Cloud Increases the Role of Acquisition in Cybersecurity

Carol Woody, PI

Christopher Alberts

John Klein

Charles Wallen

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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.

DM20-0812

Agenda

1 – Cloud Service Provider (CSP) Impact

2 – Cloud Impact Example: OT&E Practices Must Change

3 – OT&E Cybersecurity Roadmap

4 – OT&E Cybersecurity Opportunities Because of Cloud

5 – Summary

OT&E Roadmap

Cloud Service Provider (CSP) Impact

Cloud Changes

The adoption of commercial cloud technology as a virtual replacement for physical data centers represents immediate **benefits**:

- Fast scalability
- Continuous maintenance and upgrades at the highest level of technology at a lower cost
- Accessibility without geographic limitations

challenges:

- Shared responsibility for operation and controls between government and vendor
- Contractual agreements are critical and drive access and quality
- Vendor-provided and operated infrastructure mean new supply chains, broader attack surface
- Limits on direct controllability and observability – access to monitoring capabilities must be part of the contractual agreement

Cloud System Infrastructure is Continuously Dynamic

- The elements of the cloud infrastructure allocated to a system are dynamically controlled by the cloud service provider (CSP)
  - based on resource utilization factors such as load balancing, technology refresh management, and geographic distribution
- Every time a part of a system is started or restarted, it will use different physical hardware and networks, perhaps in a different physical data center
  - cloud infrastructure is accessed as a remote service through the network using scripts; configuration control is also performed using scripts.
  - software controlled by the cloud provider will automatically create a virtual environment within which the system will execute.
- Elements of the system may be migrated by the CSP to different hardware (and networks) transparently during system execution
- Every CSP continues to evolve its infrastructure independent of cloud customers; cloud environments are characterized by nearly constant change

Cloud Use Requires CSP Specific Knowledge

Cloud environments run on large, highly scalable environments that are standardized by the CSP to manage their delivery and cost.

- Standardization does not extend across suppliers, limiting portability of systems and integration among suppliers.
- Each CSP has a different set of tools and monitoring data available to their customers
- Evaluation expertise will be specific to a provider which will restrict flexibility in resource assignments for assessments.
    - risk assessments and testing will require deep knowledge of each specific CSP technology and how the system utilizes that technology (e.g., storage, load balancing, failover, ...)
    - all interaction is via software APIs and/or specialized management tools

OT&E Roadmap

Cloud Impact Example:

OT&E Practices Must Change

Cloud Challenges Existing OT&E Practices

The adoption of commercial cloud technology as a virtual replacement for physical data centers represents an organizational cultural shift beyond just the adoption of a new technology.

Cloud environments

- will fundamentally change how a program will meet mission objectives and effectively manage operational risks including cyber risk.
- limit visibility and access based on contractual agreements typically established at the start of a program or standardized across multiple programs
- require consideration of OT&E at the start instead of waiting until further into the program, which is a very different approach than DoD programs have used in the past

Major decisions that impact the availability, testability, and auditability of systems are established in the contracting phase with the cloud provider

Cloud Acquisition Decisions Will Impact All Lifecycle Phases

- Cloud contracts can severely limit what tools, data, access, and capacity are available for testing and operations
  - Current OT&E processes assume full physical access and maximum operational capacity is always available
  - Access to data about the operational environment must come from the CSP
- Quality of service (availability, latency, and throughput) will be a major issue as Cloud connections increase
  - Acceptable levels need to be established for the program with the CSP and enforced for all steps in the lifecycle
  - Program influence on these decisions will depend on the type of acquisition
- Transition issues and new types of efficiency problems will arise as parts of a mission transition to the Cloud and data must migrate in and out a Cloud
  - Responsibility for accessibility may be shared among multiple service providers which can impact quality and increase complexity of network failures
  - Cost of bringing data into the cloud environment is low, but migration out is high

