Carnegie Mellon University
Software Engineering Institute

OPERATIONAL TEST & EVALUATION (OT&E) ROADMAP FOR CLOUD-BASED SYSTEMS

Prepared for the U.S. Army Evaluation Command (AEC) Under
Project Work Plan 6-644a2

Carol Woody (project lead)
Christopher Alberts
John Klein
Charles Wallen

September 2019

Introduction

The approach the U.S. Department of Defense (DoD) and the U.S. Army use for cloud computing will impact how operational test and evaluation (OT&E) is performed by the Army Test and Evaluation Center (ATEC). While the specifics of a long-term approach continue to evolve—such as with JEDI[1] and the Defense Innovation Board's *10 Commandments for Software*[2]—the DoD has issued new guidance that provides direction to those supporting cloud-based systems. In general, this guidance reflects the increased concern for cybersecurity risk in cloud computing, which affects how computing systems should be acquired, tested, and supported. Core policy and standards documentation such as DoDI 5000.02 and the test and evaluation (T&E) guidance in the recently updated *Cybersecurity Test and Evaluation Guidebook*[3] have also significantly expanded the emphasis on cybersecurity. The impact of these documents and other guidance on the activities performed by ATEC have not been formally assessed or codified to identify the impact on cloud-based systems. To assist AEC with setting a course for its support of the DoD and the Army as they manage cloud technology and cyber risks, the Software Engineering Institute (SEI) was engaged to help build a roadmap for future T&E activities.

[1] This document is located at the following URL: https://media.defense.gov/2019/Aug/08/2002168542/-1/-1/1/UNDERSTANDING-THE-WARFIGHTING-REQUIREMENTS-FOR-DOD-ENTERPRISE-CLOUD-FINAL-08AUG2019.PDF

[2] This document is located at the following URL: https://media.defense.gov/2018/Apr/22/2001906836/-1/-1/0/DEFENSEINNOVATIONBOARD_TEN_COMMANDMENTS_OF_SOFTWARE_2018.04.20.PDFow

[3] This document is located at the following URL: https://www.acq.osd.mil/dte-trmc/docs/CSTE%20Guidebook%202.0_FINAL%20(25APR2018).pdf

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

The SEI conducted training, workshops, and detailed reviews of OT&E deliverables from several selected programs to identify the impacts that the AEC should expect when the Army shifts to cloud technology. OT&E activities related to cybersecurity and effectiveness evaluation currently rely on testers having direct access to system hardware and software, which will change to indirect access through a cloud provider's software interfaces. Critical decisions about cloud capabilities and access to data important to OT&E will be made early in an acquisition, before OT&E is actively involved. The AEC has asked the SEI to assemble the questions that these early decision makers need to consider at each point in the acquisition so that OT&E can be successful.

Each OT&E activity relies on having specific information available. Today, this information is provided by direct inspection and testing near or at the end of the development lifecycle. Cloud computing does not provide testers with physical access to computing and storage hardware and to network connections, which limits testers' ability to control and observe the system during testing. OT&E may not be able to rely on direct test and inspection to produce the information needed to assess cloud-based systems. OT&E must work with program management (PM) and development test and evaluation (DT&E) to establish equivalent information sources from cloud service providers. OT&E must innovate to provide flexible requirements-informed approaches to verify these cloud-based systems that consider the infrastructure risks introduced by cloud computing.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

