRL 6 to TRL 7.

4.4 Independent Technical Risk Assessment Considerations

OUSD(R&E) conducts ITRAs on ACAT ID (i.e., Major Capability Acquisition (MCA) pathway) programs for USD(R&E) approval, generally at each milestone or production decision, and maintains the policy and guidance for ITRAs. The Services or Agencies conduct ITRAs on ACAT IB/IC programs with the approval authority determined by the USD(R&E). For the other Adaptive Acquisition Framework (AAF) pathways, the ITRA is not required by statute or policy but can be "tailored in" by the PM or directed by the decision authority or higher.

According to DoDI 5000.88, when an ITRA is conducted, a TRA report is not required. Programs will continue to assess and document the maturity of all CTEs consistent with the TRA guidance. ITRA teams may leverage technology maturation activities and receive access to results to perform ITRAs.

Evaluation of CTEs is an essential part of an ITRA. Technology is one of eight technical areas evaluated in the full spectrum of technical risk, as outlined in the DTRAM framework. Technology-related risks often impact other DTRAM areas, such as System Development and Integration (where integration delays may occur); Mission Capability (for example, fielding with partial capability); and Reliability and Maintainability (where immature technologies can exhibit poor operational reliability, impact system safety, or affect human performance). In the DTRAM framework, Technology is evaluated across seven technical factors:

- Scope and Requirements
- Design and Architecture
- Decision and Control
- Schedule
- Resources
- Evaluation
- Performance and Quality

For further information about ITRAs, see the DoD ITRA Execution Guidance, DoDI 5000.88, and the applicable DoDI for the specific pathway. The criteria associated with the technical areas for technology risk identification are provided in the DTRAM guidance.

4.5 Technology Maturation Plan

4.5.1 Purpose of the TMP

The Technology Maturation Plan (TMP) is a management planning tool that details the steps required to mature or develop CTEs that have been assessed as immature so they are ready for project insertion. The TMP outlines the process for elevating the technology's TRL. Often the need for technology maturation is identified as a program technical risk in an ITRA or TRA, and the TMP will use the TRA report's conclusions as its road map. In such cases, even though the ITRA team may not create a formal TRA report, the TMP can serve as an effective and integrated risk mitigation tool. Activities that advance the TRL of CTEs will at the same time burn down the technical risk associated with those technologies. During decision point or Stage Gate Reviews, the TMP can serve as a reference document to prove that progress is being made in closing maturity gaps.

DoD does not have codified policy or guidance on the use or development of a TMP. Other agencies, such as NASA and DOE have TMP guidance, which indicates TMPs are a part of their TRA processes. The guidance below on developing a TMP parallels the process outlined in GAO 2020.

A number of steps are involved in preparing the TMP. As CTEs may change over time, the TMP is a "living" (fluid) document that is periodically modified.

4.5.2 Five Steps for Preparing the TMP

GAO 2020 outlined five steps to mature CTEs; these steps form the basis for GAO's recommended process for developing a TMP. For purposes of this guidebook, we discuss concepts from GAO 2020 and from DOE and NASA guides.

Figure 4-6 and the following paragraphs summarize the five steps. For more information, see GAO 2020.

Source: GAO 2020

Figure 4-6. Five Steps to Prepare a Technology Maturation Plan

Step 1: PM selects the immature CTEs for the TMP

In GAO 2020's construct, the PM typically leads the steps and designates a planning lead who facilitates the TMP development work.

The PM highlights the immature CTEs or the CTEs that have a maturity gap as indicated by the TRA report. The PM may include technologies for the TMP that are not indicated by the TRA report, such as technologies that pose a risk due to their complexity.

Step 2: PM designates a lead to complete the TMP

The PM conducts the initial research and data collection activities to initiate the TMP process and then designates a "lead" who completes the TMP. Some notes about this step follow.

- The initial research and data collection efforts begin with the TRA report (i.e., getting the current TRL)
- The PM or lead will determine the cost, schedule, and technical risks for obtaining the desired TRL for each CTE.
- Additional personnel, such as engineering staff, SMEs, or contractors, may support the TMP effort.

Step 3: Lead prepares the TMP with input from others

The lead's role is to draft and document the TMP. For each CTE identified by the PM in Step 1, the draft TMP should include:

- The approach for defining the technology development activities, scoping the effort and for identifying the steps for bringing CTEs to the desired maturity.
- The schedule, costs, and technology risks associated with technology maturation requirements.

The lead may seek input and assistance from other specialists or experts to refine and finalize the draft TMP.

Step 4: Lead submits the TMP for review and approval

The lead presents the draft TMP to the PM and LSE for review and approval. Once the draft is approved by the PM and LSE, the TMP may be provided to other key stakeholders, leadership, or other programs that have a vested interest in maturing the CTE, who may verify the TMP's methodologies and their reasonableness.

Step 5: PM implements the TMP

Once the comments from Step 4 are resolved, the PM is responsible for implementing the TMP. The PM ensures that the TMP's requirements for maturing each CTE are communicated to and implemented by the appropriate personnel throughout the program.

4.5.3 Sections of a TMP

The GAO 2020's version of a TMP (Appendix C) contains sections to outline assessments, maturation plan, schedule, and budget.

TMP Section 1, Technology Assessments of the Project

- Reviews any past assessments that contributed to the need for the TMP, including previous technology development activities.
- Lists the current TRLs for each CTE.

TMP Section 2, Technology Maturation Plan

- Describes the approach, steps, and activities for maturing technologies, including the consideration of alternative technologies. Items that should be accounted for include the following:

  - Criticality of the system to mission success or safety
  - Probability or likelihood that the technology will be successful
  - Cost, schedule, and performance penalty incurred if an alternate solution is used (agencies generally include this as part of their risk assessments and document them in the project Risk Register)
  - High-level cost estimate of the development strategy
  - Effects of the strategy on other technical portions of the project

All of the identified technology gaps and technical assumptions that require resolution or validation should be assessed for impact to the overall system design. The elements that require significant redesign, if shown not to perform as expected, are addressed early in the technology maturation process. This allows implementation of alternative approaches and other backup strategies. By including alternative technology solutions in TMPs, PMs can consider these alternatives if efforts to reach certain TRL goals prove more challenging than expected. For example, if CTEs become too resource intensive or fall too far behind schedule, PMs can consider backup solutions, such as investment trade-offs or the pursuit of backup technologies.

In preparing plans to mature each CTE, programs should identify:

- The key technologies being addressed
- The objectives of the technology development
- The technology development approach
- The scope, including
  - Specific tasks to be undertaken
  - Results needed for a claimed advancement to a higher TRL
- The responsible organization for the maturation activities
- The TRL goals for each major milestone
- The TRLs to be reached as the project or program progresses through turnover, readiness assessments, startup, and initial operations
- The cost, schedule, milestones, and risks of these activities
- Technology alternatives

- Off-ramps the program will take if results are less than required at each critical milestone.

Developing plans to mature CTEs helps PMs mitigate cost, schedule, and technical risks. Simply assuming technologies will mature on schedule and meet program requirements may obscure program risks and can have significant negative consequences to the overall program.

TMP Section 3, Technology Maturity Schedule and Summary Technology Maturity Budget

- Describes the plan to mature the technologies with the integration of the CTEs, including an analysis of the maturity gaps. This section should include a high-level schedule and budget, noting the total maturation costs for the major development activities for each CTE. Major decision points, such as proceeding with or abandoning the current technology or selecting a backup technology, should be identified in this section.

- The TMP should include recommendations for security risk mitigations and protection strategy for the CTE.

Appendix C shows the GAO 2020's TMP template with the detailed elements that should be included in the plan and a description of each element.

5 TRAs for the Adaptive Acquisition Framework Pathways

5.1 Overview

DoDD 5000.01 establishes policy and assigns responsibilities for managing all acquisition programs in the Defense Acquisition System. DoDI 5000.02 describes the Adaptive Acquisition Framework (AAF) that supports the Defense Acquisition System with the objective of delivering effective, suitable, survivable, sustainable, and affordable solutions to the end users in a timely manner. [6] To achieve this objective, the DoD uses the AAF pathways, each tailored for the unique characteristics and risk profile of the capability being acquired.

The AAF pathways are:

- Urgent Capability Acquisition (UCA)
- Middle Tier of Acquisition (MTA)
- Major Capability Acquisition (MCA)
- Software Acquisition
- Defense Business Systems (DBS) Acquisition
- Acquisition of Services

The PM will tailor the program's Acquisition Strategy depending on the pathway(s) used during development. Figure 5-1 depicts the AAF pathways and associated key events.

---

[6] DoDI 5000.02, "Operation of the Adaptive Acquisition Framework (AAF)," outlines six DoD acquisition pathways. Each pathway describes an acquisition approach that provides capability to the user while capitalizing on advanced acquisition methods and improving the DoD's ability to benefit from commercial innovation. The Defense Acquisition University (DAU) website provides additional information: aaf.dau.edu (Pathways tab).