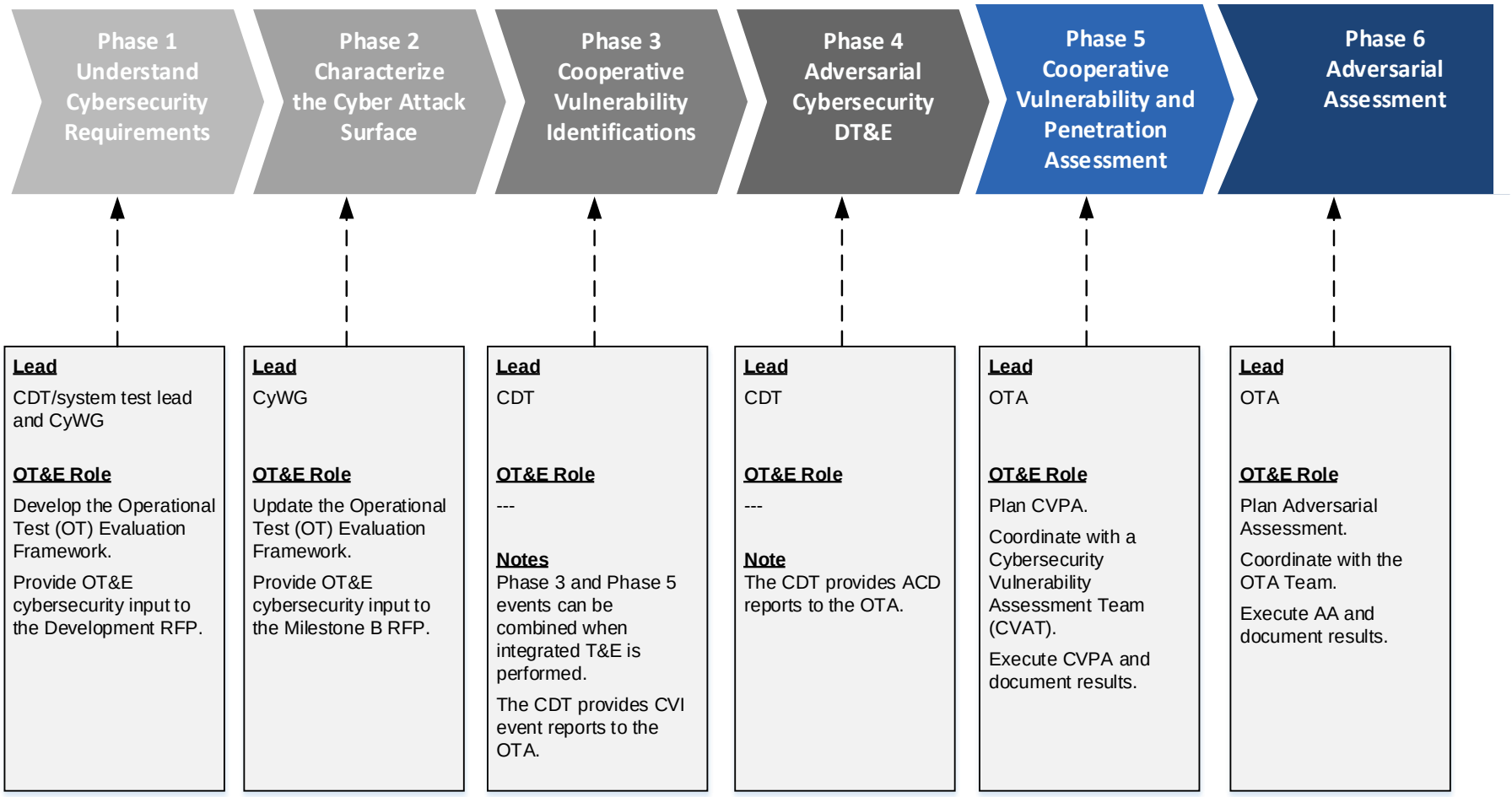
Key T&E Roles

T&E Guidebook describes the following:

