**Introduction**

The following section provides a high-level overview for adapting CCiTC methodology to existing PPs, including examples where appropriate. This approach is predicated on determining the suitability of a PP for cloud evaluations, considerations for how the security problem definition, security objectives, and security requirements are affected by cloud evaluations, and how these evaluations may relate to other cloud authorization schemes recognized by national certification bodies.

**General procedure for deriving cloud evaluation guidance for a Protection Profile of PP-Module**

1. **Process Overview**

Placeholder – insert summary of below materials here

1. **Suitability Check**

Identify whether the product type can reasonably operate in a cloud context and what the cloud use case for it is. Some examples as follows:

* The Mobile Device Management Protection Profile (MDM PP) explicitly states that an MDM Server can be deployed in a cloud setting so this is an obvious candidate to consider.
* The Network Device collaborative Protection Profile (NDcPP) defines virtual network devices as a use case, which can be virtualized as a service in a cloud deployment so this is another obvious example.
* The Hardcopy Device collaborative Protection Profile (HCD cPP) defines the capabilities of a specific multifunction device such as a printer. Since this exists solely as a physical device, there is no cloud use case for it.

Note that most existing Protection Profiles do not currently define cloud use cases. This will need to be done on a per-PP basis so that it is clear which types of products can be deployed in cloud settings and so that the Technical Community can make clear what the expectations are for the product’s intended usage and environmental protections should be in these settings. For example, with respect to the NDcPP, the existing security problem definition and environmental security objectives may not cover the case where a network device is deployed as a cloud platform or infrastructure device. The potential cloud use cases for individual product types must be considered as part of determining a PP’s suitability for supporting cloud evaluations. It is recommended that PP authors consult with product vendors for the technology type to determine whether cloud use cases for that type of product exists.

Note that the mapping activities below may help a Technical Community determine whether a PP is capable of supporting cloud evaluations as-is or whether changes to that PP would be needed. This in turn would help determine whether evaluating a particular product type in a cloud setting is actually feasible.

1. **Choose Cloud Standard/Security Controls for Mapping**

Different nations use different standards, methodologies, and assessment schemes for approval of cloud infrastructure, platforms, and software. This may also tie into more general security controls that can be examined. For example, the US standard NIST SP 800-53 defines security controls for information systems across physical, personnel, procedural, and technical domains. The FedRAMP validation process ensures that cloud infrastructure, platforms, and software can be deployed in a manner that satisfies the 800-53 security controls that the program considers to be relevant to cloud systems. FedRAMP also defines Low, Moderate, and High assessment baselines with hierarchical controls. In the MDM example discussed throughout this document, FedRAMP will be used as the cloud validation scheme for reference.

The goal of this exercise is to attempt to answer the following questions:

* Is the environment the TOE is being deployed into capable of meeting the assumptions for the operational environment that the PP or PP-Module defines? That is, if the TOE is deployed on a platform or infrastructure that has been ‘certified’ through some separate cloud validation program, is that sufficient to say the operational environment is also suitable for CC, or would additional assurances be needed?
* If the TOE itself has already been certified through some separate cloud validation program, what is the extent to which the evidence from that certification can be reused for a CC evaluation (if any)?
* Are there any obvious gaps in the PP or PP-Module where requirements or tests would need to be added or modified specifically for the case of a cloud deployment?

Once these questions have been answered for a particular cloud evaluation methodology, the idea is that the same logic could be applied to any other such methods that are used by other CCRA members.

1. **Create Outline for Mapping**

Complete a mapping document (e.g. spreadsheet) that lists out each of the following items in the PP or PP-Module being examined:

* SFRs
* Assumptions
* SARs

A template for the mapping document along with a completed sample for the MDM PP is included as an appendix to this document.

The sections below identify the process by which these should be aligned with the chosen cloud validation scheme.

