SYM-AM-20-042

PROCEEDINGS
OF THE
SEVENTEENTH ANNUAL
ACQUISITION RESEARCH SYMPOSIUM

Acquisition Research: Creating Synergy for Informed Change

May 13–14, 2020

Published: April 06, 2020

Approved for public release; distribution is unlimited.

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Cloud Increases the Role of Acquisition in Cybersecurity

Carol Woody (PI)—is a principal researcher at the Carnegie Mellon Software Engineering Institute (SEI) CERT Division. Her research focuses on building capabilities and competencies for measuring, managing, and sustaining cybersecurity for highly complex networked systems and systems of systems. Dr. Woody has successfully implemented technology solutions in banking, mining, manufacturing, and finance. She coauthored the book *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance,* published by Pearson Education as part of the SEI Series in Software Engineering. The CERT Cybersecurity Engineering and Software Assurance Professional Certificate, released in March 2018, is built from research she led.

Christopher Alberts—is a Principal Cybersecurity Analyst in the CERT Division at the Software Engineering Institute (SEI), where he leads applied research and development projects in software assurance and cybersecurity. His research interests include risk analysis, measurement and analysis, modeling and simulation, and assessment. His research has been adopted by a variety of government and industry organizations, both nationally and internationally. He has coauthored two books and published over 50 technical reports and articles. Alberts has BS and ME degrees in engineering from Carnegie Mellon University.

John Klein—is a principal member of the technical staff in the Software Solutions (SSD) Division of the Carnegie Mellon University Software Engineering Institute. In his role, he does research and consulting in scalable system architecture, working with commercial and government customers in domains that include big data and analytics, scientific computing, financial services, and command and control. He worked as an architect and manager in organizations ranging from Fortune 100 companies to pre-IPO startups in businesses that include telecommunications, video networking, and defense. Dr. Klein is a coauthor of the book *Deployment and Operations for Software Engineers.*

Charles M. Wallen—has provided consulting to public and private organizations, led industry-wide initiatives, and managed global cybersecurity risk management and governance programs at some of the largest global financial services providers. Wallen is a senior member of the technical staff at Carnegie Mellon's Software Engineering Institute (SEI) CERT Division. His work in the CERT Division includes resilience management, external dependency risk management, software assurance, and critical infrastructure protection. He was a key participant in building a new approach to managing operational risk and resilience, which ultimately led to the Resilience Management Model.

Abstract

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. There are significant benefits from moving to a computing platform that is (1) provided by an organization dedicated to technology management, which can be scaled quickly, (2) maintained at the highest level of technology at a lower cost, and (3) widely accessed without geographic limitations. But with these benefits come significant implications for operations, cybersecurity, and compliance. Major decisions that impact the availability, testability, and auditability of systems are established in the contracting phase with the cloud provider. Options for visibility into cybersecurity controls, including available analysis tools, are inherited by programs from the provisions structured by acquisition and are no longer fully within a program's control. How will a program office address its responsibilities for cybersecurity when monitoring and testing can no longer be performed directly on the equipment used by a system? While it may be easy to confirm that operational and cost objectives are being met, commercial cloud environments require new ways of confirming that cybersecurity risks are being managed.

Introduction to the Challenges of Cloud Environments

The adoption of cloud technology as a virtual replacement for physical data centers represents an organizational paradigm shift beyond just the selection and installation of a new technology. A key aspect of this new environment is the use of third-party providers, called cloud service providers (CSPs), who manage the technology environment. They own and install the infrastructure, select the hardware and software that will be available, and grant the customer pay-per-use access with limited and restricted control of the underlying infrastructure. The transition to the commercial cloud will shift what has been a physical purpose-built structure to a generic environment of hardware and software, which is outside of direct physical control of the program.

There are major benefits from moving to a computing platform that can provide dedicated expert management, access to economies of scale, efficiency, lower cost, rapid scalability, maintenance at the highest level of technology, and wide access without geographic limitations. However, these benefits come with limitations on visibility and control that impact cybersecurity assurance. These limitations must be considered in the early phases of an acquisition, when requirements are defined and vendor selections are made.

Cloud vendors are pushing organizations to establish enterprise-wide or agency-wide contracts, which takes the infrastructure decisions away from individual programs. These contracts potentially impose limitations on each program about how they can manage operations, perform development, and manage cybersecurity. They also impose limitations on the ways monitoring, testing, risk, and compliance are managed.

