Software Assurance Tips

A product of the Software Assurance Tips Team[4]

Jon Hood and Kevin Keen

Monday 12th February, 2024

1 Assess Only v. Assess and Authorize

Updated Friday 22nd March, 2024

A trend we have been seeing lately in the DoD is the misuse of the Assess Only framework. The Assess Only process was created to provide a way of assessing unique technologies below the system level which do not require an authorization like an Authority to Operate, Authority to Connect, Authority to Test, or their interim kin (ATO, ATC, ATT, IATO, IATC, IATT).[3, p. 13]

Misusing the Assess Only process results in a security hole. The primary result of misuse includes bypassing the Assess & Authorize (A&A) process protections. This evasion of the A&A process results in increased operational risk, inadequate risk management, a lack of accountability, and a misalignment with mission requirements. To help organizations identify their holes in Assess Only processes, the following items provide a litmus test for making sure that your organization does not abuse RMF policies in a dangerous way:

1.1 Assess Only Systems

Referring to "Assess Only Systems" indicates a lack of understanding of what may go through the Assess Only process. Systems (including Major Applications, PIT Systems, and SIS/CRNs) must go through the Assess & Authorize process. Organizations that refer to "Assess Only Systems" demonstrate a misunderstanding of what an assessment approval is intended to accomplish. Words have meaning, and using the wrong words creates an inconsistency which introduces weaknesses in a cybersecurity program.

The guidance in DoDI 8500.01 (Figure 1) can help in understanding this distinction.[2] Systems do not qualify for the Assess Only process.

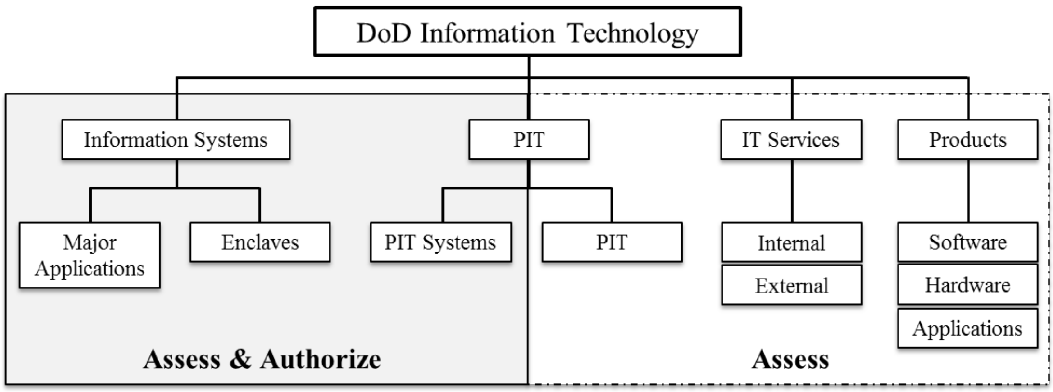

Figure 1: Assess Only and Assess & Authorize in DoD Policy

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 which can be associated with or incorporated into an already authorized boundary.[7, p. 11] For software applications, notice that the assessment is the focal point of the approval, and the system that wants to associate with that assessment should have a process for incorporating it into their boundary. This article does not delve into the assessments of single-purpose PIT components are Assessed and Approved, such as single-purpose It-enabled devices that "do not become a part of an incorporating system's authorization boundary."[5, DoD CIO Risk Management Framework Assess Only Guidance 2017]

Reciprocity requires the incorporating organization to perform due diligence when associating with an approved assessment, and that includes review of the assessment data. Organizations that treat an Assessment Approval of software as if it were a blanket, protean 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 if the process does not include reviewing the assessment data.

1.3 Assess Only ATO, ATC, and ATT

An ATO, ATC, and ATT (and by extension, their interim cousins, IATO, IATC, and IATT) begin with the word *Authority*. An *Authorization* requires the Assess *& Authorize* process. By definition, an Assess Only is not used in the place of an operational authorization.