1. **Identify SFR Impact on Cloud Deployment**

Each SFR in the PP or PP-Module is likely written in such a way that assumes on-premise deployments are used for the TOE. Analysis of the SFRs and their corresponding evaluation activities must be done to determine the impact of deploying a product in a cloud environment. Specifically:

* Are there any SFRs that allow “TSF vs TOE platform” selections to be made and if so, does the nature of how the TOE platform implements the function change based on whether the TOE platform is cloud-based versus on-premise? For example, a general-purpose operating system in a cloud environment may rely on data at rest protection that is provided by an underlying storage volume.
* Are there any evaluation activities that must be executed differently in a cloud environment, and does this potentially change based on the CSP being used?

For example, a software application may rely on cryptographic services provided by a host operating system that runs on some physical hardware. When this application runs in a cloud environment, the end user of the application is not responsible for the physical hardware. Therefore, knowledge of the potential hardware that the CSP makes available to the end user must be known so that all possible use cases for hardware processing of cryptographic functions can be assessed.

* Are there any evaluation activities that cannot be performed as written when the TOE is deployed in a cloud environment, or that can only be performed with special accommodations? For example, TLS testing requires extensive manipulation of network traffic and a CSP may automatically deploy a traffic filtering firewall that discards invalid traffic before it can even reach the TOE. Depending on the test environment, it may require coordination with the CSP to ensure that the operational environment is configured in such a way that the evaluator can verify that the TOE is performing the required function rather than an environmental component.

If there are any evaluation activities that cannot be performed as written for a cloud evaluation, the PP author must provide alternative guidance for how the evaluation activity may be modified to show that the requirement is adequately met in a cloud environment. The PP author must write any cloud-specific evaluation activities in a manner that is sufficiently generic to be achievable regardless of the CSP being used. Evaluation activities should not implicitly ‘endorse’ a given set of CSPs by virtue of being the only ones for which guidance exists.

It may be the case that a requirement simply does not apply to a cloud environment, in which case the PP author could consider defining that requirement as an implementation-based SFR that applies only to the on-premise use case.

* Are there any critical functions that are missing because of the PP or PP-Module’s current expectation that the TOE is deployed in an on-premise environment? If so, PP authors should work with technical subject matter experts to define implementation-based SFRs that apply only to the cloud use case such that the desired functionality can be covered in this situation.

Note that mappings to the desired cloud validation scheme are not critical here, at least not from a CC perspective. The expectation is that if the TOE has already been validated against a cloud validation scheme, there will be little to no re-use of that evidence because of how tailored the CC requirements are to specific tests. There may be some value to vendors pursuing cloud certification \*after\* a CC evaluation because the specific evidence could be reusable in a more general context, but the relationship likely does not flow both ways.

1. **Determine Appropriateness of Security Problem Definition**

The Security Problem Definition (SPD) of a PP or PP-Module defines the threats the TOE faces, the assumptions about the TOE’s operational environment that bounds these threats, and any organizational security policies the organization deploying the TOE may implement to help mitigate the threats in a way that the TOE cannot explicitly enforce (e.g. by defining a password policy that is stronger than what the PP or PP-Module requires).

The purpose of this activity is to consider what an appropriate operational environment would be for the TOE in a cloud setting based on the assumptions defined in the PP. In the context of cloud evaluations specifically, it is important for the end user to have confidence that these assumptions are adequately met since not all aspects of the operational environment will be in their direct control.

To determine the appropriateness of the existing SPD, the PP author should perform the following steps:

* For each assumption in the PP or PP-Module, determine if it applies to any cloud-specific use cases. If the assumption is not affected by a cloud deployment, then no further consideration is needed for it.

*Example: If there is an assumption that an environmental component is configured to communicate with the TOE to receive information from it, this is not cloud-specific because an environmental component outside of the cloud is responsible for that configuration.*

* If the assumption does apply to cloud-specific use cases, determine if it is decomposed to the most granular level or if it is a more general statement that could be made more granular. It is important to decompose assumptions to their lowest level so that all applicable security controls can be considered in the context of whether a cloud validation of the environment is sufficient to demonstrate that it can satisfy the assumptions.