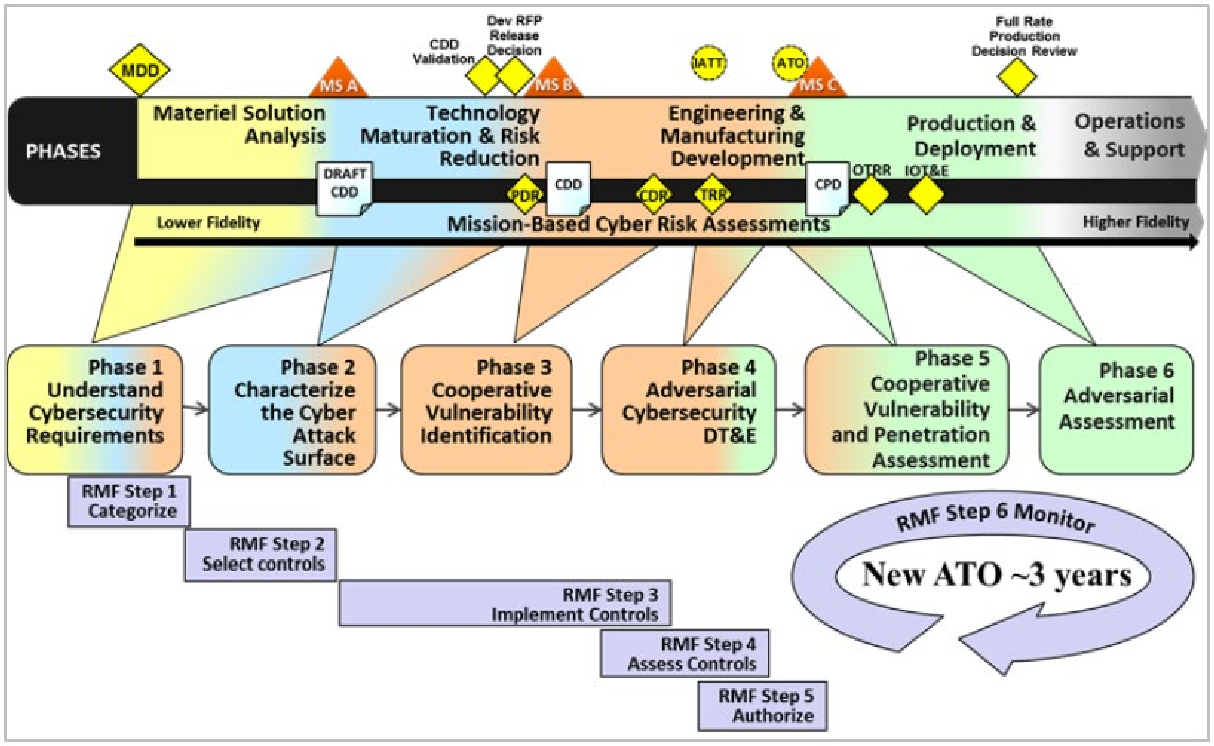

CDD Validation
Dev RFP Release Decision
Full Rate Production Decision Review
MDD
MS A
MS B
IATT
ATO
MS C
PHASES
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Production & Deployment
Operations & Support
DRAFT CDD
PDR
CDD
CDR
TRR
CPD
OTRR
IOT&E
Lower Fidelity
Mission-Based Cyber Risk Assessments
Higher Fidelity
Phase 1 Understand Cybersecurity Requirements
Phase 2 Characterize the Cyber Attack Surface
Phase 3 Cooperative Vulnerability Identification
Phase 4 Adversarial Cybersecurity DT&E
Phase 5 Cooperative Vulnerability and Penetration Assessment
Phase 6 Adversarial Assessment
RMF Step 1 Categorize
RMF Step 2 Select controls
RMF Step 3 Implement Controls
RMF Step 4 Assess Controls
RMF Step 5 Authorize
RMF Step 6 Monitor
New ATO ~3 years

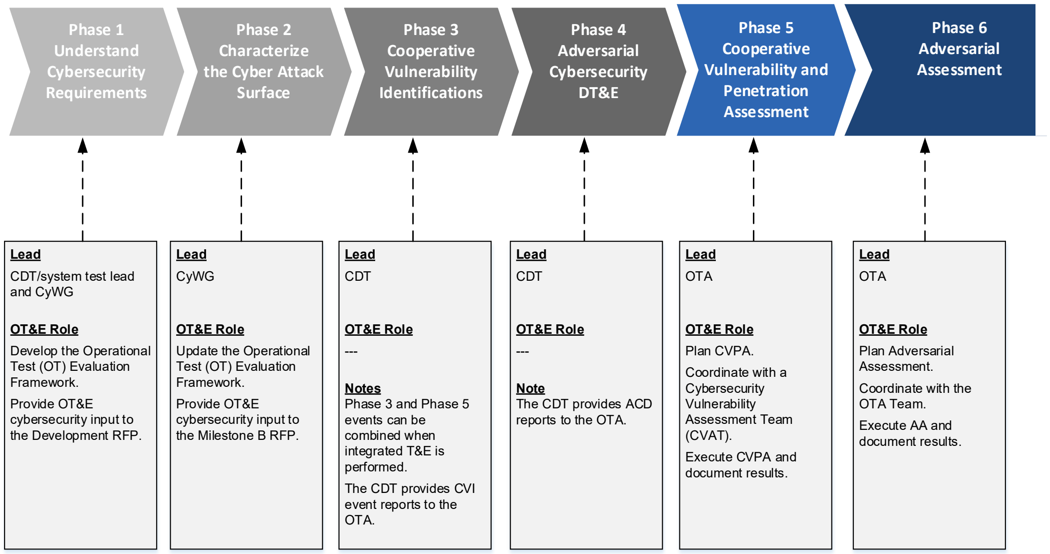
Figure 1: Interaction of RMF and T&E Cybersecurity Activities[4]