An authorized boundary which does have an ATO, ATC, or ATT may define policies for associating with an approved assessment to become an authority for the operation of IT below the system level. Those policies should include the review of Assess Only data; however, systems and networks, like the DODIN, may require a full ATO or ATC under the A&A process.[1]

Organizations which refer to an "Assess Only ATO" or "Assess Only ATC" are trying to mix Step 6 of the RMF process (Authorization) with an approval mechanism that ends at Step 5 (Assessment).

1.4 Assess Only ConMon

Taking the misuse of the Assess Only construct a step further are organizations which refer to an "Assess Only ConMon." These organizations attempt to implement Step 7 of the RMF process (Monitoring) in non-standard ways. *Monitoring* in the RMF process refers to the surveillance of authorized assets and controls approved in the Step 6 (Authorized) boundary.[6] This is one of the reasons why DoD elements often refer to this as a ConMon Authorization or Continuous ATO (cATO). Consider the wheel in Figure 2 to help understand where authorization and monitoring fall in the RMF process.

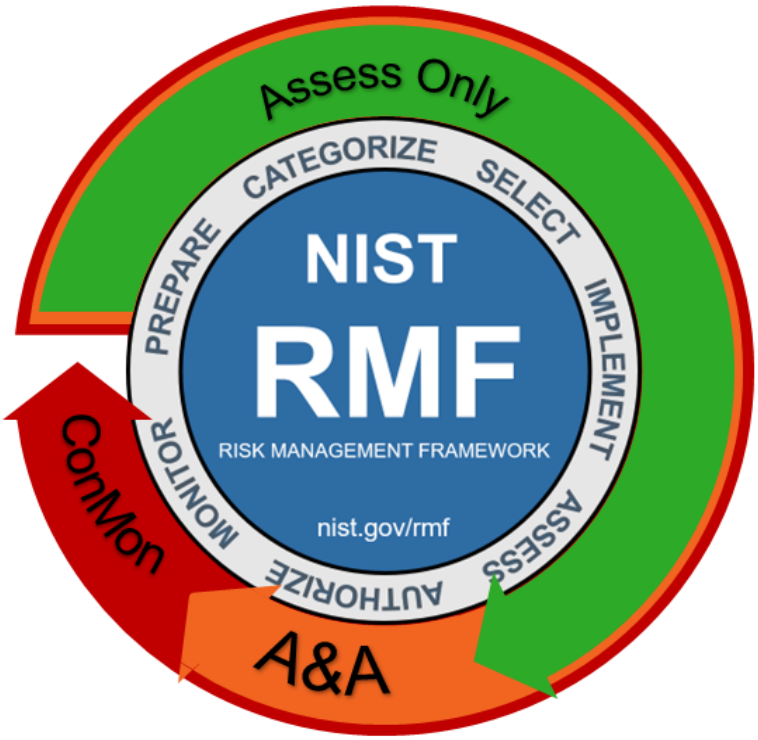

Figure 2: RMF Process Wheel

Continuous monitoring (ConMon) is a requirement for a robust continuous authorization process. It is an *operational* construct which is why it requires an Authority to *Operate* (ATO). Organizations can implement continuous assessment for products below the system level, but to redefine continuous monitoring as meaning continuous assessment gives organizations a false sense of security by bypassing Authorization and answering the final RMF step at the wrong level.

1.5 Conclusion

Organizations trying to implement the RMF process should be commended. A program doing their due diligence to implement cybersecurity principles should consider the litmus test provided here to determine if their processes comply with existing DoD guidance.

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 8500.01. Tech. rep. Incorporating Change 1, October 7, 2019. Washington, D.C.: Department of Defense, 2019. URL: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf.

[3] 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.

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

[5] SERDP-ESTCP. Legislation, Instructions, Manuals, Policies, Plans and Memos. Tech. rep. URL: https://serdp-estcp.mil/page/f7ad7b6f-e8ef-11ec-9685-026db1cbe810.

[6] 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.

[7] 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.