*Example: An assumption that the TOE is protected by a network boundary device (i.e. firewall) is granular.*

*On the other hand, a general assumption that administrators are non-malicious is not granular because there are several ways in which malicious administration can be safeguarded against. This can be made more granular by further breaking it down into assumptions that privilege escalation by non-administrators are prevented, such as by physical security controls on the infrastructure, adequate credential protection, adequate enforcement of logical data separation mechanisms, and routine penetration testing against the overall system to ensure the continuous validation of these things. It can also include background checks or other vetting of administrators and split control that requires approval of administrative decisions.*

* Once all of the assumptions related to cloud deployments are listed out in their most granular form, review the chosen scheme for any areas of overlap.

*Example: For the non-malicious administrator assumption outlined above and using FedRAMP as the chosen cloud validation scheme, the following NIST SP 800-53 controls that are used in FedRAMP can be used to show that those assumptions are met by the environment:*

* + *Credential protection: IA-5, part of FedRAMP Low*
  + *Physical protection: PE-1 through PE-4, part of FedRAMP Low (1 through 3) and Moderate (4)*
  + *Logical data separation: SC-4, part of FedRAMP Moderate*
  + *Penetration testing: CA-8, part of FedRAMP Moderate*
  + *Background checks: PS-3, part of FedRAMP High*
  + *Split control: AC-3(2), not part of any FedRAMP baseline*

The goal here should be to make a statement that asserts whether an existing cloud validation program is sufficient to validate that the cloud portion of the TOE’s operational environment is a “trusted platform” or whether it would need to be supplemented with additional evidence. Additionally, if the chosen validation program has multiple levels, types, or other distinguishing factors, the relevant one should be considered.

*Example: FedRAMP High plus additional supplementing with AC-3(2) would be needed to provide assurance that trusted administrator assumption would be met in the TOE’s chosen operational environment, based on the analysis above.*

In the context of software, if one reviews the SPD and can determine that all assumptions on the operational environment are covered by 800-53 security controls that are assessed as part of the FedRAMP Moderate baseline, they could assert that using platform and infrastructure components certified against this baseline would be sufficient to conclude that the chosen operational environment is suitable. In the case of a platform, the same process could be followed, except that only the infrastructure would need to be examined since that is the operational environment for the platform. Lastly, in the case of infrastructure, the non-technical aspects of the underlying cloud service provider (physical, personnel, and procedural controls) would be examined for the suitability of the operational environment.

Many PP assumptions are similar if not identical between PPs. For example, assumptions regarding trusted administrators or physical protection of the TOE are generally present in PPs with very similar wording between them. The MDM PP is no exception. The decomposition and mappings done for this PP could potentially be usable in other PPs without needing to come up with separate rationale for what is essentially the same process.

Additionally, there are some assumptions (addressed by operational environment objectives) that are specific to cloud environments and do not apply to on-premise use cases. Existing PPs, therefore, do not have any reference to these since they were not written with cloud evaluations in mind. The CCitC working group has compiled some sample assumptions and environmental objectives that could be considered for inclusion in PPs that support cloud evaluations; these are listed in Appendix A below. Note that this approach is similar to the NDcPP, which has assumptions and environmental security objectives that only apply in certain situations, such as when the TOE is distributed or when the TOE is virtualized.

Note also that the shared security model must be considered when looking at assumptions. Responsibility for secure deployment and configuration of the TOE may involve collaboration of up to four different groups (infrastructure vendor, platform vendor, software vendor, end user). The roles and responsibilities must be considered on a PP or PP-Module level because the trusted personnel will differ based on what layer of the cloud stack the TOE sits on. This may also vary from vendor to vendor or from product to product. For example, a CSP deploying its own software on its own cloud infrastructure may only have a single point of contact on their end and there are no cross-organizational concerns.

