1. **The TOE needs to run on a ‘trusted platform’ in a cloud environment because an environment the TOE customer does not control is inherently less trustworthy than one that they do. Therefore, some external authorization of the cloud platform is needed.**

In an on-premise deployment, there is a presumption that the end customer has full control over their own environment so no separate examination of the operational environment is necessary.

In a cloud deployment, the end customer does not have direct control over the environment so there needs to be some assurance that it provides comparable protection.

The security of the TOE is not adequate if the environment can be used to circumvent its safeguards.

Note that CC Part 1 prohibits ‘testing’ of anything outside the TOE, but ensuring a cloud platform is ‘trusted’ is analogous to a current situation. Specifically, a software TOE requires an entropy assessment report even if the TOE’s entropy source is a third party hardware or software implementation that the TOE developer does not provide. There are no evaluation workunits for this in the CEM, but the CCTL is still expected to validate this report and NIAP will not approve a product for listing on the PCL without it.

Another example of this dynamic is that NIAP will not approve mobile applications on the PCL unless the claimed mobile device platform is also approved. This is not written into the standard itself and an application vendor is free to test a product on an unvalidated mobile device platform, but from a scheme policy perspective the scheme is free to say such a test environment has no value because of the inherent lack of trust in the platform.

1. **How does a product vendor capture the cloud-specific nuances of deploying and configuring their product in the cloud in a secure manner? The operational guidance for the TOE already requires the vendor to describe how to deploy the TOE in a way that is consistent with the environmental objectives.**

AGD\_OPE.1-6: The evaluator shall examine the operational user guidance to determine that it describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

This should still be achievable in a cloud deployment. The PP may need to tailor the AGD evaluation activity to provide specific instructions for what the guidance must contain when a cloud environment is used. Alternatively, this could go into the global guidance documentation for cloud evaluations rather than being associated with a specific PP.

1. **How do we know what cloud platform security features are important? The assumptions and environmental objectives in a PP can be broken down into more specific details that exist independent of any one standard.**

Assumptions and environmental objectives are generally written at a high level, and the extent to which existing cloud standards could be used to satisfy them may be unclear as a result. For the MDM PP reference implementation, these have been decomposed into clear questions as to whether the cloud service provider has a role in addressing these and are listed below.

A.COMPONENTS\_RUNNING

* Does the platform need to provide the MDM customer with a separate way to tell if the MDM components are up and that the audit for them is running? **No, this behavior is not affected by a cloud deployment.**

A.CONNECTIVITY

* Does the platform need to provide managed devices with network connectivity to access the MDM? **No, this is outside the scope of the cloud service.**

A.MDM\_SERVER\_PLATFORM

* Does the platform have a role in ensuring that the TOE can obtain reliable time data? **Yes**
* Does the platform have a role in ensuring that user and group account management services exist to limit access to the platform? **Yes**
* Does the platform provide logon and logout services for the cloud infrastructure? **Yes**
* Does the platform provide services for remote access control? **Yes**
* Can the platform provide audit log management services if the TOE relies on local platform storage? **Yes**
* Does the platform offer boundary protection services such as a host-based firewall? **Yes**
* Does the platform offer trusted channel services if the TOE does not implement its own functionality for this? **Yes**
* Does the TOE rely on the platform for secure storage and management of keys and trust anchors? **Yes**

A.PROPER\_ADMIN

* Is the cloud platform responsible for the protection of authentication credentials? **Yes**
* Does the cloud platform enforce physical access control? **Yes**
* Is the cloud platform responsible for enforcing isolation/segmentation between the TOE and other customers using the same platform? **Yes**

A.PROPER\_USER

* Is the platform responsible for ensuring that mobile device users act appropriately? **No, this occurs entirely outside of the cloud environment.**

The TOE may also rely on a cloud platform to support the ability to acquire and apply updates, but this may depend on the platform. Specific operational examples of how a cloud MDM server is patched would be beneficial to have so that we can determine if this is something we need to expect from the platform.

The TOE may also rely on the cloud platform to provide protection of data at rest (e.g. through encryption). However, we are not sure if this is necessary to cover or if access controls provided by the platform are sufficient on their own.

There is also the notion that security assessments are performed against the trusted platform as a condition of obtaining and maintaining trust. This is covered by penetration testing and continuous monitoring. However, these are process-based and there is nothing that CC would allow the vendor to put into the AGD as validation that these processes are put into place by the provider. Further discussion is needed to see whether we can point to penetration testing and continuous monitoring as something that scheems can say are prerequisites for being a trusted platform.

Lastly, note that from doing this exercise, several feedback items came up for the MDM PP. These have been filed as Issues into the MDM github project.

Beyond these assumptions that are specific to the PP, anything from the Cloud ESR could be considered, either as an addition to any PP that intends to provide a cloud option, or as an overall policy document that applies to all cloud evaluations that individual schemes could use (unless there is no mechanism to do this within the CCRA).

1. **The intent of this decomposition is to identify whether cloud validation programs that are already in use can be used as a way to achieve the desired level of trust in the platform. National schemes can take the generic language for environmental expectations and independently determine if and how their existing cloud validation process they may have will address these.**

In the US, NIAP can require FedRAMP approval of the platform as a precondition for listing on the PCL as a matter of policy, but there is no CCRA-wide enforcement mechanism because the current CC does not allow requirements to be imposed on the OE.