A thorough up-front acquisition process is critical for establishing the operational and cyber management ground rules with the cloud provider. Essential areas that organizations must focus on to help ensure effective management throughout the contract life cycle include managing the technology infrastructure, network access, software, cost of access, use, and storage, as well as the level of support that the cloud provider will deliver.

Each of the following aspects of cloud computing is counter to current practice and will directly impact a program and how it can design, build, and field technology-supported capabilities for the Department of Defense (DoD):

- The elements of the cloud infrastructure that are allocated to a system are dynamically controlled by the CSP based on resource utilization factors such as load balancing, technology refresh management, and geographic distribution. Every time part of a system is started or restarted, it will use different physical hardware and networks, perhaps in a different physical data center, and, in some cases, 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, and cloud environments are characterized by nearly constant change. CSPs limit observability (e.g., access to system internal communications and state) and customer controllability to ensure the most efficient use of the available resources.
- The cloud infrastructure is accessed as a remote service through the network using scripts; configuration control is also performed using scripts. Through these scripts, software controlled by the cloud provider will automatically create a virtual environment within which the system will execute. In concept, this virtual environment could be anywhere in the world using any range of hardware and software assigned by the CSP.
- Cloud-based systems expand dependencies on external suppliers of software, hardware, infrastructure, and support staff to include those under the control of the CSP. CSPs limit their visibility and influence over their supplier selection and management, increasing the potential for supply chain risk.
- With the role of the CSP touching all aspects of technology, the role of acquisition teams must expand to understand and consider the importance of supplier requirements

management, auditability, and governance as part of the acquisition process. Cost and schedule considerations alone are grossly insufficient and short sighted.

- Every CSP has a business model that is designed to lock the customer into the provider and limit capabilities for easy transition to another provider. The cost of importing data into the cloud is comparatively cheap, and exporting is, by comparison, very expensive.[1] Each provider has a unique configuration and usage structure with its own network, hardware, software tools and access capabilities, availability, pricing structure, and geography. A system designed to operate at low cost on one CSP's infrastructure may be very expensive to operate on a different CSP's infrastructure.
- Using the cloud can improve some dimensions of security if the cloud provider is required to ensure the technology infrastructure is up to date, but new threats and vulnerabilities can be introduced by the CSP's rapid-tempo technology change and the expanded use of software for virtualization and system management.

Cloud Cybersecurity Considerations Drive a "Shift Left" in the Life Cycle

Today, operational and cybersecurity evaluations of software systems usually begin during the implementation phase of the development life cycle. For cloud-based systems, that is too late. At that point, decisions made by acquisition, engineering, architecture, and development dictate the limitations within which operations and cybersecurity concerns can be addressed. Through the choice of a cloud provider and the requirements the CSP must meet, acquisition essentially determines what a program can and cannot do about operations and cybersecurity. Will this be sufficient to meet program needs?

The contract with the CSP limits how the infrastructure will be built, maintained, and accessed as well as how the CSP will report on status, patching, changes, and other risk management concerns. The decisions made in structuring the contract lock in the oversight of vendor support for cybersecurity visibility and what reporting will be available. Clear rules around cyber controls and the ongoing reporting on the CSP's activities to meet the contractual requirements establish the possible level of monitoring and management that can be done. Additional controls at the acquiring organization are of little value if the CSP's underlying infrastructure and software layers are not set up to enforce the same level of concern.

Typically, cybersecurity and supply chain risk management (SCRM) have not been primary concerns for system acquisition and engineering. However, there is growing awareness that many cybersecurity threats and vulnerabilities occurring these days stem from weak cybersecurity practices in acquisition, such as poor third-party product selection and inadequate implementation of SCRM practices by vendors in their operations and with their sub-contractors. These are critical capabilities for cloud-based systems that entrust the infrastructure to a third-party (the CSP).

Engineering defines the cybersecurity characteristics of the system's data and functionality to be placed in the cloud environment and how system segments not in the cloud will interface with it. Cost considerations may impact final design choices for how data moves among cloud and non-cloud segments and which will, in turn, impact the cybersecurity of the data to be shared. Addressing these growing areas of concern requires specialized knowledge

[1] Example from NASA: https://www.theregister.co.uk/2020/03/19/nasa_cloud_data_migration_mess/

about the ways in which systems and cloud environments can be compromised and the potential impact such a compromise can have on operational success. Personnel knowledgeable in cybersecurity as well as cloud capabilities and their limitations are typically not included in early life-cycle acquisition and engineering decisions. While the cloud can provide benefits for the management of cyber risk, such as technology refresh and built-in redundancy, programs working directly with the cloud need to learn new ways to identify cyber risk, control access, verify sufficiency, and ensure recovery capabilities.