1. **Determine Impact on SARs**

While the number and level of SARs can vary widely depending on the scheme or organization authoring the PPs and PP-Configurations, the SARs from the MDM PP can serve as an initial minimal baseline for how a cloud evaluation affects the evidence that laboratories will be expected to produce. The extent to which a cloud evaluation affects this evidence is not expected to vary by technology type, but further analysis of individual PPs would be needed to confirm this. For example, when the TOE is evaluated in the cloud against the MDM PP, additional installation guidance may be needed for initial deployment in a given CSP. However, this is expected to be true of other PPs as well and not something that only affects MDM products specifically.

This process was followed for the MDM PP to determine how evaluation activities for its SARs would be affected in the case where a TOE is evaluated in the cloud. The following are considerations for PP authors for how to incorporate cloud evaluation guidance into SAR evaluation activities:

* Class ASE (Security Target) – PP authors should make it clear that any cloud-based evaluation of the TOE should clearly state the operational environment in which the TOE was tested to the greatest degree that is feasible. This is expected to include the claimed CSPs, regions, and hardware machine pools where applicable. If the CSP has functionality that the TOE relies on to support the enforcement of its security claims, such as data-at-rest protection, these should be referenced in the physical boundary of the TOE as security-relevant interfaces to the cloud.

On an individual SFR level, if the method by which the TOE meets an SFR differs when it is being evaluated in the cloud, the PP author must ensure that evaluation activities have appropriate guidance for what the Security Target needs to document when making these claims. Any implementation-based SFRs that are only claimed when the TOE is evaluated in the cloud or only when it is evaluated on-premise must also indicate clearly when those SFRs are expected to apply.

* Class ADV (Development) – Since the TOE’s evaluation in the cloud may rely on other cloud services to support the enforcement of the TOE’s claimed security functionality, PP authors should ensure that discussion on the TOE’s interfaces to the cloud are described in the context of the functional specification. If the required ADV SARs include a TOE design specification or architectural description, PP authors should provide guidance as to what is necessary to document about how the cloud version of the TOE differs from a traditional on-premise architecture.
* Class AGD (Guidance) – Preparatory procedures will differ significantly between cloud-based and on-premise TOEs. The PP author must provide guidance for the preparatory procedures that are needed for the TOE to be deployed in its claimed cloud environments. This may involve separate sections for separate CSPs if multiple CSPs are claimed in the evaluated configuration. The guidance may assume that the intended reader has basic familiarity with deploying cloud products; the PP author’s focus should be to ensure that guidance developers understand the need for the guidance to instruct users on how to replicate the evaluated configuration to the greatest extent possible.
* Class ALC (Lifecycle) – The TOE and its operational environment cannot be assumed to be static in a cloud environment. Identification of both the TOE and its operational environment is therefore critical for the user to understand the tradeoffs between compliance with the evaluated configuration of the TOE and any subsequent security or feature enhancements that may be made after it has been certified. PP authors are encouraged to include lifecycle evaluation activities for how the TOE and its environmental dependencies are identified in the evaluated configuration and how updates are delivered both to the TOE and to its underlying operational environment. It may be the case that the CSP is responsible for back-end updates to the TOE’s operational environment. The PP author should emphasize that this be clearly expressed in the life cycle documentation so that the evaluation laboratory can validate how the TOE developer takes these environmental changes into consideration when managing the life cycle of their own product and how such changes are communicated to end users.
* Class ATE (Testing) – As discussed previously, functional testing of SFR claims may or may not be different when the TOE is evaluated in the cloud. For cases where on-premise and cloud evaluation of a given SFR may differ, the PP author is expected to provide clear guidance as to the evaluation activities that are different for each use case.
* Class AVA (Vulnerability Analysis) – A vulnerability analysis of a cloud product may involve many dependencies that the TOE relies on in a way that an on-premise TOE may not be able to. Frequent changes to environmental configuration on the CSP side may not be in the control of end users and will continually change the versions of dependent components that the TOE relies upon. PP authors should provide guidance to evaluators to identify the dependencies that the TOE has in the cloud (for each claimed CSP) and conduct vulnerability research on the latest versions of those dependencies, as well as any potential vulnerabilities that are specific to the claimed CSPs. Additionally, guidance for penetration testing should be given with the understanding that the TOE may not be deployed in a fully closed environment and as such there may be limitation on the rules of engagement that must be followed with the CSP. It is expected that validation schemes will provide guidance on the penetration test efforts that will be accepted for cloud evaluations, and PP authors should incorporate such guidance into PPs for consistency.