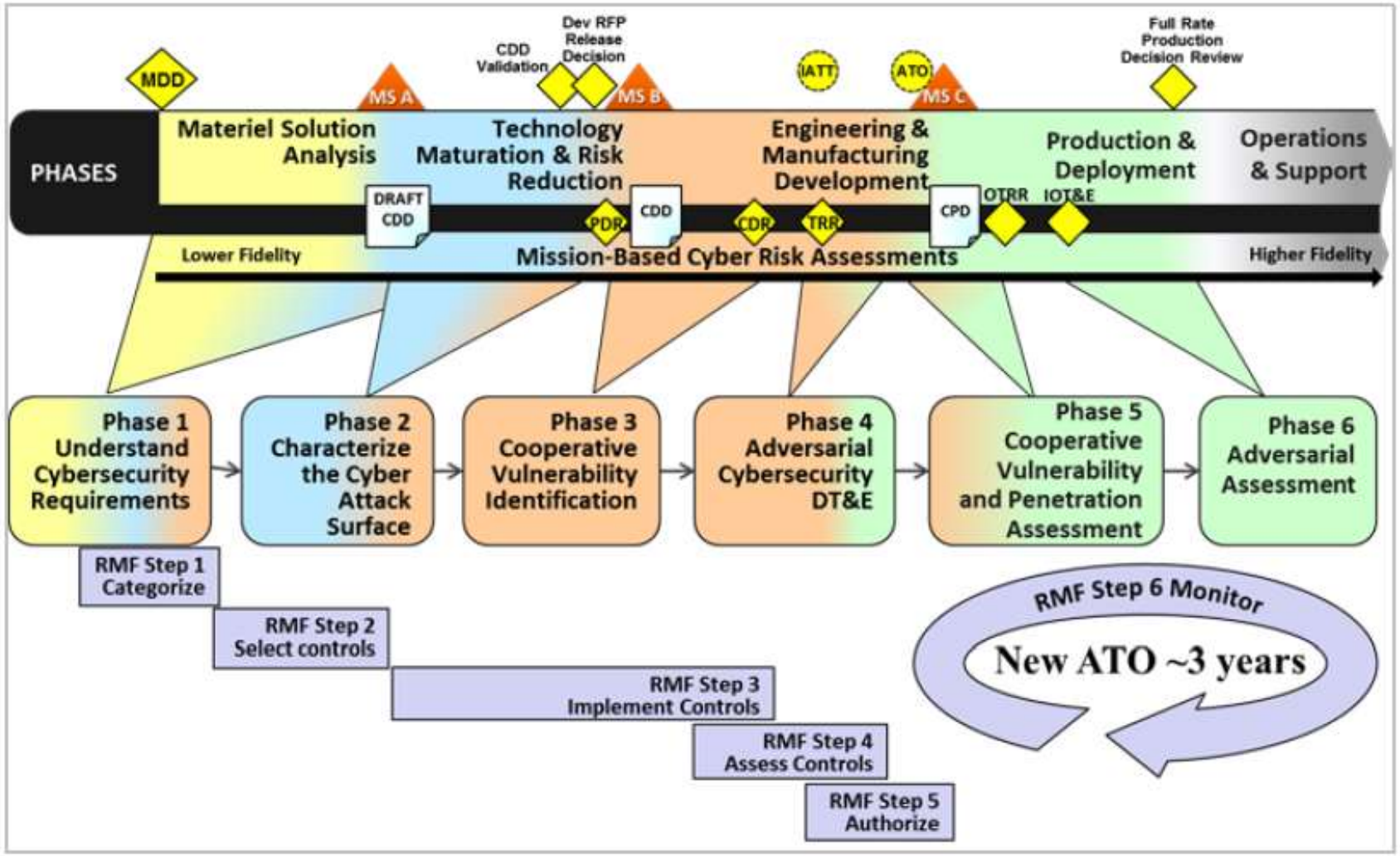
- The Chief Developmental Tester (CDT) or system test lead initiates and convenes the Cybersecurity Working Group (CyWG) as early as possible to assist with T&E tasks across the 6 phases, but this group can be convened as late as Milestone B.
- The CyWG can include
  - Operational Test Agency Representative, if invited
  - Cybersecurity OTA Technical Experts (testers/analysts/assessors), if invited

