TRUST ASSESSMENT FRAMEWORK: EXECUTIVE SUMMARY

Cloud computing, whether public, private, or hybrid, provides computational infrastructures for enterprises of all sizes. By its nature, cloud computing is a multi-tenant infrastructure, elements of which typically include all components and transport mechanisms, from the end device through the network to the computational device (container, virtual machine, or physical machine) and storage.

The challenge is to properly utilize multi-tenant infrastructure, while maximizing the business (profit, efficiency, and opportunity) -- without putting key assets at risk (or violating established standards). TCG has developed a new Trust Assessment Framework, which includes two primary components: the maturity model and an example scenario to guide users through an assessment of their multi-tenant infrastructure.

The first part of the framework, the maturity model, explains how to assess trust with an explicit understanding that the amount of trust required will depend on what is at risk. The primary components of trust are impact and assurance. The model points out that the user of a multi-tenant infrastructure must understand (be able to quantify or assign) the value of the information that will be accessible through the infrastructure; the implications of possible loss or undetected change to that information; the types of threats against the organization; and the likelihood that they will occur.

The maturity model defines six categories of harm based on ITU-T X.1254[1]. Impact is divided into four levels and the likelihood of each type of impact into three levels. This model can be visualized as a two dimensional matrix into which the four levels of required trust can be assigned. The actual assignment of the required level of trust should be based on business policy. The model notes that enterprises should have policies that govern their use of outside resources.
The final aspects that must be considered in the maturity model are assurance, policy, enforcement and rights:

- Assurance is the ability to independently verify the assertions made by an infrastructure provider.
- Policy is a set of testable statements describing the criteria necessary to mitigate risks. Enforcement requires that violations of policy be detectable.
- Good enforcement helps mitigates risk whereas poor enforcement or no enforcement raises risk.
- Finally the model points out that user a multi-tenant infrastructure user's rights are established as a matter of policy and must be measurable.

[1] International Telecommunications Union. X.1254: Entity authentication assurance framework (https://www.itu.int/rec/T-REC-X.1254-201209-I)

The second part of the framework provides an example of applying the Trust Assessment Framework to generate an assessment. The scenario is for an enterprise considering what should be required to enable mobile user to gain access to certain enterprise data. It identifies specific questions that should be asked and gives example sources for the answers to questions. The scenario includes consideration of potential harm and potential impact.

In the provided example, sufficient trust does not exist to enable the desired application. However, utilizing the artifacts of the assessment, appropriate existing mitigations are assigned to achieve the required level of trust.

The use of multi-tenant infrastructures has become pervasive. In order to properly manage business assets, businesses must evaluate the risks associated with their infrastructure usage. We encourage users to make this framework part of their assessment process. Application of this framework can be especially important in enterprises dealing with some specific compliance requirements.