

# Summary



Replacements

Insertions

Deletions

# Compare Results

9/27/2023 9:57:42 AM

Old File:	versus	New File:
CCiTc_Guidance_For_Cloud_Evals_old.pdf		CCiTc_Guidance_For_Cloud_Evals.pdf
45 page(s) (3.23 MB)		44 page(s) (3.20 MB)

Total Changes	Content	Styling and Annotations
265	 57	Replacements  2
	 29	Insertions  166
	 11	Deletions

[Go to the First Change \(page 3\)](#)



# *CC in the Cloud* Guidance for Cloud Evaluations

Version 0.1, 2022-08-17



# *CC in the Cloud* Guidance for Cloud Evaluations

Version 0.1, 2022-08-17

# Table of Contents

Preface.....	1
<del>Glossary</del>	2
Cloud Metal	2
Cloud	2
Cloud Application Software	2
Cloud Service	2
Cloud Service Offering (CSO)	2
Cloud Service Provider (CSP)	2
Hybrid Cloud	2
Multi-Cloud	2
Multi-Tenant	2
On-Premises (On-Prem)	2
Private Cloud	2
Provider	2
Service	2
Software Platform	2
TOE Platform	2
Cloud Topology	2
Cloud Host Services	2
Shared Security Model	2
Relationships Between the Trusted Platform / TOE Platform, and TOE	12
Solve Guidance for Trusted Platforms	12
TOE Identification	14
Cloud Equivalence Considerations	22
CPE Equivalence	22
Contributors Roles in Product Evaluation	22
Data Classification	23
Contributor Involvement	23
Steps to optimize a PP for TOEs in a cloud environment	24
Process Overview	24
Conformance Claims	24
Security Problem Definition	25
Security Objectives	25
Security Requirements	26
Security Assurance Requirements	26
Other considerations	27
Suggested inputs to a Security Problem Definition for Cloud evaluations	28
A. TRUSTED_PLATFORM_ADMINISTRATOR	28

# Table of Contents

Preface.....	1
<del>Cloud Topology</del>	2
<del>Software as a Service (SaaS)</del>	2
<del>Platform as a Service (PaaS)</del>	3
<del>Infrastructure as a Service (IaaS)</del>	4
Shared Security Model	6
<del>Relationships Between the Trusted Platform / TOE Platform, and TOE</del>	9
<del>Some Guidance for Trusted Platforms</del>	10
<del>TOE Identification</del>	10
<del>Cloud Equivalence Considerations</del>	10
<del>TOU Equivalency</del>	10
<del>Protection Profile Considerations</del>	10
<del>Process to optimize a PP for TOEs in a cloud environment</del>	20
<del>Suggested inputs to a Security Problem Definition for Cloud evaluations</del>	20
<del>A. TRUSTED PLATFORM ADMINISTRATOR</del>	24
<del>B. OF TRUSTED PLATFORM ADMINISTRATOR</del>	24
<del>A. TRUSTED PLATFORM CONNECTIVITY</del>	24
<del>B. OF TRUSTED PLATFORM CONNECTIVITY</del>	24
<del>A. TRUSTED PLATFORM ISOLATION</del>	24
<del>B. OF TRUSTED PLATFORM ISOLATION</del>	24
<del>A. TRUSTED PLATFORM PHYSICAL PROTECTION</del>	25
<del>B. OF TRUSTED PLATFORM PHYSICAL PROTECTION</del>	25
<del>A. TRUSTED PLATFORM REGULAR UPDATES</del>	25
<del>B. OF TRUSTED PLATFORM REGULAR UPDATES</del>	26
<del>A. TRUSTED PLATFORM RESIDUAL INFORMATION</del>	26
<del>B. OF TRUSTED PLATFORM RESIDUAL INFORMATION</del>	26
<del>A. TRUSTED PLATFORM SERVICE</del>	26
<del>B. OF TRUSTED PLATFORM SERVICE</del>	26
<del>A. OF TIMESTAMP</del>	26
<del>Guidance Documentation</del>	27
Vulnerability Assessment Methodology	29
<del>Contributors Roles in Product Evaluations</del>	30
<del>Role Clarification</del>	30
Glossary	31
<del>Core Metal</del>	31
<del>Cloud</del>	31
<del>Cloud Authorization Scheme</del>	31
<del>Cloud Service</del>	31

<del>TRUSTED PLATFORM ADMINISTRATOR</del>	28
<del>TRUSTED PLATFORM CONNECTIVITY</del>	28
<del>TRUSTED PLATFORM CONNECTIVITY</del>	29
<del>TRUSTED PLATFORM ISOLATION</del>	29
<del>TRUSTED PLATFORM ISOLATION</del>	29
<del>TRUSTED PLATFORM PHYSICAL PROTECTION</del>	29
<del>TRUSTED PLATFORM PHYSICAL PROTECTION</del>	29
<del>TRUSTED PLATFORM REGULAR UPDATES</del>	29
<del>TRUSTED PLATFORM REGULAR UPDATES</del>	30
<del>TRUSTED PLATFORM RESIDUAL INFORMATION</del>	30
<del>TRUSTED PLATFORM RESIDUAL INFORMATION</del>	30
<del>TRUSTED PLATFORM SERVICE</del>	30
<del>TRUSTED PLATFORM SERVICE</del>	30
<del>TIMESTAMP</del>	30
Global Processes	32
Introduction	32
Development Environment Sub Process	32
Security Target (STC) Sub Process	22
Guidance Documentation Sub Process	23
Development / Test Sub Process	23
Vulnerability Assessment Methodology	24
List of potential vulnerabilities	24
Defining penetration tests	24
List of attacks and strategies	24
References	25
Appendix A: Threats, Assumptions and Security Objectives for each PP.	26
Protection Profile for General Purpose Computing Platform, Version 1.0.	26
Base PP for Virtualization Version 1.1	27
Protection Profile for General Purpose Operating Systems Version 4.3	28
Protection Profile for Application Software Version 1.4	29
Appendix B: Analysis of the Assumptions and Security Objectives of the Operating Environment for an example stack of PP's	40



# Preface

The Common Criteria (CC) in the Cloud Technical Work Group (CCiTc) has developed this guidance document that provides a complimentary framework to allow for IT product evaluations in Cloud Operating Environments. It will include instructions and examples of how to extend or develop protection profiles to include cloud environments. The scope of the CCiTc is to provide for CC evaluations of IT products and not for the evaluation of [\[Cloud Services\]](#).

Such cloud environments may or may not conform to hybrid, public, or private cloud topologies and the associated Cloud Service Providers (CSP). These topologies can all be accommodated in this approach, with the distinction of administrator access and capability informing their inclusion. This effort is not meant to replace solution or service oriented frameworks or certification processes such as FedRAMP or other Cloud Authorization schemes.

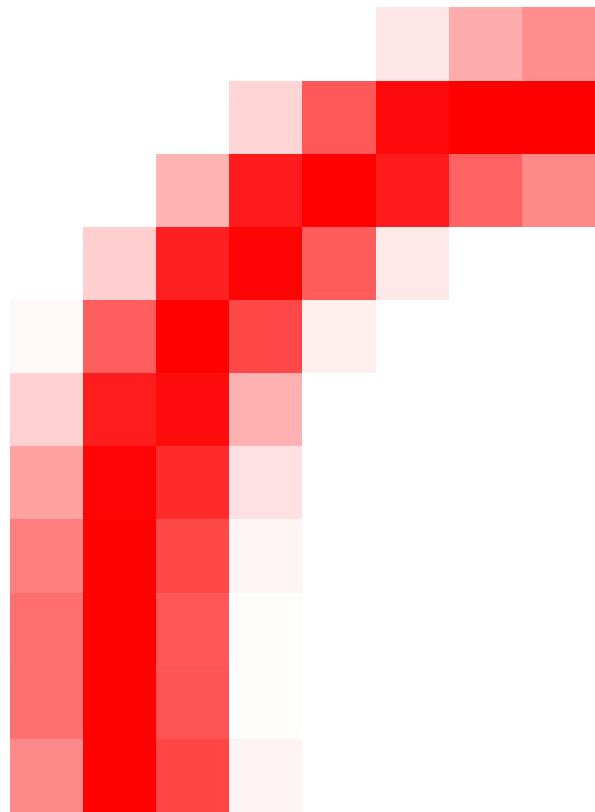
The main intended audience of this document are Protection Profile authors (e.g. iTCs and national TCs), but it is also useful to evaluators, evaluation authorities, and customers of this type of products.

# Preface

The Common Criteria (CC) in the Cloud Technical Work Group (CCiTc) has developed this guidance document that provides a complimentary framework to allow for IT product evaluations in Cloud Operating Environments. It will include instructions and examples of how to extend or develop protection profiles to include cloud environments. The scope of the CCiTc is to provide for CC evaluations of IT products and not for the evaluation of [\[Cloud Services\]](#).

Such cloud environments may or may not conform to hybrid, public, or private cloud topologies and the associated Cloud Service Providers (CSP). These topologies can all be accommodated in this approach, with the distinction of administrator access and capability informing their inclusion. This effort is not meant to replace solution or service oriented frameworks or certification processes such as FedRAMP or other Cloud Authorization schemes.

The main intended audience of this document are Protection Profile authors (e.g. iTCs and national TCs), but it is also useful to evaluators, evaluation authorities, and customers of this type of products.



# Cloud Topology

When conducting Common Criteria evaluations for IT products in cloud environments, it is crucial to recognize that the Target of Evaluation (TOE) will often encompass products designed for the cloud's unique demands. In this context, the TOE is most likely to consist of products that are capable of "lifting and shifting," meaning they can seamlessly migrate and operate in cloud environments. These types of TOEs typically fall within the three primary cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).

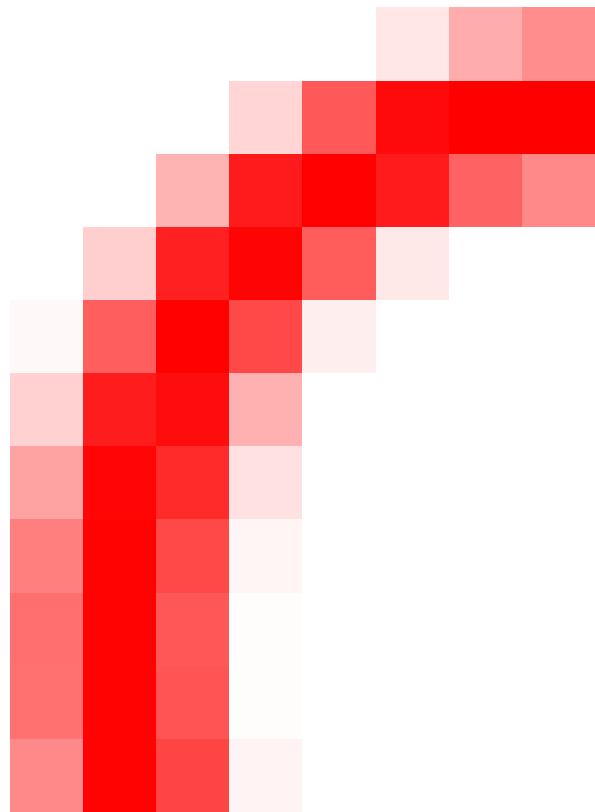
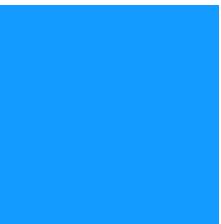
To further advance this concept, the following protection profiles are an example of how such TOEs may be evaluated in a cloud context:

## Software as a Service (SaaS)

The capability provided to the customer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. [NIST SP800-145](#)

The following PPs are examples which might be extended with CCiTC methodology to cover the above use case: cPP\_App\_SW, cPP\_DBMS, PP\_MDM

For example, if the cPP for Application Software were to be used as a baseline the cloud extensions may be applied to the existing Target of Evaluation (TOE) Boundary and TOE Platform given in the following diagram:



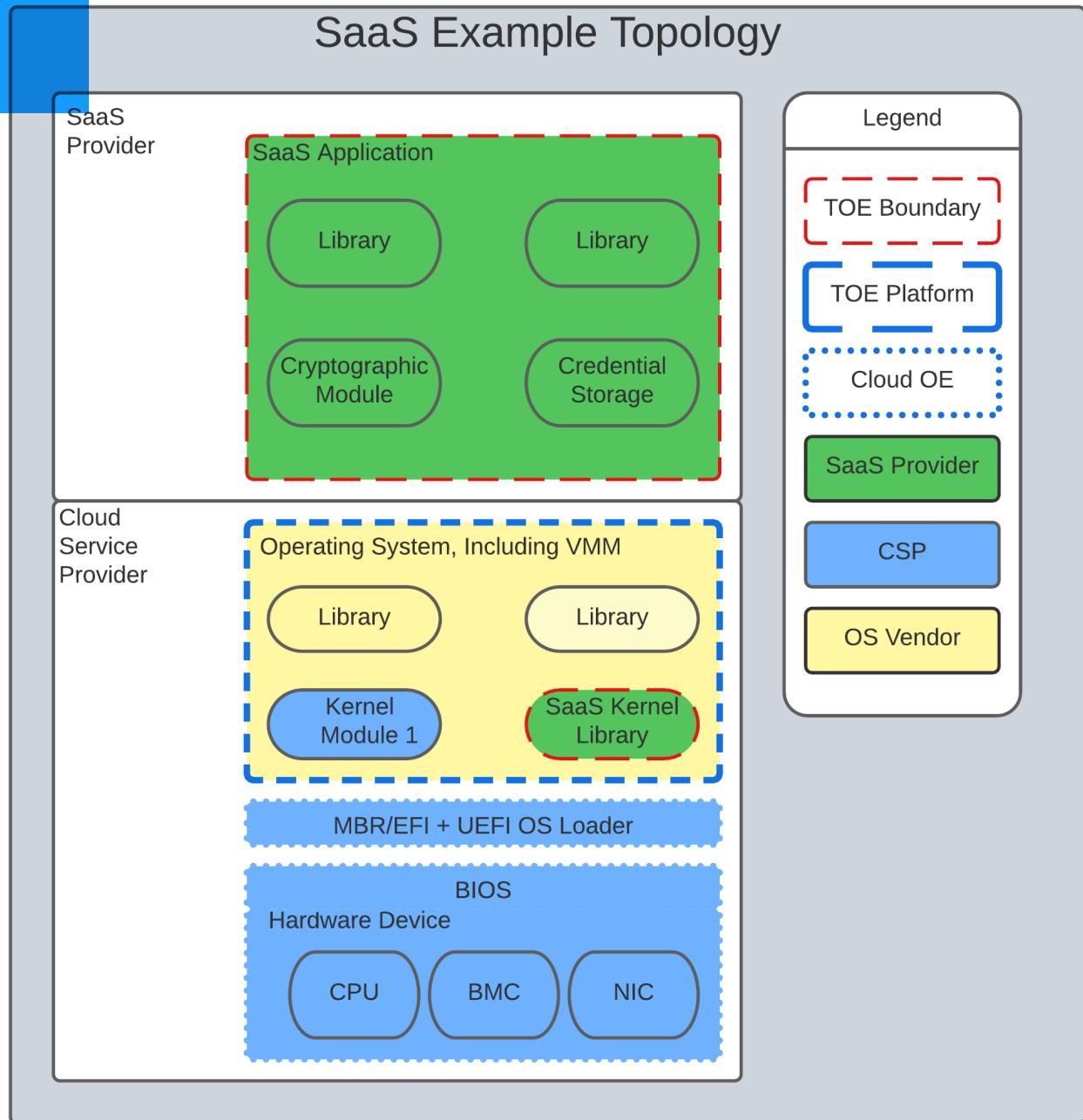
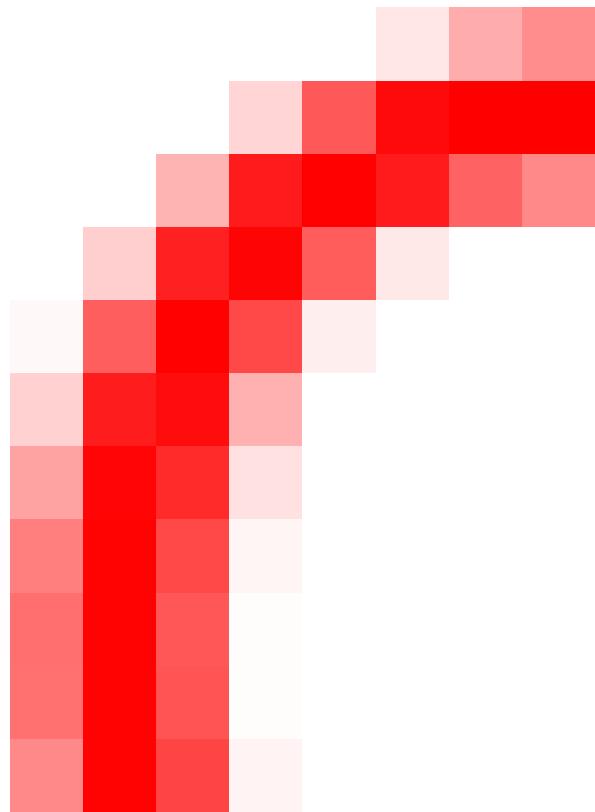


Figure 1. SaaS Example

In this example, the SaaS Application provided by the SaaS provider relies on a TOE platform from an OS Vendor which is hosted by the Cloud Service Provider on the CSP's hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration in a Cloud Operating Environment.

## Platform as a Service (PaaS)

Platform as a Service (PaaS). The capability provided to the customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. [NIST SP800-145](#)



The following PPs are examples which might be extended with CCiT\_C methodology to cover the above use case: PP\_OS, cPP\_ND

For example, if the Protection Profile for General Purpose Operating System were to be used as a baseline the cloud extensions may be applied to the existing TOE Boundary and Cloud Operating Environment given in the following diagram:

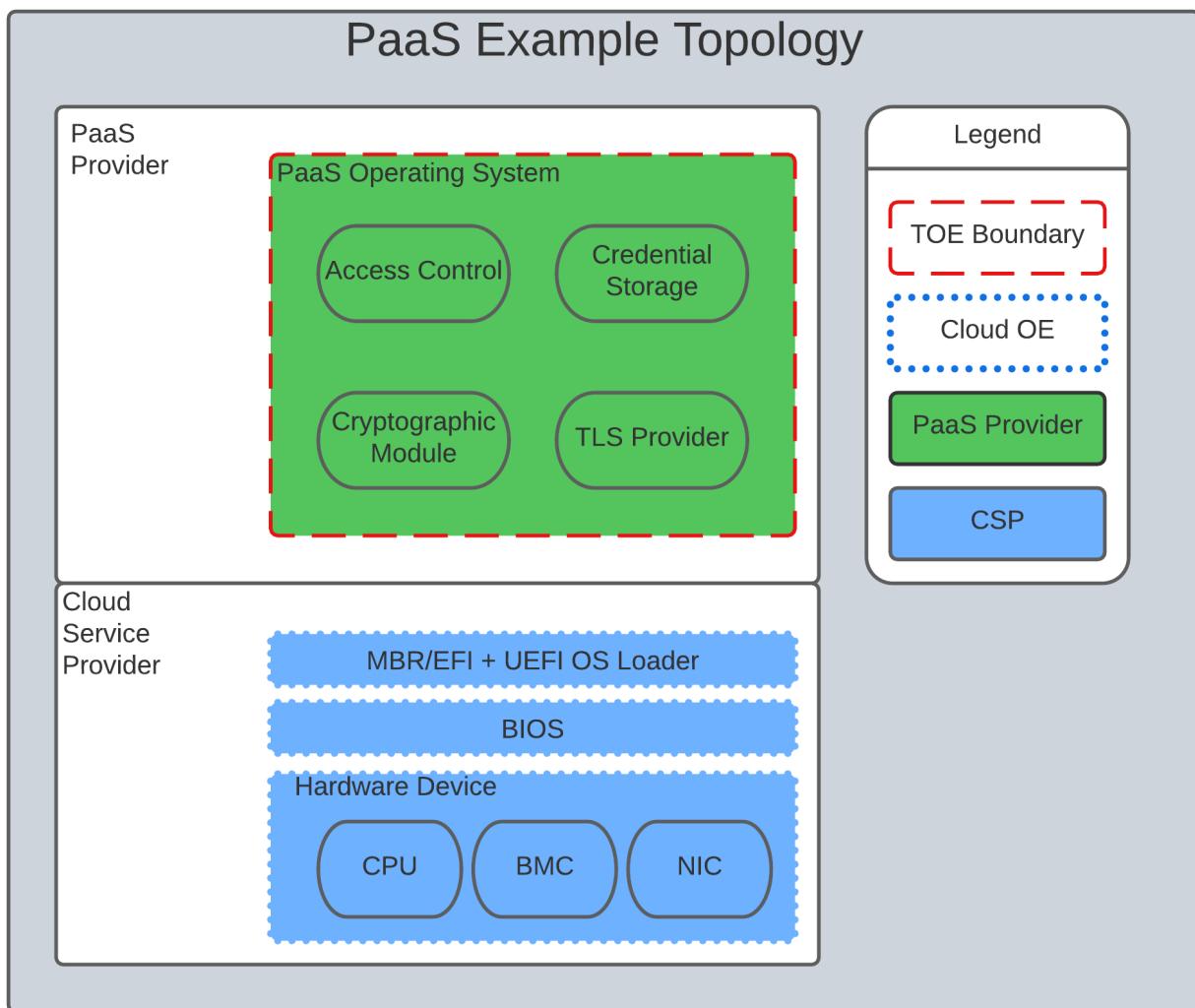
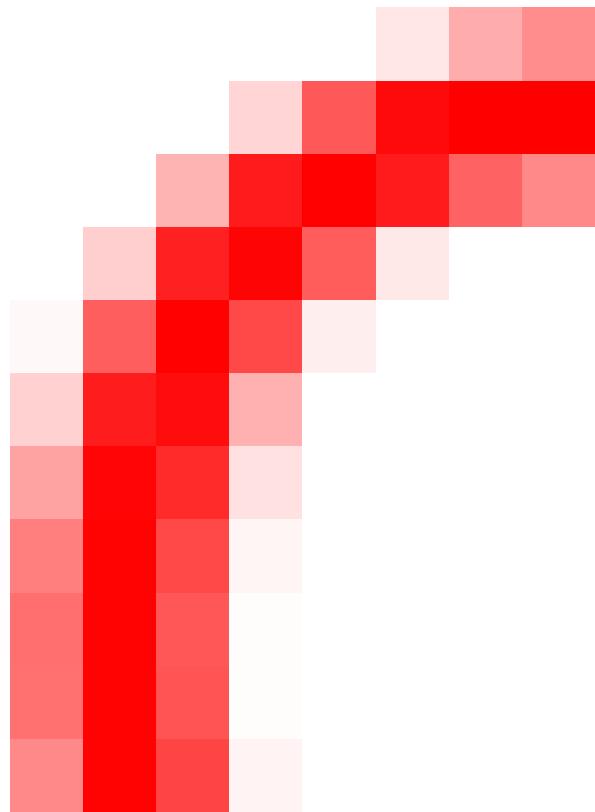
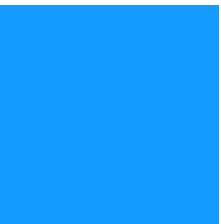


Figure 2. Paas Example

In this example, the PaaS OS provided by the PaaS provider relies on a Cloud Operating Environment which is hosted by the Cloud Service Provider on the CSPs hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration to include a Cloud Operating Environment.

## Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS). The capability provided to the customer is to provision processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select



networking components (e.g., host firewalls) [NIST SP800-145](#)

The following PPs are examples which might be extended with CCiT C methodology to cover the above use case: PP\_BASE\_VIRTUALIZATION

For example, if the Protection Profile for Virtualization were to be used as a baseline the cloud extensions may be applied to the existing TOE Boundary and Cloud Operating Environment given in the following diagram:

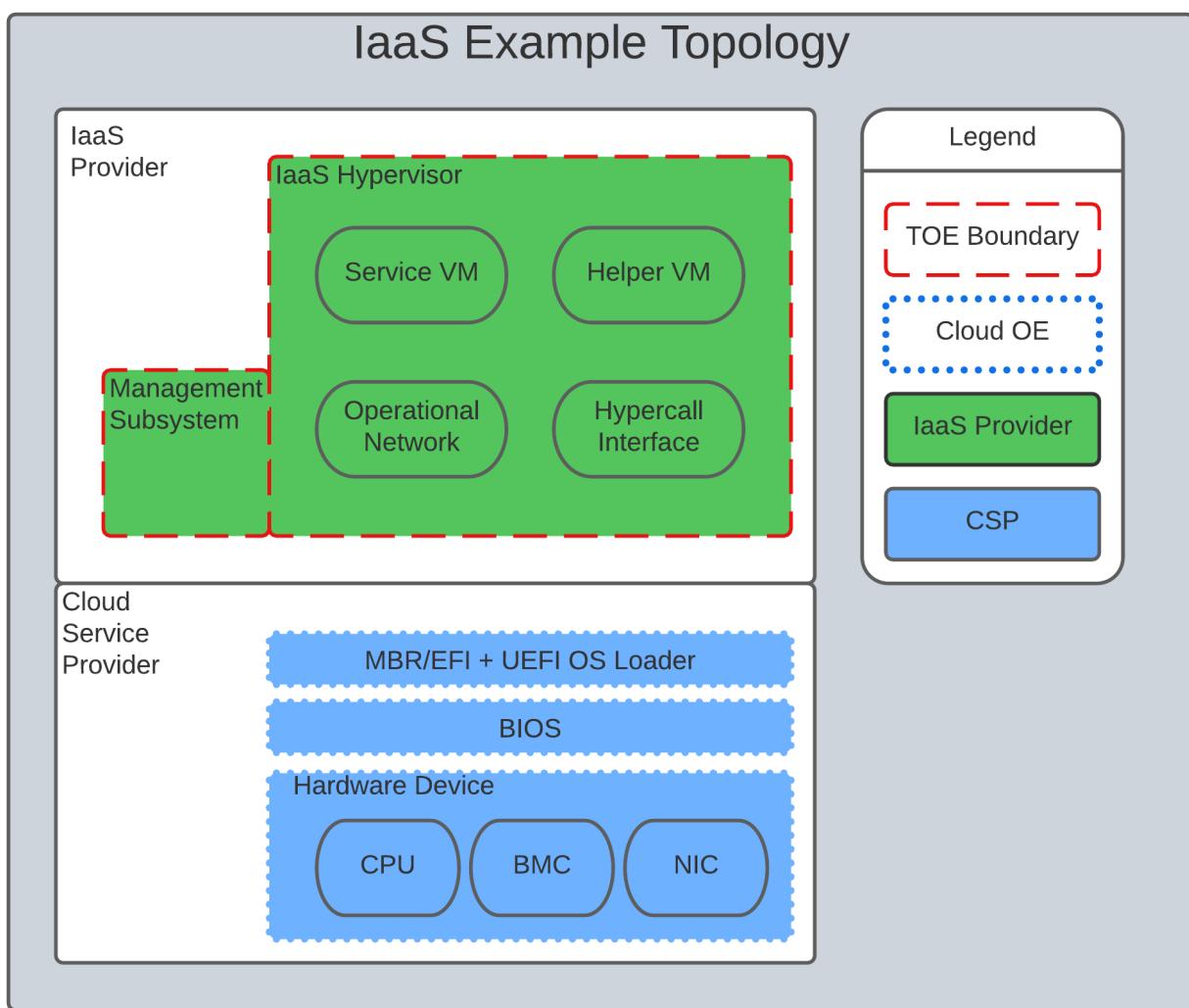
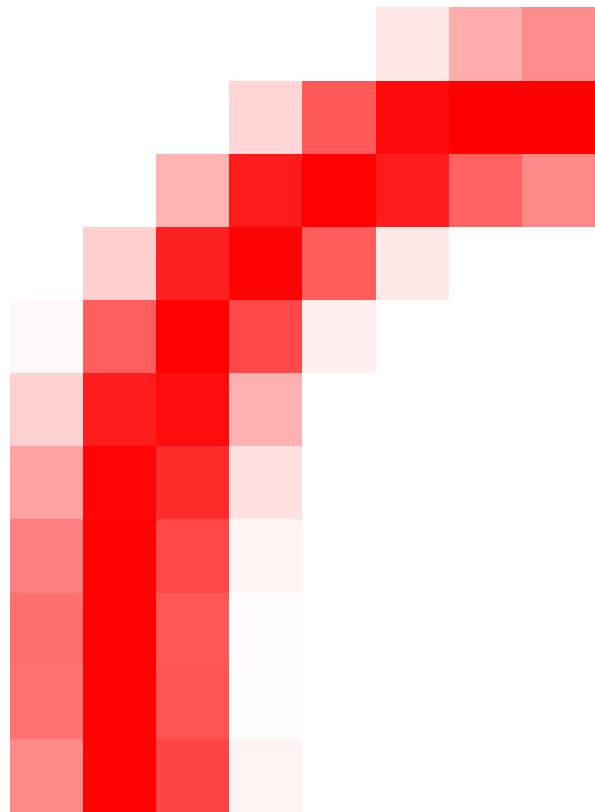
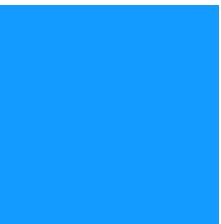


Figure 3. IaaS Example

In this example, the IaaS hypervisor provided by the IaaS provider relies on a Cloud Operating Environment which is hosted by the Cloud Service Provider on the CSPs hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration to include a Cloud Operating Environment.



# Shared Security Model

In the realm of cloud security, the shared security model is a fundamental concept that defines the division of responsibilities between the Cloud Service Provider (CSP) and their customers within a cloud environment. This model acknowledges that while the CSP is responsible for securing the underlying cloud infrastructure, the customer also bears the responsibility of securing their applications, data, and configurations within that infrastructure based on the service model. The shared security model recognizes that security is a collaborative effort, where both the CSP and the customer play crucial roles. This model is widely embraced in various cloud security frameworks, as it provides a clear model for understanding and allocating security responsibilities in a cloud environment. By delineating these responsibilities, the shared security model helps establish trust, accountability, and transparency between the CSP and the customer, ensuring a holistic approach to cloud security.

This concept is also useful for CCiTC evaluations and mirrors the relationship found with the TOE and TOE Platform. To emphasize the enhanced requirements for Cloud Infrastructure we will refer to the shared responsibility model in terms of the TOE and the Trusted Platform.

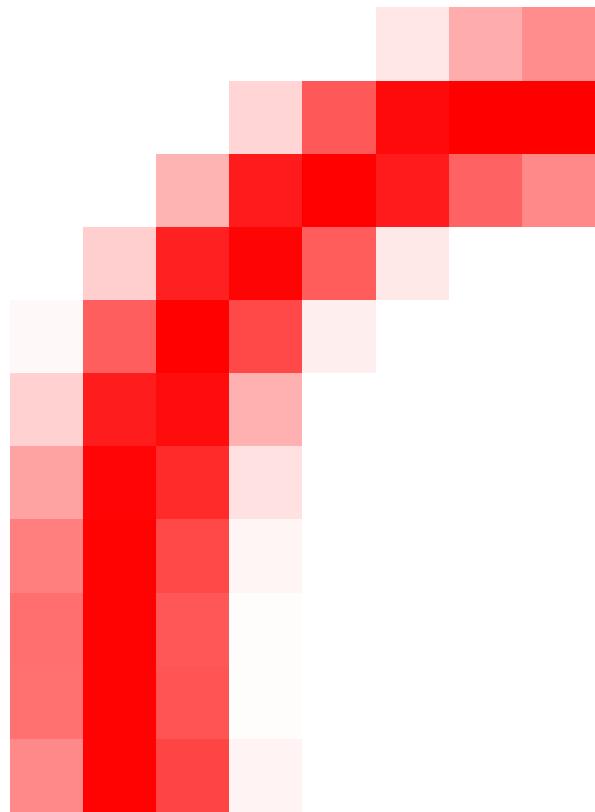
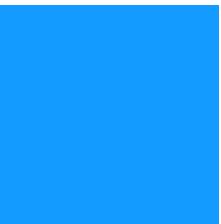
In the majority of use cases the TOE administrator (the CSP customer) is responsible for the secure utilization and customization of the cloud services provided by the CSP. This includes managing user access controls, configuring security settings, and implementing appropriate security measures aligned with their specific requirements. These elements may map appropriately to existing SFRs such as management functions defined by the FMT class in CC Part 2 (FMT\_SMF) with or without refinement for CCiTC. The TOE administrator ensures that the TOE (cloud tenant) operates securely within the parameters set by the CSP (TOE Platform).

While the CSP maintains the security and availability of the TOE Platform, the TOE administrator (customer) is assumed to be tasked with safeguarding their applications, data, and configurations within the cloud environment. They actively manage security controls, such as authentication mechanisms, encryption protocols, and network access policies, to protect their assets and mitigate potential risks.

The evaluation and assessment of the shared security model must take into account both the TOE administrator (customer) and the TOE Platform (CSP). The CSP, as the TOE Platform, undergoes evaluation against relevant security standards, certifications, and best practices to demonstrate the effectiveness of the underlying cloud infrastructure's security controls. See the Trusted Platform section for more information on the required security assessments for the TOE Platform.

Simultaneously, the TOE administrator (customer) is responsible for implementing and managing security controls and configurations within their own cloud environment. They utilize the provided security features, adhere to the CSP's policies and guidelines, and maintain appropriate security configurations to ensure the integrity and confidentiality of their data.

There are certain areas where the shared security model can be somewhat blurred. For example, with many CC evaluations, the TOE or TOE Security Functional Interface (TSFI) is expected to exclusively generate TOE audit events. In the context of a virtualized network device deployed on a public cloud, certain CC requirements, such as FAU\_GEN.1 (Audit Generation), would need to be modified to account for the consumption of logs provided by the Cloud Service Provider (CSP).



FAU\_GEN.1 requires the TOE (virtualized network device) to generate audit records for security-relevant events. However, in a cloud environment, the CSP typically manages the underlying infrastructure and maintains centralized logging systems. As a result, the TOE may rely on the CSP's log management capabilities and consume the logs provided by the CSP rather than generating its own audit records.

To accommodate this scenario, the collaborative protection profile for the virtualized network device on the public cloud should specify the requirements for log consumption from the CSP's logging infrastructure. This would include defining the format, content, and frequency of logs to be provided by the CSP. Additionally, the protection profile should address the integrity and confidentiality of these logs during transmission and storage.

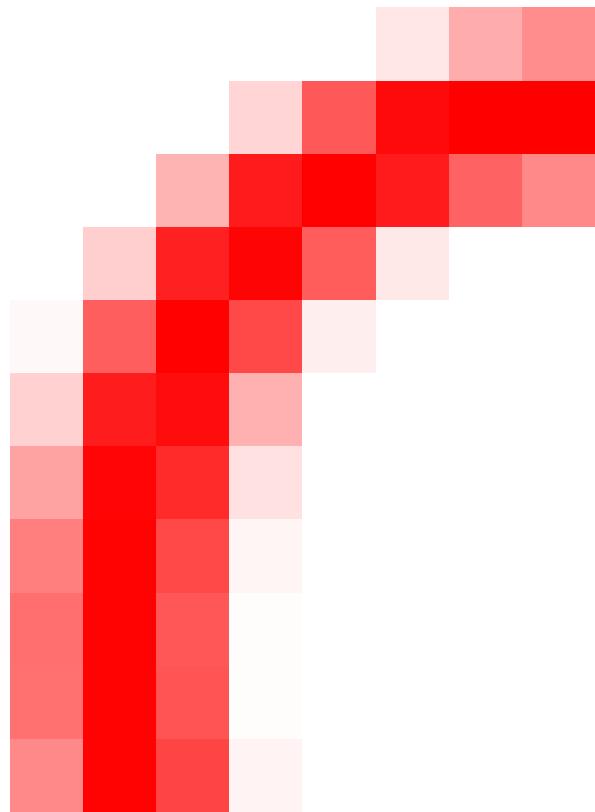
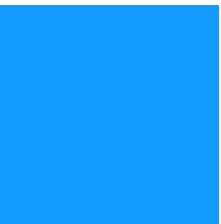
The modified CC requirements would then focus on the TOE's capability to securely receive, process, and analyze the logs provided by the CSP. The TOE should be able to extract relevant security events from the logs and correlate them with its own internal security policies. Furthermore, it should have the ability to raise alerts or initiate appropriate actions based on the analysis of the consumed logs.

By adapting CC requirements like FAU\_GEN.1 to encompass log consumption from the CSP, the protection profile enables the virtualized network device to leverage the logging capabilities provided by the CSP while maintaining compliance with CC standards. This ensures that security-relevant events are properly logged, analyzed, and acted upon in the cloud environment, contributing to a comprehensive security posture for the virtualized network device.

Additionally, it may be important to add a third element to the shared security model for CCiTC evaluations. This would be the inclusion of the TOE Vendor in addition to the TOE Administrator and CSP. The TOE Vendor may be responsible for providing TOE security updates, maintaining a trusted update channel and infrastructure, or even applying these updates on behalf of the TOE Administrator. This is a common feature with traditional SaaS use cases. In such cases where a TOE vendor is expected to share responsibilities in the security model, PP Authors must make the appropriate refinements, additions, or iterations of related elements in their PPs. This is a scenario that may be more common in TOE types that are meant to incorporate physical hardware into Cloud Infrastructure such as an HSM. However, CCiTC evaluations are not limited to a particular deployment model. It is also expected that there will be evaluations of TOEs that are integral to a CSPs cloud stack from hardware to application layers.

Ultimately, by designating the customer as the TOE administrator, the shared security model reinforces their active involvement in the secure administration of the cloud services. The CSP, as the TOE Platform, provides the underlying infrastructure, while the TOE administrator assumes the responsibility of effectively configuring, managing, and monitoring the TOE to meet their specific security objectives and compliance requirements.

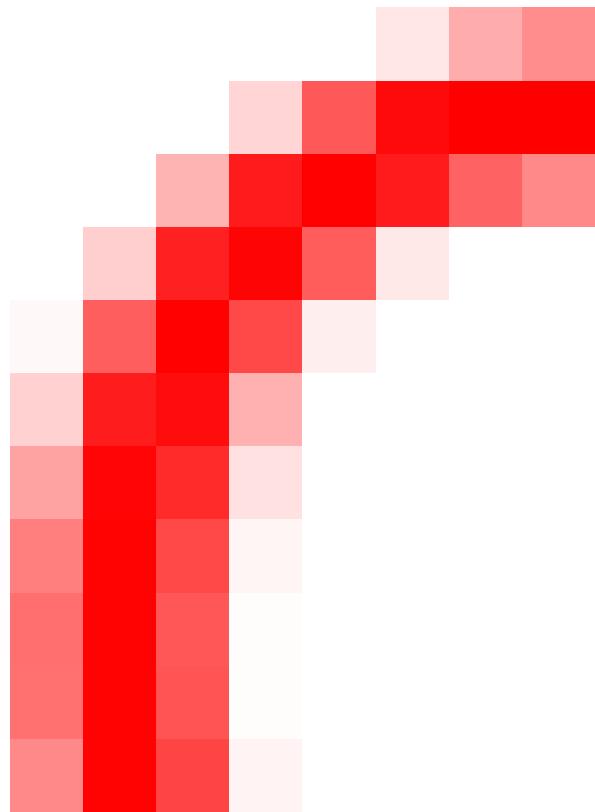
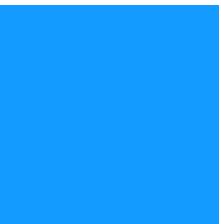
To ensure that customers acting as TOE administrators, who are familiar with Common Criteria but may have limited knowledge of cloud infrastructure and security, can effectively manage the TOE within the shared security model, it is important for the authors of protection profiles to adapt the Administrator Guidance Document (AGD) requirements accordingly. This includes providing clear instructions, accessible language, and practical guidance tailored to TOE administrators. By modifying the AGD requirements in this manner, the authors of protection profiles can ensure that TOE administrators can confidently manage the TOE within the shared security model, bridging the



gap between Common Criteria expertise and the challenges of managing security in a cloud environment.

Additionally, The TSS, which defines the security functionality and assurance requirements of the TOE, can be modified by the authors of protection profiles to provide clear explanations tailored to evaluators limited knowledge of cloud infrastructure and security. The modified TSS should include detailed information such that it is clear how the TSFI or SFR enforcing features interact in a cloud context with the TOE Platform.

By adapting the TSS and AGD requirements in this manner, the authors of protection profiles can ensure that TOE administrators with limited knowledge of cloud infrastructure and security can confidently manage the TOE within the shared security model. These modifications provide clear and accessible guidance, empowering TOE administrators to make informed decisions, configure the TOE securely, and fulfill their security responsibilities effectively.



# Relationships Between the Trusted Platform / TOE Platform, and TOE

We need to explain that the Trusted Platform exists underneath the TOE Platform and is provided by the CSP.

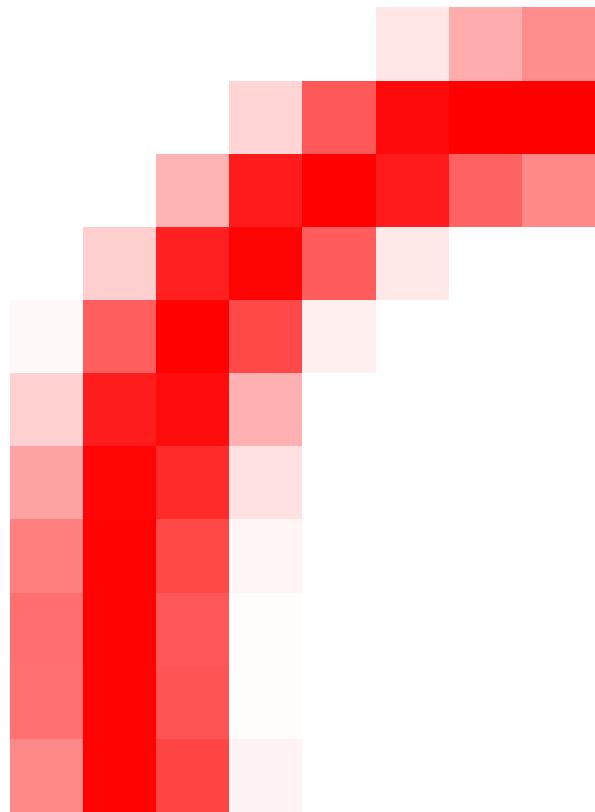
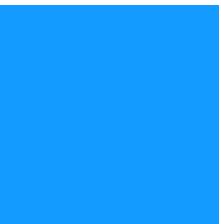
The TOE Platform may or may not exist on top of the Trusted Platform, but is specifically what is providing functionality to the TOE.

If the TOE Platform does not exist as the TOE is capable of meeting all PP SFRs independently, then a Trusted Platform would still be needed to provide a hosting environment for the TOE.

For example, for a TOE that is a Software Application, the TOE Platform would be the Operating System and the Trusted Platform would be the underlying virtualization solution provided by the CSP.

