**Trusted Provider:**

Proven success

Acceptable gov cloud risk mitigation framework such as FedRamp, C5, SecNum etc

Visibility into when security relevant changes will happen. For example updating to TLS 1.3.—SOC2 may cover.

Data Privacy policies need to be available <https://www.itgovernance.eu/en-ie/iso-27001-ie>

What does a Trusted Provider provide?

* Network segmentation

**Trusted Platform:**

* CC certificate for O/S, V/M, GPCP? Need to define what is an acceptable delay
* FIPS algorithm validation certs (US/Can) Need to define what is an acceptable delay
* Additional higher level frameworks such as IL5, IL6 would be a plus

<Cloud providers update underlying systems frequently.>

What is a Trusted Platform as it relates to CC in the Cloud? A trusted platform’s definition depends on the protection profile(s) being evaluated against. A platform provides the operating environment for a given TOE that typically meets the requirements for a particular evaluated configuration. Components of a platform may include: a general purpose operating system, virtualization hypervisor, various network components and servers needed to run the software. Some technology won’t need all of the components listed above because, for example, an O/S is contained in an appliance such as a network device.

How do platforms become trusted platforms? The CC in the Cloud TWG suggests the following minimum requirements would be needed:

1. A Common Criteria certificate for each relevant component in the platform being utilized by the TOE.

Questions for NIAP/Sponsor:

* What items in the platform stack need CC? Do you want hardware (e.g. servers) evaluated?
  + Only include the relevant platform? The layer being utilized by the TOE?
  + In other similar approaches like JIL the entire stack needs CC. Need to define if process reviews like FedRamp is good enough.
  + ACTION: Send an email with this question to Matt and Tom

<Look at ESR>

For example, the NDcPP depends the virtualization provider and/or the underlying hardware. As opposed to the Software App cPP utilizes the O/S for most of it’s security functionality.

Start with a variant of an N-Tier Architecture.

Questions to ask? Is it serverless?

Serverless functions would need a CSP-validated runtime environment.

What do the Cloud Authorizations not cover that we need to gain trust? To discuss next time!

SP 800-53 provides common controls across FEDRamp, CSA STAR, and ISO 27017 which can map to PPs. What can be leveraged to satisfy SARs of SFR AAs?

Data segmentation/isolation of customer data and how a trusted provider implements this in the platform.

* Differentiation of control plane vs user plane in public cloud platforms. How is architecture responsible for ensuring that CSP operators cannot access cloud user data?
  + Zero Knowledge Encryption?
    - Probably not as zero knowledge proofs focus mostly on blockchain implementations.
  + Is there a way to implement this without a KMS?
* There are FEDRamp controls that ensure D@RE keys cannot be accessed by the CSP. Does this mandate hybrid key management or on-prem KMS?
  + MOD\_FEEM can be leveraged for this capability. However, the PP requires password authentication which is not great for cloud environments where API/Token combinations are used via KMIP.

What does a trusted platform provide?

* Consistent platform / operational environment
* Physical Security
* Personnel Security
* Auditing
* Data Sovereignty / Isolation
* Tenant Isolation – Virtualization PP provides SFRs for VM security features such as libvirt / virtio / qemu / etc. However, the GPOS PP does not have SFRs for validating container sandboxing implementations such as secompfilter, etc.
  + This is a fairly large gap for cloud OEs.
* Network Segmentation -