Testing Cybersecurity in the Cloud

Historically, testing technology systems has been a key control to help ensure that performance and cyber risks meet requirements. Cloud-based systems can continue to benefit from effective testing strategies but require that contractual terms facilitate establishing how those tests are conducted and reported on. Cloud-based systems can be effectively tested only in the cloud. All applications are deployed to the cloud, which is the infrastructure. A separate integration lab would have to duplicate the cloud infrastructure, which is generally not feasible or effective. This limitation introduces several immediate challenges. First, all testing activities require (1) network access to the cloud and (2) funding to cover the cloud’s variable pay-per-use costs. This funding requirement is important because testing in the cloud incurs costs from running the system under test, running test clients, storing test input or output data, and accessing test results. Second, because all interaction with the cloud occurs through software APIs, the personnel who interact with the cloud to conduct testing must possess a threshold level of competence in software tools and basic software engineering to script these APIs and tailor available test tools to address the desired testing in this environment.

Testing a system in a cloud environment requires a different approach because the infrastructure is established virtually based on available infrastructure components and uses different physical components for each process. Every time a system starts in the cloud, it runs on a different network and on different hardware based on availability and cloud distribution decisions. Consistency cannot be assumed, and replication of exact operational conditions is impossible. Every test run samples a subset of the CSP’s environment, and the system must run for sufficient time with enough independent repetitions to effectively characterize and confirm the system under test.

All cloud access occurs over wide area networks, which necessitates increased care when defining test configurations to ensure that they represent how the system will be deployed and used. Personnel who assess testing needs, configurations, replicated state, time synchronization, and communications must understand the fundamentals of distributed computing systems; this knowledge is not critical for testing in current data-center-based operational environments.

Test designers must understand the following:

- how the characteristic to be verified is performed in a cloud environment
- the roles of the acquiring organization and the CSP during testing

For example, many cloud-based storage systems have high internal redundancy, so availability requirements may be satisfied without traditional failover or backup/restore functions. Using the cloud for testing opens new opportunities (e.g., making large-scale or long-duration tests more affordable), implementing higher availability and making recovery easier, and leveraging a common platform across a range of shared system tasks. However, poorly designed tests can be expensive to run or may even inadvertently trigger the cloud provider to invoke rate limiting, which prevents accurately characterizing the system.

Case Study: Impact of Cloud-Based System on OT&E

Currently, Operational Test & Evaluation (OT&E) activities related to cybersecurity evaluation rely on testers having *direct access* to system hardware and software, which changes to *indirect access* through a cloud provider's software interfaces. Critical decisions about cloud capabilities and access to data important to OT&E are made early in an acquisition, before OT&E is actively involved. Relevant questions that these early decision-makers need to consider at each point in the acquisition should be defined to aid a program in ensuring that OT&E can be successful for cloud-based systems.

Each OT&E activity relies on the availability of specific information. Today, this information is provided by direct inspection and testing near or at the end of the development life cycle. Cloud computing does not provide testers with physical access to computing and storage hardware or 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 & Evaluation (DT&E) to establish equivalent information sources from cloud service providers and ensure that reporting by the CSP provides the information needed to help ensure systems are meeting the cyber and performance requirements that have been established. OT&E must innovate to provide flexible requirements-informed approaches to verify that these cloud-based systems consider the infrastructure risks introduced by cloud computing.

Many program decisions made early in the acquisition life cycle 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 partner with program managers to establish workable OT&E approaches or prepare the service to accept the risks that remain. Cybersecurity Test and Evaluation (T&E) activities take place in six phases across the life cycle; these efforts all build off of the previous steps, with the final two phases being OT&E. Phases 1−6 are shown in Figure 1, mapped to the segments of the acquisition life cycle where they are typically performed.