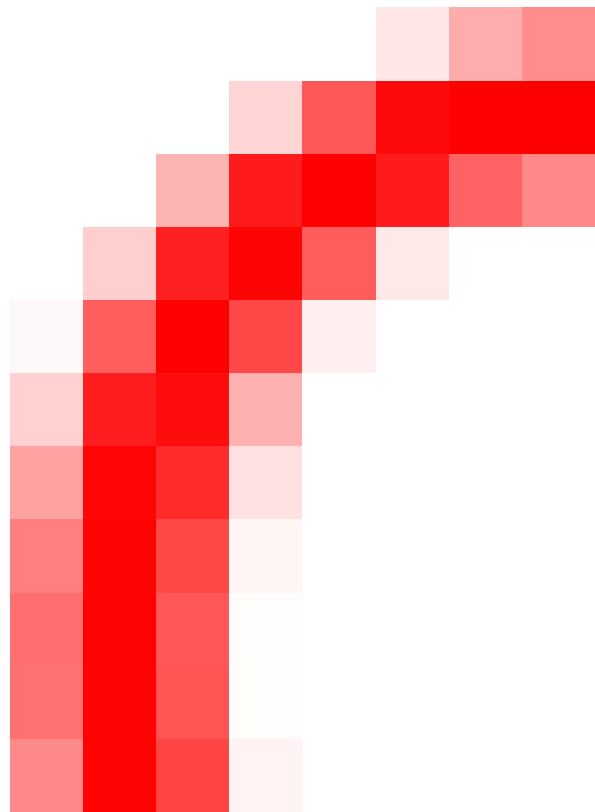
If the TOE is a General Purpose Operating System (GPOS) then the TOE Platform would be the underlying hypervisor and the Trusted Platform would include the hardware layer and below from the CSP.

If the TOE is a General Purpose Compute Platform (GPCP) then no TOE Platform is applicable and the Trusted Platform would be the power, cooling, and physical security provided by the CSP.



# Scheme Guidance for Trusted Platforms

Placeholder for issue #106



# TOE Identification

When deploying a Target of Evaluation (TOE) to public cloud infrastructure, proper identification and distinction of the TOE instances are crucial. This ensures accurate tracking, management, and application of security controls specific to each TOE instance within the cloud environment. In this section, we will explain how TOE identification can be established when deploying TOE instances on popular public cloud platforms such as AWS, Azure, and Oracle Cloud Infrastructure.

## AWS (Amazon Web Services):

In AWS, TOE instances can be provisioned as either bare metal instances or virtual machines (VMs) based on the specific requirements. AWS offers different services such as Amazon EC2 (Elastic Compute Cloud) for VM instances and Amazon EC2 Bare Metal instances for bare metal deployment. During the provisioning process, unique identifiers such as instance IDs, resource tags, and naming conventions can be utilized to supplement TOE identification. By assigning descriptive tags and naming conventions, TOE administrators can easily distinguish and manage each TOE instance.

**Name and tags** [Info](#)

Name  
e.g. My Web Server [Add additional tags](#)

**Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS Images

Recents | My AMIs | **Quick Start**

Ubuntu | Windows | Red Hat | SUSE Linux | Debian | [Browse more AMIs](#)

**Amazon Machine Image (AMI)**

**Amazon Linux 2023 AMI**  
ami-0889a44b331db0194 (64-bit (x86)) / ami-08fc6fb8ad2e794bb (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**  
Amazon Linux 2023 AMI 2023.0.20230503.0 x86\_64 HVM kernel-6.1

**Architecture**  
64-bit (x86) [AMI ID](#) ami-0889a44b331db0194 [Verified provider](#)

**Summary**

Number of instances [Info](#)  
1

Software image (AMI)  
Amazon Linux 2023 AMI 2023.0.20230503.0 x86\_64  
HVM kernel-6.1  
ami-0889a44b331db0194

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

**Launch instance** [Review commands](#)

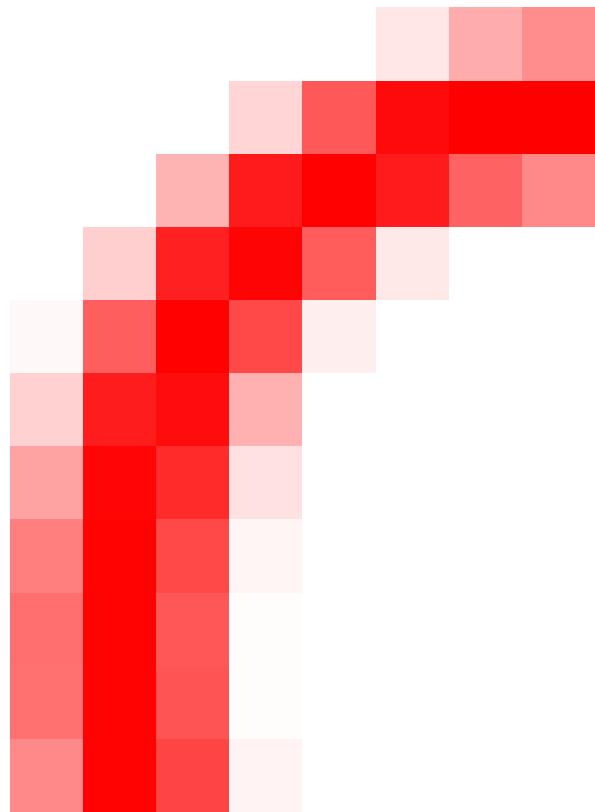
**Instance type** [Info](#)

Instance type  
**t2.micro** Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true  
On-Demand Windows pricing: 0.0162 USD per Hour  
On-Demand SUSE pricing: 0.0116 USD per Hour  
On-Demand RHEL pricing: 0.0716 USD per Hour  
On-Demand Linux pricing: 0.0116 USD per Hour

All generations [Compare instance types](#)

Figure 4. AWS Example



The screenshot shows the AWS CloudWatch Metrics interface. On the left, there's a sidebar with a search bar and a 'Name and tags' section. The main area displays a table of metrics. Each row contains a metric name, its ARN, a detailed description, and a 'Free tier eligible' status indicator. To the right of the table, there are several configuration sections: 'Number of instances' (set to 1), 'Software Image (AMI)' (Amazon Linux 2023 AMI 2023.0.2), 'Virtual server type (instance type)' (t2.micro), 'Firewall (security group)' (New security group), 'Storage (volumes)' (1 volume(s) - 8 GiB), and a note about the free tier.

Name	ARN	Description	Free tier eligible
Amazon Linux 2023 AMI	arni-0889a44b331db0194	(64-bit (x86)) / ami-08fc6fb8ad2e794bb (64-bit (Arm)) Virtualization: hvm ENA enabled: true Root device type: ebs	✓
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type	arni-03c7d01cf4dedc891	(64-bit (x86)) / ami-0c5338a495eb1c939 (64-bit (Arm)) Virtualization: hvm ENA enabled: true Root device type: ebs	✓
Deep Learning AMI GPU PyTorch 2.0.0 (Amazon Linux 2) 20230406	arni-0405edac781bf558d	(64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Deep Learning AMI GPU TensorFlow 2.12.0 (Amazon Linux 2) 20230324	arni-0fbf75205e2d757a1	(64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Deep Learning AMI GPU PyTorch 1.12.1 (Amazon Linux 2) 20230324	arni-0368028f5ecf3ec97	(64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Amazon Linux 2 LTS with SQL Server 2019 Standard	arni-0874d82d2138e9fd1	(64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Amazon Linux 2 LTS with SQL Server 2017 Standard	arni-02160391b456f1164	(64-bit (x86))	

**Number of instances** [Info](#)  
1

**Software Image (AMI)**  
Amazon Linux 2023 AMI 2023.0.2  
HVM kernel-6.1  
arni-0889a44b331db0194

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
New security group

**Storage (volumes)**  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 75 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Figure 5. AWS Example

This screenshot shows the AWS Lambda 'Create Function' wizard, Step 2: 'Configure function settings'. It lists several instance types (t2.micro, t2.nano, t2.small, t2.medium) with their details and pricing. A 'Free tier eligible' status is indicated for each. To the right, there are sections for 'Firewall (security group)' (New security group), 'Storage (volumes)' (1 volume(s) - 8 GiB), and a note about the free tier. At the bottom, there are 'Cancel', 'Launch', and 'Review' buttons.

Instance type	Family	CPU	Memory	Current generation	Pricing	Status
t2.micro	t2	1 vCPU	1 GiB Memory	Current generation: true	On-Demand Windows pricing: 0.0162 USD per Hour On-Demand SUSE pricing: 0.0116 USD per Hour On-Demand RHEL pricing: 0.0716 USD per Hour On-Demand Linux pricing: 0.0116 USD per Hour	Free tier eligible
t2.nano	t2	1 vCPU	0.5 GiB Memory	Current generation: true	On-Demand Linux pricing: 0.0058 USD per Hour On-Demand SUSE pricing: 0.0058 USD per Hour On-Demand Windows pricing: 0.0081 USD per Hour	
t2.micro	t2	1 vCPU	1 GiB Memory	Current generation: true	On-Demand Windows pricing: 0.0162 USD per Hour On-Demand SUSE pricing: 0.0116 USD per Hour On-Demand RHEL pricing: 0.0716 USD per Hour On-Demand Linux pricing: 0.0116 USD per Hour	✓
t2.small	t2	1 vCPU	2 GiB Memory	Current generation: true	On-Demand Windows pricing: 0.032 USD per Hour On-Demand Linux pricing: 0.023 USD per Hour On-Demand RHEL pricing: 0.083 USD per Hour On-Demand SUSE pricing: 0.053 USD per Hour	

**Firewall (security group)**  
New security group

**Storage (volumes)**  
1 volume(s) - 8 GiB

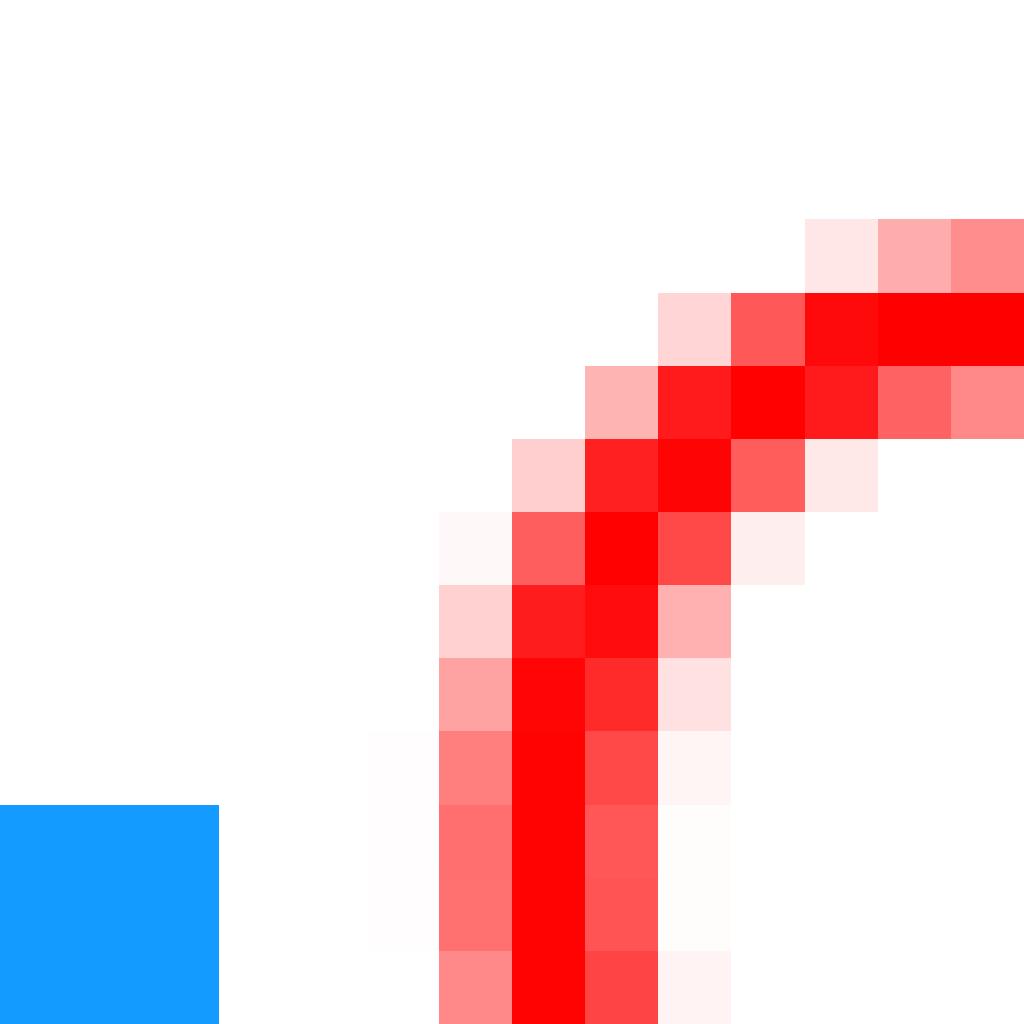
**Free tier:** In your first year includes 75 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

**Cancel** **Launch** **Review**

Figure 6. AWS Example

Azure:

In Azure, TOE instances can be created using Virtual Machines or Azure Dedicated Hosts for bare metal deployment. When deploying VM instances, Azure assigns a unique resource ID, which can be used for TOE identification. Additionally, Azure Resource Manager (ARM) tags and labels can be assigned to each TOE instance for effective identification and categorization. These tags can include metadata such as TOE name, version, environment, or any other relevant information that aids in TOE management and identification.



All services >

## Select SQL deployment option

Microsoft

Feedback

**How do you plan to use the service?**

**SQL databases**  
Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

**Create** **Show details**

**SQL managed instances**  
Best for most migrations to the cloud. Lift-and-shift ready.

Resource type

**Create** **Show details**

**SQL virtual machines**  
Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

Image

High availability

**Create** **Show details**

**SQL virtual machine**  
SQL virtual machines offer full administrative control over the SQL Server instance and underlying OS for migration to Azure.

**Featured capabilities:**

- ✓ SQL Server and OS access
- ✓ Expansive SQL Server and OS version support
- ✓ Automated manageability features for SQL Server

Figure 7. Azure Example

All services >

## Select SQL deployment option

Microsoft

Feedback

**How do you plan to use the service?**

**SQL databases**  
Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

**Create** **Show details**

**SQL managed instances**  
Best for most migrations to the cloud. Lift-and-shift ready.

Resource type

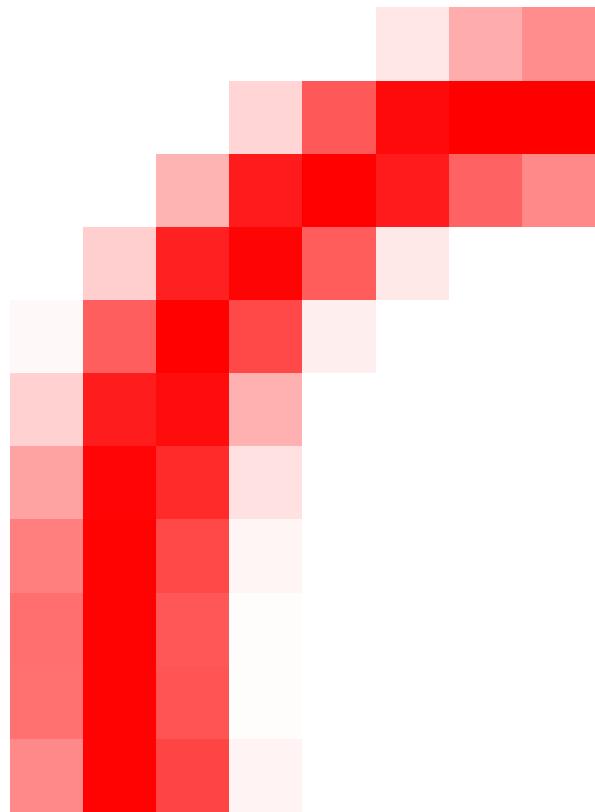
**Create** **Show details**

**SQL virtual machines**  
Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

Image

Free SQL Server License: SQL Server 2022 Developer on Windows Server 2022  
  
  
  
  
Free SQL Server License: SQL Server 2022 Developer on Red Hat Enterprise Linux HA 8.6  
  
  
  
  
Free SQL Server License: SQL Server 2022 Developer on Ubuntu Pro 20.04

Figure 8. Azure Example



All services &gt; Select SQL deployment option &gt;

## Create a virtual machine

X

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Monitoring](#) [Advanced](#) [SQL Server settings](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="SecurityDemoSub_697710"/>
Resource group *	<input type="text" value="(New) Resource group"/> <a href="#">Create new</a>

**Instance details**

Virtual machine name *	<input type="text"/>
Region *	<input type="text" value="(US) East US"/>
Availability options	<input type="text" value="Availability zone"/>
Availability zone *	<input type="text" value="Zones 1"/>
<small> ⓘ You can now select multiple zones. Selecting multiple zones will create one VM per zone. <a href="#">Learn more</a></small>	
Security type	<input type="text" value="Trusted launch virtual machines"/> <a href="#">Configure security features</a>
Image *	<input type="text" value="SQL Server 2022 Enterprise on Windows Server 2022 - x64 Gen2"/> <a href="#">See all images</a>   <a href="#">Configure VM generation</a>

[Review + create](#)[< Previous](#) [Next : Disks >](#)[Give feedback](#)**Figure 9. Azure Example**

All services &gt; Select SQL deployment option &gt;

## Create a virtual machine

X

 ⓘ Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size \*

[See all sizes](#)**Administrator account**

Username \*

Password \*

Confirm password \*

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*

None  
 Allow selected ports

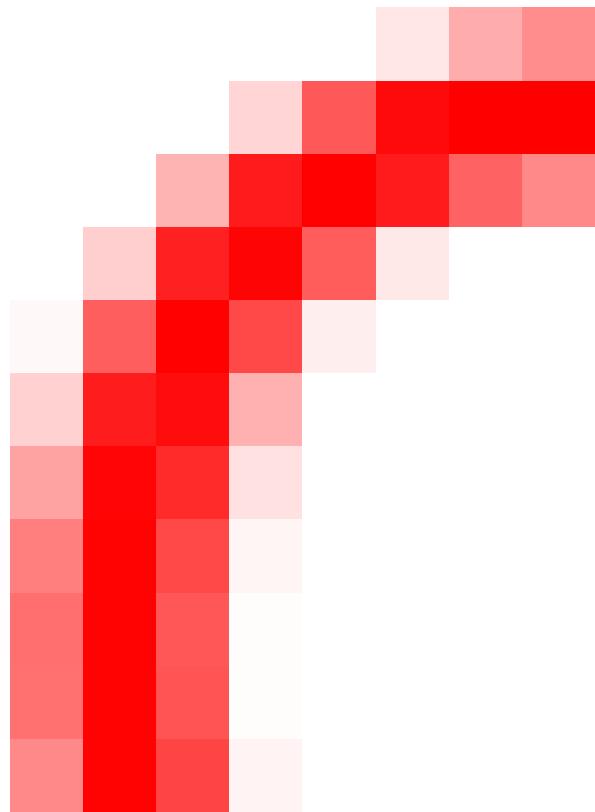
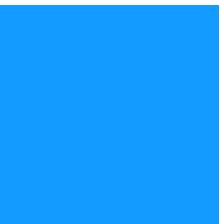
Select inbound ports \*

**Licensing**Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing

Windows Server license? \*

[Review Azure hybrid benefit compliance](#)[Review + create](#)[< Previous](#) [Next : Disks >](#)[Give feedback](#)**Figure 10. Azure Example**



All services &gt; Select SQL deployment option &gt;

**Create a virtual machine**

X

Basics Disks Networking Management Monitoring Advanced SQL Server settings Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)**Network interface**

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ

Public IP ⓘ

NIC network security group ⓘ

- None
- Basic
- Advanced

Public inbound ports \* ⓘ

- None
- Allow selected ports

Select inbound ports \*

Source IP Address ⓘ

- Any
- Specific IP Source Range

**⚠ This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

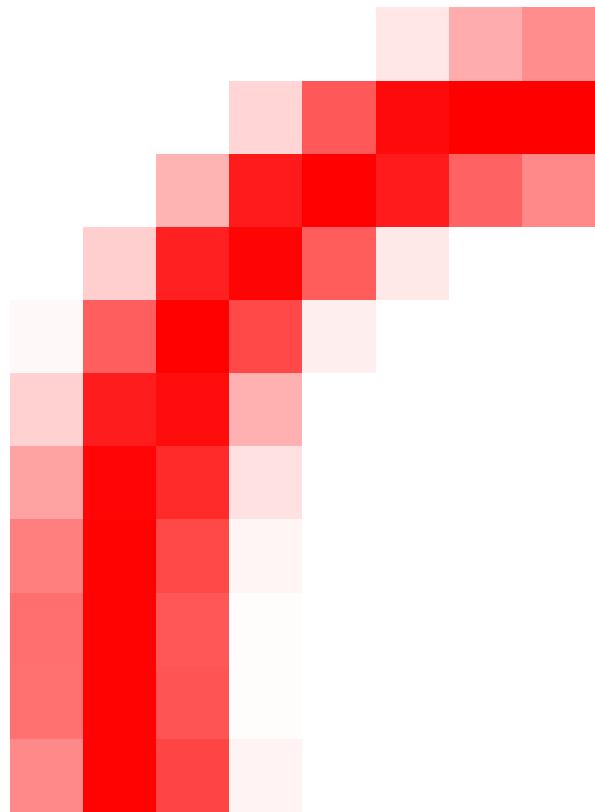
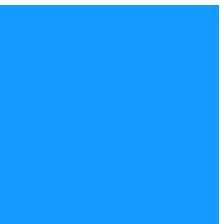
**Review + create**

&lt; Previous

Next : Management &gt;

[Give feedback](#)**Figure 11. Azure Example****Oracle Cloud Infrastructure:**

Oracle Cloud Infrastructure (OCI) enables the deployment of TOE instances using Oracle VMs or bare metal compute shapes. OCI assigns a unique OCID (Oracle Cloud Identifier) to each compute instance, serving as a reliable identifier for TOE instances. Administrators can further enhance TOE identification by leveraging OCI's tagging system, which allows the assignment of user-defined tags. These tags can be utilized to categorize and identify TOE instances based on their specific attributes and requirements.



## Create compute instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name

instance-20230712-0824

Create in compartment



### Placement

[Collapse](#)

The availability domain helps determine which shapes are available.