If other schemes have ratified a PP that has a cloud option, they must determine at a scheme level what independent validation or other assurance mechanism is sufficient to say the platform is trusted. This can be issued as a scheme policy or PP annex, similar to how NIAP already approaches cryptographic algorithm and entropy validation.

1. **Applying the decomposition of assumptions to the US, if an MDM TOE is evaluated in the cloud, a FedRAMP Moderate approval is sufficient for the lab/vendor to trust that the OE will meet the MDM PP’s assumptions.**

This is because the FedRAMP Moderate baseline will show that the OE implements the following controls that map to the PP assumptions:

* A.COMPONENTS\_RUNNING:
  + N/A
* A.CONNECTIVITY:
  + N/A
* A.MDM\_SERVER\_PLATFORM:
  + AC-2 (account management)
  + AC-3 (logical access control)
  + AC-17 (remote access)
  + AU-8 (time stamps)
  + AU-9 (protection of local audit storage)
  + AU-9(2) (remote storage of audit data)
  + IA-5 (protection of stored credentials)
  + SC-7(12) (implementation of network boundary protection)
  + SC-8 (protection of data in transit)
  + SC-28 (protection of stored data at rest) – *note that SC-28(3) also exists specifically for protection of cryptographic keys but this enhancement is not part of any FedRAMP baselines*
* A.PROPER\_ADMIN
  + IA-5 (protection of stored credentials)
  + PE-1 (physical access control policy)
  + PE-2 (physical access authorizations)
  + PE-3 (enforcement of physical access controls)
  + PE-4 (physical protection of transmission points)
* A.PROPER\_USER
  + N/A – this assumption applies to mobile device users, and the mobile devices themselves exist outside the cloud infrastructure

Other controls that are referenced in the section above as potentially applicable include the following:

* CA-8 (penetration testing)
* CM-14 (signed updates) – *not associated to any FedRAMP control baselines*
* SC-4 (segmentation/isolation)
* SC-28 (protection of data at rest)
* SC-28(1) (cryptographic protection of data at rest)

FedRAMP validation includes a large number of other controls, but this is outside our scope because they don’t relate directly to assumptions or OE objectives in the PP. So only a subset of the FedRAMP validation matters for CC purposes.

1. **The initial expectation is that all MDM PP evaluation activities can be tested as written when the MDM is deployed in a cloud environment. If this is not true, MDM vendors need to identify which specific evaluation activities cannot be performed and why this is the case.**

Example: testing for trusted protocols (TLS, SSH) have specific scenarios for how the TOE handles various invalid traffic. The cloud service provider may implement a stateful traffic filter firewall that blocks traffic from the CCTL before it ever reaches the TOE, and there may not be a way to disable or circumvent this in a test environment. Any situation like this must be communicated so we can determine whether there are any SFRs that are difficult to validate in a cloud deployment.

The most obvious vendors to contact would be Ivanti (MobileIron) and VMware (Workspace ONE UEM) as they are the only two vendors with MDM products that have gone through both CC and FedRAMP.

1. **With respect to MDM PP evaluation activities, an existing cloud validation of the MDM itself (e.g. FedRAMP SaaS) is expected to have limited utility for reuse of evidence for CC. But a CC validation of an MDM in a cloud environment could provide a lot of value as inputs to a FedRAMP validation of it (whether done in parallel or one after the other).**

In general, the expectation will be that the CCTL will need to perform all of the appropriate evaluation activities in the PP, except to the extent that existing CAVP validations can be reused.

FedRAMP requirements will generally not map cleanly to PP evaluation activities so from a time and effort standpoint, it is more efficient to do the CC testing than it is to sift through FedRAMP evidence to find test results that may overlap with what the PP requires.

The most interesting relationship here is the other direction—a CC certified product in a cloud environment could conceivably allow many FedRAMP controls to be satisfied by default if the product vendor subsequently takes the product through FedRAMP. NIAP and the FedRAMP PMO should discuss the reuse potential here. 800-53 controls are already mapped to SFRs, so this would be a logical starting point for determining what is reusable.

The mapping sheet that was created for the workshop lists the 800-53 controls that are mapped to the PP evaluation activities for each of the MDM PP SFRs. FedRAMP would need to determine whether the CC testing required for these SFRs is sufficient to address all or part of the required testing for the mapped controls. For example, showing a TLS implementation conforms to SC-8 in a FedRAMP validation may only involve a configuration scan showing that the use of TLS 1.2 is enforced. NIAP validation goes significantly above and beyond this with regards to testing the actual implementation of the TLS protocol, so this could be a case where the existing CC testing automatically suffices for that control and the FedRAMP 3PAO can simply cite the validated Security Target as evidence that the TLS implementation meets the control.

1. **The goal of a cloud MDM evaluation is to have a CC certificate be awarded where the TOE’s operational environment includes at least one cloud platform. The certificate authorization scheme has discretion to say whether the intended cloud platforms are appropriate for use by the organizations covered by that scheme.**

In the US, FedRAMP Moderate is a minimum baseline to be eligible for the OE but individual agencies/organizations may enforce a higher baseline (similar to how CSfC will only use a CC evaluation if an appropriate subset of SFR selections are made).

A product vendor targeting deployment in a DoD IL4/IL5 environment, for example, would need to ensure that the tested environment meets all of the DoD’s additional requirements above and beyond the minimum baseline needed for their product to be listed on the NIAP PCL.