An example of this as applied to recommendations for the MDM PP is listed below.

* ADV\_FSP.1 – generally, the evidence used to satisfy ADV\_FSP.1 in the current generation of PPs and PP-Modules is the Security Target itself, with the occasional need for additional domain-specific documentation on a per-technology basis. This may be impacted by a TOE being deployed in the cloud if the cloud deployment affects the external interfaces that the TOE has.
* AGD\_OPE.1 – the evidence used for operation of the TOE may be affected by the TOE being deployed in a cloud environment. However, the CCitC working group is expected to create universal guidance for how this evidence is affected by cloud deployments, independent of any specific type of product. It is strongly recommended to make use of this guidance so that the presentation of admin guidance intended for use in cloud settings is consistent across vendors and product types.
* AGD\_PRE.1 – the evidence used for initial setup of the TOE may be affected by the TOE being deployed in a cloud environment. However, the CCitC working group is expected to create universal guidance for how this evidence is affected by cloud deployments, independent of any specific type of product. It is strongly recommended to make use of this guidance so that the presentation of admin guidance intended for use in cloud settings is consistent across vendors and product types.
* ALC\_CMC.1 – this is not impacted by a cloud deployment because the method by which the TOE is identified and labeled will not change based on this.
* ALC\_CMS.1 – this is not impacted by a cloud deployment because the method by which the TOE is identified and labeled will not change based on this.
* ATE\_IND.1 – this is not impacted by a cloud deployment except to the extent that the TOE being deployed in a cloud affects how the actual tests are performed.
* AVA\_VAN.1 – the vulnerability assessment process for the TOE and its dependencies will not be affected by the environment it is deployed in. However, in the cloud context specifically, it may be appropriate to require that the operational environment does have some safeguards in place that are assessed through a vulnerability assessment and penetration testing process. Additionally, a cloud deployment of the TOE may involve third-party dependencies that must be considered, and penetration testing of the TOE in the cloud environment may require special accommodation from the cloud service provider.

The high-level takeaways from this are as follows:

* The same notion of needing the operational environment to be a “trusted platform” applies here – deploying the TOE in a cloud platform and infrastructure that has had some sort of third-party validation is important because it helps the evaluator understand the extent to which the TOE relies on the platform and gives assurance that a vulnerable platform does not introduce any significant potential exploits of the TOE itself.
* The impact of a cloud deployment on how the TOE is evaluated is generally not going to be specific to a particular PP or PP-Configuration; following general CCitC guidance for this should be suitable in most cases.

1. **Determine Impact on SFRs**

Depending on the PP or PP-Module, it may be required for the TSF to implement all of the claimed SFRs or that some claims of reliance on platform functionality are allowed.

Regardless of where an SFR is actually implemented, deployment in a cloud environment versus on-prem may affect how that SFR is tested. For example, cryptographic algorithm validation for a given function would require the evaluator to know what specific hardware devices the TOE can run on when deployed in a cloud, which would require an inventory of all of the hardware used by the cloud service provider for the desired cloud to be provided to the evaluator. Low-level protocol testing may also be affected if a given cloud service provider implements network boundary protection that either requires special permission to disable or cannot be disabled altogether.