Availability domain

AD 1

SMQQ:UK-LONDON-1-AD-1

AD 2

SMQQ:UK-LONDON-1-AD-2

AD 3

SMQQ:UK-LONDON-1-AD-3

[Show advanced options](#)

[Edit](#)

### Security

**Shielded instance:** Disabled

**Confidential computing:** Disabled

### Image and shape

[Collapse](#)

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Image



Oracle Linux 8  
Image build: 2023.06.30-0



[Change image](#)

Shape

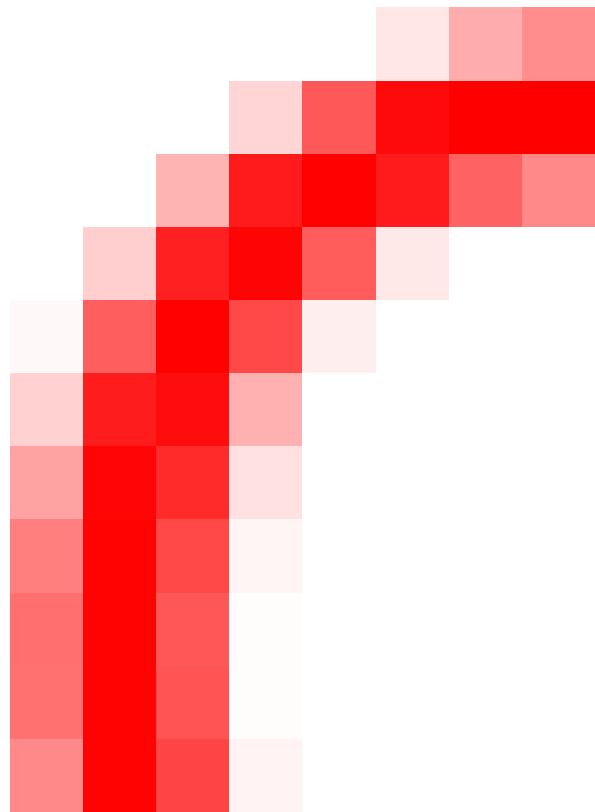
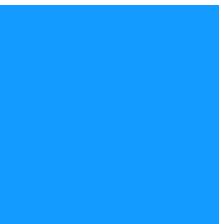
VM.Standard.E1.Flex

[Create](#)

[Save as stack](#)

[Cancel](#)

Figure 12. OCI Example



## Select an image

 Oracle Linux

 Ubuntu

 Red Hat

 CentOS

 Windows

 SUSE

 AlmaLinux

 Rocky Linux

 Marketplace

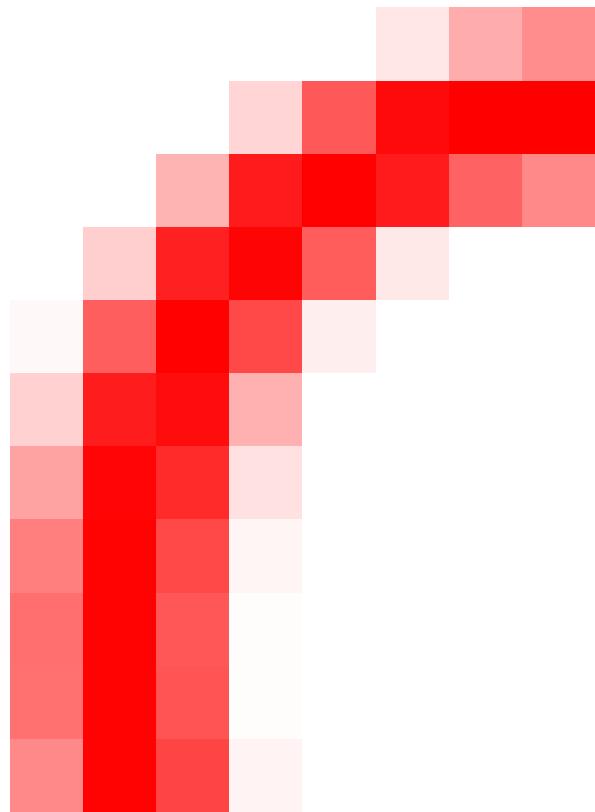
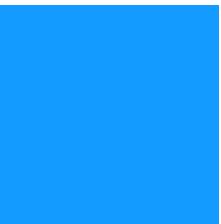
 My images  
Custom images & boot volumes

Compartment

Search...

Image name	Publisher	Price	Security
<input type="checkbox"/> Oracle Autonomous Linux 7.9	Oracle	Free	 
<input type="checkbox"/> Oracle Autonomous Linux 8.7	Oracle	Free	 
<input type="checkbox"/> Oracle Autonomous Linux 8.8	Oracle	Free	 
<input type="checkbox"/> Oracle Linux 6.10	Oracle	Free	
<input type="checkbox"/> Oracle Linux 7.9	Oracle	Free	  
<input checked="" type="checkbox"/> Oracle Linux 8	Oracle	Free	  
<input type="checkbox"/> Oracle Linux 9	Oracle	Free	 
<input type="checkbox"/> Oracle Linux 9 Minimal	Oracle	Free	
<input type="checkbox"/> Oracle Linux Cloud Developer 8	Oracle	Free	
1 selected		Showing 9 items < 1 of 1 >	

Figure 13. OCI Example



## Browse all shapes

A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Instance type

### Virtual machine

A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

### Bare metal machine

A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation. 

**Image:** Oracle Linux 8

Shape name	OCPUs 	Memory (GB)	Security
<input type="checkbox"/> BM.Standard.A1.160	160	1024	
<input type="checkbox"/> BM.Standard.E4.128	128	2048	  

**Network bandwidth (Gbps):** 100

**Maximum VNICs:** 256 

**Local disk:** Block storage only

 [Hide advanced BIOS settings](#)

These settings are for advanced users. They cannot be changed after you create the instance. [How do I choose the right BIOS settings?](#)

Provision only a percentage of cores and disable the rest

Reduces licensing costs for applications that use a core-based licensing model. The instance itself is billed for the full shape. Value is rounded up to the nearest whole number.

25%  50%  75%  100%  
Use 25% of available cores Use 50% of available cores Use 75% of available cores Use 100% of available cores

Customize the non-uniform memory access (NUMA) setting

The NUMA nodes per socket (NPS) setting configures how the memory is interleaved between cores and memory channels in the CPU.

NPS0  NPS1  NPS2  NPS4

Enable simultaneous multithreading (SMT)

Allows multiple independent hardware execution threads per core (OCPUs). When disabled, only one thread can run on each core.

Enable access control service

Allows the platform to enforce PCIe device isolation, required for VFIO device pass-through.

Enable virtualization instructions

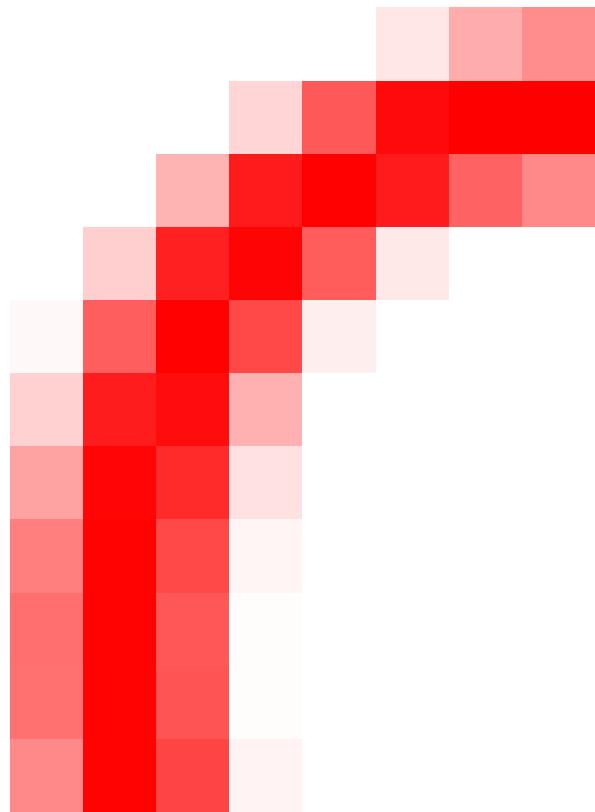
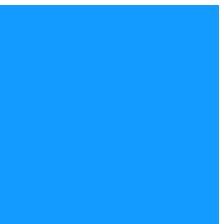
Enables virtualization instructions, such as Secure Virtual Machine for AMD shapes or VT-x for Intel shapes.

Enable the input-output memory management unit (IOMMU)

Controls whether IO memory access goes through the IOMMU.

Figure 14. OCI Example

By utilizing unique identifiers, resource tags, naming conventions, and metadata labels provided by the respective cloud platforms, TOE identification can be effectively established in public cloud infrastructure deployments. These identification mechanisms aid in maintaining clear visibility, control, and management of TOE instances, enabling administrators to enforce security controls and monitor the specific security posture of each deployed TOE instance within the public cloud environment.



# Cloud Equivalence Considerations

Common Criteria is about products not systems or services. This guidance operates on the principle that products must be tested individually on each desired cloud service offering.

When writing Security Targets, the Cloud Service Offering (including the cloud region or datacenter) must be detailed in the TOE evaluated configuration details. CSOs cannot inherently be assumed to be equivalent. For instance, CSPs may have separate environments between government or commercial customers. However, if existing cloud authorizations exist for multiple regions or datacenters this may inform equivalency claims. Especially if the Trusted Platform meets the assumptions and objectives of the PP and is consistent across multiple cloud regions. Each CC scheme has the option to define a policy for acceptance criteria.

## CPU Equivalency

In the process of evaluating IT products within a cloud context, precision and consistency in labeling Operational Environments (OEs) are of paramount importance. This section outlines the essential guidelines for labeling OEs according to the specific characteristics of the technology stack involved. This guidance aligns with the Cryptographic Module Validation Program (CMVP).

Applicable guidance shall be followed when labeling Operational Environments. Such as:

For a Type 1 (or native) hypervisor, where the hypervisor runs directly on the hardware, the OE listing shall include the guest OS, hypervisor, and processor using the following format: “Guest OS on hypervisor on Processor.” An example is “Microsoft Windows 11 on VMWare ESXi 7.0 on Intel Xeon W (Rocket Lake).”

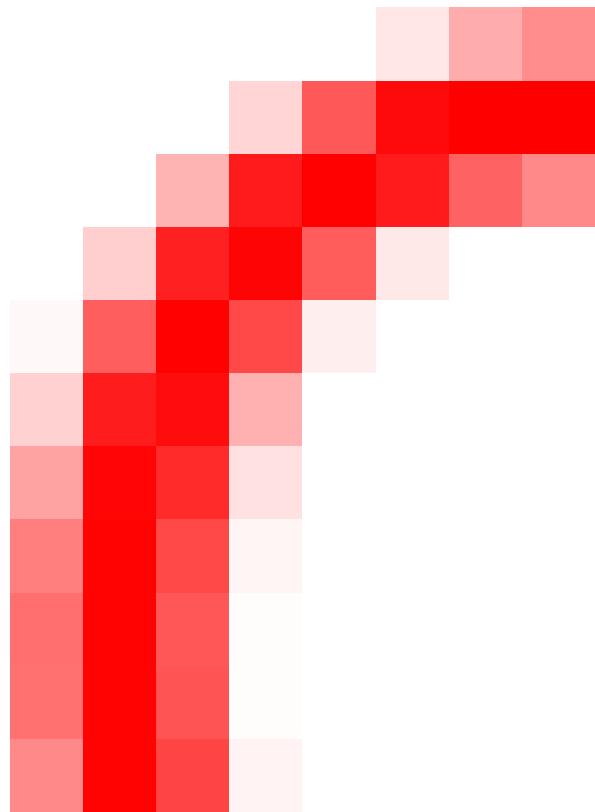
For a Type 2 (or hosted) hypervisor, where the hypervisor runs on a host operating system (OS), the OE listing shall include the guest OS, hypervisor, host OS, and processor using the following format: “Guest OS on hypervisor on Host OS on Processor.” An example is “Microsoft Windows 11 on Parallels Desktop 17 on macOS Monterey on Intel Core i7 (Kaby Lake).”

Algorithm tests may also be performed using containers. The OE listing shall include the container, runtime, host OS, and processor using the following format: “container on runtime on host OS on processor.” An example is “Ubuntu 20.04 Docker Image on Docker Engine 20 on Ubuntu 20.04 on Intel Xeon W (Rocket Lake).”

TOE’s that are being evaluated in a cloud context are expected to be able to conclusively demonstrate knowledge of the underlying TOE Platform for these specifics. If SFR enforcing functionality is agnostic to the TOE platform, such equivalency claims may be made.

E.g. CPU model / OS / Hypervisor / Guest OS / Container shall be defined where appropriate.

At this time, if a TOE is reliant on the OE for cryptographic operations, there is no need to leverage the related collateral that explicitly states operation for a given Cloud Provider. This equivalence rationale should also be considered when a TOE vendor is reliant upon a CSP for algorithm certification and many TOE platforms are claimed.



# Protection Profile Considerations

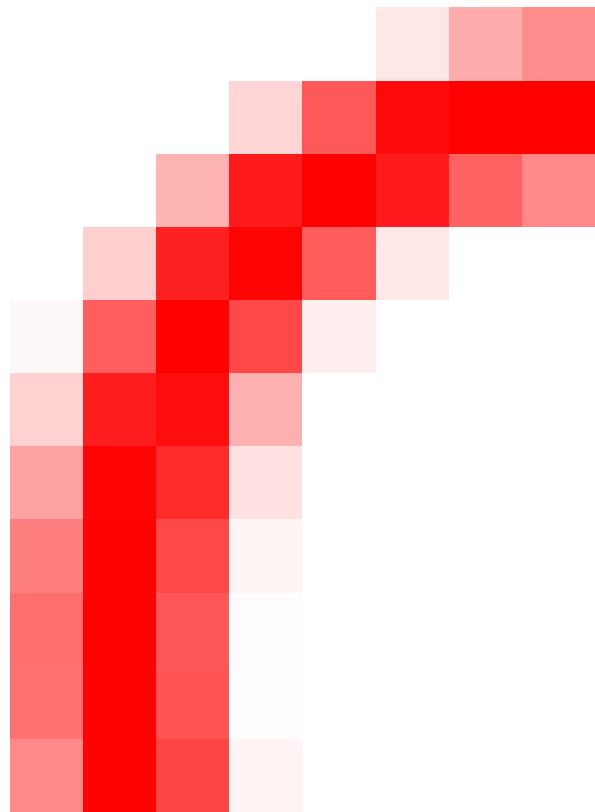
The following section provides both a high level overview as well as a detailed example for adapting CCiTC methodology to existing Protection Profiles. This approach is predicated on mapping the assumptions, security objectives, and security requirements of the PP to the cloud environment.

## Process to optimize a PP for TOEs in a cloud environment.

The list below encompasses a structured process for the essential task of updating Protection Profiles to align with the unique requirements of cloud-based evaluations.

### Process Overview

- Review this guidance document and associated instructions
- Map Assumptions, Security Objections for the Operational Environment, and Organizational Security Policies to applicable authorization scheme(s) as a reference implementation (FedRamp, C5, etc)
  - Summarize this mapping in generic language for wider Cloud Authorization adoption i.e. consideration in other authorization schemes
    - Determine the extent to which SFRs and SARs in the PP can rely on the OE to be satisfied so that the extent to which the TSF may need to rely on cloud services can be determined.
  - Identify SFR challenges in a cloud operational environment
    - For example certain requirements collecting test evidence may be complicated by the cloud operational environment and may not be directly accessible due to cloud isolation.
      - Many TOEs that will operate in a cloud environment will utilize object storage as provided by the CSP. These objects will often be encrypted either by the TOE itself or by the CSP. For instances in which the CSP is providing encryption of the storage object, it is expected that the TOE vendor or evaluator will not be able to perform assurance activity tests with regards to Key Destruction. PP authors will be expected to make modifications to related SFRs to allow for CSP Key Destruction or Zeroization as additional selections.
      - Such modifications may be made by iterating the underlying SFR in a base PP into a "Cloud" PP module which provides the cloud-specific selections and assurance activities.
    - Identify SAR challenges with either new/updated SAR's and/or determine if applicable
      - For example AVA may have different considerations for a cloud operating environment depending on the TOE or PP. See [Vulnerability Assessment Methodology](#) for more information.
  - Edit cPP/PP and add new optional or selection based SFRs/SARs for cloud evaluations



- Update cPPs supporting documents with new cloud requirements and applicable assurance activities.

## Conformance Claims

It is not expected that changes would be required to the Conformance Claims chapter.

PP editors may consider including a reference to this guidance document within the updated PP.

## Security Problem Definition

This chapter describes security problems in terms of threats, assumptions and organizational security policies.

Appendix A details the Threats, Assumptions, Security Objectives for the TOE, and Security Objectives for the operational environment for a number of PP's of interest.

Generally within the PP's proposed, the Network Device and Application Software PPs are used the most.

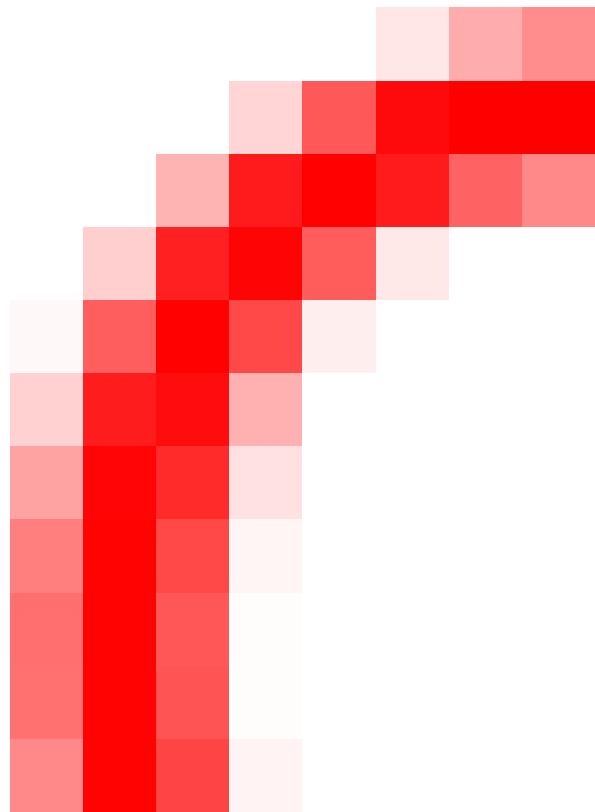
In Appendix B specific aspects of the Assumptions and Security Objectives for the Operational Environment were considered to determine whether assumptions made for each PP of interest are consistent and could be satisfied by a cloud environment. The analysis found that the assumptions and Security Objectives of the Operating Environment for PP's of interest are consistent: There are generally only three categories: Platform Integrity, Proper (Non-Malicious User) and Proper (Trusted) Admin. The virtualization PP considers also Physical Security but this not considered by the other PPs.

It is not necessarily expected that a cloud environment will introduce new threats, assumptions or organizational security policies, although the PP writers may wish to consider whether existing threats, assumptions and organization security policies should be refined to provide more explanation in the case of cloud. For example, threat models may consider the impact of potential ubiquitous access and multi-tenancy to either add to existing threats, assumptions and organizational security policies or refine them.

## Security Objectives

Security Objectives for the TOE map to security functionalities/services of the TOE itself so it is not expected that changes would be required.

As described in Appendix B of this document, the Security Objectives of the Operating Environment provide the general requirements that should be satisfied by the cloud environment. It is proposed that PP's should include an appendix as guidance for an evaluator to assess whether the cloud environment for the TOE satisfies the Security Objectives of the Operating Environment of the PP. In the context of the PP's highlighted, where the assurance level is low (no development security requirements, vulnerability requirements at AVA\_VAN.1: public search), the assumptions and Security Objectives of the Operating Environment should be sufficiently satisfied by any suitable cloud security certification process recognized by a national government supporting Common Criteria, that addresses the environment being used(e.g. lowest level Fedramp, BSI C5 baseline,



ISO27017).

The Security Objectives rationale is not expected to change, unless additional threats, assumptions or security objectives have been added.

## **Security Requirements.**

It is expected that some additional application notes would be appended to a PP regarding Security Requirements.

Security Functional Requirements should be each considered carefully as to whether there may be dependency on the cloud platform.

For example, Cryptographic Support (FCS) may include cryptographic operations using services of the platform, or random number generation derived from platform entropy sources. Others example would be any SFRs around boot integrity and maybe key destruction.

Depending on the type of technology and the associated test scenarios some modification to SFRs will be necessary.

A product that operates identically outside of a cloud operating environment may not require changes.

A product that is only designed to operate in a cloud-native context may need refinements to requirements to the PP.

## **Security Assurance Requirements.**

Classes ASE and ADV are not expected to require change.

Class AGD will be evaluated similarly but the developer must provide guidance both the AGD\_PRE and AGD\_OPE that work for the cloud platform.