Cybersecurity Test and Evaluation Guidebook
https://www.acq.osd.mil/dte-trmc/docs/CSTE%20Guidebook%202.0_FINAL%20(25APR2018).pdf

T&E Phases: *OT&E Role*



T&E Cybersecurity Activities

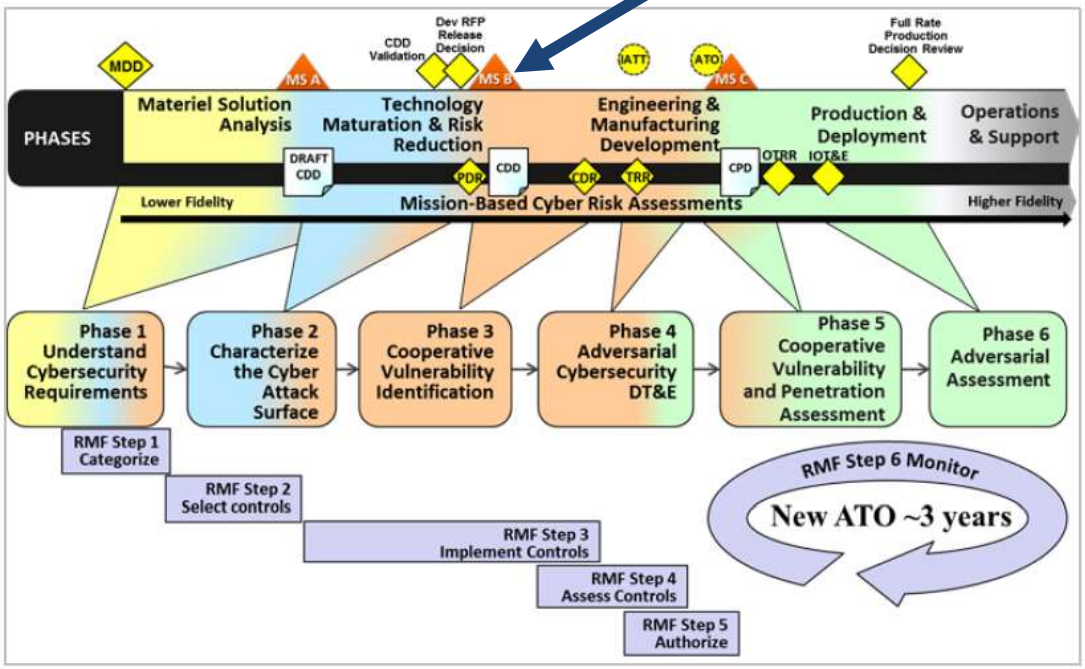


Where Do We See Cloud Decisions Made?

Use Existing Clouds

DevSecOps Prep

Initiating planning for OT&E at Milestone B is too late



OT&E Roadmap

OT&E Cybersecurity Roadmap

Establishing a Path for OT&E in the Cloud

Key decisions need to be made at each of the six phases

All cloud access occurs over wide area networks – OT&E will need access and processing capability within the cloud

- Personnel who assess testing needs, configurations, replicated state, time synchronization, and communications must understand the fundamentals of distributed computing systems
- Defining test configurations to ensure that they represent how the system will be deployed and used will be challenging.

Section C.6 of the *Cybersecurity Test and Evaluation Guidebook V 2.0.* provides information about the level of risk that can be inherited from the CSP, but this must be tailored to each program

Phase 1: Understand Cybersecurity Requirements (1)

Determine how responsibility will be shared with the CSP for:

- 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 the continuous monitoring of cloud operational readiness
- oversight and governance of external providers and their suppliers, including cloud providers

Phase 1: Understand System Cybersecurity Requirements (2)

How does this system interact with other systems? How will the locations of the other systems' impact security and operational effectiveness, and their associated responsibility for secure interfaces?