To determine how a PP or PP-Module can fit in with a cloud environment, it is necessary for technical subject matter experts to review the evaluation activities for each SFR to determine whether:

* The test activity can be performed as-is if the TOE is deployed in a cloud environment
* The test activity can be performed if the TOE is deployed in a cloud environment, but some modifications or other special conditions are needed.
  + What modifications would these be and does this depend on the cloud service provider? e.g., different providers may have different constraints.
* The test activity cannot be performed if the TOE is deployed in a cloud environment.
  + Why is the activity not doable and does this depend on the cloud service provider? e.g., different providers may have different constraints.

The goal of this should be to determine what technical hurdles exist, if any, to performing the existing tests in a cloud deployment. If any tests require modification for cloud-specific scenarios, a consensus will need to be reached within the technical community as to what modifications are needed and whether or not this still provides an acceptable level of product assurance. The national schemes that approve the PP or PP-Module for use must also approve of this; it should not be assumed that any such changes are automatically acceptable.

Note that mappings to the desired cloud validation baseline is not critical here, at least not from a CC perspective. The expectation is that there will be minimal re-use of existing validation evidence because of how tailored the CC requirements are to specific tests. There may be some value to vendors pursuing cloud certification \*after\* a CC evaluation because the specific evidence could be reusable in a more general context, but the relationship likely does not flow both ways.

1. **Determine Need for New SFRs**

There is no guarantee that the existing PP or PP-Module SFRs are sufficient to cover the required security functionality. Technical community consultation with subject matter experts will be needed to determine whether any additional SFRs are needed specifically for the cloud use case. Specific examples of these will be provided in the future as they are developed, and can be incorporated into PPs to address security functionality not covered in a current evaluation.

1. **Map to Other Applicable Cloud Programs**

One the assumptions for the TOE’s operational environment are mapped to the referenced cloud validation scheme for determination of what can be considered a “trusted platform” for the TOE and the SFRs and SARs have been assessed to determine how cloud deployment affects the validation process, the output of this can be mapped to other cloud validation programs.

If starting with FedRAMP, a non-US cloud validation scheme will not use NIST SP 800-53 to associate security controls with required system behavior, but such a scheme would likely have significant overlap, just with a different naming scheme.

This process should be applied to any nations that wish to support the use of CC in the Cloud but first need to understand how such a certification would fit in to their existing validation programs.

1. **Key Takeaways**

Conceptually, a PP or PP-Config should allow a TOE to be evaluated in a cloud deployment.

However, not all clouds are created equal. Some method is needed to ensure that if the TOE depends on a cloud platform or infrastructure, there is sufficient trust in the security of those things to say they are eligible to be used as the TOE’s operational environment.

While cloud validation of the environment is an essential part of gaining sufficient trust to deploy the TOE in a cloud setting, such a validation of the TOE itself may only offer minimal value in terms of evidence reuse. This is due to the specific granularity of CC evidence. However, the benefits may flow the opposite direction; due to the high level of rigor of a CC evaluation, the evidence from such a certification could potentially be reused for a higher-level cloud certification.

On a general level, the CC in the Cloud working group is developing guidance documentation that should be usable across all cloud CC evaluations that covers the cloud-specific requirements for operational and preparatory procedures. Such guidance should be applied uniformly across all PPs to ensure consistent presentation between technology types.

On a per-PP level, it will be necessary for technical communities to determine the underlying assumptions that the TOE relies on a cloud service provider to satisfy, the extent to which existing SFRs can be tested in a cloud setting, any workarounds or updates to the required activities for those tests that cannot be done strictly as written, and any cloud-specific SFRs that need to be added as implementation-dependent requirements to ensure that cloud-specific threats are adequately mitigated. This information may also depend on the specific cloud service provider being used, so consultation with a wide variety of software vendors, cloud service providers, and end users is recommended to ensure the broadest possible set of use cases are being considered.

Security best practices are well-established principles and the cloud validation schemes used by different nations should have significant overlap. Once the applicability of one validation scheme is assessed as a reference, the process for adapting this to other such schemes should be straightforward. Ultimately the buy-in of individual CCRA participants will affect the cloud validation schemes that need to be assessed for a given PP or PP-Module.