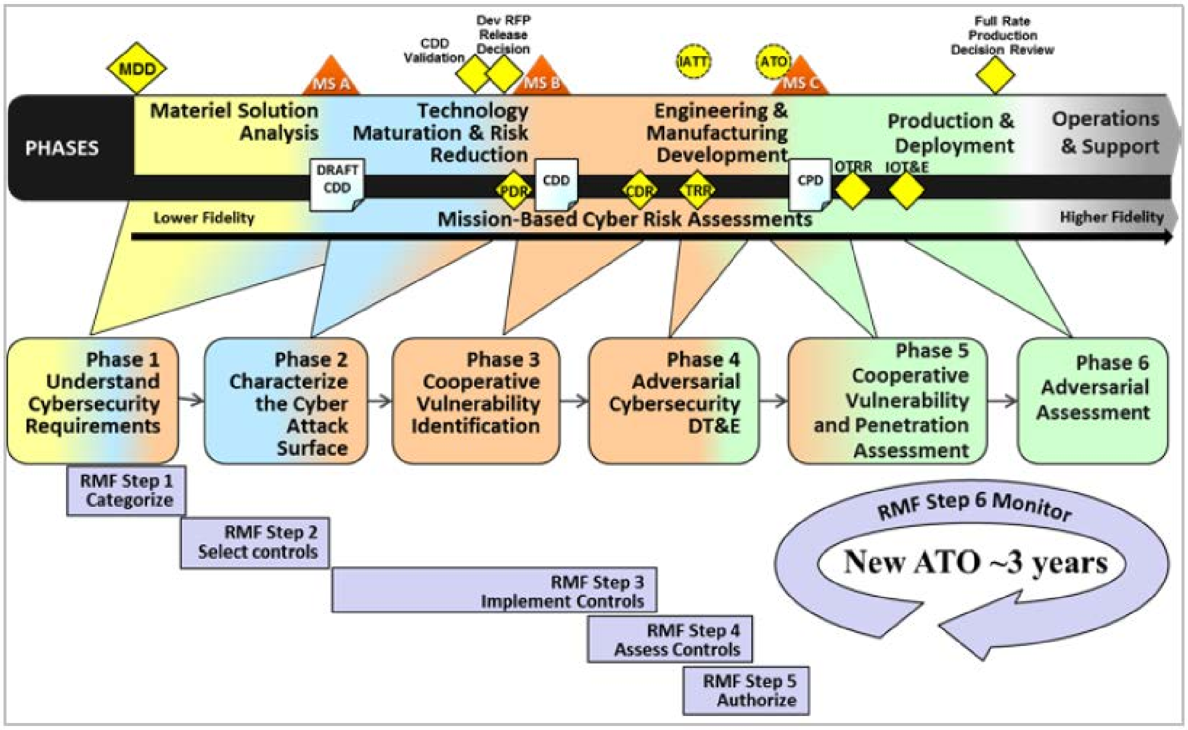
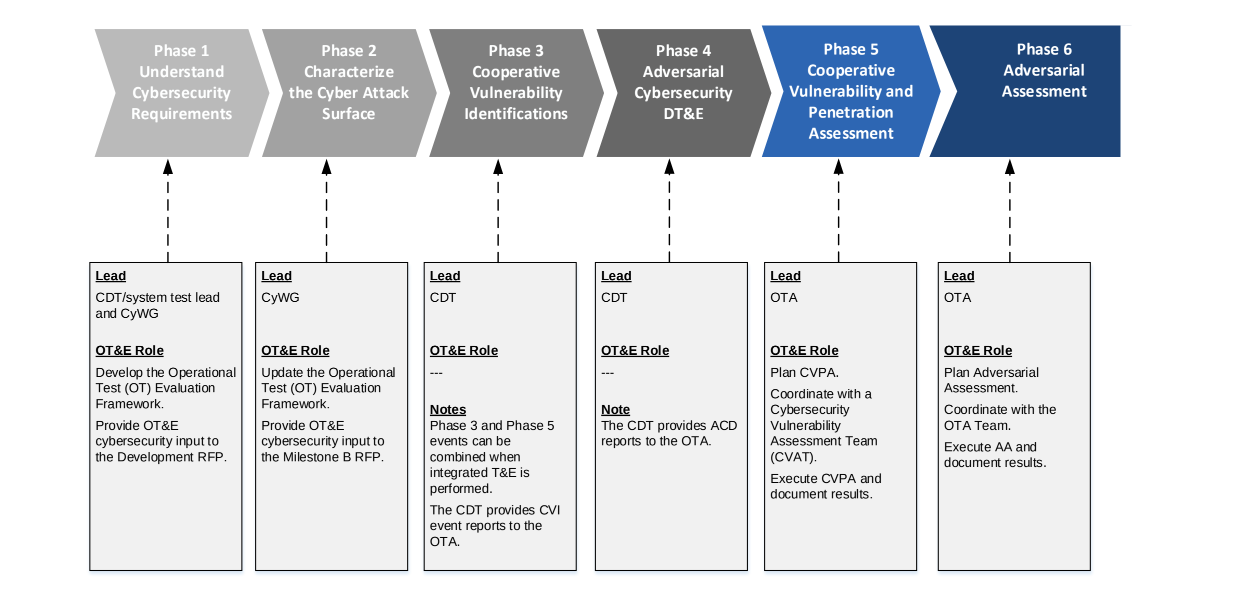

