**CMMC Practice Evaluation Framework**

Each of the practices will be tested during the assessment. The outcome ratings are Pass, Fail, and N/A. For scores of Pass and Fail there is a rating source which should be assigned a category of Standard, Judgement, Inherited, Reciprocity or Mixture. Failure to score each practice with one of these ratings will be considered an incomplete assessment and require correction before a certification can be issued.

**N/A Practices**

In the case of N/A, the practice needs to be specified as N/A by the OSC. When the OSC represents that the practice is N/A it will not be subject to testing per-say. However, the assessment team will be asked to indicate if any counter evidence was observed that would indicate that the practice is relevant. This should not be considered the responsibility of the assessor to prove the practice is N/A. But instead affords the assessor the ability to indicate that an N/A practice is relevant if that comes to their attention. At the end of the assessment the assessment team will be asked to answer the following question for each N/A practices:

*QUESTION 1 - During the course of the assessment, was any information obtained that would indicate that the OSC’s representation that this practice is not applicable is not accurate? Note: the assessor is under no obligation to seek out or validate this practice is N/A but during the course of the wider assessment could potentially identify such counter information. If answering Yes, the assessor will indicate the practice as Fail. If no the assessor will indicate the practice as N/A.*

As an example, let’s consider an assessment where the OSC indicates that they do not use wireless devices and therefore certain practices like AC.3.012 are N/A. This would be indicated during the planning phase of the assessment and the assessor would design their testing plans accordingly. The assessment team is not obligated to try to prove that wireless is not in place, so test procedures like scanning for wireless networks is not expected. However, if in the course of the assessment the team is examining a network diagram and notices that it indicates there is a portion of the network that includes WiFi. The assessment team would need to make a determination. The assessment team would need to conduct procedures to determine if this WiFi reference is accurate and if so would likely exercise their judgement and conclude: “Yes, information was obtained that indicates the OSC’S representation was not accurate.” Reaching this conclusion would result in a score of Fail for this practice. The rating source would be judgement.

In the same example, if the assessor identifies a reference to WiFi on network diagrams and during follow-up procedures with the OSC determines that WiFi is not in use then there is likely a different outcome. In this case the assessor would be able to use their judgement and conclude: “No, information was not obtained that indicates the OSC’s representation was not accurate.” Accordingly, the assessor would indicate this practice is N/A. The rating source would be judgement. However, the assessor will need to consider the implications of the inaccurate network diagram on their determination of other practices.

**Inherited Practices (Pass / Fail)**

In the case of Inherited, the practice needs to be specified as such by the OSC. When the OSC represents that the practice is Inherited it will not be subject to testing per-say. However, the assessment team will be asked to indicate if any counter evidence was observed that would indicate that the practice is actually performed by the OSC. This should not be considered the responsibility of the assessor to prove the practice is Inherited. But instead affords the assessor the ability to indicate that an Inherited practice is applicable for the OSC if that comes to their attention. At the end of the assessment the assessment team will be asked to answer the following question for each Inherited practice:

*QUESTION 2 - During the course of the assessment, was any information obtained that would indicate that the OSC’s representation that this practice is inherited is not accurate? Note: the assessor is under no obligation to seek out or validate this practice is inherited but during the course of the wider assessment could potentially identify such counter information. If answering Yes, the assessor will indicate the practice as Fail. If no the assessor will indicate the practice as Pass or Fail based on the status of that practice that is being inherited.*

For example, if an OSC uses a co-lo facility for their data center. If that data center has obtained a CMMC ML-3 then the OSC might point to that for satisfying practice PE.1.132. In that case the assessor would be obligated to answer the question above. If the answer is Yes they would fail the practice. If the answer was No then the OSC would inherit the outcome, in this case Pass. The rating source would be inherited.

**Applicable Practices (Pass / Fail)**

For practices that are applicable, the assessor will need to plan and design tests that adhere to the assessment methodology and test the practices. At the conclusion of the assessment, the assessment team needs to answer the following questions.

*QUESTION 3A - In the assessment team’s judgement, was sufficient evidence obtained that indicates the design and operating effectiveness of the practice provides reasonable assurance that the OSC is adequately satisfying the spirit and intent of the CMMC requirement? If answering yes, the assessment team would indicate a result of Pass for this practice. If answering no, the assessment result would indicate Fail.*

*QUESTION 3B - Was the testing abnormal in any way such as reliance on evidence that follows the spirit of the assessment methodology but is not exactly in keeping or that otherwise required more significant judgement from the assessment team? Note: this should be less common and will likely be leveraged by the C3PAO and CMMC-AB staff as they conduct their QA procedures. The answer is Yes or No. If Yes the assessment team will fill in the additional field to provide detail on the situation and indicate the source of judgement.*

The following questions are helpful in determining the answer to question 3A. The assessor and C3PAO should leverage these to help in reaching their conclusion.