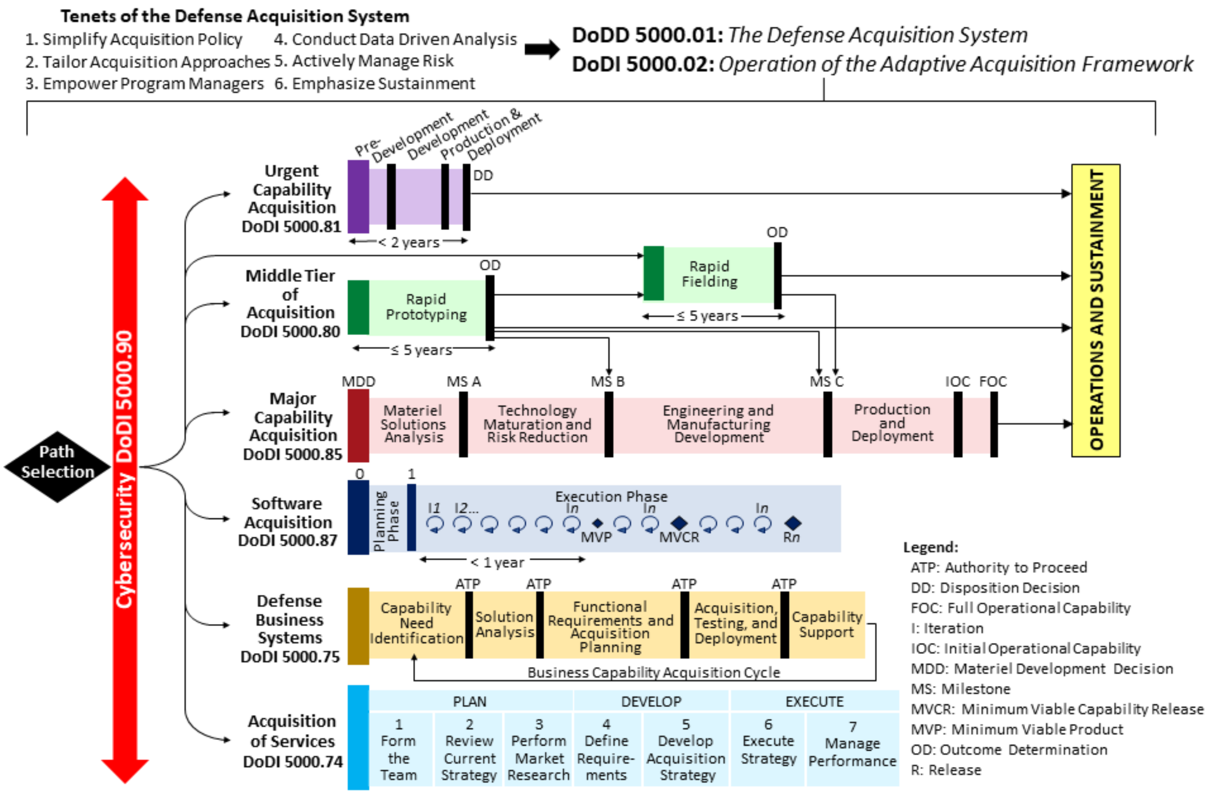


Figure 5-1. Adaptive Acquisition Framework

Table 5-1 provides guidance for conducting TRAs for the AAF pathways.

Table 5-1. TRA Guidance for AAF Pathways

AAF Pathway	Purpose	DoDI Reference	TRA Relevance
Urgent Capability Acquisition (UCA)	To field capabilities to fulfill urgent existing or emerging operational needs or quick reactions in less than 2 years.	DoDD 5000.71 and DoDI 5000.81 establish policies and provide procedures for urgent operational needs and other quick reaction capabilities acquisition.	The preferred capability development solution should be based on technologies that are proven, matured and available in accordance with DoDI 5000.81. Thus, a TRA may not be required for programs on the UCA Pathway, but as with the Rapid Fielding MTA pathway some consideration should be given to the novelty of the proposed operational environment. In a case where a preferred capability solution includes new technology insertion or technology refreshment where technology maturation has not been assessed, a tailored TRA may be required. If the TRA reveals technology maturation deficiencies, decision

AAF Pathway	Purpose	DoDI Reference	TRA Relevance
			makers should determine whether the deficiencies should be resolved prior to fielding and what risk can be accepted. For software development, decision makers should integrate a core set of high-level secure software development practices such as the Secure Software Development Framework (SSDF) – that can be integrated into each System Development Lifecycle (SDLC). However, security and cybersecurity requirements still must be included and met as part of the development.
Middle Tier of Acquisition (MTA)	To rapidly develop fieldable prototypes within an acquisition program to demonstrate new capabilities or rapidly field production quantities of systems with proven technologies that require minimal development.	DoDI 5000.80 establishes policy, assigns responsibilities, and prescribes procedures for the MTA pathway,	**Rapid Prototyping Path**: If a fieldable prototyping solution included the use of proven technologies that requires minimal development, a TRA for this path may not be required. In a case where the prototyping solution involves new technology insertion or technology refreshment in which technology maturation not assessed, a tailored TRA for this path should focus on whether the technology is sufficiently mature to be developed and fielded within the 5-year timeframe. The tailored TRA should be conducted within the planning phase to help shape the Acquisition Strategy and set the requirements for prototype development, including security and cybersecurity requirements. **Rapid Fielding Path:** A full TRA for this path may not be necessary, as the technology should be fieldable with no development necessary. The review for this path should focus on whether the application of these mature technologies in the intended operational environment would be sufficiently new or novel to motivate assessment. For example, rapid fielding of an existing vehicle developed for desert operations might require assessment if deployment to jungle environments were planned.

AAF Pathway	Purpose	DoDI Reference	TRA Relevance
Major Capability Acquisition (MCA)	To acquire and modernize military unique programs that provide enduring capability.	DoDI 5000.85 establishes policy, assigns responsibilities, and prescribes procedures for the major capability acquisition pathway.	See Section 5.1 TRAs for Major Capability Acquisition in this document.
Software Acquisition	To facilitate rapid and iterative delivery of software capability (e.g., software-intensive systems or software-intensive components or sub-systems) to the user.	DoDI 5000.87 establishes policy, assigns responsibilities, and prescribes procedures for the software acquisition pathway.	The program should consider conducting a tailored TRA during the Pre-Development Planning Phase or early in the Development Planning phase, to determine the technologies maturation level in software development and construction process (design, code, test, build, integrate, release), and cybersecurity requirements.
Defense Business Systems (DBS) Acquisition	To acquire information systems that support DoD business operations.	DoDI 5000.75 establishes policies and provides procedures for the DBS acquisition pathway.	While unlikely, A TRA may be necessary if the DBS acquisition includes unproven hardware technology or software development in addition to or instead of GOTS or COTS integration.
Acquisition of Services	To acquire services from the private sector including knowledge-based, construction, electronics and communications, equipment, facilities, product support, logistics, medical, research and development, and transportation services.	DoDI 5000.74 and the online Service Acquisition Mall establish policies and provide procedures for the defense acquisition of services pathway.	Acquiring services will not require a TRA unless the service being acquired involves the use of a novel or unproven technology in order to satisfy the service requirements.

5.2 TRAs for Major Capability Acquisition

The MCA pathway is used to acquire and modernize military-unique programs that provide enduring capability. These acquisitions typically follow a structured analyze, design, develop, integrate, test, evaluate, produce, and support approach. This process is designed to support MDAPs, major systems, and other complex acquisitions. Acquisition and product support processes, reviews, and documentation will be tailored based on the program size, complexity, risk, urgency, and other factors. Software-intensive components may be acquired via the software acquisition pathway, with the outputs and dependencies integrated with the overall major capability pathway.

5.2.1 Milestone B TRA

The Milestone B decision authorizes a program to enter the EMD phase and commit the required investment resources to support the award of phase contracts. Requirements for this milestone may have been satisfied at the Development RFP release decision point; however, if significant changes have occurred between the two decisions that would alter the decisions made at the earlier point, those changes will be addressed at the Milestone B review.

This review requires demonstration that all sources of risk have been adequately mitigated to support a commitment to design, development, and production. Risk sources include, but are not limited to, technology, threat projections, security, engineering, integration, manufacturing, sustainment, and cost risk. All programs must include validated capability requirements. As directed, MDAPs and programs in other categories require full funding in the Future Years Defense Program (FYDP), compliance with affordability/program goals demonstrated through technical assessments, and Independent Cost Estimates.

Decisions

- The Milestone Decision Authority will approve entry into the EMD phase and formally initiate the program by approving the Acquisition Program Baseline.
- The ADM will document program decisions, EMD phase exit criteria, approval of the Low-Rate Initial Production (LRIP) quantity, and specific technical event-based criteria for initiating production or fielding at Milestone C.

5.2.2 Milestone C TRA

Milestone C is the point at which a program is reviewed for entrance into the Production and Deployment (P&D) phase.

The following information typically will be considered at Milestone C: the results of developmental test and evaluation and any early operational test and evaluation; evidence that the production design is stable; the results of an operational assessment (if conducted); the maturity of the software; any significant manufacturing, security, and cybersecurity risks; the status of critical intelligence parameters and intelligence mission data requirements relative to fielding timelines; evidence from integrated test that includes both developmental and operational testing; and full funding.

Decisions

The Milestone Decision Authority's decision to approve Milestone C will authorize the program to proceed to the P&D phase, enter LRIP or begin limited deployment for Automated Information Systems, and award contracts for the phase.

High-Cost First Article Combined Milestone B and C Decisions

Some programs such as spacecraft and ships will not produce prototypes during EMD for use solely as test articles because of the high cost of each article. In that case, the first article produced will be tested and evaluated and then fielded as an operational asset. The acquisition approach for these programs can be tailored by measures such as combining development and initial production investment commitments and a combined Milestone B and C. Additional decision points with appropriate criteria may be established for subsequent production commitments.

6 Other Types of Readiness Levels

6.1 Manufacturing Readiness Levels

Manufacturing readiness and technology readiness go hand in hand. Manufacturing Readiness Levels (MRLs), in conjunction with TRLs, are key measures that define risk when a technology or process is matured and transitioned to a system.

It is common for manufacturing readiness to be paced by technology readiness or design stability because manufacturing processes cannot mature until the product technology and product designs are stable. Because of this interrelationship, the MRL criteria were designed to include an advised level of technology readiness to encourage manufacturing personnel to work closely with the technologist.

Although there is a general relationship between MRLs and TRLs, there is no direct one-to-one requirement. Programs under the MCA pathway generally have longer development life cycles, whereas UCA or MTA pathways have tighter timelines in which design and manufacturing concerns may have a greater impact on programmatic risk.

6.1.1 Manufacturing Readiness Assessments

Manufacturing Readiness Assessments (MRAs) are assessments of manufacturing maturity using the MRL criteria. MRAs identify and manage manufacturing risk in acquisition, decreasing the risk involved in the transition of new technology to weapon system applications. MRL criteria provide a structured approach to estimate the current manufacturing maturity. MRAs identify, quantify, and prioritize manufacturing risks and mitigation efforts.

While TRLs are a metric used to assess the maturity of technologies from a performance perspective, TRLs do not answer manufacturing or transition to production questions such as:

- Is the technology producible?
- Can the system be produced at the required rates and quantities?
- What is the projected production cost? Is the technology affordable?
- Can the system be made in a production environment or only in a laboratory?
- What investments are required for production facilities and manufacturing processes?

- Are key materials and components available?
- What are the material lead times?

Used in conjunction with TRLs, MRLs are key measures that define risk when a technology or process is matured and transitioned to a system. The numbers represent a non-linear ordinal scale that identifies what maturity should be as a function of where a program is in the acquisition life cycle.