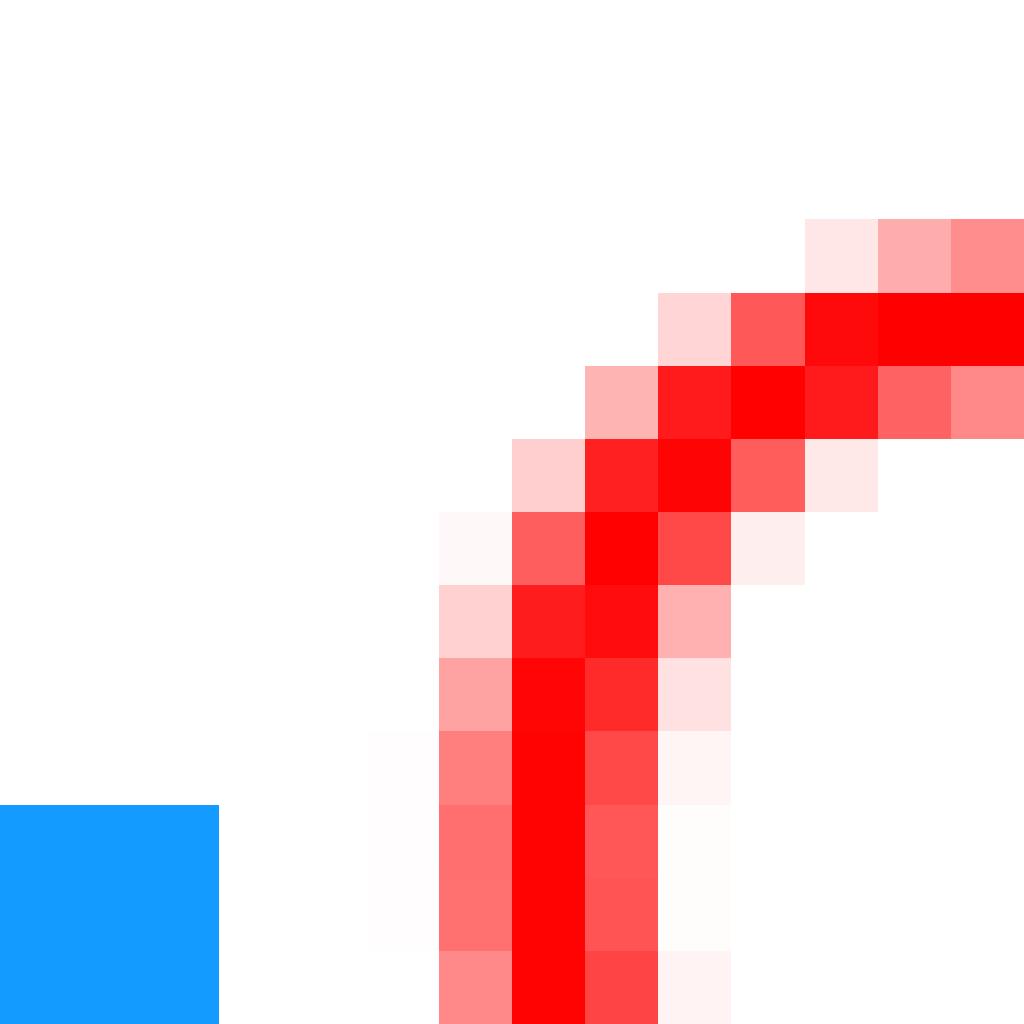
There also may be two scenarios for guidance:

- i. A developer providing guidance for their TOE to be installed and operated in a cloud environment. This may look very similar to the guidance for a typical ‘on-prem’ installation.
- ii. A developer providing guidance for their TOE to be installed and operated on their own cloud environment. In this case the developer may provide installation and operational instructions specific to their cloud platform.

Class ALC changes expected to be minimal and should be resolved with minor adjustments. However, it is likely that care will be required around Flaw remediation and similar ALC aspects (including ALC\_TSU\_EXT.1.1 Timely Security Updates) as how they would work in a cloud platform.

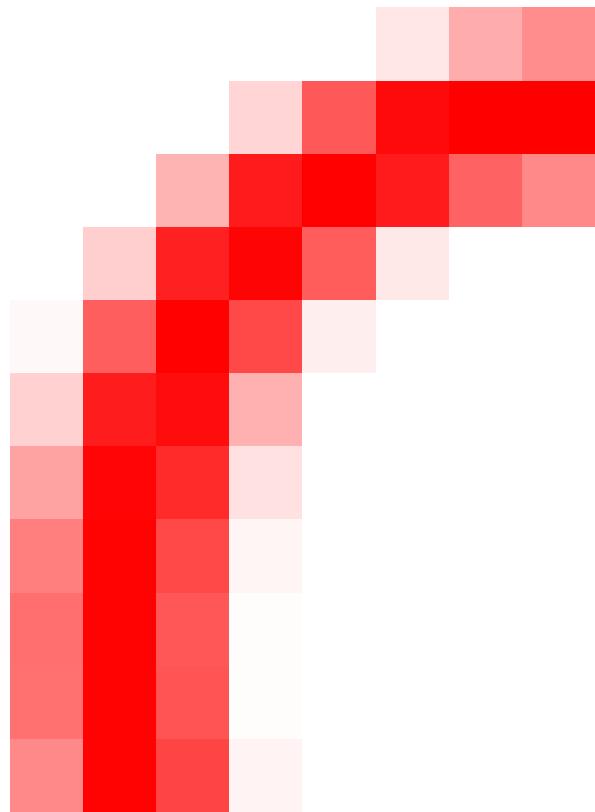
Class ATE will require some additional application notes required around ‘provide the OS for testing’ for a cloud environment.

Class AVA would not be expected to require significant additional application notes.



## Other considerations

A text search of the term ‘platform’ is likely to highlight areas of a PP that will require modification in order to support evaluations in a Cloud environment (if not already resolved with the activities in sections 3.1-3.6



# 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.

Threats are not considered here, since they map to Security Objectives for the TOE rather than Assumptions and Security Objectives for the Operating Environment. A threat, as an adverse action performed by a threat agent on an asset, is not contextual to the operating environment of the TOE. However, an author may choose to review the listed threats detailed in a PP in the context of cloud evaluations.

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

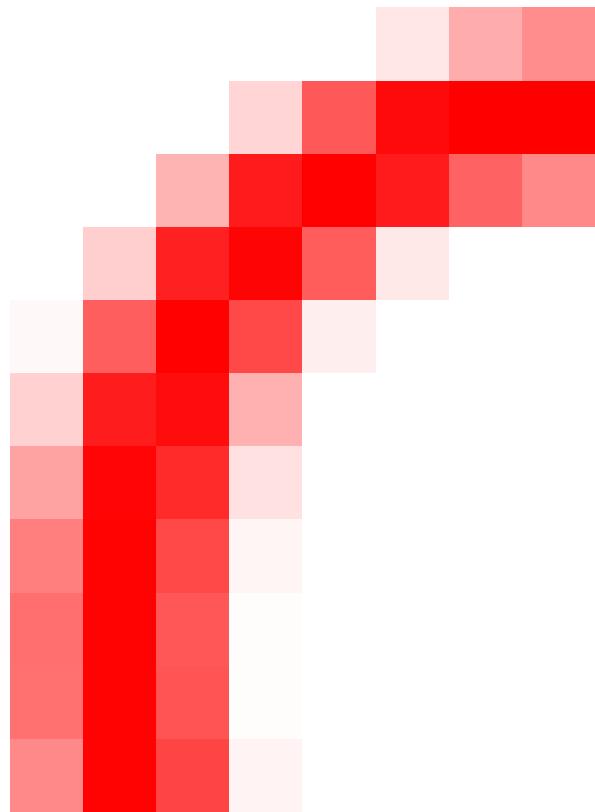
The Security Administrators for the Trusted Platform are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the TOE. The TOE is not expected to be capable of defending against a malicious Trusted Platform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

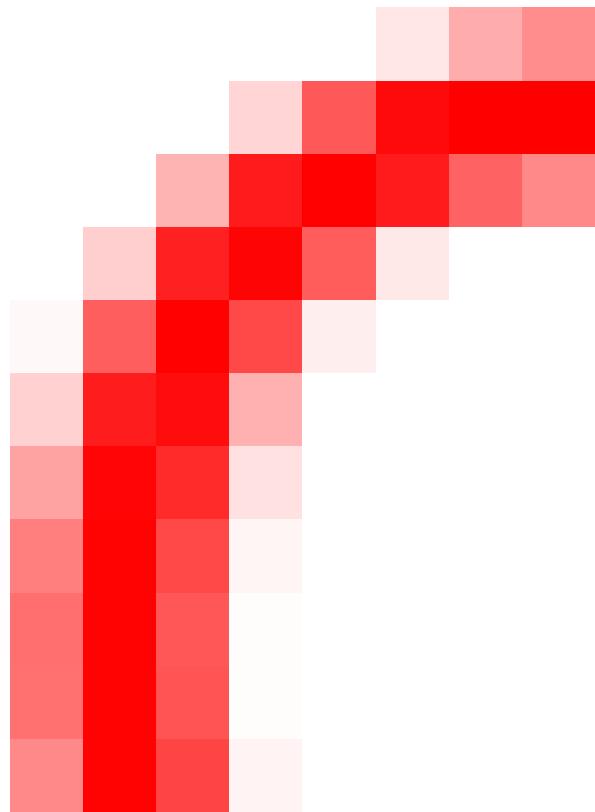
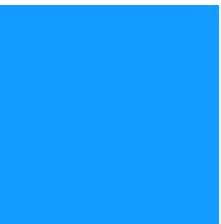
The TOE is assumed to be physically protected in its Trusted Platform environment and not subject to physical attacks that compromise the security or interfere with the TOEs physical interconnections and correct operation. This protection is assumed to be sufficient to protect the TOE and the data it 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.

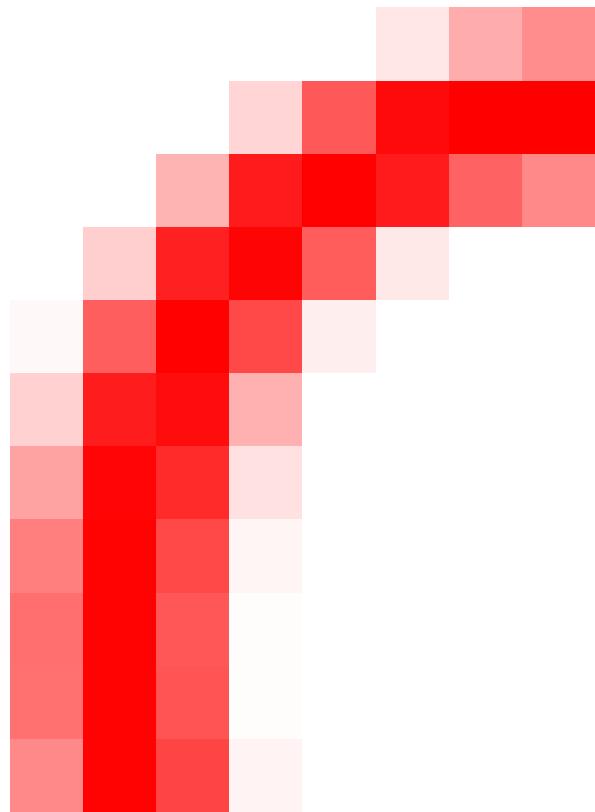
## **OE.TRUSTED\_PLATFORM\_SERVICE**

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
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

## Guidance Documentation

If existing documentation exists for a CSP it should be leveraged. Each CSP that is tested shall provide instructions for deployment of the TOE. Consultants and vendors shall provide necessary supplemental guidance as it supports deploying the TOE as evaluated in the cloud. In addition, functionality that is included but not evaluated shall be clearly identified.

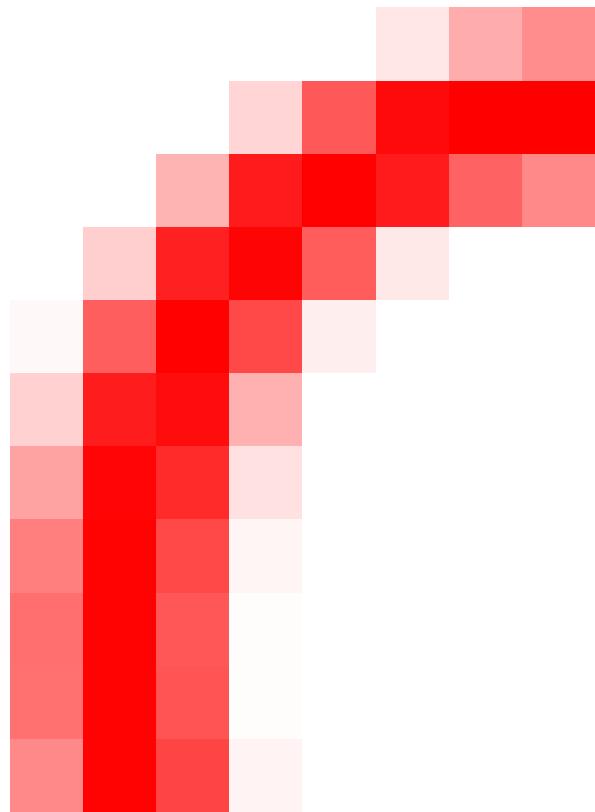
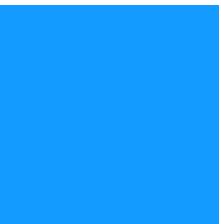
It is important to distinguish here that not all expected elements of a traditional AGD document can be translated for Cloud Environments. It may be necessary to exclude or supplement these guidance requirements depending on the topology of the product and the cloud service provider. In some circumstances, the Cloud Provider is the only entity that may fulfill these guidance requirements to ensure that the TOE is deployed in the tested configuration.

## Guidance For Establishing Test Environments on Cloud Infrastructure

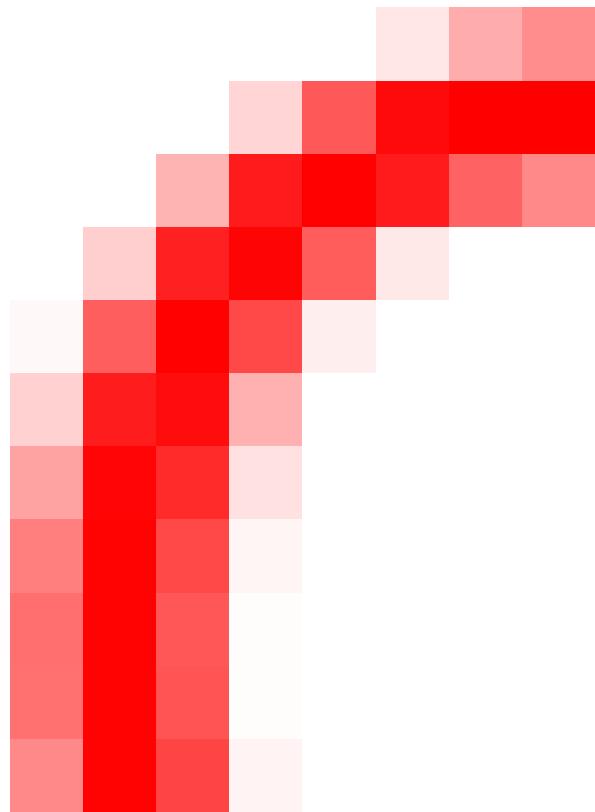
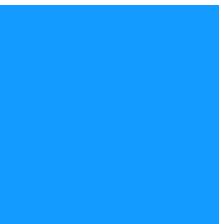
As Common Criteria testing requires unique test environments for each TOE that are isolated to prevent contamination of test results, testing on Public Cloud infrastructure raises some initial concerns.

In general, the necessity to abstract from underlying hardware layers is dictated by the TOE type in Protection Profiles. For instance, the cPP for Application Software relies only on the underlying OS and makes no distinction on whether that OS is virtualized or not. In this scenario bare metal isolation in the cloud testing would be unnecessary and a multi-tenancy environment is acceptable.

An evaluator should be prepared to create and offer cloud testing infrastructure to TOE developers. This environment must establish controls provided by the CSP to establish effective isolation equivalent to on-prem testing to ensure the integrity of results. This may involve isolated VLANs,



ACLs, Compute Resources, etc on multi-tenant infrastructure. This information will need to be captured and presented to Evaluation Authorities as evaluation deliverables.

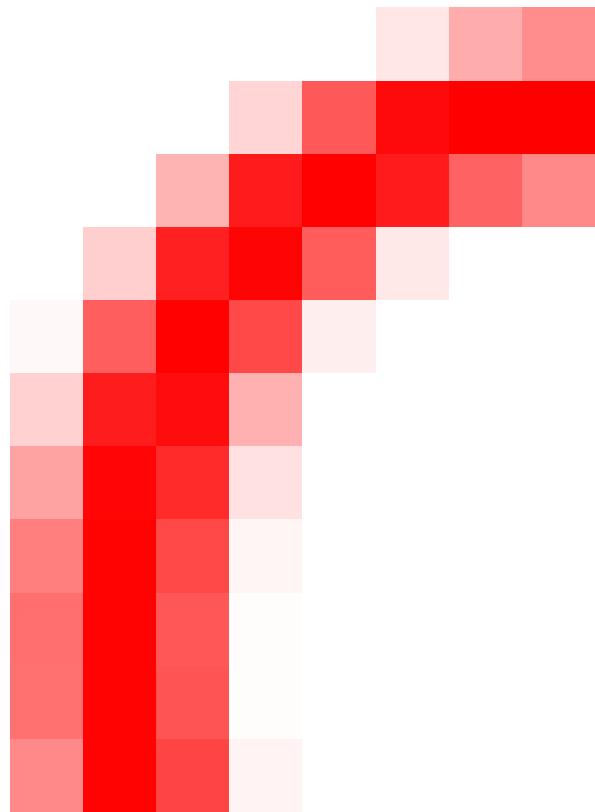
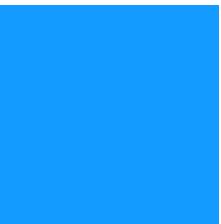


# Vulnerability Assessment Methodology

In general, the AVA methodology shall be sufficient for most TOE types. However, certain edge cases may present themselves.

As we have introduced a trusted platform concept, underlying vulnerabilities in the cloud operating environment can be treated as they are in traditional OE analysis.

However, when applicable vulnerabilities are discovered or suspected for TOEs operating in a cloud environment the means in which evaluators are expected to shift negative test coverage must utilize cloud attack vectors. I.e. service portal, management plane, etc.



# Contributors Roles in Product Evaluations

## Roles Clarification

### **Administrator**

Entity that has a level of trust with respect to all policies implemented by the TOE security functionality [CC:2022 Part 1]

### **Customer**

A customer of the Cloud Service Provider. Also may be the administrator for the TOE

### **Developer**

Organization responsible for the development of the TOE [CC:2022 Part 1]

### **Cloud Service Provider (CSP)**

A cloud service provider, or CSP, is an entity that offers some component of cloud computing; typically infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS) to other businesses or individuals.

### **Evaluation Authority (EA)**

Body operating an evaluation scheme [CC:2022 Part 1]

### **Evaluator**

Individual assigned to perform evaluations in accordance with a given evaluation standard and associated evaluation methodology [CC:2022 Part 1]

### **Evaluator Guidance**

Placeholder for Issue #74

# Glossary

The following definitions are used throughout the document. It is important that each term be clearly understood in order that guidance documentation for the evaluation process be put in context.

## Bare Metal

A bare-metal server is a physical computer server that is used by one customer, or tenant, only. Each server offered for rental is a distinct physical piece of hardware that is a functional server on its own.

## Cloud

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

## Cloud Authorization Scheme

A regulatory body or entity that authorizes cloud service offerings for use by their respective governmental agencies or regulated industries.

## Cloud Service

A Cloud Service is any system that provides on-demand availability of computer system resources, e.g; data storage and computing power, without direct active management by the user.

## Cloud Service Offering (CSP)

An offering provided to a customer by a Cloud Service Provider

## Cloud Service Provider (CSP)

A cloud service provider, or CSP, is a company that offers some component of cloud computing; typically infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS) to other businesses or individuals. == Hosting Environment

The Hosting Environment consists of everything that is outside the TOE boundary and is equivalent to the CC term "Operational Environment."

## Hybrid Cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private,

# Glossary

The following definitions are used throughout the document. It is important that each term be clearly understood in order that guidance documentation for the evaluation process be put in context.

## Bare Metal

A bare-metal server is a physical computer server that is used by one customer, or tenant, only. Each server offered for rental is a distinct physical piece of hardware that is a functional server on its own.

## Cloud

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

## Cloud Authorization Scheme

A regulatory body or entity that authorizes cloud service offerings for use by their respective governmental agencies or regulated industries.

## Cloud Service

A Cloud Service is any system that provides on-demand availability of computer system resources, e.g; data storage and computing power, without direct active management by the user.

## Cloud Service Offering (CSP)

An offering provided to a customer by a Cloud Service Provider

## Cloud Service Provider (CSP)

A cloud service provider, or CSP, is a company that offers some component of cloud computing; typically infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS) to other businesses or individuals. == Hosting Environment

The Hosting Environment consists of everything that is outside the TOE boundary and is equivalent to the CC term "Operational Environment."

## Hybrid Cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private,

community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

## **Multi-Cloud**

A cloud deployment model in which a cloud service customer uses public cloud services provided by two or more cloud service providers

## **Multi-Tenant**

Multi-Tenant uses a shared infrastructure to provide services for multiple cloud customers. Multi-Tenancy means that multiple customers of a cloud vendor are using the same computing resources. Despite the fact that they share resources, cloud customers are logically separated from each other, and their data is isolated.

## **On-Premises (On-Prem)**

On-premises refers to IT infrastructure hardware and software applications that are administered on-site at the customer by the customer. The customer has direct control of on-premises IT assets including security, upkeep, and the physical location. Traditionally, Common Criteria has assumed on-premises environments.

There are existing cloud deployment models in which a CSP will deploy infrastructure locally within a customer's physical control as an extension of a Cloud Service. As the CSP maintains administrative control of the infrastructure this shall not be considered an "on-premises" model.

## **Private Cloud**

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple customers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

## **Product**

Part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.

## **Service**

A set of related IT components provided in support of one or more business processes.

## **Trusted Platform**

A Trusted Platform is the underlying hosting environment for the TOE that is sufficient to meet the assumptions and environmental security objectives of the PPs and modules the TOE claims.

community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

## **Multi-Cloud**

A cloud deployment model in which a cloud service customer uses public cloud services provided by two or more cloud service providers

## **Multi-Tenant**

Multi-Tenant uses a shared infrastructure to provide services for multiple cloud customers. Multi-Tenancy means that multiple customers of a cloud vendor are using the same computing resources. Despite the fact that they share resources, cloud customers are logically separated from each other, and their data is isolated.

## **On-Premises (On-Prem)**

On-premises refers to IT infrastructure hardware and software applications that are administered on-site at the customer by the customer. The customer has direct control of on-premises IT assets including security, upkeep, and the physical location. Traditionally, Common Criteria has assumed on-premises environments.

There are existing cloud deployment models in which a CSP will deploy infrastructure locally within a customer's physical control as an extension of a Cloud Service. As the CSP maintains administrative control of the infrastructure this shall not be considered an "on-premises" model.