Many program decisions made early in the acquisition lifecycle will materially impact the information that will be available to OT&E. It will be incumbent on OT&E to clearly communicate its information needs and concerns to program managers and to partner with them to establish workable OT&E approaches or prepare the Army to accept the risks that remain. Cybersecurity T&E activity takes place in six phases across the lifecycle; these efforts all build off of previous steps with the final two phases focusing specifically on OT&E. Phases 1-6 are shown in Figure 1, mapped to the segments of the lifecycle where they are typically performed.

Cybersecurity OT&E has an indirect role in phases 1-4 at the invitation of program management; however, OT&E participation is essential and should be included in the development of plans and requirements development from the onset. OT&E has a leadership responsibility for phases 5-6. However, in some programs phases 3 and 5 are combined, based on system maturity and available test conditions, with DT&E and OT&E partnering to address their work together since they are addressing similar tasks. Figure 2 outlines OT&E participation in each of these six phases.

[4] Cybersecurity Test and Evaluation Guidebook V 2.0, April 28, 2018 Figure 3-4, p.14

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.


Phase 1 Understand Cybersecurity Requirements
Phase 2 Characterize the Cyber Attack Surface
Phase 3 Cooperative Vulnerability Identifications
Phase 4 Adversarial Cybersecurity DT&E
Phase 5 Cooperative Vulnerability and Penetration Assessment
Phase 6 Adversarial Assessment
Lead
CDT/system test lead and CyWG
OT&E Role
Develop the Operational Test (OT) Evaluation Framework.
Provide OT&E cybersecurity input to the Development RFP.
Lead
CyWG
OT&E Role
Update the Operational Test (OT) Evaluation Framework.
Provide OT&E cybersecurity input to the Milestone B RFP.
Lead
CDT
OT&E Role

Notes
Phase 3 and Phase 5 events can be combined when integrated T&E is performed.
The CDT provides CVI event reports to the OTA.
Lead
CDT
OT&E Role

Note
The CDT provides ACD reports to the OTA.
Lead
OTA
OT&E Role
Plan CVPA.
Coordinate with a Cybersecurity Vulnerability Assessment Team (CVAT).
Execute CVPA and document results.
Lead
OTA
OT&E Role
Plan Adversarial Assessment.
Coordinate with the OTA Team.
Execute AA and document results.

Figure 2: OT&E Role in each T&E Cybersecurity Activity[5]

Preparation will be a critical success factor for OT&E in addressing systems using the cloud. The importance of early preparation in managing cyber risk was highlighted by National Institute of Standards and Technology (NIST) in its latest update to the Risk Management Framework (RMF) described in NIST 800-37 Rev. 2[6]. Many decisions that directly impact phases 5 and 6 will be finalized in earlier phases and even before the lifecycle begins.

Cloud computing brings significant changes to all phases of T&E, including the following:

- Cloud providers will share responsibility for system operation and security controls.
- Governance and contractual agreements are critical to establishing the cloud providers' roles and responsibilities for performance and information sharing.
- Vendor-provided and operated infrastructure will result in expanded supply chains and a broader attack surface.
- Frequent and rapid changes to technology environments require more dynamic and ongoing approaches to managing the risks posed by those changes. While many changes may be transparent to cloud users, oversight capabilities must be established contractually to ensure appropriate controls are managed effectively.
- Controllability and observability for cloud operations will be limited by contractual provisions.

The cloud's software-defined environments and network-only access calls for increasing the use of automation during testing to create the test environment, execute tests, and collect and analyze results. This responsibility is currently unassigned. Whoever takes on this responsibility for OT&E will need to

[5] Developed from information provided in the Cybersecurity Test and Evaluation Guidebook V 2.0, April 28, 2018.

[6] This document is available at the following location: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

address the validation and verification of the automated procedures and processes and the level to which the evidence produced by the automated tests should be trusted.

