Suggested inputs to a Security Problem Definition for Cloud evaluations

In the case where a TOE is hosted on a Trusted Platform, platform related Assumptions and associated Security Objectives for the Operating Environment should be fulfilled by that Trusted Platform.

Below are a suggested set of Assumptions and Security Objectives for the Operating Environment that may be incorporated into a protection profile. The table provides a mapping between them and also to Cloud Authorization Scheme Controls - Cisco CCF v2.0, which provides further mapping to individual Cloud Authorization Schemes. Such mapping in a Protection Profile may be used by an evaluator to confirm that the selected Trusted Platform has been validated by an appropriate Cloud Authorization Scheme to have controls fulfilling the Assumptions and associated Security Objectives for the Operating Environment.

It should be noted that the these suggested additions for a TOE hosted on a Trusted Platform does not necessarily replace all the Assumptions and Security Objectives for the Operating Environment. For example, Assumptions around no general-purpose computing capabilities, no through traffic protection, trusted admin at the level of the TOE, non-malicious/trusted/proper users, and TOE updates are unlikely to be fulfilled by the Trusted Platform.

A.TRUSTED_PLATFORM_ADMINISTRATOR

The Security Administrators for the Trusted Platform are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the TOE. The TOE is not expected to be capable of defending against a malicious Trusted Platform Administrator that actively works to bypass or compromise the security of the TOE.

OE.TRUSTED_PLATFORM_ADMINISTRATOR

Trusted Platform Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

A.TRUSTED_PLATFORM_CONNECTIVITY

All connections to and from Trusted Platforms and between separate parts of the TSF are physically and/or logically protected within the Trusted Platforms to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

OE.TRUSTED_PLATFORM_CONNECTIVITY

All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and

logical protection techniques.

A.TRUSTED_PLATFORM_ISOLATION

It is assumed that the Trusted Platform provides, and is configured to provide, sufficient isolation between software running in Trusted Platforms on the same physical platform. Furthermore, it is assumed that the Trusted Platform adequately protects itself from software running inside Trusted Platforms on the same physical platform.

OE.TRUSTED_PLATFORM_ISOLATION

The Trusted Platform isolation is configured to reduce the attack surface of the TOE as much as possible while supporting TOE functionality. The isolation is operated in a manner that reduces the likelihood that TOE operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the isolation should be configured to make use of features that leverage the virtualisation privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

A.TRUSTED_PLATFORM_PHYSICAL_PROTECTION

The TOE is assumed to be physically protected in its Trusted Platform environment and not subject to physical attacks that compromise the security or interfere with the TOEs physical interconnections and correct operation. This protection is assumed to be sufficient to protect the TOE and the data it contains. As a result, there are no further requirements on physical tamper protection or other physical attack mitigations. The TOE is not expected to defend against physical access to the TOE that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the TOE.

OE.TRUSTED_PLATFORM_PHYSICAL_PROTECTION

Trusted Platforms, that operate within data centers or in other access-controlled environments, are expected to receive a considerable degree of protection from these environments. In addition to physical protection, these environments often provide malware-detection and behaviour-monitoring services for computing assets.

A.TRUSTED_PLATFORM_REGULAR_UPDATES

The Trusted Platform software/firmware is assumed to be updated by the Trusted Platform Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

OE.TRUSTED_PLATFORM_REGULAR_UPDATES

The Trusted Platform software/firmware is updated by an Trusted Platform Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.TRUSTED_PLATFORM_RESIDUAL_INFORMATION

The Trusted Platform Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on platform equipment when the equipment is discarded or removed from its operational environment.

OE.TRUSTED_PLATFORM_RESIDUAL_INFORMATION

The Trusted Platform ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on equipment when the equipment is discarded or removed from its operational environment.

A.TRUSTED_PLATFORM_SERVICE

The TOE relies upon a trustworthy platform and local network from which it provides administrative capabilities.

The TOE relies on this platform to provide a range of security-related services including reliable timestamps, user and group account management, user authentication, user authorization, logon and logout services via a local or network directory service, remote access control, and audit log management services to include offloading of audit logs to other servers. The platform is expected to be configured specifically to provide TOE services, employing features such as a host-based firewall, which limits its network role to providing TOE functionality.

OE.TRUSTED_PLATFORM_SERVICE

The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE. The Trusted Platform service shall be managed according to known, accepted and trusted policies. Any information provided by the Trusted Platform and used to support user authentication and authorization used by the TOE is correct and up to date.

OE.TIMESTAMP

Reliable timestamp is provided by the operational environment for the TOE.

Table 1. Rationale for Environmental Security Objectives and Cloud Authorization Scheme Controls

Assumption	**Environmental Objective Addressing the Assumption**	**Cloud Authorization Scheme Controls - Cisco CCF v2.0**
A.TRUSTED_PLATFORM_ADMINISTRATOR	OE.TRUSTED_PLATFORM_ADMINISTRATOR	111,141,142,144,145,146,152,153,159,169,198,199,200
A.TRUSTED_PLATFORM_CONNECTIVITY	OE.TRUSTED_PLATFORM_CONNECTIVITY	104

Assumption	Environmental Objective Addressing the Assumption	Cloud Authorization Scheme Controls - Cisco CCF v2.0
A.TRUSTED_PLATFORM_ISOLATION	OE.TRUSTED_PLATFORM_ISOLATION	173,215,223
A.TRUSTED_PLATFORM_PHYSICAL_PROTECTION	OE.TRUSTED_PLATFORM_PHYSICAL_PROTECTION	42,43,44,59,60,207
A.TRUSTED_PLATFORM_REGULAR_UPDATES	OE.TRUSTED_PLATFORM_REGULAR_UPDATES	310,314,315
A.TRUSTED_PLATFORM_RESIDUAL_INFORMATION	OE.TRUSTED_PLATFORM_RESIDUAL_INFORMATION	63,80,81,82,83
A.TRUSTED_PLATFORM_SERVICE	OE.TRUSTED_PLATFORM_SERVICE	70,76,107,108,117,140,160,276,280,310,311,318
	OE.TIMESTAMP	212