Dev RFP Release Decision
CDD Validation
Full Rate Production Decision Review
MDD
MS A
MS B
IATT
ATO
MS C
PHASES
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Production & Deployment
Operations & Support
DRAFT CDD
PDR
CDD
CDR
TRR
CPD
OTRR
IOT&E
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[2](diagram acronyms not used in the paper)[3]

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 planning and requirements development from the onset for cloud-based systems. OT&E has 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, since they are addressing similar tasks. Figure 2 outlines OT&E participation in each of these six phases.

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

[3] ATO- Authority to Operate; CDD-Capabilities Development Document; CDR-Critical Design Review; CPD-Capabilities Production Document; IATT-Interim Authority to Test; IOT&E-Initial Operational Test & Evaluation; MDD-Material Development Decision; MS A, MS B, MS C- Milestone A, B, C; OTRR-Operational Rest Readiness Review; PDR- Preliminary Design Review; RFP – Request for Proposal; TRR-Test Readiness Review


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[4] *(diagram acronyms not used in the paper)*[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 the 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 are finalized in earlier phases and even before the life cycle begins.

Cloud computing brings significant changes to all phases of T&E:

- Cloud providers 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 that appropriate controls are managed effectively.
- Controllability and observability of cloud operations are limited by contractual provisions.

The cloud's software-defined environments and network-only access call for increasing the use of automation during testing to create the test environment, execute tests, and collect

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

[5] AA-Analysis of Alternatives; ACD-Adversarial Cybersecurity DT&E; CDT- Chief Developmental Tester; CVI-Cooperative Vulnerability Identification; CVPA-Cooperative Vulnerability and Penetration Assessment; CyWG-Cybersecurity Working Group; OTA- Operational Test Agency; RFP-Request for Proposal

[6] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

and analyze results. This responsibility is currently unassigned. Whoever takes responsibility, OT&E will need to 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.

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, there is an additional 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. Since the cloud environment is constantly changing, establishing these review mechanisms can be challenging.

The importance of considering all T&E needs in early phases of the acquisition process cannot be overstated. To this aim, questions that should be raised and addressed at each of the phases were assembled. The remainder of this section outlines what issues must be addressed at each of the six phases to ensure that OT&E can be successfully addressed.

Phase 1: Understand Cybersecurity Requirements

Expected Life-Cycle Context: Material Solution Analysis (Analysis of Alternatives [AoA])

Note: 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]

- 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

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

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

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?

How similar is this OT&E effort to prior efforts, and do those similarities provide insights into risk concerns and available testing capabilities?

- 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 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?

Will a cyber-disruption impact analysis be conducted to help establish requirements?

- test and evaluation (Are planned cloud resources sufficient for testing?)
- Is there sufficient observability to test the system without physical access?
- Is there sufficient visibility into actions performed by the cloud provider to confirm requirements?
- 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 life cycle of the system?

OT&E exit criteria for Phase 1 confirms the following:

- 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

Expected Life-Cycle Context: Technology Maturation and Risk Reduction

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?

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; risks need to be addressed end to end across the life cycle 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 the size of the data set, 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?

What responsibilities are assigned to the cloud provider?

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

What responsibilities are 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)?

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

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

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?

Is there sufficient funding allocated for OT&E use of cloud services during testing?

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?

OT&E exit criteria for Phase 2 confirms the following:

- 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

Expected Life-Cycle 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 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?

- Some evidence will be generated by the cloud provider.
- 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? 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?

OT&E exit criteria for Phase 3 confirm the following:

- DT&E plans for sharing data, artifacts, tools, and so forth 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

Expected Life-Cycle 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? 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 confirm the following:

- 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

Expected Life-Cycle Context: Production and Deployment

In terms of cloud capabilities and testing evidence, are there gaps between what is expected 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?