Unlike the current Army approach where a system has an assigned information technology (IT) infrastructure and some control of changes, cloud providers dynamically assign available infrastructure as system execution needs occur. Cloud providers continually update this available infrastructure to address the operational needs of all of their customers and to minimize the provider's own costs to deliver services to customers. To ensure that operational risk is effectively addressed, system developers using cloud providers should be encouraged to provide mechanisms for continuous monitoring as part of their delivery structure. Otherwise, the Army will need to identify mechanisms or triggers that will signal changes in the environment that warrant additional T&E testing or re-testing to confirm operational readiness after system fielding.

The importance of taking into consideration all T&E needs in early phases cannot be overstated. To this aim, the remainder of this document provides questions that should be raised and addressed at each phases of the acquisition lifecycle.

Phase 1: Understand Cybersecurity Requirements

Phase Leader: System Test Lead

Expected Lifecycle Context: Material Solution Analysis (Analysis of Alternatives (AoA))

Notes: These questions need to be addressed for each alternative under consideration; answers may not be fully formed at this phase and consideration may need to carry over to other phases; questions not addressed before the contract is signed with the cloud vendor will require contract modifications to address significant gaps.

- What type of cloud usage is planned (e.g., infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), hybrid)? Determine how responsibility will be shared with the cloud service provider (CSP) for the following[7]:
  - test security requirements for the system or application
  - data protection requirements for confidentiality, availability, and integrity
  - breach notification criteria and responsive actions timeline and reporting
  - operational requirements related to automated monitoring, system and data recovery, air gap, etc.
  - latency and service level expectations for critical workflows
  - mechanisms for continuous monitoring of cloud operational readiness

[7] Cybersecurity Test and Evaluation Guidebook V 2.0, April 28, 2018 section C.6 provides information about the level of risk that will be inherited from the CSP

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

  - oversight and governance of external providers and their suppliers (include cloud providers)
- How does this system interact with other systems, and how will the locations of the other systems impact security and operational effectiveness, and associated responsibility for secure interfaces? This question must consider the following:
  - How does the provider handle importing and exporting of data between cloud and non-cloud systems (exporting from cloud environments typically involve much greater costs)?
  - How does the provider handle interfaces to systems running in the same cloud?
  - How does the provider handle interfaces to systems running in different clouds?
  - What system data will be stored in the cloud and how will it be accessed, verified, and tested?
  - What tools for testing and test evidence will be available from the cloud provider?
  - What test options are available to the program office, Army cybersecurity test and evaluation offices, or service operational test agencies (OTA)?
  - Are available capabilities sufficient for T&E of the system?
  - How will gaps be addressed?
  - How will data removal (i.e., in the event of a change in cloud provider, moving to a new cloud "owner") be managed and verified?
- How similar is this test and engineering effort to prior OT&E efforts that may provide insights into risk concerns and available testing capabilities? (Access to experience from other programs and services will be valuable for widely shared DoD cloud environments such as JEDI; policies for information sharing may be needed to establish this level of inter-service cooperation.)
- Has OT&E worked on other systems that use this cloud provider?
- Has OT&E worked on other cloud-based systems with system and data risk levels that are comparable to this system?
- Is there prior experience to be considered?
- If this system is compromised through the cloud provider, what is the potential impact?
- Does the planned cloud environment merit an early evaluation of the provider's "prevent, mitigate, and recover" cybersecurity measures?
- Will a cyber disruption impact analysis be conducted to help establish requirements?
- What cloud capabilities are needed for requirements validation? (While these concerns might be addressed today during phase 2 or later, the SEI included them in phase 1 because of the DoD approach to organization level contracts, which will force each program to determine if a given contract is suitable for their requirements.)
- Are planned cloud resources sufficient for testing? To answer this question, consider the following:
  - Is there sufficient observability to perform testing of the system without physical access?
  - Is there sufficient visibility into actions performed by the cloud provider to confirm requirements?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

  - Is there sufficient controllability and observability into actions performed by the cloud provider to adequately test the system?
  - Are the artifacts required to verify that the system meets protection requirements sufficient?
  - Are test access credentials to cloud data sufficient to verify data protections?
  - Is funding for the planned cloud pay-per-use expenses during the testing process sufficient?
- What mechanisms or triggers need to be established to identify when additional T&E testing or re-testing should be conducted over the lifecycle of the system?