## **Private Cloud**

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple customers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

## **Product**

Part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.

## **Service**

A set of related IT components provided in support of one or more business processes.

## **Trusted Platform**

A Trusted Platform is the underlying hosting environment for the TOE that is sufficient to meet the assumptions and environmental security objectives of the PPs and modules the TOE claims.

- The evaluation authority determines sufficiency and may publish a policy.
- Components of a platform may include, e.g., an operating system, virtualization hypervisor, network components or switches, and the hardware needed to run the software.

## TOE Platform

A TOE Platform is the underlying combination of software, firmware, or hardware required for TOE operation that is sufficient to meet the assumptions and environmental security objectives of the PPs and modules the TOE claims.

Standalone physical devices will not utilize a TOE Platform in their respective protection profiles.

- The evaluation authority determines sufficiency and may publish a policy.
- Components of a platform may include, e.g., an operating system, virtualization hypervisor, network components or switches, and the hardware needed to run the software.

## TOE Platform

A TOE Platform is the underlying combination of software, firmware, or hardware required for TOE operation that is sufficient to meet the assumptions and environmental security objectives of the PPs and modules the TOE claims.

Standalone physical devices will not utilize a TOE Platform in their respective protection profiles.

# Cloud Topology

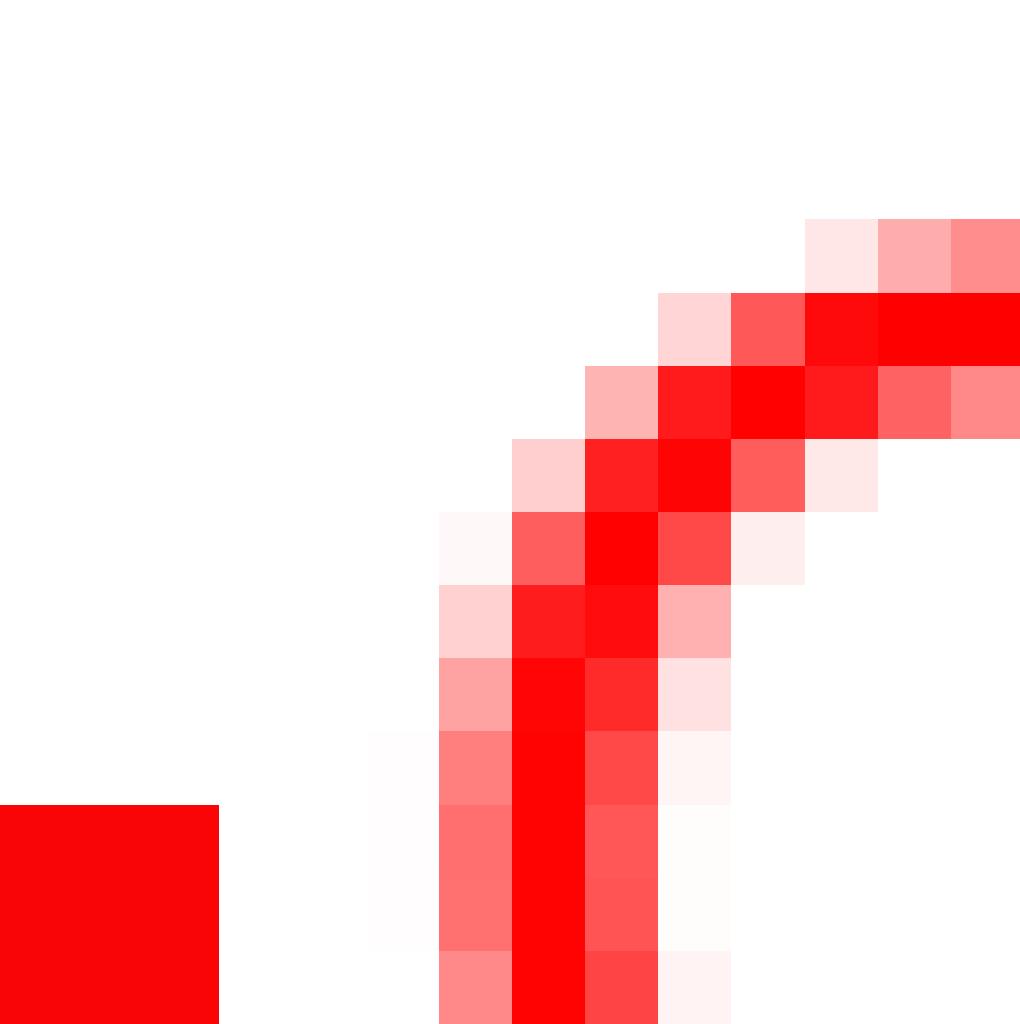
## Cloud Use Cases

### Software as a Service (SaaS)

The capability provided to the customer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. [NIST SP800-145](#)

The following PPs are examples which might be extended with CCitC methodology to cover the above use case: cPP\_App\_SW, cPP\_DBMS, PP\_MDM

For example, if the cPP for Application Software were to be used as a baseline the cloud extensions may be applied to the existing Target of Evaluation (TOE) Boundary and TOE Platform given in the following diagram:



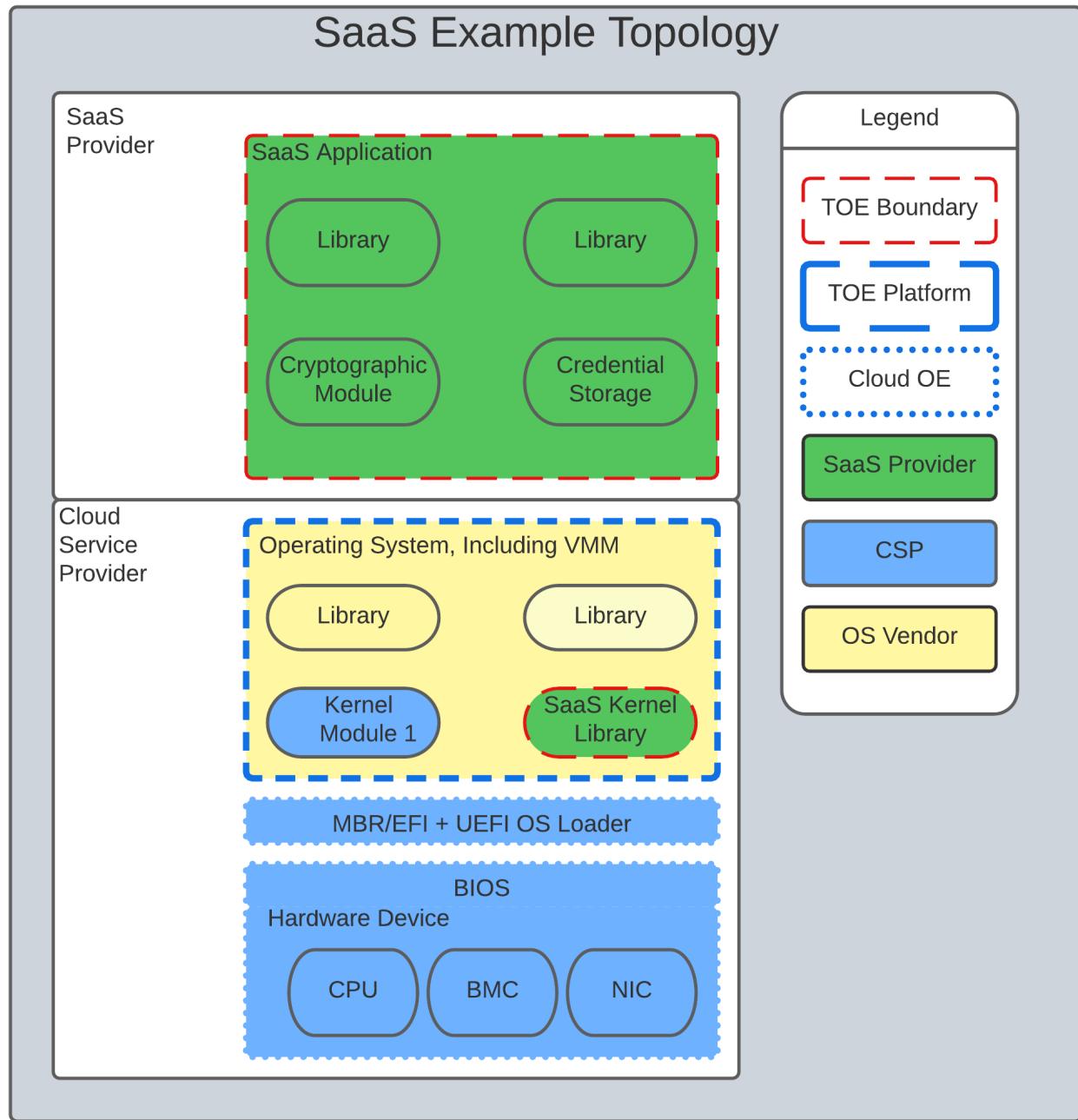


Figure 1. SaaS Example

In this example, the SaaS Application provided by the SaaS provider relies on a TOE platform from an OS Vendor which is hosted by the Cloud Service Provider on the CSP's hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration in a Cloud Operating Environment.

## Platform as a Service (PaaS)

Platform as a Service (PaaS). The capability provided to the customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. ~~NIST SP800-145~~

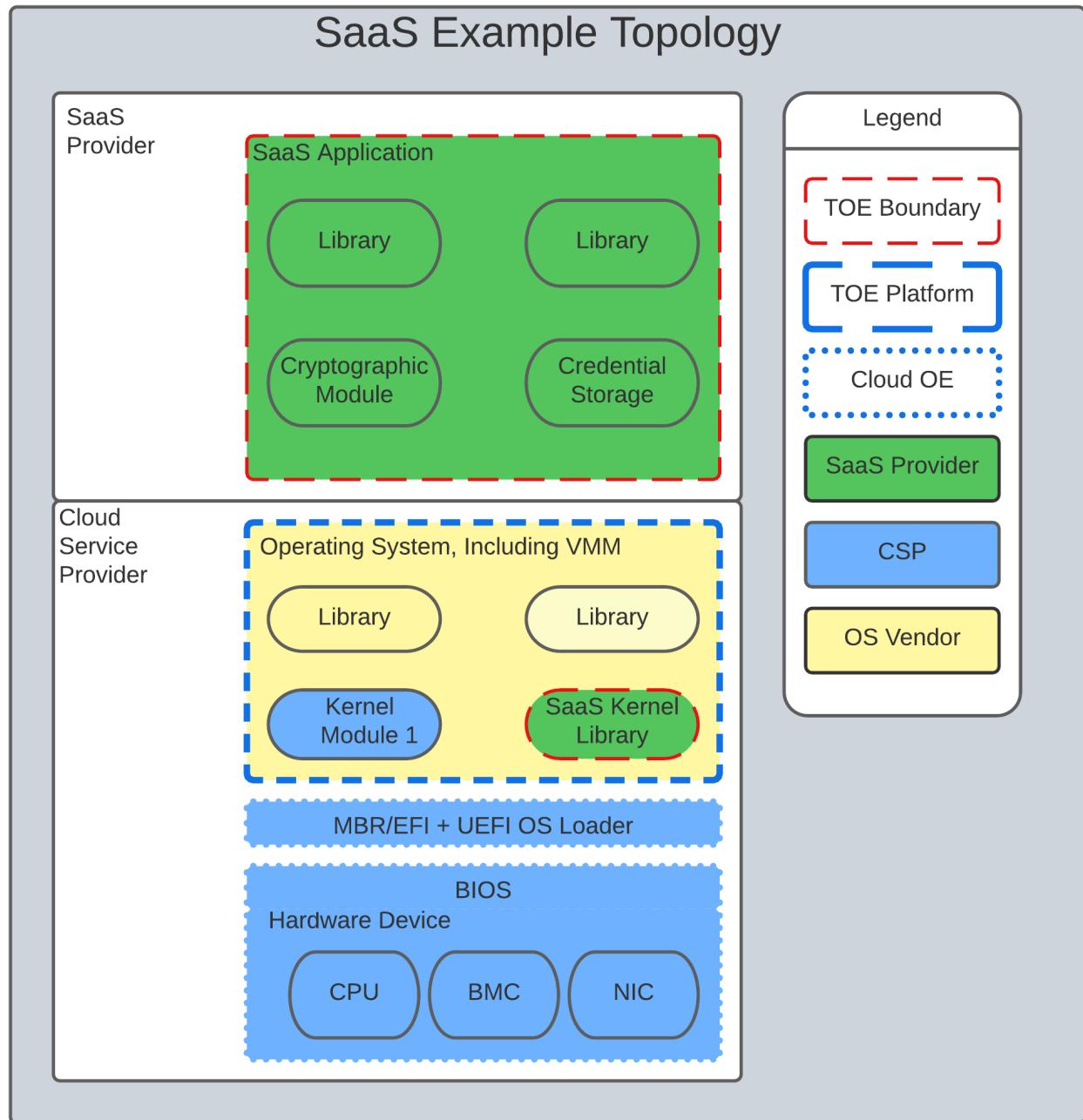


Figure 1. SaaS Example

In this example, the SaaS Application provided by the SaaS provider relies on a TOE platform from an OS Vendor which is hosted by the Cloud Service Provider on the CSP's hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration in a Cloud Operating Environment.

## Platform as a Service (PaaS)

Platform as a Service (PaaS). The capability provided to the customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. [NIST SP800-145](#)

The following PPs are examples which might be extended with CCiTc methodology to cover the above use case: PP\_OS, cPP\_ND

For example, if the Protection Profile for General Purpose Operating System were to be used as a baseline the cloud extensions may be applied to the existing TOE Boundary and Cloud Operating Environment given in the following diagram:

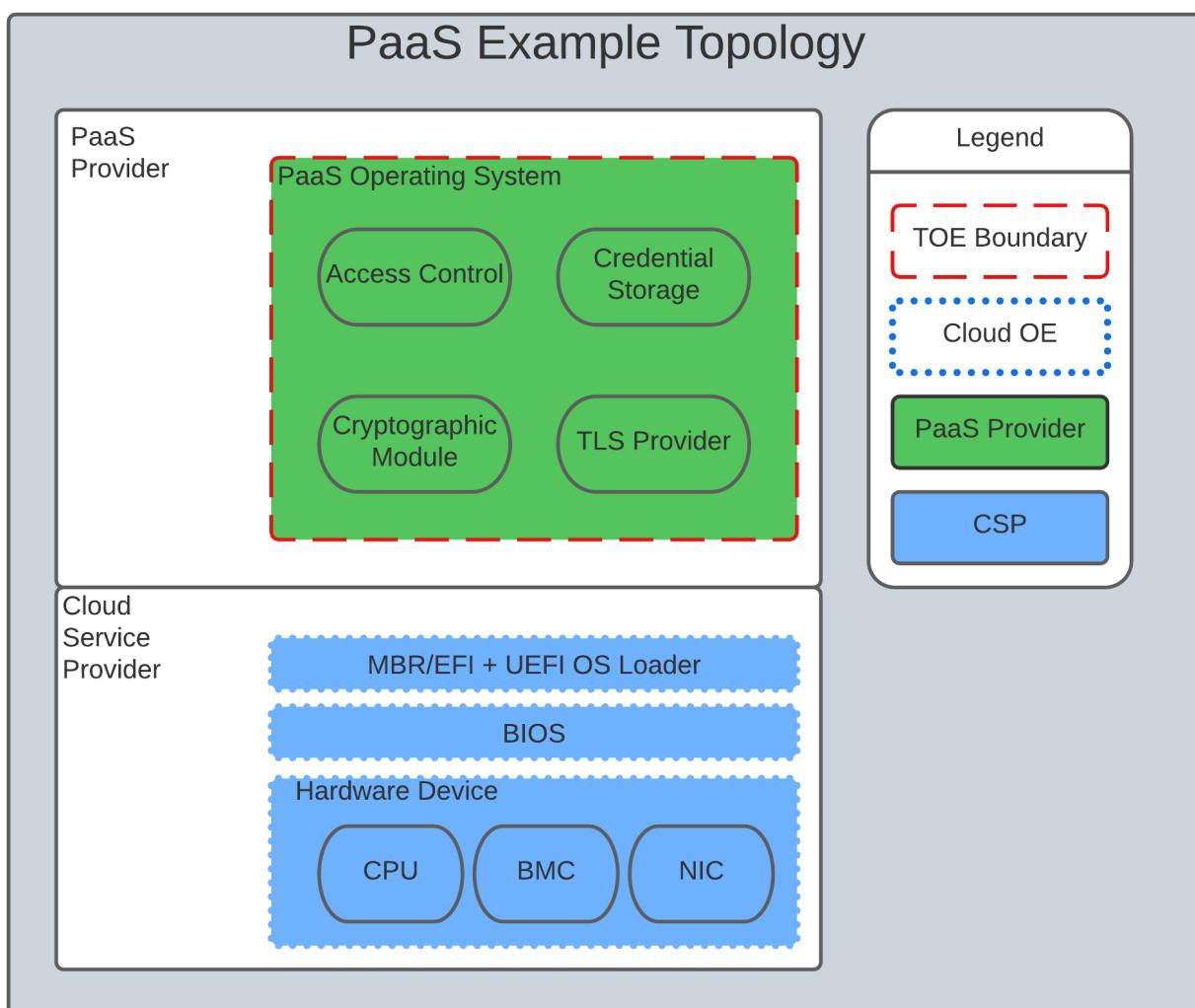


Figure 2. Paas Example

In this example, the PaaS OS provided by the PaaS provider relies on a Cloud Operating Environment which is hosted by the Cloud Service Provider on the CSPs hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration to include a Cloud Operating Environment.

## Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS). The capability provided to the customer is to provision processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select

The following PPs are examples which might be extended with CCiTc methodology to cover the above use case: PP\_OS, cPP\_ND

For example, if the Protection Profile for General Purpose Operating System were to be used as a baseline the cloud extensions may be applied to the existing TOE Boundary and Cloud Operating Environment given in the following diagram:

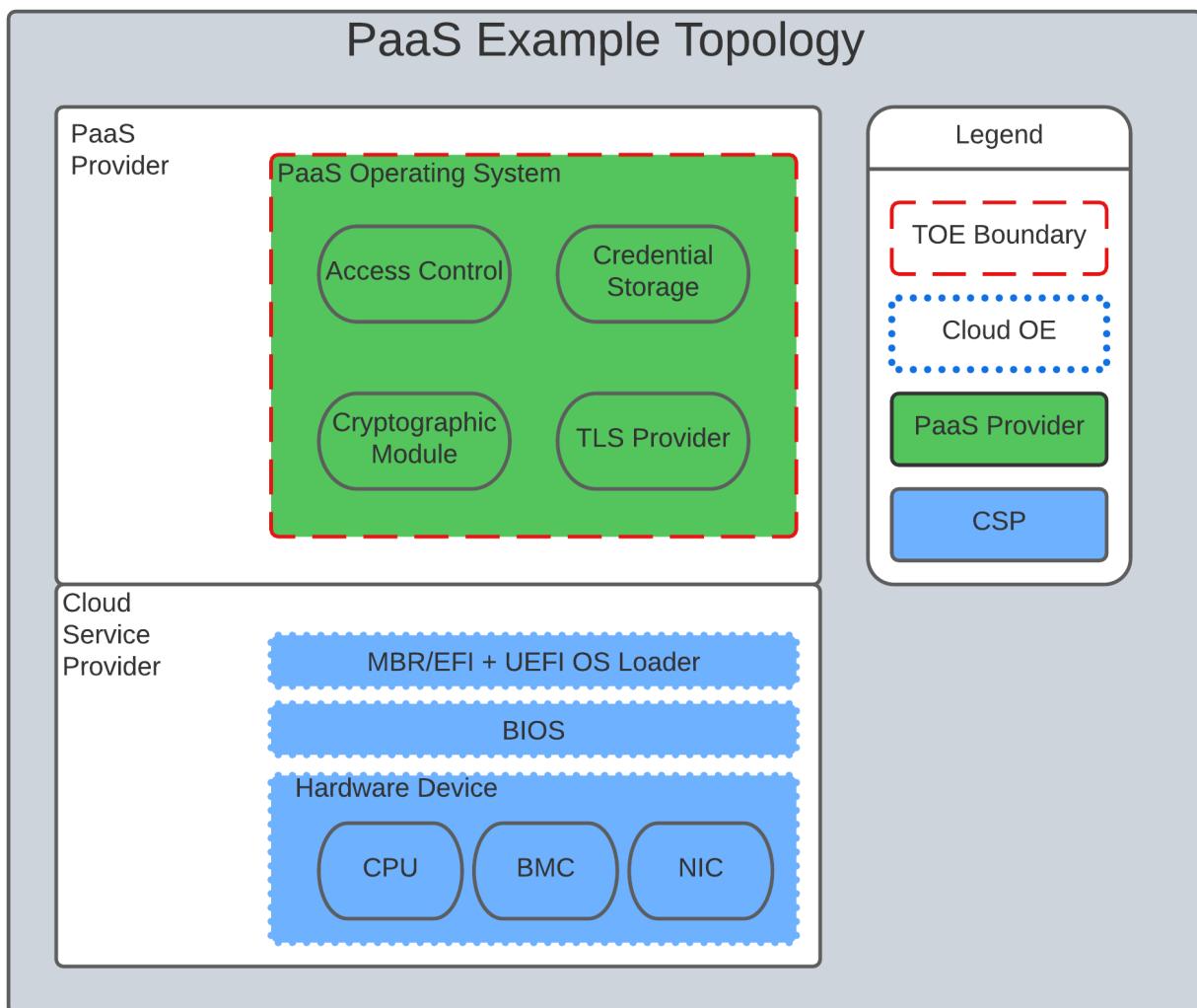


Figure 2. Paas Example

In this example, the PaaS OS provided by the PaaS provider relies on a Cloud Operating Environment which is hosted by the Cloud Service Provider on the CSPs hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration to include a Cloud Operating Environment.

## Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS). The capability provided to the customer is to provision processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select

networking components (e.g., host firewalls) [NIST SP800-145](#)

The following PPs are examples which might be extended with CCitC methodology to cover the above use case: PP\_BASE\_VIRTUALIZATION

For example, if the Protection Profile for Virtualization were to be used as a baseline the cloud extensions may be applied to the existing TOE Boundary and Cloud Operating Environment given in the following diagram:

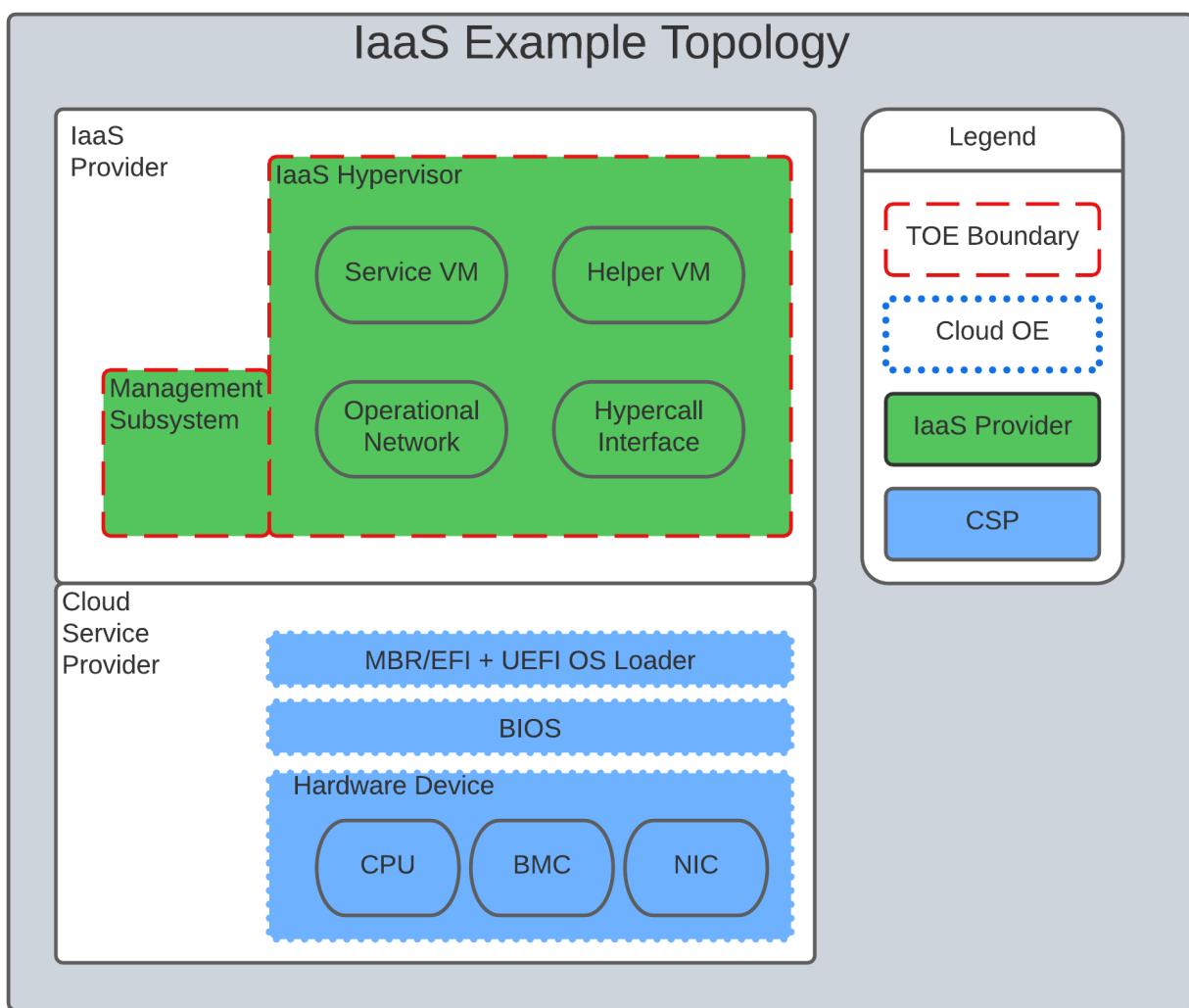


Figure 3. IaaS Example

In this example, the IaaS hypervisor provided by the IaaS provider relies on a Cloud Operating Environment which is hosted by the Cloud Service Provider on the CSPs hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration to include a Cloud Operating Environment.

networking components (e.g., host firewalls) [NIST SP800-145](#)

The following PPs are examples which might be extended with CCiT C methodology to cover the above use case: PP\_BASE\_VIRTUALIZATION

For example, if the Protection Profile for Virtualization were to be used as a baseline the cloud extensions may be applied to the existing TOE Boundary and Cloud Operating Environment given in the following diagram:

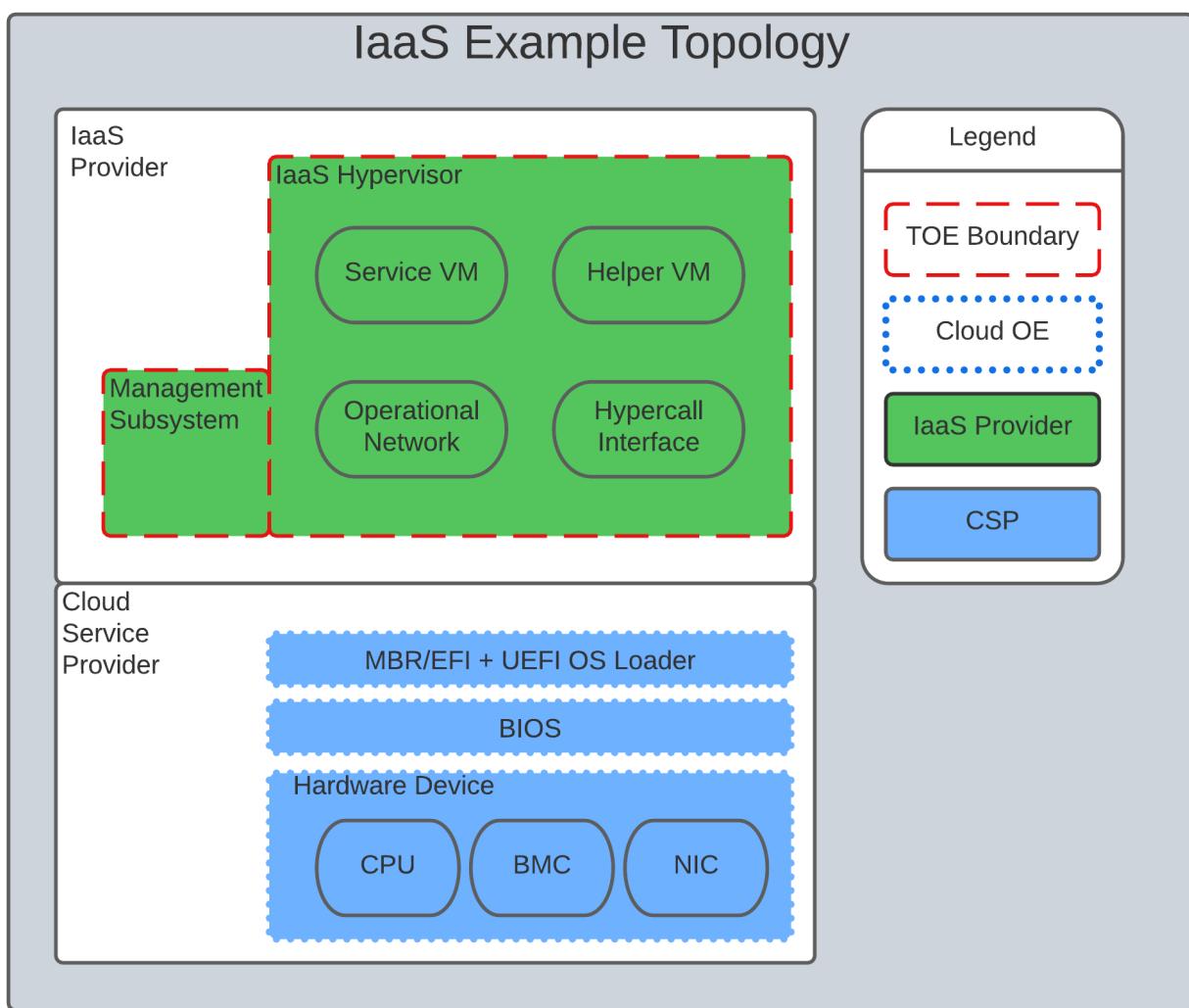


Figure 3. IaaS Example

In this example, the IaaS hypervisor provided by the IaaS provider relies on a Cloud Operating Environment which is hosted by the Cloud Service Provider on the CSPs hardware. In this Cloud evaluation scenario, additional requirements and assurance activities could be prescribed to expand the evaluated configuration to include a Cloud Operating Environment.

# Shared Security Model

In the realm of cloud security, the shared security model is a fundamental concept that defines the division of responsibilities between the Cloud Service Provider (CSP) and their customers within a cloud environment. This model acknowledges that while the CSP is responsible for securing the underlying cloud infrastructure, the customer also bears the responsibility of securing their applications, data, and configurations within that infrastructure based on the service model. The shared security model recognizes that security is a collaborative effort, where both the CSP and the customer play crucial roles. This model is widely embraced in various cloud security frameworks, as it provides a clear model for understanding and allocating security responsibilities in a cloud environment. By delineating these responsibilities, the shared security model helps establish trust, accountability, and transparency between the CSP and the customer, ensuring a holistic approach to cloud security.

This concept is also useful for CCiTC evaluations and mirrors the relationship found with the TOE and TOE Platform. To emphasize the enhanced requirements for Cloud Infrastructure we will refer to the shared responsibility model in terms of the TOE and the Trusted Platform.

In the majority of use cases the TOE administrator (the CSP customer) is responsible for the secure utilization and customization of the cloud services provided by the CSP. This includes managing user access controls, configuring security settings, and implementing appropriate security measures aligned with their specific requirements. These elements may map appropriately to existing SFRs such as management functions defined by the FMT class in CC Part 2 (FMT\_SMF) with or without refinement for CCiTC. The TOE administrator ensures that the TOE (cloud tenant) operates securely within the parameters set by the CSP (TOE Platform).

While the CSP maintains the security and availability of the TOE Platform, the TOE administrator (customer) is assumed to be tasked with safeguarding their applications, data, and configurations within the cloud environment. They actively manage security controls, such as authentication mechanisms, encryption protocols, and network access policies, to protect their assets and mitigate potential risks.

The evaluation and assessment of the shared security model must take into account both the TOE administrator (customer) and the TOE Platform (CSP). The CSP, as the TOE Platform, undergoes evaluation against relevant security standards, certifications, and best practices to demonstrate the effectiveness of the underlying cloud infrastructure's security controls. See the Trusted Platform section for more information on the required security assessments for the TOE Platform.

Simultaneously, the TOE administrator (customer) is responsible for implementing and managing security controls and configurations within their own cloud environment. They utilize the provided security features, adhere to the CSP's policies and guidelines, and maintain appropriate security configurations to ensure the integrity and confidentiality of their data.

There are certain areas where the shared security model can be somewhat blurred. For example, with many CC evaluations, the TOE or TOE Security Functional Interface (TSFI) is expected to exclusively generate TOE audit events. In the context of a virtualized network device deployed on a public cloud, certain CC requirements, such as FAU\_GEN.1 (Audit Generation), would need to be modified to account for the consumption of logs provided by the Cloud Service Provider (CSP).

# Shared Security Model

In the realm of cloud security, the shared security model is a fundamental concept that defines the division of responsibilities between the Cloud Service Provider (CSP) and their customers within a cloud environment. This model acknowledges that while the CSP is responsible for securing the underlying cloud infrastructure, the customer also bears the responsibility of securing their applications, data, and configurations within that infrastructure based on the service model. The shared security model recognizes that security is a collaborative effort, where both the CSP and the customer play crucial roles. This model is widely embraced in various cloud security frameworks, as it provides a clear model for understanding and allocating security responsibilities in a cloud environment. By delineating these responsibilities, the shared security model helps establish trust, accountability, and transparency between the CSP and the customer, ensuring a holistic approach to cloud security.

This concept is also useful for CCiTC evaluations and mirrors the relationship found with the TOE and TOE Platform. To emphasize the enhanced requirements for Cloud Infrastructure we will refer to the shared responsibility model in terms of the TOE and the Trusted Platform.

In the majority of use cases the TOE administrator (the CSP customer) is responsible for the secure utilization and customization of the cloud services provided by the CSP. This includes managing user access controls, configuring security settings, and implementing appropriate security measures aligned with their specific requirements. These elements may map appropriately to existing SFRs such as management functions defined by the FMT class in CC Part 2 (FMT\_SMF) with or without refinement for CCiTC. The TOE administrator ensures that the TOE (cloud tenant) operates securely within the parameters set by the CSP (TOE Platform).

While the CSP maintains the security and availability of the TOE Platform, the TOE administrator (customer) is assumed to be tasked with safeguarding their applications, data, and configurations within the cloud environment. They actively manage security controls, such as authentication mechanisms, encryption protocols, and network access policies, to protect their assets and mitigate potential risks.

The evaluation and assessment of the shared security model must take into account both the TOE administrator (customer) and the TOE Platform (CSP). The CSP, as the TOE Platform, undergoes evaluation against relevant security standards, certifications, and best practices to demonstrate the effectiveness of the underlying cloud infrastructure's security controls. See the Trusted Platform section for more information on the required security assessments for the TOE Platform.

Simultaneously, the TOE administrator (customer) is responsible for implementing and managing security controls and configurations within their own cloud environment. They utilize the provided security features, adhere to the CSP's policies and guidelines, and maintain appropriate security configurations to ensure the integrity and confidentiality of their data.

There are certain areas where the shared security model can be somewhat blurred. For example, with many CC evaluations, the TOE or TOE Security Functional Interface (TSFI) is expected to exclusively generate TOE audit events. In the context of a virtualized network device deployed on a public cloud, certain CC requirements, such as FAU\_GEN.1 (Audit Generation), would need to be modified to account for the consumption of logs provided by the Cloud Service Provider (CSP).

FAU\_GEN.1 requires the TOE (virtualized network device) to generate audit records for security-relevant events. However, in a cloud environment, the CSP typically manages the underlying infrastructure and maintains centralized logging systems. As a result, the TOE may rely on the CSP's log management capabilities and consume the logs provided by the CSP rather than generating its own audit records.

To accommodate this scenario, the collaborative protection profile for the virtualized network device on the public cloud should specify the requirements for log consumption from the CSP's logging infrastructure. This would include defining the format, content, and frequency of logs to be provided by the CSP. Additionally, the protection profile should address the integrity and confidentiality of these logs during transmission and storage.

The modified CC requirements would then focus on the TOE's capability to securely receive, process, and analyze the logs provided by the CSP. The TOE should be able to extract relevant security events from the logs and correlate them with its own internal security policies. Furthermore, it should have the ability to raise alerts or initiate appropriate actions based on the analysis of the consumed logs.

By adapting CC requirements like FAU\_GEN.1 to encompass log consumption from the CSP, the protection profile enables the virtualized network device to leverage the logging capabilities provided by the CSP while maintaining compliance with CC standards. This ensures that security-relevant events are properly logged, analyzed, and acted upon in the cloud environment, contributing to a comprehensive security posture for the virtualized network device.

Additionally, it may be important to add a third element to the shared security model for CCiTC evaluations. This would be the inclusion of the TOE Vendor in addition to the TOE Administrator and CSP. The TOE Vendor may be responsible for providing TOE security updates, maintaining a trusted update channel and infrastructure, or even applying these updates on behalf of the TOE Administrator. This is a common feature with traditional SaaS use cases. In such cases where a TOE vendor is expected to share responsibilities in the security model, PP Authors must make the appropriate refinements, additions, or iterations of related elements in their PPs. This is a scenario that may be more common in TOE types that are meant to incorporate physical hardware into Cloud Infrastructure such as an HSM. However, CCiTC evaluations are not limited to a particular deployment model. It is also expected that there will be evaluations of TOEs that are integral to a CSPs cloud stack from hardware to application layers.

Ultimately, by designating the customer as the TOE administrator, the shared security model reinforces their active involvement in the secure administration of the cloud services. The CSP, as the TOE Platform, provides the underlying infrastructure, while the TOE administrator assumes the responsibility of effectively configuring, managing, and monitoring the TOE to meet their specific security objectives and compliance requirements.

To ensure that customers acting as TOE administrators, who are familiar with Common Criteria but may have limited knowledge of cloud infrastructure and security, can effectively manage the TOE within the shared security model, it is important for the authors of protection profiles to adapt the Administrator Guidance Document (AGD) requirements accordingly. This includes providing clear instructions, accessible language, and practical guidance tailored to TOE administrators. By modifying the AGD requirements in this manner, the authors of protection profiles can ensure that TOE administrators can confidently manage the TOE within the shared security model, bridging the

FAU\_GEN.1 requires the TOE (virtualized network device) to generate audit records for security-relevant events. However, in a cloud environment, the CSP typically manages the underlying infrastructure and maintains centralized logging systems. As a result, the TOE may rely on the CSP's log management capabilities and consume the logs provided by the CSP rather than generating its own audit records.

To accommodate this scenario, the collaborative protection profile for the virtualized network device on the public cloud should specify the requirements for log consumption from the CSP's logging infrastructure. This would include defining the format, content, and frequency of logs to be provided by the CSP. Additionally, the protection profile should address the integrity and confidentiality of these logs during transmission and storage.

The modified CC requirements would then focus on the TOE's capability to securely receive, process, and analyze the logs provided by the CSP. The TOE should be able to extract relevant security events from the logs and correlate them with its own internal security policies. Furthermore, it should have the ability to raise alerts or initiate appropriate actions based on the analysis of the consumed logs.

By adapting CC requirements like FAU\_GEN.1 to encompass log consumption from the CSP, the protection profile enables the virtualized network device to leverage the logging capabilities provided by the CSP while maintaining compliance with CC standards. This ensures that security-relevant events are properly logged, analyzed, and acted upon in the cloud environment, contributing to a comprehensive security posture for the virtualized network device.

Additionally, it may be important to add a third element to the shared security model for CCiTC evaluations. This would be the inclusion of the TOE Vendor in addition to the TOE Administrator and CSP. The TOE Vendor may be responsible for providing TOE security updates, maintaining a trusted update channel and infrastructure, or even applying these updates on behalf of the TOE Administrator. This is a common feature with traditional SaaS use cases. In such cases where a TOE vendor is expected to share responsibilities in the security model, PP Authors must make the appropriate refinements, additions, or iterations of related elements in their PPs. This is a scenario that may be more common in TOE types that are meant to incorporate physical hardware into Cloud Infrastructure such as an HSM. However, CCiTC evaluations are not limited to a particular deployment model. It is also expected that there will be evaluations of TOEs that are integral to a CSPs cloud stack from hardware to application layers.

Ultimately, by designating the customer as the TOE administrator, the shared security model reinforces their active involvement in the secure administration of the cloud services. The CSP, as the TOE Platform, provides the underlying infrastructure, while the TOE administrator assumes the responsibility of effectively configuring, managing, and monitoring the TOE to meet their specific security objectives and compliance requirements.

To ensure that customers acting as TOE administrators, who are familiar with Common Criteria but may have limited knowledge of cloud infrastructure and security, can effectively manage the TOE within the shared security model, it is important for the authors of protection profiles to adapt the Administrator Guidance Document (AGD) requirements accordingly. This includes providing clear instructions, accessible language, and practical guidance tailored to TOE administrators. By modifying the AGD requirements in this manner, the authors of protection profiles can ensure that TOE administrators can confidently manage the TOE within the shared security model, bridging the

gap between Common Criteria expertise and the challenges of managing security in a cloud environment.

Additionally, The TSS, which defines the security functionality and assurance requirements of the TOE, can be modified by the authors of protection profiles to provide clear explanations tailored to evaluators limited knowledge of cloud infrastructure and security. The modified TSS should include detailed information such that it is clear how the TSFI or SFR enforcing features interact in a cloud context with the TOE Platform.

By adapting the TSS and AGD requirements in this manner, the authors of protection profiles can ensure that TOE administrators with limited knowledge of cloud infrastructure and security can confidently manage the TOE within the shared security model. These modifications provide clear and accessible guidance, empowering TOE administrators to make informed decisions, configure the TOE securely, and fulfill their security responsibilities effectively.

gap between Common Criteria expertise and the challenges of managing security in a cloud environment.

Additionally, The TSS, which defines the security functionality and assurance requirements of the TOE, can be modified by the authors of protection profiles to provide clear explanations tailored to evaluators limited knowledge of cloud infrastructure and security. The modified TSS should include detailed information such that it is clear how the TSFI or SFR enforcing features interact in a cloud context with the TOE Platform.

By adapting the TSS and AGD requirements in this manner, the authors of protection profiles can ensure that TOE administrators with limited knowledge of cloud infrastructure and security can confidently manage the TOE within the shared security model. These modifications provide clear and accessible guidance, empowering TOE administrators to make informed decisions, configure the TOE securely, and fulfill their security responsibilities effectively.

# Relationships Between the Trusted Platform / TOE Platform, and TOE

We need to explain that the Trusted Platform exists underneath the TOE Platform and is provided by the CSP.

The TOE Platform may or may not exist on top of the Trusted Platform, but is specifically what is providing functionality to the TOE.

If the TOE Platform does not exist as the TOE is capable of meeting all PP SFRs independently, then a Trusted Platform would still be needed to provide a hosting environment for the TOE.

For example, for a TOE that is a Software Application, the TOE Platform would be the Operating System and the Trusted Platform would be the underlying virtualization solution provided by the CSP.

If the TOE is a General Purpose Operating System (GPOS) then the TOE Platform would be the underlying hypervisor and the Trusted Platform would include the hardware layer and below from the CSP.

If the TOE is a General Purpose Compute Platform (GPCP) then no TOE Platform is applicable and the Trusted Platform would be the power, cooling, and physical security provided by the CSP.