DoDI 5000.88 requires the PM to identify and manage manufacturing, producibility, and quality risks throughout the program's life cycle. This policy establishes general target maturity criteria for each life cycle phase leading to the production decision. Assessments of manufacturing readiness using the MRL criteria are considered a best practice. MRL assessment criteria create a measurement scale and vocabulary for assessing and discussing manufacturing maturity and risk. Using the MRL criteria, an assessment of manufacturing readiness is a structured approach for evaluation of manufacturing processes, procedures, and techniques for technology, components, items, assemblies, subsystems, and systems. An MRA is performed to:

- Define current level of manufacturing maturity.
- Identify maturity shortfalls and associated costs and risks.
- Provide the basis for management of manufacturing maturation and risk.

The difference between TRLs and MRLs is as follows:

- MRLs are used to assess the maturity of a given technology, system, subsystem, or component from a manufacturing perspective.
- TRLs are used to assess the maturity of an individual technology.

6.1.2 DoD MRL Deskbook

The DoD Manufacturing Readiness Level (MRL) Deskbook provides best practices for conducting assessments of manufacturing readiness using the MRL criteria. It is intended for those tasked with conducting MRAs, as well as acquisition PMs, systems engineers, manufacturing managers, and managers of technology development and pre-systems acquisition technology demonstration projects.

For additional information about manufacturing readiness, and details in the MRL Matrix, see, the MRL Deskbook (2022).

6.1.3 DoD MRL Descriptions

MRLs are based on a scale from 1 to 10 with 10 being the most mature manufacturing process (Table 6-1).

Table 6-1. DoD Manufacturing Readiness Levels

MRL	Description
1	Basic manufacturing implications identified
2	Manufacturing concepts identified
3	Manufacturing proof of concept developed
4	Capability to produce the technology prototype in a laboratory environment
5	Capability to produce prototype components in a production-relevant environment
6	Capability to produce a prototype system or subsystem in a production-relevant environment
7	Capability to produce system, subsystems, or components in a production-representative environment
8	Pilot line capability demonstrated; ready to begin LRIP
9	Low-rate production demonstrated; capability in place to begin FRP
10	Full-Rate Production demonstrated and lean production practices in place

6.2 Integration Readiness Levels

Integration readiness levels (IRLs) measure the integration maturity between two or more components. IRLs, together with TRLs, form the basis of the System Readiness Level (SRL), which is discussed in the next section. IRL values range from 0 to 9 (Figure 6-1) (GAO 2020 citing Sauser et al.).

GAO 2020 modified the original IRL scale definitions, as proposed by Sauser, to make them consistent with the foundation of the TRL scale and to reflect the DoD development approach. These are depicted in the chart below (GAO 2020 citing Sauser et al.).

IRLs help the systems engineer identify development areas requiring additional engineering, and they reduce the risk in maturing and integrating components into a system. IRLs provide a common measure of comparison for both new system development and technology insertion.

Table 14: Integration Readiness Levels

IRL	Definition	Evidence Description
0	No integration	No integration between specified components has been planned or intended
1	A high-level concept for integration has been identified.	Principle integration technologies have been identified Top-level functional architecture and interface points have been defined High-level concept of operations and principal use cased has been started
2	There is some level of specificity of requirements to characterize the interaction between components	Inputs/outputs for principal integration technologies/mediums are known, characterized and documented Principal interface requirements and/or specifications for integration technologies have been defined/drafted
3	The detailed integration design has been defined to include all interface details	Detailed interface design has been documented System interface diagrams have been completed Inventory of external interfaces is completed and data engineering units are identified and documented
4	Validation of interrelated functions between integrating components in a laboratory environment	Functionality of integrating technologies (modules/functions/assemblies) has been successfully demonstrated in a laboratory/synthetic environment Data transport method(s) and specifications have been defined
5	Validation of interrelated functions between integrating components in a relevant environment	Individual modules tested to verify that the module components (functions) work together External interfaces are well defined (e.g., source, data formats, structure, content, method of support, etc.)
6	Validation of interrelated functions between integrating components in a relevant end-to-end environment	End-to-end Functionality of Systems Integration has been validated Data transmission tests completed successfully
7	System prototype integration demonstration in an operational high-fidelity environment	Fully integrated prototype has been successfully demonstrated in actual or simulated operational environment Each system/software interface tested individually under stressed and anomalous conditions
8	System integration completed and mission qualified through test and demonstration in an operational environment	Fully integrated system able to meet overall mission requirements in an operational environment System interfaces qualified and functioning correctly in an operational environment
9	System integration is proven through successful mission proven operations capabilities	Fully integrated system has demonstrated operational effectiveness and suitability in its intended or a representative operational environment Integration performance has been fully characterized and is consistent with user requirements

Disclaimer: The IRL scale does not attempt to address or account for programmatic lifecycle activities or responsibilities. This scale is intended to be used to assign integration readiness levels based on the applicable definitions and supported by the evidence descriptions.

Source: GAO 2020 citing Marc Austin and Donald York, Conference on Systems Engineering Research

Figure 6-1. Integration Readiness Levels

6.3 System Readiness Levels

The SRL index is a function of the individual TRLs in a system and their integration points with other technologies (i.e., IRLs; see 6.2). The interplay of these ratings correlates to the nine-level SRL index. GAO 2020 defined the SRL index (Figure 6-2) based on the current state of development of a system in relation to DoD's life cycle phases.

Table 15: System Readiness Levels

Level	SRL Definition
9	System has achieved initial operational capability and can satisfy mission objectives
8	System interoperability should have been demonstrated in an operational environment
7	System threshold capability should have been demonstrated at operational performance level using operational interfaces
6	System component integrability should have been validated
5	System high-risk component technology development should have been complete; low-risk system components identified
4	System performance specifications and constraints should have been defined and the baseline has been allocated
3	System high-risk immature technologies should have been identified and prototyped
2	System materiel solution should have been identified
1	System alternative materiel solutions should have been considered

Source: GAO presentation of NSA SRA Handbook SRL information. | GAO-20-48G

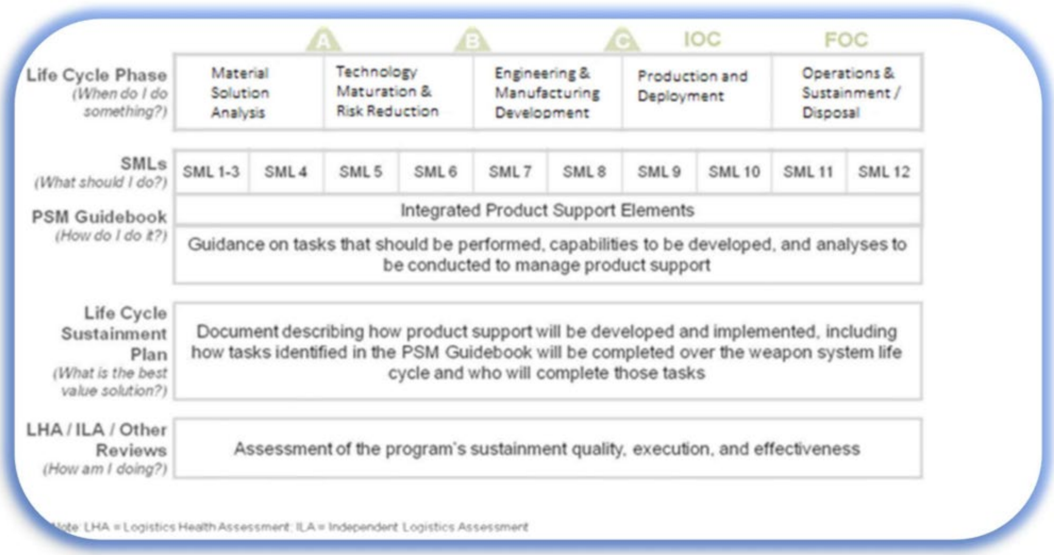
Figure 6-2. System Readiness Levels

6.4 Sustainment Maturity Levels

Developing and fielding the product support package takes place over time. Support packages depend on variables such as operating doctrine, changes in technology, and commercial and Government repair capabilities. During this progression, the program can benefit from a consistent metric to measure the maturity of the implementation process and to convey the progress across the various communities.

The Product Support Manager can use the SML concept to assess the program’s progress in implementing the product support strategy, including the design and resultant product support package to achieve the sustainment metrics consisting of the Sustainment Key Performance Parameter, Key System Attributes, Additional Performance Attributes, and lower-level metrics that drive sustainment performance. The SML concept addresses the full range of support options, from traditional organic-based to full commercial-based product support, without prescribing a specific solution. In addition, the SML approach can be applied across major subsystems to provide a common, consistent, repeatable means of articulating and understanding the product support package maturity.

Achieving SMLs along an indicated timeline helps the Product Support Manager develop the program's product support approach to achieve the best-value solution (Figure 6-3). Achieving up-front levels can also help in designing support actions to reduce total ownership cost (PSM Guidebook 2022). It also helps ensure the program is using adequate supportability analysis concepts such as Failure Mode, Effects, and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Reliability-Centered Maintenance (RCM) Analysis, Level of Repair Analysis (LORA), and Maintenance Task Analysis (MTA). Using an SML construct can also help ensure the program can improve the product support strategy continuously based on actual data collected during testing and operation.



Source: Product Support Manager Guidebook 2022

Figure 6-3. Sustainment Maturity Levels

See the Product Support Manager Guidebook (2022) for additional information on SMLs.

Appendix A: Guidance and Best Practices for Identifying Critical Technology Elements

A.1 Systems Engineering Context for Identifying CTEs

Program systems engineering activities should include identifying CTEs as an aspect of risk management. As a first step, the program should examine any identified critical program information (CPI) to see whether CPI items are also CTEs for purposes of the TRA.

In addition to CPI, functional analysis may be useful to the process of identifying CTEs. In functional analysis, the program system engineers describe and evaluate the system in qualitative and quantitative terms for the functions each technology must accomplish to support the required performance characteristics. Functional analysis forms the bridge between requirements and system design, as the program selects among alternative designs, allocating scarce resources (such as cost, weight, power, and space) and guiding the choice of optimal design points. As part of this selection process, the program typically evaluates different technologies for maturity, performance, cost, and manufacturability. The systems engineering process is a sensible context in which to identify the system's CTEs and to understand their maturity, that is, their readiness for application to the system design.

Two systems engineering outputs are important to identifying CTEs: (1) the functional architecture, which allocates functional and technical performance requirements, and (2) the physical architecture (design), which breaks down the system design into all its constituent subsystems and components.