Phase 2 Exit Criteria

OT&E exit criteria for phase 1 should confirm that all the following tasks have been completed:

- Risk-oriented requirements have been documented and actions are underway for the disposition of those risks.
- RFP language review confirms that testing needs (including cloud) are sufficiently covered.
- The operational test evaluation framework includes consideration of test approach that supports availability and testability for the cloud.
- Documentation is created to show what system data will reside in the cloud and what interfaces will control the flow of data into and out of the cloud (Refer to sample scenarios provided in the SEI cloud training material).
- Cloud provider capabilities are specified and access to required evidence for testing is documented.
- A plan is in place for handling unaddressed issues about the cloud that will be carried to phase 2.

Phase 2: Characterize the Cyber Attack Surface

Phase Leader: System Test Lead

Expected Lifecycle Context: Technology Maturation and Risk Reduction

- What threat and vulnerability concerns need to be covered by OT&E testing related to cloud usage?
- What specific attack experience is available for the selected cloud provider?
  - Type of data and configuration impact on risk concerns?
  - What level of data risk is to be assigned to the cloud provider?

Software development environments (including software factories) are migrating to (or are already using) the cloud, even in cases where the operational system is not cloud-based. Consideration must be given to protection issues that may arise based on movement of development to this new environment;

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

risks need to be addressed end to end across the lifecycle and all aspects of the architecture and configuration. If new cybersecurity risks are identified, how should these be addressed in the OT&E plan?

- Where and how will test data be selected, processed, transmitted, and stored? (Depending on data set size, there are cost considerations. Generating, storing, and analyzing data in the cloud may save time and may cost less than transferring test data out of the cloud.)
- What testing will be done and by whom?

The following questions address the responsibilities assigned to the cloud provider:

- What testing evidence will be available from the cloud provider (e.g., vulnerability scanning, third-party assessments, red team, and penetration[8] testing)?
- What tools will the cloud provider be using to perform its testing?

The following questions address the responsibilities assigned to OT&E:

- What tools and options are available for testing access to the cloud?
- What data are required?
- Are available tools and cloud services accessible by OT&E sufficient to address the needed testing (e.g., workload generation, test drivers, monitoring and data collection, data aggregation and analysis)?
- What cloud capabilities are needed for requirements validation?

The following questions deal with security threats that the Army must address in the cloud and RMF controls that it will implement:

- What suitability and effectiveness requirements must be established and tested using cloud resources and tools, and what approach must be applied?
- What controllability and observability must be established to perform testing based on limitations of physical access?
- What is needed for getting access to system data from the cloud service provider?
- What artifacts are required to verify meeting protection requirements?
- How will access credentials to the cloud be structured so that testing can be done to verify that data protection capabilities and controls are working properly?
- Is there sufficient funding allocated for OT&E use of cloud services during testing?
- What potential exists for reuse of prior OT&E work (especially work on other systems with similar cloud usage)?
- Has OT&E worked on other systems that use this cloud provider?

[8] For example, see the Cloud Penetration Testing Playbook from Cloud Security Alliance (CSA), located at the following URL: https://cloudsecurityalliance.org/working-groups/top-threats/#_overview

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

- Has OT&E worked on other cloud-based systems with system and data risk levels that are comparable to this system?
- What refinement is needed to confirm a level of similarity to identify what is new that would raise additional risk?

Phase 2 Exit Criteria

The OT&E exit criteria for phase 2 should confirm that all the following tasks have been verified or completed:

- System architecture and data flows are documented to establish the baseline for operations planning and risk management.
- Threats to the system (including cloud content and interfaces) are well described.
- Security controls to be implemented are established.
- Suitability and effectiveness testing plans such as the OTA system evaluation plan and PM Test and Evaluation Master Plan are sufficient.
- OT&E understanding is clear as to the testing to be provided by the cloud provider and the testing it is to handle.
- Communication contacts are established with all cloud providers.
- A plan is in place to gain access to the evidence the cloud provider is supplying.
- A plan is in place to gain access and use of testing capabilities that OT&E will need.
- A plan is in place for handling unaddressed issues about the cloud that will be carried to phase 3.