- importing and exporting data between cloud and non-cloud systems (Exporting from cloud environments typically involves much greater costs.)
- interfaces to systems running in the same cloud
- interfaces to systems running in different clouds

Phase 1: Understand Cybersecurity Requirements (3)

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 (T&E) 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 (e.g., in the event of change to the cloud provider, new cloud “owner”) be managed and verified?

Phase 1: Understand Cybersecurity Requirements (4)

If the cloud provider's systems are compromised, what is the potential impact for the development and operational mission of the program?

Does the planned cloud environment merit an early evaluation of the provider's prevent, mitigate, and recover cybersecurity measures?

OT&E exit criteria for Phase 1

- ✓ Risk-oriented requirements were documented and actions are underway for the disposition of those risks.
- ✓ The request for proposal (RFP) language review confirms that testing needs (including for the cloud) are sufficiently covered.
- ✓ The Operational Test Evaluation Framework considers a test approach that supports availability and testability for the cloud.
- ✓ Documentation is created to identify which system data will reside in the cloud and which interfaces will control the flow of data into and out of the cloud.
- ✓ Cloud provider capabilities are specified, and access to required evidence for testing is documented.
- ✓ There is a plan for handling unaddressed issues about the cloud that will be carried to Phase 2.

Phase 2: Characterize the Cyber Attack Surface (1)

What threat and vulnerability concerns need to be tested by OT&E related to cloud usage?

- What specific attack experience is available for the selected cloud provider?
- How could the cloud infrastructure impact program data and configuration risk concerns?
- What level of data risk should be assigned to the cloud provider?

Phase 2: Characterize the Cyber Attack Surface (2)

What responsibilities are assigned to the cloud provider?

- What testing evidence (e.g., vulnerability scanning, third-party assessments, red team, and penetration testing [CSA 2019]) will be available from the cloud provider?
- What tools will the cloud provider use to perform its testing?

What responsibilities assigned to OT&E?

- What tools and options are available for testing access to the cloud?
- What data is 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, and data aggregation and analysis)?

Phase 2: Characterize the Cyber Attack Surface (3)

What cloud capabilities are needed for requirements validation?

- security threats to be addressed in the cloud and RMF controls to be implemented
- suitability and effectiveness requirements to be tested using cloud resources and tools, and the approach to be applied

What controllability and observability are required to perform testing based on the limitations of physical access?

- What is needed to get 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 data-protection capabilities and ensure that controls are working properly?

OT&E exit criteria for Phase 2

- ✓ 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 clearly understands the testing to be provided by the cloud provider and the testing OT&E will handle.
- ✓ Communication contacts are established with all cloud providers.
- ✓ There is a plan for access to evidence the cloud provider is supplying.
- ✓ There is a plan for accessing and using the testing capabilities OT&E will need.
- ✓ There is a plan for handling unaddressed issues about the cloud that will be carried to Phase 3.

Phase 3: Cooperative Vulnerability Identification (combine with Phase 5?)

What data and artifacts from DT&E will be available to OT&E to address similar activities in Phase 5?

What tools can be 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/why will this differ from OT&E usage in Phase 5?

What potential exists for the 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?

What options are available to OT&E in the event that DT&E and the cloud provider cannot deliver what is planned?

OT&E exit criteria for Phase 3

- ✓ DT&E plans for sharing data, artifacts, tools, etc. with OT&E
- ✓ a planned cloud environment for OT&E and how it differs (if at all) from DT&E
- ✓ a plan for the completion of the OT&E Test and Evaluation Master Plan (TEMP)
- ✓ updated communication processes and procedures, which are established with all cloud providers
- ✓ an updated plan for accessing the evidence that the cloud provider supplies
- ✓ an updated plan for accessing and using the testing capabilities OT&E will need

Phase 4: Adversarial Cybersecurity DT&E (Combine with Phase 6?)

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? How will these lessons impact OT&E?