The functional architecture establishes what the system accomplishes in descriptive and quantitative terms. The physical architecture includes a representation of the software and hardware products necessary to realize the concept. The physical architecture forms the basis for design definition documentation, for example, specifications, baselines, the system and software architectures, and the requirements documentation, which may include the Initial Capabilities Document, Capability Development Document, System Performance Specification, system architecture, and other requirements-driven systems engineering and management products.

Similar approaches are present in the systems engineering of software systems. Although some terminology differs, the software architectural design process incorporates similar functional analysis and design synthesis.

A.2 Environments

Environment is an essential element of CTEs. TRL 6 (required for approval at Milestone B), must be demonstrated (hardware) or validated (software) in a *relevant* environment. TRL 7 (the required level at Milestone C) must be demonstrated in an *operational* environment (hardware and software). Table 2-1 and Table 2-2 of the body of this guide, and Appendix C (page 79), provide additional information regarding hardware and software TRLs.

> ***Best Practice***
>
> *The Independent Review Team (IRT) should present clear, convincing, and succinct data that shows what is known and not known about the environment and should explain the similarities and dissimilarities between the demonstrated and expected environments. The IRT should determine the definition of "relevant" and "operational" before the IRT attempts to determine Technology Readiness Levels.*

Generally, the requirement statement for the system will describe the environment in which the system must operate. This environment may be *external* or *internal*. The external, or imposed, environment may be natural or man-made, friendly or hostile (e.g., weather, terrain, friendly or hostile jamming, enemy fire). The internal environment is more important for identifying and evaluating CTEs. Also called the *realized* environment, the internal environment is an aspect of the design that allows the CTE to accomplish its purpose. The Independent Review Team (IRT) should analyze the design including the expected performance envelope and conditions for each hardware or software element.

Environments will most likely include the following:

- **Physical environment.** For instance, mechanical components, processors, servers, and electronics; kinetic and kinematic; thermal and heat transfer; electrical and electromagnetic; threat (e.g., jammers); climatic—weather, temperature, particulate; network infrastructure

- **Logical environment.** For instance, software interfaces; security interfaces; Web-enablement; operating systems; service-oriented architecture(s); communication protocols; layers of abstraction; virtualization; coalition, federation, and backward compatibility

- **Data environment.** For instance, data formats, structures, models, schemas, and databases; anticipated data rates latency, jitter, transit loss, synchronization, and throughput; data packaging and framing

- **Security environment.** For instance, connection to firewalls; security protocols and appliqués; nature of the cyber adversary, methods of attack, and trust establishment; security domains

- **User and use environment.** For instance, scalability; ability to be upgraded; user training and behavior adjustments; user interfaces; organizational change/realignments with system impacts; implementation plan

Various environments are almost certain to be relevant to any specific system. If the operational view and system view of the design or architecture have been used to identify potential CTEs, they can be used to help identify the environment, especially the logical and data environments. System requirements can help identify the environment. In addition, the program should use interoperability documents and Interface Control Documents (ICDs) to identify the environments in which the candidate CTEs will operate. Key questions that can help guide the definition of the environment for the CTE candidates might include the following:

- Is the physical/logical/data/security environment in which this CTE has been demonstrated similar to the intended environment? If not, how is it different?

- Is the CTE going to be operating at or outside its usual performance envelope? Do the design specifications address the behavior of the CTE under these conditions? What is unique or different about this proposed operational environment?

- Do test data, reports, or analyses that compare the demonstrated environment to the intended environment exist? If modeling and simulation are important aspects of that comparison, are the analysis techniques common and generally accepted?

Sections A.2.1–A.2.4 provide additional examples of questions and sources of information to help define the environment.

Best Practice

Information for identifying CTEs should include results of design analyses that define performance expectations of components and the data and physical conditions in which they operate.

A.2.1 Defining the Physical Environment

The following questions may be helpful to the program in identifying and evaluating the physical environment (and whether it is new or novel) for candidate CTEs:

- What are the expected conditions (vibration, movement, exposure to heat, and so forth) in which the candidate CTE will operate? Do any data or analysis show how the demonstrated environment resembles the expected extremes?

- What is the electromagnetic environment in which the candidate CTE will operate? Has the CTE been tested or demonstrated in that full environment?

- What is the server/processor/network environment? How does the designer know that the CTE will operate in that environment?

- What interfaces will be used? How do they compare with interfaces used previously?

- What network infrastructure will be used? How will the load over this infrastructure be affected by the new system?

A.2.2 Defining the Logical and Data Environments

Operational and systems architectures can be used to help determine the logical and data environments in which the CTE will operate. Designs, requirements documents, or system and software architectures also can be useful. Whether the CTE is a commercial off-the-shelf/government off-the-shelf (COTS/GOTS) software package or a network card, the CTE has a logical relationship to other systems and to the outside world. Those logical relationships—the logical environment—may or may not resemble the proposed DoD environment. Furthermore, the databases and their configuration (e.g., partitioned, replicated, stand-alone) and the anticipated transaction rates in the proposed DoD system may differ from previous environments in which the CTE has operated. The program should document and evaluate these differences for relevance. Sometimes, a developer will use an interface simulation or ersatz data to try to replicate the logical and data environments.

Questions that may be helpful in identifying and evaluating the logical and data environments for candidate CTEs include the following:

- What are the expected logical relationships between the CTE and the rest of the system? between the CTE and the outside world?

- What are the expected data rates? the expected data formats?

A.2.3. Defining the Security Environment

The security environment for DoD computer systems differs greatly from that of the commercial sector. The risk of losing human life and the need to absorb all this risk contribute to the environment in which DoD operates. Therefore, any computer system connected to the Global Information Grid (GIG) must consider cyber warfare as part of its intended environment.

It may be useful to address independently the threats faced by a system and the security provided by a system. The types of attacks, the sophistication needed by an attacker to execute the attack, and the consequences of a successful attack must be considered.

These notions constitute the threat portion of the operational environment. When considering the security services that the system will provide in its operational environment, CTE developers and evaluators should consider the system assets, the security objectives for each asset, and their effect on the system as a whole. Each CTE and its interfaces must be assessed for both the threats presented against the system under review and their inherent vulnerabilities to develop a comprehensive view of risks to the system. Furthermore, because the GIG serves as the data transfer backbone for the DoD, any computer system designed to transfer data to another system, regardless of how data is transferred, must also address issues related to the use of the system as a pathway to more critical systems. The threats posed to other systems on the GIG by a potential compromise of the computer system being assessed in the TRA must be considered. Also, because of the interdependencies of systems introduced by the GIG architecture, the ability of a system to contain a cyber attack and prevent the attack from compromising other systems connected to it/dependent upon it should also be assessed.

The following is a list of questions that may be helpful to the program for identifying and evaluating the security environment for candidate CTEs:

- Does the intended DoD use for a CTE have a different risk tolerance than previous uses of the technology?

- What duress is expected in a cyber-warfare environment? What is the threat?

- Does the CTE depend on external systems for its own security? What if those systems fail?

- Does the CTE depend on external systems to assess its own operational status? What if those systems fail?

- What are the hardware and software interfaces? In what state are they likely to be when the CTE is under duress or attack? Can the CTE function if the interfaces or adjacent entities are less than fully operational?

- Have the threats and vulnerabilities to the CTE and system been initially assessed and the corresponding risk(s) determined? Can the risk(s) be mitigated to an acceptable level?

- How does the security environment change in a disconnected, interrupted, low-bandwidth situation?
- How dependent is the CTE on software updates to remain functional?
- How will a user know if a CTE is under duress or attack?
- Does the CTE need to respond to an attack? If so, how?
- Does the CTE store or pass information? Is it required to verify the authenticity of that information?
- On what cryptography standards does the CTE rely? Are hardware and software resources sufficient to run them?
- How reliant is the CTE on user implementation of itself? Of its interfaces?
- How is the CTE likely to be tampered with or altered if compromised?
- With what entities (e.g., coalitions, military departments, other federal agencies) does the CTE have to interoperate?
- Are the conditions that define the environment expected to change over the lifetime of the CTE? If so, how?

A.2.4. Defining the User and Use Environment

The user and use environments are closely tied to the physical environment. These two environments deal with the interactions between the human users and the physical system in many possible scenarios and sequences.

Following are example questions for identifying and evaluating the user and use environment for candidate CTEs:

- What is the expected user environment? How do the number of users and the way in which they will use the system compare with what has been done before?
- What are the expectations for growth over time? Is it likely that usage will increase significantly beyond those expectations?
- Is the human-machine interface new? Are unusual dexterity, cognitive ability, or vision requirements placed on the user?
- Does the technology require an unusually long or difficult training regimen?

- For autonomous systems, does the user have to develop unprecedented trust in the technology for it to be effective?

- Have all interfaces between existing processes and the new system changed correspondingly?

- Has an implementation or roll-out plan been considered for the new system?

A.3. Sample Questions for Identifying CTEs by Domain

Identifying CTEs depends on effective questioning to clarify the intended purpose, qualities, and environment for a technology. Following are sample questions for several categories of systems. Programs and reviewers should tailor questions to the actual system and application.

A.3.1 Aircraft

Following are example questions to ask when identifying CTEs for aircraft development:

- **Aerodynamic configuration.** Does the design incorporate a configuration that has not been used in flight? How similar is the configuration to that of aircraft that are successful? Does the configuration impose limitations on control authority, stability, structural rigidity, or strength? Is stability acceptable at high angles of attack? Are stability and control acceptable during configuration changes in flight? Is stability dependent on software control?

- **Flight performance.** Is the lift-to-drag (L/D) ratio being used in range calculations consistent with that being achieved by operating aircraft? Has this L/D ratio been confirmed by wind tunnel tests corrected to full-scale, trimmed conditions? Are takeoff and landing distances based on achievable lift coefficients and installed thrust?

- **Control.** How is the aircraft controlled, and how does it interact with the operator? How much autonomy is it required to have? Can it operate without human intervention? Are there safety concerns in autonomous modes? Is the control system dependent on any new software capabilities using AI/ML? Has control software been demonstrated before or is it new or modified development? Are any control algorithms used new or novel?

- **Airframe structure and weight.** Is the structural weight fraction consistent with operating aircraft of the same type?[7] Are lower fractions justified by use of more

[7] The structural weight fraction should be within historical bounds.

efficient materials or structural designs? Do the materials and structures possess stiffness and fatigue properties suitable to the application and has this capability been demonstrated with full-scale sections and representative loads?

- **Propulsion.** Do the engine hot sections rely on new materials? Have these materials been tested to the temperatures, loads, and dynamic environment of expected flight? Are the results for thrust and specific fuel consumption (SFC) from ground tests consistent with the estimates? Have the inlets been tested at flight flow rates?