Phase 3: Cooperative Vulnerability Identification

Phase Leader: Chief Development Tester (CDT)

Expected Lifecycle Context: Engineering & Manufacturing Development

- What data and artifacts from DT&E will be available to OT&E to address similar activities in phase 5?
- What tools can be put in place that are supported by the cloud provider and are available to DT&E and OT&E for oversight and risk management?
- How will the cloud environment be used for DT&E testing and how and why will this environment differ from OT&E usage in phase 5?
- What potential exists for reuse of DT&E evidence (e.g., tests, artifacts, tools)?
- What additional evidence is needed to complete OT&E activities and where should it be sourced? Here are some possibilities:
  - Some evidence will be generated by cloud provider.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

  - Some evidence will be generated by DT&E and shared with OT&E.
  - Some cloud evidence will be generated by OT&E.
  - Some cloud evidence will be reused from other sources.
- What lessons has DT&E learned in working with the cloud provider and how will these lessons impact OT&E?
- What options are available to OT&E in the event that DT&E and the cloud provider cannot deliver what is planned?

Phase 3 Exit Criteria

The OT&E exit criteria for phase 3 should confirm that all the following tasks have been completed:

- DT&E plans are in place for sharing data, artifacts, tools, etc., with OT&E.
- The cloud environment for OT&E has been planned and how it differs (if at all) from DT&E has been described.
- A plan for completion of OT&E Test and Evaluation Master Plan (TEMP) is in place.
- Updated communication processes and procedures are established with all cloud providers.
- An updated plan is in place for gaining access to the evidence that the cloud provider is supplying.
- An updated plan is in place for gaining access and use of the testing capabilities that OT&E will need.

Phase 4: Adversarial Cybersecurity DT&E

Phase Leader: Chief Development Tester (CDT)

Expected Lifecycle Context: Engineering & Manufacturing Development

- What data and artifacts from DT&E will be available to OT&E to address similar activities in phase 6?
- What lessons has DT&E learned in working with the cloud provider and how will these lesssons impact OT&E?
- What potential exists for reuse of DT&E tests, artifacts, tools, etc.?
- What options are available to OT&E in the event that DT&E and the cloud provider cannot deliver what is planned?

Phase 4 Exit Criteria

The OT&E exit criteria for phase 4 should confirm that all the following tasks are completed:

- Confirmation of DT&E shared data, artifacts, tools, etc., with OT&E.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

- Lessons learned by DT&E while using the cloud environment and available tools for testing have been documented.
- Mitigation plans are in place for issues encountered by DT&E while working with the cloud provider for testing and use of evidence shared from the cloud provider
- Updated communication processes and procedures are established with all cloud providers.
- An updated plan is in place for gaining access to evidence that the cloud provider is supplying.
- An updated plan is in place for gaining access and use of the testing capabilities that OT&E will need.

Phase 5: Cooperative Vulnerability and Penetration Assessment

Phase Leader: Operational Test Agency (OTA)

Expected Lifecycle Context: Production and Deployment

- Are there any gaps between what is expected in terms of cloud capabilities and testing evidence and what is provided that need to be addressed?
- Confirm that data and artifacts from the cloud provider and DT&E are available to OT&E as expected.
- Confirm that cloud capabilities and tools are available to OT&E as expected.
- What options are available for OT&E to address the identified gaps?

Phase 5 Exit Criteria

The OT&E exit criteria for phase 5 should confirm that all the following tasks have been completed:

- Planned OT&E activities are complete.
- Lessons learned by OT&E while using the cloud environment and available tools for testing have been documented.
- Materials, tools, and artifacts that are available for reuse in OT&E on future systems with the same cloud provider have been collected, documented, and archived.

Phase 6: Adversarial Assessment

Phase Leader: Operational Test Agency (OTA)

Expected Lifecycle Context: Production and Deployment

- What gaps in expected cloud capabilities and testing evidence need to be addressed?

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

- Confirm that data and artifacts from the cloud provider and DT&E are available to OT&E as expected.
- Confirm access to cloud capacity and tools are available to OT&E as expected.
- What options are available for OT&E to address the identified gaps?
- What mechanisms or triggers have been established to identify when additional T&E testing or re-testing should be conducted?

Phase 6 Exit Criteria

The OT&E exit criteria for phase 6 should confirm that all the following activities have been completed:

- Planned OT&E activities are complete.
- Mechanisms or triggers have been established to identify when additional T&E testing or re-testing should be conducted.
- Lessons learned by OT&E while using the cloud environment and available tools for testing are documented.
- Materials, tools, and artifacts that are available for reuse in OT&E on future systems with the same cloud provider have been collected, documented, and archived.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2019 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0936