What potential exists for reusing 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?

OT&E exit criteria for Phase 4

- ✓ DT&E data, artifacts, tools, etc. shared with OT&E
- ✓ lessons learned by DT&E in using the cloud environment and the tools available for testing
- ✓ mitigation plans for issues encountered by DT&E in working with the cloud provider for testing and using evidence shared by the cloud provider
- ✓ updated communication processes and procedures, which are established with all cloud providers
- ✓ an updated plan for accessing evidence that the cloud provider supplies
- ✓ an updated plan for accessing and using the testing capabilities OT&E will need

Phase 5: Cooperative Vulnerability and Penetration Assessment

Are there gaps between what is expected and what is provided that need to be addressed?

What options are available for OT&E to address the identified gaps?

OT&E exit criteria for Phase 5

- ✓ completion of planned OT&E activities
- ✓ lessons learned by OT&E in using the cloud environment and the tools available for testing
- ✓ the collection, documentation, and archiving of materials, tools, and artifacts, which are available for reuse in the OT&E of future systems using the same cloud provider

Phase 6: Adversarial Assessment

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

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?

OT&E exit criteria for Phase 6

- ✓ the completion of planned OT&E activities
- ✓ mechanisms or triggers that were established to identify when additional T&E testing or re-testing should be conducted
- ✓ lessons learned by OT&E in using the cloud environment and the tools available for testing
- ✓ the collection, documentation, and archiving of materials, tools, and artifacts, which are available for reuse in the OT&E of future systems using the same cloud provider

OT&E Roadmap

OT&E Cybersecurity Opportunities Because of Cloud

Can OT&E Take Advantage of Opportunities to Improve T&E Assessments for Cloud?

- OT&E has the opportunity to regularize (and reduce cost for) the Cloud evaluation once they have experience with a provider. This will require collecting and **sharing data across programs using the same Cloud provider** which is not currently done.
- Dynamics of Cloud environment encourage building in the ability to **test continuously**. As tests are built for a Cloud provider they can be deployed early and often in the development steps and continued into sustainment for continuous monitoring.

How can OT&E Ensure Cloud Requirements are Sufficient for Operational Use?

- Cloud requirements may be in place before OT&E is involved.
  - How can OT&E make their testing needs known in advance so programs will not be facing gaps and potentially unexpected costs to address OT&E mandates?
  - Services are reviewing operating cost models for Cloud—OT&E should ensure these include testing.
  - Currently OT&E is involved in the review of the Requirements Definition Package (RDP) in Task 1, but this may be too late.

OT&E Roadmap

Summary

Summary

From our analysis of cloud-based systems, we identified challenges in the following areas that will impact OT&E:

- acquisition and contracting decisions
- partnering needs with suppliers and developers
- updating for current processes and procedures
- adoption of new and refined methods and tool
- enhancing staff technical competency
- defining triggers for continuous monitoring and reassessment

Cloud operational validation is a challenge that does not fit entirely within the control of individual programs. Currently each evaluation is treated as unique when there is value in sharing information across programs using the same shared platforms.

Looking Forward

The challenges for Cloud will also apply as systems transition to other new technologies. Existing approaches will need to be replaced with more effective and valuable cyber risk management capabilities.

Continuous monitoring needs would indicate value in repeatability. How should shared inherited risk be considered:

- Can prior OT&E work (especially work on other systems with similar cloud usage) be reused?
- 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?
- What analysis is needed to confirm a similar risk level and to identify what is new in the current system that would raise additional risk?

Reference: Acquisition Research Symposium at Naval Postgraduate School (ARP/NPS)

The paper my team authored

Cloud Increases the Role of Acquisition in Cybersecurity

along with the others accepted at the symposium are available for download at the ARP/NPS site

https://event.nps.edu/conf/app/researchsymposium/home#!/page/148

See panel #22 for the Cloud paper

Contact Information

Carol Woody, Ph.D.

cwoody@cert.org

Web Resources

https://sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=48574

http://www.sei.cmu.edu/