- **Payloads.** Does the aircraft preliminary design include a comparable SWaP growth margin for the planned applicable mission equipment, weapons, sensors, or countermeasure technologies? Have wind tunnels tests confirmed safe platform/weapon separation distances/aerodynamics? How has the design/integration of the mission equipment minimized potential interference between radiating and receiving sensors/jammers or countermeasures?

- **Rotors and hubs.** Has the rotor type been used before in a similar application? Has testing been limited to static conditions? Has a similar type of rotor been tested at a relevant scale? What is the test basis for the durability estimates for the rotor and hub? Do the cyclic and collective control mechanisms differ from common practice? How have they been tested?

- **Mission equipment.** The appropriate questions differ greatly for the different roles aircraft play. Advanced technology might be incorporated in weapon carriage and employment, in cargo handling, in surveillance, in communications, and elsewhere. General questions include the following: What limits the operational effectiveness of this design? How is advanced technology contributing to more effective performance of the aircraft mission? Are any of these technologies unproven in this application? What requirements for the aircraft program depend on mission payloads? Are the requirements for the payload consistent with those of the aircraft platform? Is software for mission payloads existing or new development? Has ground equipment used for programming mission systems met cybersecurity requirements?

- **Avionics.** Have all certification-related risks been addressed (e.g., software verification/code coverage per DO-178, safety of flight, flight worthiness)?

- **Software.** Has an analysis of software defects, technical debt, reliability highlighted any potential risks that should be remediated prior to release?

A.3.2 Ground Vehicles

Usually, but not always, a vehicle system under consideration is similar to an existing class of vehicles and their functions, so the CTEs likewise may be related. Military systems usually are categorized as combat vehicles (e.g., tanks), tactical vehicles (e.g., High Mobility Multipurpose Wheeled Vehicles (HMMWVs)), or utility vehicles (e.g., sedans or special-purpose vehicles).

A first step for identifying ground vehicle CTEs is to exploit the association and the functional similarities that are common between existing systems and the proposed system by characterizing (quantitatively wherever possible) the functions of the new system and those of comparative existing systems. The second step is to carry out comparisons of the proposed technologies of the new system to identify whether these technologies are new or just new or novel in application. This comparison may not cover all new technologies, in which case the program and reviewers will need to develop ways to assess whether the technologies are critical. The fact that they have not been used previously is an indicator that they are candidate CTEs because they need to be tested.

Following are example questions to ask when identifying CTEs for ground vehicles. They address the principal functions of mobility, firepower, and protection. In an actual case, programs and reviewers could also develop questions using a software architecture and requirements documents built upon the template for vehicles found in MIL-HDBK-881A, *Work Breakdown Structures for Defense Materiel Items.* Special mission equipment and other items also should be considered.

- **Mobility (e.g., power package/drive train, suspension/ steering).** How do mobility characteristics (range, speed, agility, endurance, and so forth) compare with existing vehicles? Is the suspension system proven for the weight and mobility required of the concept system? Has the suspension system been proven to provide a robust, reliable, and stable platform for stationary and on-the-move firing for the type of armaments systems intended for the concept vehicle? Have the engine characteristics (power per unit weight, SFC, cooling and thermal signature characteristics, and so forth) been proven in service? Are the power train elements new or in new environments or with extended performance envelopes? Is the mobility subsystem dependent on any new software capabilities using AI/ML? Is firmware for components of the mobility subsystem new development, or modified and reuse of existing firmware?

- **Control.** How is the vehicle controlled, and how does it interact with the operator? How much autonomy is it required to have? Can it operate without human intervention? Are there safety concerns in autonomous modes? Is the control system dependent on any new software capabilities using AI/ML? Has control software been demonstrated before or is it new or modified development?

- **Firepower (e.g., armament, fire control, automatic loading).** Are the weapons new? Is new ammunition to be developed? What is the nature of the new ammunition? Will the unit have an autoloader? If so, is it new? Has ammunition and autoloader compatibility been established? Has a weapon that has the intended characteristics ever been mated with a platform comparable to the weight and structure characteristics of the vehicle platform? Are firing data available on force and motion characteristics of the weapon for all the intended natures of ammunition? Will fire control software require new or modified development? Is the fire control software dependent on new capabilities, e.g., integration of new sensor feeds?

- **Protection (e.g., hull/frame, turret assembly).** Are full-scale data available to demonstrate that the intended passive protection is adequate for all features and required aspects of the design configuration? If not, what are the alternative approaches, and what data are available to demonstrate that these approaches meet the need? Are reactive armor applications intended, and are data available to allow a flexible design that meets system needs? Does the reactive armor meet logistic requirements (e.g., are there insensitive explosive mandates)? Is the use of an active protection system (APS) intended? If so, what data are available to demonstrate its efficacy?

A.3.3 Missiles

Following are example questions to ask when identifying CTEs for missile development:

- **Guidance and control.** Has the type of guidance under consideration been used before? If so, was it successful in the similar application? Do the field of view, field of regard, scan rate, slew rate, sensitivity, acuity, or any other performance parameters exceed what other affordable guidance systems have achieved? Has the guidance system been tested in prototype form? Has it been tested from a tower, in captive carry, or in flight? Has it been tested against realistic targets in realistic environments? Are the sensor range and the missile control time constant compatible with the dynamics of the end game? What significance does software and firmware have in achieving expected performance requirements for guidance and control? What software development is necessary?

- **Propulsion and structure.** Is there a propellant that can meet the specific impulse requirement and have acceptable burn rates, safety characteristics, physical characteristics, and cost? What size batches of this propellant have been made? What size test motors have been fired? Has the combination of case, insulation, grain support, and grain configuration ever been used in a rocket motor? Does the design have any special features (e.g., multiple burn, throttling, air-burning)? Does the propulsion require software and firmware control development?

A.3.4 Ships, Submarines, and Naval Weapon Systems

The at-sea environment poses unique challenges to new technologies and systems. The new system will have pose questions that apply to all combat systems and other questions that are appropriate for all hull, mechanical, and electrical systems.

Following are example questions to ask when identifying CTEs for surface ship, submarine, and naval weapon systems:

- **Combat systems.** Has the weapon system been tested at sea to establish its firing accuracy in a realistic environment? Has the effect of ship motion and weather variables on targeting been considered? Has the weapon been cleared by the Weapon Systems Explosive Safety Review Board (WSERB) to be placed on board a ship or submarine? Does the weapon warhead meet insensitive munitions requirements? Has the sensor system been tested in realistic at-sea conditions for wave motions and accelerations? Are batteries and power supplies needed by the sensor system compatible with the ship's power grid? Is the system safe or does it present hazards in case of fire or shock? Has the weapon or sensor system been evaluated for maintenance requirements and logistics needs since the ship is a closed system that must carry its own spares? What software is needed for the combat systems and is there new development necessary?

- **Ship and submarine hull, mechanical, and electrical systems.** Does the new system or hull itself use new materials? Have these materials been evaluated for corrosion at sea? How does the weight of a new hull compare with previous designs? If the new hull system comes from a commercial application, has it been evaluated for military usage? For a subsystem, has it been to sea on a ship or submarine previously? For a new hull or a new material, can it withstand the effect of a collision or grounding incident? For a submarine hull, can it withstand cyclic contraction and expansion with depth changes? Does the new system make the ship more vulnerable in any way? For new propulsion systems, does the new system provide an improvement in propulsive efficiency? Does the new system increase or decrease the ship or submarine signature? Does the new system increase the draft of the ship, thus limiting the ports in which it can operate? Does the propulsion system cavitate during operation, thus reducing efficiency? Does the hull, mechanical, or electrical systems require new software development?

- **Submarine-specific issues.** Has the new system been tested at depth? Does it meet the Submarine Safety Certification Program (SUBSAFE) [8] requirements? Does the new

[8] SUBSAFE is a U.S. Navy quality assurance program to maintain the safety of the submarine fleet. All systems exposed to sea pressure or critical to flooding recovery are subject to SUBSAFE. All work performed and all

system add to the submarine acoustic or non-acoustic signature in any way? Does the system generate underwater sound that is detrimental to marine life?

- **Surface-ship-specific issues.** Will the system or subsystem be adversely affected by the motions and accelerations caused by waves? Will the system or subsystem increase the ship's drag in any way? Will the system or subsystem have an environmentally unacceptable discharge?

A.3.5 Information Systems

Following are example questions to ask when identifying CTEs for information systems:

- **General questions (particularly for COTS products).** Does this candidate CTE claim to implement standards that provide critical functionality? How was the compliance to these standards verified? Is there familiarity with the element from other projects? How is the commercial use of this candidate CTE different from the DoD use? Will this candidate CTE work in large-scale environments such as the DoD GIG? What aspects of the system design are dependent on unique features or particular versions of the candidate CTE? Will these unique features be sustained in future versions? Would this candidate CTE be modified, tailored, extended, or enhanced from its original state? Who will perform these modifications? How complex are these modifications? What version of this candidate CTE has been tested? Is this the same version that will enter production? Does this candidate CTE depend on other systems? Does the candidate CTE conform with the required size, weight, and power (SWAP) requirements? Have evaluations been performed with respect to Zero Trust and Cyber Security guidance in order to determine degrees of risk to the enterprise, infrastructure or personnel? For cloud computing products, have all relevant CIO standards and guidelines been adhered to?

- **Terminal hardware.** Terminal hardware consists of video displays, audio/ sound systems, keyboards, touch-screen terminals, personal digital assistants (PDAs) and so forth. Are there extenuating physical environment considerations for size, weight, visibility in daylight, or usability? What software development is necessary for terminal hardware?

- **Processing hardware.** Processing hardware consists of processors, memory, servers, supercomputers, mainframes, blade servers (self-contained, all-inclusive computer servers with a design optimized to minimize physical space), and so forth. Are needed software development environments supported? Have any significant changes been

---

materials used on those systems are tightly controlled to ensure the material in the assembly and the methods of assembly, maintenance, and testing are correct.

made to the operating system and other systems software? Are processors able to handle average and peak processing loads? How does needed processing power scale with the number of users?

- **Storage hardware.** Storage hardware consists of disk drives, magnetic tapes, redundant array of inexpensive disks (RAID), controllers, and so forth. Is the storage media new? How is storage being connected to the processing hardware? Is storage balanced with processing capacity? How will storage scale with increasing processing capacity?