OT&E exit criteria for Phase 5 confirm the following:

- 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

Expected Life-Cycle Context: Production and Deployment

What gaps in expected cloud capabilities and testing evidence 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 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?

OT&E exit criteria for Phase 6 confirm the following:

- 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

Conclusion and Next Steps

Commercial cloud environments are popular for many good reasons, including scalability, lower cost, higher efficiency, security, compliance, and geographic accessibility. Success in capturing these benefits depends on the ability of organizations to move to a new management paradigm that recognizes the importance of clearly defined agreements with CSPs based on system requirements that can be validated. Included in the paradigm shift is the importance of recognizing that a CSP’s environment is highly dynamic, requiring careful governance and oversight to address the nearly continuous change that is typical of these systems.

The validation process is a challenge that cannot be addressed using the kind of testing (aka OT&E) that has characterized the management of performance and cyber risks for internally managed DoD environments. Instead, the relationships with the CSP must be defined and managed over the life of the agreements as driven by system requirements that must be initially established in the earliest phase of the acquisition process.

In our analysis of cloud-based systems, as described in the provided case study, we identified challenges in the following areas that will require changes to key operational and cyber risk management activities that are impacted by the shift to cloud infrastructure:

- acquisition and contracting
- partnering with suppliers and developers
- updates to processes and procedures
- new and refined methods and tools
- enhanced staff technical competencies
- continuous monitoring and established triggers for reassessment

The level of change needed to establish appropriate operational and cybersecurity management for cloud and cloud-like environments is too great for individual programs to handle in an ad hoc manner. Change of this nature must be planned and well-managed to provide effective results. As cloud contracts and technology evolve, further change will be required, so planning needs to include a component for continuous change.

While the specifics of a long-term approach continue to evolve—for example, JEDI[9] and the Defense Innovation Board's *10 Commandments for Software*[10]—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, including guidance on how computing systems should be acquired, tested, and supported. Core policy and standards documentation, such as DoDI 5000.02 and the T&E guidance in the recently updated *Cybersecurity Test and Evaluation Guidebook,*[11] have also significantly expanded the emphasis on cybersecurity. The impact of this and other guidance on the activities performed by OT&E has not been formally assessed or codified to fully address the impact on the management of cybersecurity for cloud-based systems.

References

Cloud Security Alliance (CSA). (2019). Cloud penetration testing playbook. Cloud Security Alliance Top Threats Working Group. Retrieved from https://cloudsecurityalliance.org/working-groups/top-threats/#_overview.

Defense Innovation Board (DIB). (2018). Ten commandments of software. DoD. Retrieved from https://media.defense.gov/2018/Apr/22/2001906836/-1/-1/0/DEFENSEINNOVATIONBOARD_TEN_COMMANDMENTS_OF_SOFTWARE_2018.04.20.PDFow

DoD. (2018). *Cybersecurity Test and Evaluation Guidebook, V 2.0.* Defense Acquisition University. Retrieved from https://www.dau.edu/cop/test/DAU%20Sponsored%20Documents/Cybersecurity-Test-and-Evaluation-Guidebook-Version2-change-1.pdf

[9] https://media.defense.gov/2019/Aug/08/2002168542/-1/-1/1/UNDERSTANDING-THE-WARFIGHTING-REQUIREMENTS-FOR-DOD-ENTERPRISE-CLOUD-FINAL-08AUG2019.PDF

[10] https://media.defense.gov/2018/Apr/22/2001906836/-1/-1/0/DEFENSEINNOVATIONBOARD_TEN_COMMANDMENTS_OF_SOFTWARE_2018.04.20.PDFow

[11] https://www.acq.osd.mil/dte-trmc/docs/CSTE%20Guidebook%202.0_FINAL%20(25APR2018).pdf

DoD. (2019). JEDI: Understanding the warfighting requirements for DoD Enterprise Cloud. Retrieved from https://media.defense.gov/2019/Aug/08/2002168542/-1/-1/1/UNDERSTANDING-THE-WARFIGHTING-REQUIREMENTS-FOR-DOD-ENTERPRISE-CLOUD-FINAL-08AUG2019.PDF

National Institute of Standards and Technology Joint Task Force (NIST). (2018, December). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (SP 800-37 Rev. 2). National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Sharwood, S. (2020, March 19). NASA to launch 247 petabytes of data into AWS—But forgot about eye-watering cloudy egress costs before lift-off. *The Register*. Retrieved from https://www.theregister.co.uk/2020/03/19/nasa_cloud_data_migration_mess/

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net