Software Assurance Tips

A product of the Software Assurance Tips Team[3]

Jon Hood

Monday 12th February, 2024

1 Assess Only v. Assess and Authorize

Updated Thursday 8th February, 2024

A disturbing trend we have been seeing lately in the DoD is the misuse of the Assess Only framework. The Assess Only process has been created to provide a standard way of assessing technologies below the system level which do not require an authorization (ATO, ATC, IATT, etc.).[2, p. 13]

Misusing the Assess Only process results in a security hole in your programs. This includes bypassing the Assess & Authorize (A&A) process protections, prodigal spending of taxpayer resources, and inefficient "kingdom building."

The following items serve as a litmus test for determining if your organization is abusing DoD policy in a dangerous way:

1.1 Assess Only Systems

Does your organization refer to "Assess Only Systems?" Systems (including Major Applications, PIT Systems, and SIS/CRNs) must go through the Assess & Authorize process. Organizations that create an "Assess Only Systems" channel demonstrate a fundamental misunderstanding of what an approved assessment is intended to accomplish.

1.2 What is Being Approved

There are two flavors of the Assess Only process. A program may use the *Assess & Approve* process to approve single-purpose, non-connecting IT-enabled devices and services, or they can use the *Assess & Incorporate* process to approve an assessment that can be associated with or incorporated into an already authorized boundary.[5, p. 11] For software applications, notice that the assessment is what gets approved, and the system that wants to associate with that assessment must have a process for incorporating it into their boundary.

Organizations that treat an Assessment Approval of software as if it were an approval of the product (rather than an approval of the assessment) are bypassing the authorization mechanism in RMF and the reciprocity controls of their organization.

1.3 Assess Only ATO

An ATO is an *Authority* to Operate. There is no such thing as an Assess only ATO. An *Authority* to Operate requires the Assess *& Authorize* process. By definition, Assess Only is not an authorization. If your organization tells leadership that the Assess Only process results in something like an ATO, they are likely treating the process as their Wish.com ATO.

1.4 Assess Only ATC

As with the ATO, an Authority to Connect is also an authorization and requires the Assess & Authorize process. A network that already has an ATO can define connection requirements, and resources on the DODIN have defined that process under A&A.[1] If your organization tells leadership that the Assess Only process grants them an ATC, they are likely treating the process as their Alibaba ATC.

1.5 Assess Only ConMon

Since the only devices approved under the Assess Only process are ones that are not network connected, continuous monitoring (ConMon) is implemented at the system level which incorporates an approved assessment to athorize a network-enabled products below the system level. Continuous monitoring refers to the final step of the RMF process, *Monitoring*, which takes place after a system is authorized.[4] A ConMon is an operational construct which is why it requires an Authority to

Operate (ATO). If your organization is conducting RMF out of order and insisting on a non-existent ConMon Assess Only, they are likely treating the process as their Temu ConMon.

1.6 Conclusion

Organizations which try to implement the RMF processes should be commended. Organizations that try to hide black-box processes around non-existent authorization pathways should be called out and exposed. If you provide the technical leadership for your organization, consider the litmus test above.

References

[1] Defense Information Systems Agency. Defense Informatoin System Network (DISN) Connection Process Guide Tech. rep. Fort Meade, Maryland, 2023. URL: https://dl.dod.cyber.mil/wp-content/uploads/connect/pdf/unclass-DISN_CPG.pdf.

[2] Department of Defense. Department of Defense Instruction 8510.01. Risk Management Framework for DoD Sy Tech. rep. Washington, D.C.: Department of Defense, 2022. URL: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf.

[3] Jon Hood, ed. SwATips. https://www.SwATips.com/.

[4] National Institute of Standards and Technology. Risk Management Framework for Information Systems and Or Tech. rep. Special Publication (SP) 800-37 Revision 2. Washington, D.C.: U.S. Department of Commerce, 2018. DOI: 10.6028/NIST.SP.800-37r2. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[5] Laura Vaglia and Jey Castleberry. Facility Related Control System Inventory. Tech. rep. 2017. URL: https://usarsustainabilitydotcom.files.wordpress.com/2017/12/facility-related-control-system-inventory.pdf.