- **Networking hardware.** Networking hardware consists of routers, switches, access points, network interface cards (NICs), local area network/wide area network (LAN/WAN) components, storage area network (SAN) components, and so forth. Do requirements for bandwidth, delay, jitter, loss, and availability imply that new or modified hardware is required? Is wireless performance acceptable in the expected electromagnetic environment? Is the network able to grow in physical size and bandwidth while still satisfying key performance requirements?

A.3.6 Networked Communications and Data Management Systems

Example questions to ask when identifying CTEs for networked communications and data management systems are as follows:

- Do the requirements for throughput, data latency, jitter, loss, security, or reliability imply that a new or novel technology is required? Have the network routers been used before within the required performance envelope? Are new or novel media access control, coding, or routing algorithms needed? Is the multiplexing schema new? Is the topology (logical and hardware) new? Do the peak and average data rates require new hardware or algorithms in the system?

- If the network includes wireless technology, have the wireless devices been used previously in the anticipated electromagnetic environment? Does the way in which data sources or uses interface to the network imply a need for a new interface (logical or hardware)? Does the ICD identify any interfaces that are new or novel?

- If the network includes commercially available elements, such as Asynchronous Transfer Mode (ATM)[9] and optical components, have these elements been

---

[9] ATM is an electronic digital data transmission technology that is implemented as a network protocol. The goal was to design a single networking strategy that could transport real-time video and audio as well as image files, text, and e-mail.

demonstrated for their intended use? Do they support the data rates, switching schema, routing, and any other needed performance?

- Do the DoD information assurance (IA) requirements create a new or novel security environment? Is the network or data management system relying on other systems to provide security functions? Do DoD IA requirements and regulations place requirements on this system or its elements because of its interfaces with other systems?

- Do requirements for scalability and the capability to upgrade imply the need for new algorithms? Does the scale of the system imply a new environment for the network?

A.3.7 Business Systems

DoD business systems often use COTS products to achieve a new capability. Following are example questions to ask when identifying CTEs for business systems:

- Are the logical and data environments for each COTS element new or novel? Do special data synchronization requirements or needs that imply the need for new wrapper algorithms? Has the COTS system been run in the intended operating system environment or on the intended target workstations and servers?

- Is a new suite of hardware (servers, networks, and so forth) needed to run the business system? Will the interfaces for the server require a new or novel hardware or software technology? Will new processors be required? If so, will these processors support the anticipated speeds?

- Do the DoD IA requirement imply a new security environment? Have the selected COTS products been demonstrated or tested with the IA technologies chosen for the system? Do the data rates and reliability requirements in war versus those in peacetime imply a new or novel environment for the system? Can the existing network infrastructure handle the anticipated data-flow requirements?

- Have requirements from outside the Capability Development Document (CDD) been considered? For example, consider the Health Insurance Portability and Accountability Act (HIPAA) for a medical system or the Privacy Act for a personnel system. Are the laws and regulations for DoD use the same as those for any COTS implementation?

- What consideration do the requirements have for the responsiveness and timeliness across the system? If a requirement exists, what information and activities are available to show that the entire suite of IT (COTS applications, networks, servers, and so forth) will meet those expectations? If no such requirements exist, how will the installers understand and judge the ability to provide a system that the users will find acceptable?

- How will the COTS products ensure consistency and timeliness of data? Do the COTS products have mechanisms or techniques to assure users that they have the latest data from an authoritative source? How will the authoritative data set be promoted and managed across the system? How will it be maintained to ensure that it is updated in a timely manner? Does the system have enough capacity to handle the anticipated data storage and communication requirements?

- How do issues of scalability affect the selected COTS products? Have the products been run in organizations with similar numbers of users, similar sizes of data sets, and similar suites of applications? Is the system scalable to an organization commensurate with its anticipated use in DoD? Is that scalability affected by any other chosen technologies (e.g., IA)?

- Have all the software and hardware components been used together in a similar manner and with similar interfaces? How does the DoD environment differ from the environments in which the components have been used previously?

A.3.8 Mission Planning Systems

Mission planning systems often include a combination of COTS/GOTS software and developmental software to integrate software systems. Usually for these systems, the components are mature in their *original* environment. What needs to be determined is how the newly integrated environment differs. Following are example questions to ask when identifying CTEs for mission planning systems:

- Are there new logical or data relationships for each component? Are the algorithms used to create interfaces new or novel? Are new hardware components needed to enable interoperability?

- Do the information exchange requirements (IERs) require many more interfaces than previously achieved? Does this imply a new logical or security environment?

- Will the components run on a new hardware system? on a new network?

- Will the need to upgrade the components introduce new algorithms or technologies?

A.3.9 Embedded Systems inside of Tactical Systems

The embedded software in tactical systems is often inextricably linked to the requirements and performance of the developmental hardware. However, the developmental responsibility for hardware and software may be separate. Following are example questions to ask when identifying CTEs for embedded software in tactical systems:

- How does the performance of the hardware rely on the software, and vice versa?
- Can the requirements be clearly mapped to those met with hardware and those met with software?
- Have the algorithms been proven to work in a simulated environment? How is that environment different from the operational environment?
- Do the data dissemination requirements imply a new or novel technology or environment?
- Does timeliness imply new or novel algorithms or hardware? Does the quality of the data (e.g., engagement quality) imply special processing that has not been done previously?
- Does the tactical system have an interface with non-tactical systems that have significantly different performance requirements?
- Are the number of software systems or lines of code unprecedented? Do the IERs imply a new or novel technology?
- Does the software provide a degree of autonomy? Is the decision tree well characterized? Should other approaches to autonomy be considered?

Appendix B: Suggested TRA Outline

The TRA report should consist of: (1) a short description of the program; (2) a list of critical technology elements (CTEs) that pose a potential risk of program execution success, with the PM's assessment of the maturity of those technologies as demonstrated in a relevant environment and a description of any risk-mitigation plans; (3) the SME team membership and credentials; (4) SME team findings, conclusions, supporting evidence, and major dissenting opinions; and (5) a cover letter signed by the CAE approving the report; forwarding any requests for waivers of the 10 USC 4252 certification requirement with supporting rationale, and providing other technical information deemed pertinent by the CAE and PM. The CAE and PM can provide any supplemental material as desired.

The following outline is a skeletal template for TRA submissions:

B.1 Technology Readiness Assessment

1.0 Executive Summary

2.0 Introduction

- 2.1 Purpose

3.0 Program Overview

- 3.1 Program Objective
- 3.2 Program Description
- 3.3 System Description

4.0 Program Technology Risks Summary and Readiness Assessment

- 4.1 Process Description [Would this be better in the introduction?]
- 4.2 Technologies Assessed
- 4.3 PM's and SME Team's Assessments of Technology Risk and Technology Demonstration in a Relevant Environment
  - 4.3.1 First Technology
  - 4.3.2 Next Technology

5.0 Summary of Findings

Following is an annotated version of the TRA template.

Executive Summary (One Page)

1. Executive Summary

2. Introduction

2.1 Purpose (One Paragraph)

Provides a short introduction that includes the program name, the system name if different from the program name, and the milestone or other decision point for which the TRA was performed. For example, "This document presents an independent TRA for the UH-60M helicopter program in support of the MS B decision. The TRA was performed at the direction of the UH-60M Program Manager."

3. Program Overview

3.1 Program Objective (One Paragraph)

States what the program is trying to achieve (e.g., new capability, improved capability, lower procurement cost, reduced maintenance or manning, and so forth). For MS B, refers to the Capability Development Document (CDD) that details the program objectives.

3.2 Program Description (One Page or Less)

Briefly describes the program or program approach—not the system. It should identify the program increments or spirals covered by the TRA, if relevant. The following questions may help shape the program description:

- Does the program provide a new system or a modification to an existing operational system? Is it an evolutionary acquisition program? If so, what capabilities will be realized by increment?
- When is the Initial Operational Capability (IOC)?
- Does the program have multiple competing prime contractors?
- Into what architecture does the system fit?
- Does the program's success depend on the success of other acquisition programs?

3.3. System Description (Nominally 5 Pages)

Describes the overall system, the major subsystems, and components to give an understanding of what is being developed and to show what is new, unique, or special about them. This information should include the systems, components, and technologies to be assessed. Describes how the system works (if this is not obvious).

4 Technology Risk Summary and Assessment

4.1 Process Description (Nominally 2 Pages)

Tells the composition of the SME team and what organizations or individuals were included. Identifies the special expertise of these participating organizations or individuals. This information should establish the subject matter expertise and the independence of the SME team. Members should be experts in relevant fields. Usually, the PM will provide most of the data and other information that form the basis of a TRA.

Tells how technologies to be assessed were identified (i.e., the process and criteria used and who identified them). States what analyses and investigations were performed when making the assessment.

4.2 Technologies Assessed

Lists the technologies included in the TRA and why they were selected as critical. Describes the relevant environment in which each technology was assessed. Normally, this would be the operational environment in which the system is intended to perform; however, this can be adjusted if the technology's environment will be controlled while it operates in the system in question.

Includes a table that lists the technology name and includes a few words that describe the technology, its function, and the environment in which it will operate. The names of these technologies should be used consistently throughout the document.

Includes any technologies that the SME team considers critical and that have not been included in previously fielded systems that will operate in similar environments.

Note that the technologies of interest here are not routine engineering or integration risk elements. They are items that require more than the normal engineering development that would occur in design for production as opposed to technology maturation programs.

4.3 Technology Demonstration and Assessment

4.3.1 First Technology

Describe the technology. Describes the function it performs and, if needed, how it relates to other parts of the system. Provides a synopsis of development history and status. If necessary, this synopsis can include facts about related uses of the same or similar technology, numbers of hours breadboards were tested, numbers of prototypes built and tested, relevance of the test conditions, and results achieved.

Describes the environment in which the technology has been demonstrated.

Provides a brief analysis of the similarities between the demonstrated environment and the intended operational environment.

States whether the assessed technology has been demonstrated in a relevant environment or not.

Provides data, including references to papers, presentations, data tables, and facts that support the assessments as needed. These references/tables/graphs can be included as an appendix.

Provides a summary of planned risk-mitigation activities showing how those activities will reduce the risk of the technology to acceptable levels.

Provides the SME team's concurrence or non-concurrence and the rationale therefore, and the SME team's assessment of the adequacy of proposed risk mitigation plans.

4.3.2 Next Technology

For the other technologies assessed, this paragraph and the following paragraphs (e.g., 4.3.3, 4.3.4, and so forth) present the same type of information that was presented in paragraph 4.3.1.