* How confident is the assessment team that this business unit, supporting units and any applicable enclaves will continue to demonstrate institutionalization/habit and persistence for the targeted practices, controls, and related processes, policies and plans going forward?
* Will the rating give the OSC or DoD false confidence in their CMMC practice implementation and rating?
* Will the rating undermine or weaken other aspects of the organization’s CMMC implementation efforts?
* Is the rating consistent with other practice ratings already determined?

Another key consideration is the type of evidence. Generally speaking, testing, demonstration and/or direct observation of a practice (i.e. viewing the configuration) is more persuasive than if you examine an artifact (i.e. read the policy that says it should be set to X) which is still more persuasive than affirmation (i.e. inquiring of personnel that say it should be set to X). The assessor should give careful consideration to this hierarchy of persuasion when exercising their judgement.

Let us consider an examples of this in practice. In this case, the assessment team is evaluating AT.2.056 and notes that one of the system administrators says they do not recall a security training but there is a record of them attending the training. The assessment team would need to evaluate the facts and circumstances. The team might consider the following: Was the training recent and should be more easily remembered? Does the OSC capture signatures or electronic sign-on for attendance or was it just a roster of names? Did any other attendee remember the system administrator attending the training? After weighing these considerations, the assessment team will need to answer the above questions. If the assessment team concludes that the system administrator received the training they would still need to conclude on the design and operating effectiveness. If there is no mechanism to ensure that all required attendees completed the training, the assessment team might conclude that the practice is not designed effectively. This would result in a Fail for the practice. Because the failure did not relate to the system administrator question and instead is based on a design flaw the team should answer No to the abnormality question. If the assessment team concludes that the system administrator did not attend the training (i.e. an operating effectiveness issue), this too would result in an outcome of Fail. In relation to the abnormality question the answer would be Yes because there is mixed evidence. Similarly if the assessment team concludes that the system administrator did attend the training and there were no other concerns the outcome would be Pass. In relation to the abnormality question the team would indicate Yes as there is still mixed evidence.

For another example, let’s consider AC.2.006. During the assessment the team identifies that the use of portable storage device is prohibited by policy. When further examining the system configurations it was noted that workstations and laptops are prohibited from using portable storage devices via group policy. However, the assessment team noted that the servers in the data center are not subject to the same configuration. The assessment further noted that the only individuals who could enter the data center are also system administrators that would have the ability to modify the group policy related to portable storage devices. Therefore in the assessor’s judgement, the configuration that was not enabled for servers does not create a risk different than the risk that an administrator turns off the policy to use a portable device and then turns it back on again. Therefore the assessment team can conclude that “sufficient evidence was obtained that indicates the design and operating effectiveness of the practice provides reasonable assurance that the OSC is adequately satisfying the spirit and intent of the AC.2.006 requirement.” Accordingly, the assessment team would indicate Pass for this practice. They would also indicate Yes for the abnormality question because more significant judgement was required to reach this conclusion.

**Combination Practices (Pass / Fail)**

If the environment is complex and therefore a practice has portions that are N/A, inherited and applicable the assessor will need to apply the guidance above for each portion as applies. The only difference is that the result for the practice would only be pass if all portions are pass. If any portion fails then the entire practice fails.

For example, let’s examine an OSC that has a combination of on premises and co-lo data centers employed in their scope. For practice PE.1.132 is partially satisfied by inheritance in combination with a portion that is handled directly by the OSC then the outcome would be the combination. So if the inherited portion would be a pass and the assessor also concludes that the applicable portion is pass then the final outcome is pass.

Rating Outcome – Pass

Rating Source - Mixed

Yes

All Pass?

Evaluate each portion (applicable, N/A and inherited) separately

Practice a combination?

Yes

Yes

No

Question 3B?

Yes

No

Yes

Yes

Question 3A?

Question 3B?

No

No

Yes

Rating Outcome – N/A

Rating Outcome – Fail

Rating Source - Judgement

Question 1?

No

Applicable?

Question 2?

Yes

Yes

No

Rating Outcome – Fail

Rating Source - Inherited

Rating Outcome – Pass

Rating Source - Inherited

No

Inherited ?

Rating Outcome – Fail

Rating Source - Judgement

Rating Outcome – Fail

Rating Source - Standard

Rating Outcome – Pass

Rating Source - Judgement

Rating Outcome – Pass

Rating Source - Standard

No

No

Rating Outcome – Fail

Rating Source - Mixed