5 Summary of Findings (One Page)

Includes a table that lists the technologies that were assessed, the degree of risk associated with each, recommended mitigation measures if any, and whether each was demonstrated in a relevant environment. Summarizes any technologies for which the PM and the SME team are in disagreement as to the degree of risk or whether the technology has been demonstrated in a relevant environment.

B.2 TRA Report Template from GAO 2020

GAO 2020 says this example of a TRA report template "identifies the types of information that should be included. Each organization should tailor the template to accommodate how it will report the TRA information. For example, some organizations prepare briefing charts as a TRA report to comport with their own internal practices. Others prepare detailed reports with specific formatting requirements. At a minimum, organizations should ensure that the suggested reporting elements in the figure are included."

Figure 10: Technology Readiness Assessment (TRA) Report Template

TRA REPORT TEMPLATE

EXECUTIVE SUMMARY

Briefly state who requested the Technology Readiness Assessment (TRA), what organization was responsible for conducting the TRA, what technology was assessed. Provide a summary table of the critical technologies and corresponding Technology Readiness Levels (TRL) rating determination made by the TRA team for each.

INTRODUCTION

Background

Provide project/program overview and background information (i.e., general description of the program and the technology system, including the critical technologies to be assessed).

Purpose and Scope of the TRA

Provide an explanation of why the TRA was conducted (i.e. program management's review for maturing technologies, TRA required for a decision point, etc.), and scope of the assessment. Reference applicable decision memos and planning documents.

TRA Process

Provide an overview, and plan of actions and milestones to conduct the TRA. Reference planning documents.

RESULTS

Provide the following for each critical technology assessed:

- Technology Reviewed: Provide a detailed description of the technology that was assessed. The level of detail can vary depending on the phase of development, design characteristics, and scope of review. Organizations should strive to provide a sufficient amount of information to facilitate an understanding of the technology assessed.
- Function: Describe the functions of the critical technologies.
- Relationship to Other Systems: Describe how the critical technologies interface with other systems.
- Development History and Status: Summarize pertinent development activities that have occurred to date on the critical technology.
- Relevant Environment: Describe relevant parameters inherent to the critical technology or the function it performs as it relates to the intended operational environment.
- Comparison of the Relevant Environment and the Demonstrated Environment

Describe differences and similarities between the environment in which the critical technology has been tested and the intended environment when fully operational. The demonstrated environment must correspond to the identified relevant environment for the TRL to be justified.

- Technology Readiness Level Determination

State the TRL determined for the critical technology and provide the basis justification for the TRL.

- Operational Requirement: Describe the required/traceable system functional performance and enabling features for the critical technology elements.
- Test Results: describe the analytical reports, test reports, or other information that was used to test the readiness, and functionality of the critical technology.

EXECUTIVE APPROVAL

- Provide statement or memo that shows executive management review and approval of the TRA report.

ATTACHMENTS

Include the following planning documents:

- TRA Plan
- Supporting documentation for identification of critical technologies
- Completed tables: TRL Questions for critical technologies
- List of support documentation for TRL determination
- TRL Summary table
- Lessons Learned
- Team biographies

Source: GAO analysis of agency documents. | GAO-20-48G

Figure B-1. TRA Report Template

Appendix C: Technology Maturation Plan Template

TECHNOLOGY MATURATION PLAN (TMP) TEMPLATE

INTRODUCTION

Purpose of the Project

Provide a brief summary of the project's mission, status, technology(s) being deployed, etc. During early technology development, the project may be specified or identified. It could be a broad area announcement, a description of a capability gap that the critical technology is being developed to address, or a requirement.

Purpose of the TMP

Describe the objectives and content of the TMP and relate it to the status of the project and any upcoming major milestone reviews.

TECHNOLOGY ASSESSMENTS OF THE PROJECT

Summary of Previous Independent Technical Reviews

Summarize any previous Independent Technical Reviews or other technical assessments that may have contributed to the need for a TRA and the TMP.

Summary of Previous Technology Readiness Assessment(s)

Describe the results of previous TRAs with emphasis on the latest TRA that is driving the TMP. Include the definition of TRLs as used in the TRA. Discuss the critical technologies that were determined for the project.

Technology Heritage

Summarize the previous technology development activities that brought the technology to its current state of readiness. Include discussions of any full-scale deployments of the technology in similar applications.

Current Project Activities and Technology Maturation

Describe ongoing technology development activities (if any) that were initiated prior to the TMP. Completion of these activities should define the starting point for the TMP.

Management of Technology Maturity

Indicate the project office/organizations that will be responsible for managing the activities described in the TMP. Include a brief discussion of key roles and responsibilities.

TECHNOLOGY MATURATION PLAN

Development of Technology Maturation Requirements

Describe the approach used in defining the required technology development activities that will be conducted as described in the TMP. These could include evaluating incomplete questions in the risk assessments, value engineering, or other tools used.

Life-Cycle Benefit

Briefly discuss life-cycle benefits to the project that will result from successful completion of the TMP technology development activities.

Specific TMPs

Maturation plans for each critical technology will be described following the format below for each critical technology that was defined in the latest TRA.

Source: GAO 2020

Figure C-1. TMP Template

TECHNOLOGY MATURATION PLAN (TMP) TEMPLATE *(continued)*

Critical Technology A

- Key technology addressed *(Describe function of the critical technology in the project).*
- Objective *(Succinctly state the objective of the critical technologies).*
- Current State *(Describe current status of critical technology—including TRL assigned in the latest TRA).*
- Technology Development Approach *(Describe the needed technology development work to sufficiently address the maturity gaps, and mature the technology to the next TRL or acceptable maturity goal. This could include the performing organization, location, etc.)*
- Scope *(Provide a list of the key steps to be taken in performing the work, including a table with milestones, performance targets, TRL to be achieved at milestones or stage gates, and rough order of magnitude of the cost and schedule of development. Include the risks associated with the planned strategy and off ramps/decision points if results are less than expected.)*

Critical Technology B (etc., as needed)

TECHNOLOGY MATURITY SCHEDULE

Provide and briefly discuss a high-level schedule of the major technology development activities for each critical technology. Any major decision points such as proceeding with versus abandoning the current technology, selection of a backup technology, etc. should be included. Detailed schedules should be given in test plans or used for status meetings during implementation.

SUMMARY TECHNOLOGY MATURITY BUDGET

Present the rough order of magnitude costs to reach a predetermined TRL for each major technology development activity for all critical technologies in the project. Include the total technology maturation costs.

REFERENCES

- **Appendix A**

  Previous independent reviews and assessments (if applicable to support information in Section 2)
- **Tables 1, 2, 3, etc.**

  Table(s) for each critical technology, listing of test activities, planned completion date, performance targets, resulting TRL as each increment of testing is completed, and rough order of magnitude costs.
- **Table X.**

  Technology maturity budget for project
- **Figure 1.**

  Process flow diagram (for technology being assessed)
- **Figure 2.**

  Technology maturity schedule
- **Figure 3.**

  Project execution strategy diagram

Source: GAO 2020

Figure C-1. TMP Template *(continued)*

Glossary

Breadboard: Integrated components that provide a representation of a system/subsystem and that can be used to determine concept feasibility and to develop technical data. Typically configured for laboratory use to demonstrate the technical principles of immediate interest. May resemble final system/subsystem in function only.

Component Acquisition Executive: A CAE is a single official within a DoD component that is responsible for all acquisition functions within that component. The CAEs are responsible for all acquisition functions within their Component.

Critical Program Information: U.S. capability elements that contribute to the warfighters' technical advantage, which, if compromised, undermine U.S. military preeminence. U.S. capability elements may include but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

Critical Technology: *See* Critical Technology Element

Critical Technology Element: A Critical Technology Element (CTE) is a new or novel technology that a platform or system depends on to achieve successful development or production or to successfully meet a system operational threshold requirement.

Decision Authority/Maker: The official responsible for oversight and key decisions of programs. The official may be the Defense Acquisition Executive, CAE, or the Program Executive Officer, or other designated official by the CAE.

Defense Acquisition Executive: A DAE is the individual responsible for supervising the Defense Acquisition System. The DAE takes precedence on all acquisition matters after the Secretary of Defense (SECDEF) and the Deputy Secretary of Defense (DEPSECDEF).

Engineering and Manufacturing Development (EMD) Phase: The EMD Phase is where a system is developed and designed before going into production. The EMD Phase starts after a successful Milestone B which is considered the formal start of any program. The goal of this phase is to complete the development of a system or increment of capability, complete full system integration, develop affordable and executable manufacturing processes, complete system fabrication, and test and evaluate the system before proceeding into the Production and Deployment (PD) Phase.

Evaluator: SME identified by the PM to certify the maturity of the CTE of the program.

High Fidelity: Addresses form, fit, and function. A high-fidelity laboratory environment would involve testing with equipment that can simulate and validate all system specifications within a laboratory setting.

Low Fidelity: A representative of the component or system that has limited ability to provide anything but first-order information about the end product. Low-fidelity assessments are used to provide trend analysis.

Materiel Solution Analysis (MSA) Phase: The MSA Phase assesses potential solutions for a needed capability in an Initial Capabilities Document and satisfies the phase-specific Entrance Criteria for the next program milestone designated by the Milestone Decision Authority (MDA). The MSA phase is critical to program success and achieving materiel readiness because it's the first opportunity to influence systems supportability and affordability by balancing technology opportunities with operational and sustainment requirements. During this phase, various alternatives are analyzed to select the materiel solution and develop the Technology Development Strategy to fill any technology gaps.

Milestone B: Milestone B is the juncture to enter the EMD acquisition phase. It is considered the official start of an acquisition program where major commitments of resources are made. Statutes and DoD policy require documentation, such as a TRA, for Major Defense Acquisition Programs (MDAPs). See Weapon Systems Acquisition Reform Act (WSARA), Pub. L. No. 111-23, § 204, 123 Stat. 1704, 1723-24 (May 22, 2009); DoD Instruction 5000.02, at 7, para. 5(c)(3).

Milestone Decision Authority: The Milestone Decision Authority (MDA) is the acquisition executive of a Major Defense Acquisition Program (MDAP) responsible for ensuring that all regulatory requirements and acquisition procedures are in compliance with DoD Instruction 5000.02. The MDA assesses a program's readiness to proceed to the next acquisition phase and determines if a program has met its phase exit requirements and can proceed into the next acquisition phase during a milestone review in terms of cost, schedule, and performance.

Model: A functional form of a system, generally reduced in scale, near or at operational specification. Models will be sufficiently hardened to allow demonstration of the technical and operational capabilities required of the final system.

Operational Environment: An operational environment is a set of operational conditions, representative of the full spectrum of operational employments, which are applied to a CTE as part of a system prototype (TRL 7) or actual system (TRL 8) in order to identify whether any previously unknown or undiscovered design problems might impact required (threshold) functionality.

Prototype: A physical or virtual model used to evaluate the technical or manufacturing feasibility or military utility of a particular technology or process, concept, end item, or system.

Relevant Environment: A relevant environment is a set of stressing conditions, representative of the full spectrum of intended operational employments, which are applied to a CTE as part of a component (TRL 5) or system/subsystem (TRL 6) to identify whether any design changes to support the required (threshold) functionality are needed.

Simulated Operational Environment: Either (1) a real environment that can simulate all the operational requirements and specifications required of the final system or (2) a simulated environment that allows for testing of a virtual prototype. Used in either case to determine whether a developmental system meets the operational requirements and specifications of the final system.

Technology Readiness Assessment (TRA): Technology Readiness Assessment (TRA) (10 USC 2366b) is a formal, metrics-based process and accompanying report that assesses the maturity of critical hardware and software technologies called Critical Technology Elements (CTEs) to be used in systems. It is conducted by an Independent Review Team (IRT) of subject matter experts. All DoD acquisition programs must have a formal TRA at Milestone B and at Milestone C. A preliminary assessment is due for the Development RFP Release Decision Point.

Technology Readiness Level (TRL): TRLs are a method of estimating the technology maturity of CTE of a program during the Acquisition Process. They are determined during a Technology Readiness Assessment (TRA) that examines program concepts, technology requirements, and demonstrated technology capabilities.

Acronyms

AAF	Adaptive Acquisition Framework
ACAT	Acquisition Categories
ADM	Acquisition Decision Memorandum
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
CAD	Computer-aided design
CAE	Component Acquisition Executive
CHIEF	Comprehensive Human Integration Evaluation Framework
CFD	Computational fluid dynamics
CONOPS	Concept of Operations
CPI	Critical Program Information
CT	Critical Technology (GAO term)
CTE	Critical Technology Element
DAE	Defense Acquisition Executive
DBS	Defense Business Systems
DoD	Department of Defense
DOE	Department of Energy
DOF	Degree of freedom
DDR&E	Director, Defense Research and Engineering
EMD	Engineering and Manufacturing Development
GAO	Government Accountability Office
GATES	Global Air Transportation Execution Systems
GFM	Government Freight Management
GIG	Global Information Grid
HFW	Human Factors Workbench
HFRM	Human Factors Risk Manager
HMD	Helmet-mounted display
HSIF	Human Systems Integration Framework
HWIL	Hardware-in-the-loop

IA	Information assurance
IMS	Integrated Master Schedule
IR	Infrared
IRL	Integration Readiness Level
IRT	Independent Review Team
ITRA	Independent Technical Risk Assessment
IT	Information Technology
ITV	in-transit visibility
LRIP	Low-Rate Initial Production
MEMS	Microelectromechanical Systems
MRL	Manufacturing Readiness Level
NASA	National Aeronautics and Space Administration
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MRA	Manufacturing Readiness Assessment
MTA	Middle Tier of Acquisition
MTS	Movement Tracking System
P&D	Production and Deployment
PDR	Preliminary Design Review
PEO	Program Executive Office
PM	Project Manager
QoS	Quality of Service
RI3	Risk Identification: Integration and 'Ilities
RF	Radio frequency
S&T	Science and Technology
SME	Subject Matter Expert
SMLs	Sustainment Maturity Levels
SRL	System Readiness Level
STMS	Surface Transportation Management System

TD	Technology Development
TDS	Technology Development Strategy
TMP	Technology Maturation Plans
TRA	Technology Readiness Assessment
TRL	Technology Readiness Level
UCA	Urgent Capability Acquisition
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(R&E)	Under Secretary of Defense for Research and Engineering
WBS	Work Breakdown Structure
XML	eXtensible Markup Language

References

10 USC 4252. Major Defense Acquisition Programs: Certification Required before Milestone B Approval, January 13, 2021.

10 USC 4272. Independent technical risk assessments. January 1, 2022.

Department of Defense Independent Technical Risk Assessment Execution Guidance. Office of the Under Secretary of Defense for Research and Engineering, December 2020. https://ac.cto.mil/wp-content/uploads/2020/12/DoD-ITRA-ExecGuide-2020s.pdf

Department of Defense Systems Engineering Plan (SEP) Outline. Version 4.1. Office of the Under Secretary of Defense for Research and Engineering, May 2023.

DoD Directive 5000.01. “The Defense Acquisition System.” Office of the Under Secretary of Defense for Acquisition and Sustainment, September 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf

DoD Directive 5000.71. “Rapid Fulfillment of Combatant Commander Urgent Operational Needs and Other Quick Action Requirements.” Office of the Under Secretary of Defense for Acquisition and Sustainment, October 2022. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500071p.pdf

Department of Energy. “Standard Review Plan (SRP): Technology Readiness Assessment Report.” Office of Environmental Management, March 2010.

DoD Instruction 5000.02. “Operation of the Adaptive Acquisition Framework.” Under Secretary of Defense for Acquisition and Sustainment, January 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf

DoD Instruction 5000.74. “Defense Acquisition of Services.” Office of the Under Secretary of Defense for Acquisition and Sustainment, January 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500074p.pdf

DoD Instruction 5000.75. “Business Systems Requirements and Acquisition.” Office of the Under Secretary of Defense for Acquisition and Sustainment, January 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF

DoD Instruction 5000.80. “Operation of the Middle Tier of Acquisition.” Office of the Under Secretary of Defense for Acquisition and Sustainment, December 2019. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500080p.PDF

DoD Instruction 5000.81. “Urgent Capability Acquisition.” Office of the Under Secretary of Defense for Acquisition and Sustainment, December 2019. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500081p.PDF

DoD Instruction 5000.83. “Technology and Program Protection to Maintain Technological Advantage.” Office of the Under Secretary of Defense for Research and Engineering, July 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf?ver=2020-07-20-150345-930

DoD Instruction 5000.85. “Major Capability Acquisition.” Office of the Under Secretary of https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500085p.pdf

DoD Instruction 5000.86. "Acquisition Intelligence." Office of the Under Secretary of Defense for Acquisition and Sustainment and Office of the Under Secretary of Defense for Intelligence and Security, September 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500086p.PDF

DoD Instruction 5000.87. "Operation of the Software Acquisition Pathway." Office of the Under Secretary of Defense for Acquisition and Sustainment, October 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF

DoD Instruction 5000.88. "Engineering of Defense Systems." Office of the Under Secretary of Defense for Research and Engineering, November 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500088p.PDF

DoD Instruction 7041.03. "Economic Analysis for Decision-making." Director of Cost Assessment and Program Evaluation, September 2015. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/704103p.pdf

Defense Technical Risk Assessment Methodology (DTRAM), version 6.4. Office of the Under Secretary of Defense for Research and Engineering, May 2023. https://ac.cto.mil/wp-content/uploads/2021/01/DTRAM-0-1.pdf

Eckstein, Megan, "How the U.S. Navy Is Creating the 'Nirvana of One Combat System." *Defense News,* February 8, 2023.

GAO. *Best Practices: Better Management of Technology Development Can Improve Weapon System Outcomes.* Washington, D.C.: General Accounting Office, July 1999. https://www.gao.gov/assets/nsiad-99-162.pdf

GAO. *Columbia Class Submarine: Immature Technologies Present Risks to Achieving Cost, Schedule, and Performance Goals*. GAO-18-158. Washington, D.C.: Government Accountability Office, December 2017. https://www.gao.gov/assets/gao-18-158.pdf

GAO. *Technology Readiness Assessment Guide*. GAO-20-48G. Washington, D.C.: Government Accountability Office, January 2020. https://www.gao.gov/assets/gao-20-48g.pdf

GAO. Technology Readiness Assessment Guide (Draft). Provisional draft released for public comment. GAO-16-410G. Washington, D.C.: Government Accountability Office, August 2016.

Manufacturing Readiness Level (MRL) Deskbook. OSD Manufacturing Technology Program in Collaboration with Joint Service/Industry MRL Working Group, Department of Defense, October 2022. http://www.dodmrl.org/

MIL-STD-881E. Work Breakdown Structures for Defense Materiel Items, October 2020. https://cade.osd.mil/Content/cade/files/coplan/MIL-STD-881E%20Final.pdf

MIL-HDBK-881A. Work Breakdown Structures for Defense Materiel Items, July 30, 2005, National Aeronautics and Space Administration, "Technology Readiness Assessment Best Practices Guide." Office of the Chief Technologist. https://ntrs.nasa.gov/api/citations/20205003605/downloads/%20SP-20205003605%20TRA%20BP%20Guide%20FINAL.pdf

O'Neil. "Development of a Human Systems Integration Framework for Coast Guard Acquisition." June 1, 2014. DTIC Accession Number: ADA608012.

Product Support Manager Guidebook. Office of the Under Secretary of Defense for Acquisition and Sustainment, May 2022. https://www.dau.edu/tools/t/Product-Support-Manager-(PSM)-Guidebook

Risk Identification: Integration & Ilities (RI3) Guidebook version 1.2. Prepared for the Technology Development Subprocess Developing and Sustaining Warfighting Systems Process by the Implementation Team. December 2008.

Technology Readiness Assessment (TRA) Deskbook. Department of Defense, May 2005.

Technology Readiness Assessment (TRA) Deskbook. Director, Research Directorate, Office of the Director of Defense Research and Engineering, July 2009. https://www.skatelescope.org/public/2011-11-18_WBS-SOW_Development_Reference_Documents/DoD_TRA_July_2009_Read_Version.pdf

Technology Readiness Assessment (TRA) Guidance. Assistant Secretary of Defense for Research and Engineering, April 2011. https://www.afacpo.com/AQDocs/TRA2011.pdf

Websites

Defense Acquisition University Adaptive Acquisition Framework (AAF) Pathways https://aaf.dau.edu/aaf/aaf-pathways/

DAU Human Systems Integration (HSI) Community of Practice https://www.dau.edu/cop/hsi/Pages/Default.aspx

Technology Readiness Assessment Guidebook

Office of the Executive Director for Systems Engineering and Architecture
Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301
osd-sea@mail.mil
https://www.cto.mil/sea/