# Relationships Between the Trusted Platform / TOE Platform, and TOE

We need to explain that the Trusted Platform exists underneath the TOE Platform and is provided by the CSP.

The TOE Platform may or may not exist on top of the Trusted Platform, but is specifically what is providing functionality to the TOE.

If the TOE Platform does not exist as the TOE is capable of meeting all PP SFRs independently, then a Trusted Platform would still be needed to provide a hosting environment for the TOE.

For example, for a TOE that is a Software Application, the TOE Platform would be the Operating System and the Trusted Platform would be the underlying virtualization solution provided by the CSP.

If the TOE is a General Purpose Operating System (GPOS) then the TOE Platform would be the underlying hypervisor and the Trusted Platform would include the hardware layer and below from the CSP.

If the TOE is a General Purpose Compute Platform (GPCP) then no TOE Platform is applicable and the Trusted Platform would be the power, cooling, and physical security provided by the CSP.

# Scheme Guidance for Trusted Platforms

Placeholder for issue #106

# Scheme Guidance for Trusted Platforms

Placeholder for issue #106

# TOE Identification

When deploying a Target of Evaluation (TOE) to public cloud infrastructure, proper identification and distinction of the TOE instances are crucial. This ensures accurate tracking, management, and application of security controls specific to each TOE instance within the cloud environment. In this section, we will explain how TOE identification can be established when deploying TOE instances on popular public cloud platforms such as AWS, Azure, and Oracle Cloud Infrastructure.

## AWS (Amazon Web Services):

In AWS, TOE instances can be provisioned as either bare metal instances or virtual machines (VMs) based on the specific requirements. AWS offers different services such as Amazon EC2 (Elastic Compute Cloud) for VM instances and Amazon EC2 Bare Metal instances for bare metal deployment. During the provisioning process, unique identifiers such as instance IDs, resource tags, and naming conventions can be utilized to supplement TOE identification. By assigning descriptive tags and naming conventions, TOE administrators can easily distinguish and manage each TOE instance.

**Name and tags** [Info](#)

Name  
e.g. My Web Server [Add additional tags](#)

**Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS Images

Recents | My AMIs | **Quick Start**

Ubuntu | Windows | Red Hat | SUSE Linux | Debian | [Browse more AMIs](#)

**Amazon Machine Image (AMI)**

**Amazon Linux 2023 AMI**  
ami-0889a44b331db0194 (64-bit (x86)) / ami-08fc6fb8ad2e794bb (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**  
Amazon Linux 2023 AMI 2023.0.20230503.0 x86\_64 HVM kernel-6.1

**Architecture**  
64-bit (x86) [AMI ID](#) ami-0889a44b331db0194 [Verified provider](#)

**Summary**

Number of instances [Info](#)  
1

Software image (AMI)  
Amazon Linux 2023 AMI 2023.0.20230503.0 x86\_64  
HVM kernel-6.1  
ami-0889a44b331db0194

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

**Launch instance** [Review commands](#)

**Instance type** [Info](#)

Instance type  
**t2.micro** [Free tier eligible](#)

Family: t2 1 vCPU 1 GiB Memory Current generation: true  
On-Demand Windows pricing: 0.0162 USD per Hour  
On-Demand SUSE pricing: 0.0116 USD per Hour  
On-Demand RHEL pricing: 0.0716 USD per Hour  
On-Demand Linux pricing: 0.0116 USD per Hour

All generations [Compare instance types](#)

Figure 4. AWS Example

# TOE Identification

When deploying a Target of Evaluation (TOE) to public cloud infrastructure, proper identification and distinction of the TOE instances are crucial. This ensures accurate tracking, management, and application of security controls specific to each TOE instance within the cloud environment. In this section, we will explain how TOE identification can be established when deploying TOE instances on popular public cloud platforms such as AWS, Azure, and Oracle Cloud Infrastructure.

## AWS (Amazon Web Services):

In AWS, TOE instances can be provisioned as either bare metal instances or virtual machines (VMs) based on the specific requirements. AWS offers different services such as Amazon EC2 (Elastic Compute Cloud) for VM instances and Amazon EC2 Bare Metal instances for bare metal deployment. During the provisioning process, unique identifiers such as instance IDs, resource tags, and naming conventions can be utilized to supplement TOE identification. By assigning descriptive tags and naming conventions, TOE administrators can easily distinguish and manage each TOE instance.

**Name and tags** [Info](#)

Name  
e.g. My Web Server [Add additional tags](#)

**Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS Images

Recents | My AMIs | **Quick Start**

Ubuntu | Windows | Red Hat | SUSE Linux | Debian | [Browse more AMIs](#)

Amazon Machine Image (AMI)

**Amazon Linux 2023 AMI**  
ami-0889a44b331db0194 (64-bit (x86)) / ami-08fc6fb8ad2e794bb (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

Description  
Amazon Linux 2023 AMI 2023.0.20230503.0 x86\_64 HVM kernel-6.1

Architecture  
64-bit (x86) [AMI ID](#) ami-0889a44b331db0194 [Verified provider](#)

**Summary**

Number of instances [Info](#)  
1

Software image (AMI)  
Amazon Linux 2023 AMI 2023.0.20230503.0 x86\_64  
HVM kernel-6.1  
ami-0889a44b331db0194

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#) [Launch instance](#) [Review commands](#)

**Instance type** [Info](#)

Instance type  
**t2.micro** Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true  
On-Demand Windows pricing: 0.0162 USD per Hour  
On-Demand SUSE pricing: 0.0116 USD per Hour  
On-Demand RHEL pricing: 0.0716 USD per Hour  
On-Demand Linux pricing: 0.0116 USD per Hour

All generations [Compare instance types](#)

Figure 4. AWS Example

The screenshot shows the AWS CloudWatch Metrics search interface. On the left, there is a search bar with the placeholder "Search metrics" and a dropdown menu labeled "Name and tags". Below the search bar is a table listing various AWS Lambda functions with their ARNs, names, and metric names. The table includes columns for "Metric name", "Function name", "ARN", and "Unit". A legend indicates that a blue checkmark means "Free tier eligible". On the right side of the interface, there are several sections: "Number of instances" (1), "Software Image (AMI)" (Amazon Linux 2023 AMI 2023.0.2), "Virtual server type (instance type)" (t2.micro), "Firewall (security group)" (New security group), "Storage (volumes)" (1 volume(s) - 8 GiB), and a note about the free tier.

Figure 5. AWS Example

The screenshot shows the AWS Lambda function creation wizard, Step 2: Configure instance type. It lists several instance types: t2.micro, t2.nano, t2.small, and t2.medium. Each entry provides details like family, vCPU count, memory, current generation, and pricing for Windows, SUSE, RHEL, and Linux. A search bar at the top is highlighted. To the right, there are sections for "Firewall (security group)" (New security group), "Storage (volumes)" (1 volume(s) - 8 GiB), and a note about the free tier. At the bottom right are "Cancel", "Launch", and "Review" buttons.

Figure 6. AWS Example

Azure:

In Azure, TOE instances can be created using Virtual Machines or Azure Dedicated Hosts for bare metal deployment. When deploying VM instances, Azure assigns a unique resource ID, which can be used for TOE identification. Additionally, Azure Resource Manager (ARM) tags and labels can be assigned to each TOE instance for effective identification and categorization. These tags can include metadata such as TOE name, version, environment, or any other relevant information that aids in TOE management and identification.

**Name and tags**

Number of instances: 1

**Software Image (AMI)**  
Amazon Linux 2023 AMI 2023.0.2  
HVM kernel-6.1  
ami-0889a44b331db0194

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
New security group

**Storage (volumes)**  
1 volume(s) - 8 GiB

**Note:** Free tier: In your first year includes 75 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Figure 5. AWS Example

**Instance type**

**Firewall (security group)**  
New security group

**Storage (volumes)**  
1 volume(s) - 8 GiB

**Note:** Free tier: In your first year includes 75 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Figure 6. AWS Example

Azure:

In Azure, TOE instances can be created using Virtual Machines or Azure Dedicated Hosts for bare metal deployment. When deploying VM instances, Azure assigns a unique resource ID, which can be used for TOE identification. Additionally, Azure Resource Manager (ARM) tags and labels can be assigned to each TOE instance for effective identification and categorization. These tags can include metadata such as TOE name, version, environment, or any other relevant information that aids in TOE management and identification.

[All services >](#)

## Select SQL deployment option

Microsoft



### How do you plan to use the service?



#### SQL databases

Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

Single database

[Create](#)[Show details](#)

#### SQL managed instances

Best for most migrations to the cloud. Lift-and-shift ready.

Resource type

Single instance

[Create](#)[Show details](#)

#### SQL virtual machines

Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

Image

[Create](#)[Hide details](#) High availability

#### SQL virtual machine

SQL virtual machines offer full administrative control over the SQL Server instance and underlying OS for migration to Azure.

**Featured capabilities:**

- SQL Server and OS access
- Expansive SQL Server and OS version support
- Automated manageability features for SQL Server

*Figure 7. Azure Example*[All services >](#)

## Select SQL deployment option

Microsoft



### How do you plan to use the service?



#### SQL databases

Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

Single database

[Create](#)[Show details](#)

#### SQL managed instances

Best for most migrations to the cloud. Lift-and-shift ready.

Resource type

Single instance

[Create](#)[Show details](#)

#### SQL virtual machines

Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

Image

Free License: SQL Server 2016 SP3 Develop...

- Please select an offer
- SQL Server 2022 on Windows Server 2022
  - Free SQL Server License: SQL Server 2022 Developer on Windows Server 2022
  - SQL Server 2022 Enterprise on Windows Server 2022
  - SQL Server 2022 Standard on Windows Server 2022
  - SQL Server 2022 Web on Windows Server 2022
  - SQL Server 2022 on RHEL 8
  - Free SQL Server License: SQL Server 2022 Developer on Red Hat Enterprise Linux HA 8.6
  - SQL Server 2022 Enterprise on Red Hat Enterprise Linux HA 8.6
  - SQL Server 2022 Standard on Red Hat Enterprise Linux HA 8.6
  - SQL Server 2022 Web on Red Hat Enterprise Linux HA 8.6
  - SQL Server 2022 on Ubuntu Pro 20.04
  - Free SQL Server License: SQL Server 2022 Developer on Ubuntu Pro 20.04

*Figure 8. Azure Example*

[All services >](#)

## Select SQL deployment option

Microsoft



### How do you plan to use the service?



#### SQL databases

Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

[Create](#)[Show details](#)

#### SQL managed instances

Best for most migrations to the cloud. Lift-and-shift ready.

Resource type

[Create](#)[Show details](#)

#### SQL virtual machines

Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

Image

[Create](#)[Hide details](#) High availability

#### SQL virtual machine

SQL virtual machines offer full administrative control over the SQL Server instance and underlying OS for migration to Azure.

**Featured capabilities:**

- SQL Server and OS access
- Expansive SQL Server and OS version support
- Automated manageability features for SQL Server

*Figure 7. Azure Example*[All services >](#)

## Select SQL deployment option

Microsoft



### How do you plan to use the service?



#### SQL databases

Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

[Create](#)[Show details](#)

#### SQL managed instances

Best for most migrations to the cloud. Lift-and-shift ready.

Resource type

[Create](#)[Show details](#)

#### SQL virtual machines

Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

Image

Please select an offer

SQL Server 2022 on Windows Server 2022

Free SQL Server License: SQL Server 2022 Developer on Windows Server 2022

SQL Server 2022 Enterprise on Windows Server 2022

SQL Server 2022 Standard on Windows Server 2022

SQL Server 2022 Web on Windows Server 2022

SQL Server 2022 on RHEL 8

Free SQL Server License: SQL Server 2022 Developer on Red Hat Enterprise Linux HA 8.6

SQL Server 2022 Enterprise on Red Hat Enterprise Linux HA 8.6

SQL Server 2022 Standard on Red Hat Enterprise Linux HA 8.6

SQL Server 2022 Web on Red Hat Enterprise Linux HA 8.6

SQL Server 2022 on Ubuntu Pro 20.04

Free SQL Server License: SQL Server 2022 Developer on Ubuntu Pro 20.04

*Figure 8. Azure Example*

All services &gt; Select SQL deployment option &gt;

## Create a virtual machine

X

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Monitoring](#) [Advanced](#) [SQL Server settings](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="SecurityDemoSub_697710"/>
Resource group *	<input type="text" value="(New) Resource group"/> <a href="#">Create new</a>

**Instance details**

Virtual machine name *	<input type="text"/>
Region *	<input type="text" value="(US) East US"/>
Availability options	<input type="text" value="Availability zone"/>
Availability zone *	<input type="text" value="Zones 1"/>
<small> ⓘ You can now select multiple zones. Selecting multiple zones will create one VM per zone. <a href="#">Learn more</a></small>	
Security type	<input type="text" value="Trusted launch virtual machines"/> <a href="#">Configure security features</a>
Image *	<input type="text" value="SQL Server 2022 Enterprise on Windows Server 2022 - x64 Gen2"/> <a href="#">See all images</a>   <a href="#">Configure VM generation</a>

[Review + create](#)[< Previous](#) [Next : Disks >](#)[Give feedback](#)**Figure 9. Azure Example**

All services &gt; Select SQL deployment option &gt;

## Create a virtual machine

X

 ⓘ Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size \*

[See all sizes](#)**Administrator account**

Username \*

Password \*

Confirm password \*

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*

None  
 Allow selected ports

Select inbound ports \*

**Licensing**Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing

Windows Server license? [\(?\)](#)[Review Azure hybrid benefit compliance](#)[Review + create](#)[< Previous](#) [Next : Disks >](#)[Give feedback](#)**Figure 10. Azure Example**

All services &gt; Select SQL deployment option &gt;

## Create a virtual machine

X

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Monitoring](#) [Advanced](#) [SQL Server settings](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ SecurityDemoSub\_697710

Resource group \* ⓘ (New) Resource group [Create new](#)

**Instance details**

Virtual machine name \* ⓘ

Region \* ⓘ (US) East US

Availability options ⓘ Availability zone

Availability zone \* ⓘ Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘ Trusted launch virtual machines [Configure security features](#)

Image \* ⓘ SQL Server 2022 Enterprise on Windows Server 2022 - x64 Gen2 [See all images](#) | [Configure VM generation](#)

[Review + create](#) [< Previous](#) [Next : Disks >](#) [Give feedback](#)

**Figure 9. Azure Example**

All services &gt; Select SQL deployment option &gt;

## Create a virtual machine

X

Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

Size \* ⓘ Standard\_E16ds\_v4 - 16 vcpus, 128 GiB memory (1.378,24 \$/month) [See all sizes](#)

**Administrator account**

Username \* ⓘ

Password \* ⓘ

Confirm password \* ⓘ

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \* ⓘ  None  Allow selected ports

Select inbound ports \* ⓘ RDP (3389)

**Licensing**

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing Windows Server license? ⓘ

[Review Azure hybrid benefit compliance](#)

[Review + create](#) [< Previous](#) [Next : Disks >](#) [Give feedback](#)

**Figure 10. Azure Example**

All services > Select SQL deployment option >

## Create a virtual machine

X

Basics Disks Networking Management Monitoring Advanced SQL Server settings Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ

Public IP ⓘ

NIC network security group ⓘ

- None
- Basic
- Advanced

Public inbound ports \* ⓘ

- None
- Allow selected ports

Select inbound ports \*

RDP (3389)

Source IP Address ⓘ

- Any
- Specific IP Source Range

**⚠ This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

[Review + create](#)

[< Previous](#)

[Next : Management >](#)

[Give feedback](#)

Figure 11. Azure Example

## Oracle Cloud Infrastructure:

Oracle Cloud Infrastructure (OCI) enables the deployment of TOE instances using Oracle VMs or bare metal compute shapes. OCI assigns a unique OCID (Oracle Cloud Identifier) to each compute instance, serving as a reliable identifier for TOE instances. Administrators can further enhance TOE identification by leveraging OCI's tagging system, which allows the assignment of user-defined tags. These tags can be utilized to categorize and identify TOE instances based on their specific attributes and requirements.

All services > Select SQL deployment option >

## Create a virtual machine ...

X

Basics Disks Networking Management Monitoring Advanced SQL Server settings Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ

Public IP ⓘ

NIC network security group ⓘ

- None
- Basic
- Advanced

Public inbound ports \* ⓘ

- None
- Allow selected ports

Select inbound ports \*

RDP (3389)

Source IP Address ⓘ

- Any
- Specific IP Source Range

**⚠ This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

[Review + create](#)

[< Previous](#)

[Next : Management >](#)

[Give feedback](#)

Figure 11. Azure Example

### Oracle Cloud Infrastructure:

Oracle Cloud Infrastructure (OCI) enables the deployment of TOE instances using Oracle VMs or bare metal compute shapes. OCI assigns a unique OCID (Oracle Cloud Identifier) to each compute instance, serving as a reliable identifier for TOE instances. Administrators can further enhance TOE identification by leveraging OCI's tagging system, which allows the assignment of user-defined tags. These tags can be utilized to categorize and identify TOE instances based on their specific attributes and requirements.

## Create compute instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name

instance-20230712-0824

Create in compartment



### Placement

[Collapse](#)

The availability domain helps determine which shapes are available.

Availability domain

AD 1

SMQQ:UK-LONDON-1-AD-1

AD 2

SMQQ:UK-LONDON-1-AD-2

AD 3

SMQQ:UK-LONDON-1-AD-3

[Show advanced options](#)

[Edit](#)

### Security

**Shielded instance:** Disabled

**Confidential computing:** Disabled

### Image and shape

[Collapse](#)

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Image

Oracle Linux 8

Image build: 2023.06.30-0



[Change image](#)

Shape

VM Standard EA Flex

[Create](#)

[Save as stack](#)

[Cancel](#)

Figure 12. OCI Example

## Create compute instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name

instance-20230712-0824

Create in compartment



### Placement

[Collapse](#)

The availability domain helps determine which shapes are available.

Availability domain

AD 1

SMQQ:UK-LONDON-1-AD-1

AD 2

SMQQ:UK-LONDON-1-AD-2

AD 3

SMQQ:UK-LONDON-1-AD-3

[Show advanced options](#)

[Edit](#)

### Security

**Shielded instance:** Disabled

**Confidential computing:** Disabled

### Image and shape

[Collapse](#)

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Image



Oracle Linux 8  
Image build: 2023.06.30-0



[Change image](#)

Shape

VM Standard EA Flex

[Create](#)

[Save as stack](#)

[Cancel](#)

Figure 12. OCI Example

## Select an image

**Oracle Linux**  
✓

**Ubuntu**

**Red Hat**

**CentOS**

**Windows**

**SUSE**

**AlmaLinux**

**Rocky Linux**

**Marketplace**

**My images**  
Custom images & boot volumes

Compartment

Search...

Image name	Publisher	Price	Security
<input type="checkbox"/> Oracle Autonomous Linux 7.9	Oracle	Free	
<input type="checkbox"/> Oracle Autonomous Linux 8.7	Oracle	Free	
<input type="checkbox"/> Oracle Autonomous Linux 8.8	Oracle	Free	
<input type="checkbox"/> Oracle Linux 6.10	Oracle	Free	
<input type="checkbox"/> Oracle Linux 7.9	Oracle	Free	
<input checked="" type="checkbox"/> Oracle Linux 8	Oracle	Free	
<input type="checkbox"/> Oracle Linux 9	Oracle	Free	
<input type="checkbox"/> Oracle Linux 9 Minimal	Oracle	Free	
<input type="checkbox"/> Oracle Linux Cloud Developer 8	Oracle	Free	

1 selected
Showing 9 items
◀ 1 of 1 ▶

Figure 13. OCI Example

## Select an image

**Oracle Linux**  
✓

**Ubuntu**

**Red Hat**

**CentOS**

**Windows**

**SUSE**

**AlmaLinux**

**Rocky Linux**

**Marketplace**

**My images**  
Custom images & boot volumes

Compartment

Search...

Image name	Publisher	Price	Security
<input type="checkbox"/> Oracle Autonomous Linux 7.9	Oracle	Free	
<input type="checkbox"/> Oracle Autonomous Linux 8.7	Oracle	Free	
<input type="checkbox"/> Oracle Autonomous Linux 8.8	Oracle	Free	
<input type="checkbox"/> Oracle Linux 6.10	Oracle	Free	
<input type="checkbox"/> Oracle Linux 7.9	Oracle	Free	
<input checked="" type="checkbox"/> Oracle Linux 8	Oracle	Free	
<input type="checkbox"/> Oracle Linux 9	Oracle	Free	
<input type="checkbox"/> Oracle Linux 9 Minimal	Oracle	Free	
<input type="checkbox"/> Oracle Linux Cloud Developer 8	Oracle	Free	

1 selected
Showing 9 items < 1 of 1 >

Figure 13. OCI Example

## Browse all shapes

A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Instance type

### Virtual machine

A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

### Bare metal machine

A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation. 

**Image:** Oracle Linux 8

Shape name	OCPUs 	Memory (GB)	Security
<input type="checkbox"/> BM.Standard.A1.160	160	1024	
<input type="checkbox"/> BM.Standard.E4.128	128	2048	  

**Network bandwidth (Gbps):** 100

**Maximum VNICs:** 256 

**Local disk:** Block storage only

 [Hide advanced BIOS settings](#)

These settings are for advanced users. They cannot be changed after you create the instance. [How do I choose the right BIOS settings?](#)

- Provision only a percentage of cores and disable the rest

Reduces licensing costs for applications that use a core-based licensing model. The instance itself is billed for the full shape. Value is rounded up to the nearest whole number.

25%  50%  75%  100%  
Use 25% of available cores Use 50% of available cores Use 75% of available cores Use 100% of available cores

- Customize the non-uniform memory access (NUMA) setting

The NUMA nodes per socket (NPS) setting configures how the memory is interleaved between cores and memory channels in the CPU.

NPS0  NPS1  NPS2  NPS4

- Enable simultaneous multithreading (SMT)

Allows multiple independent hardware execution threads per core (OCPUs). When disabled, only one thread can run on each core.

- Enable access control service

Allows the platform to enforce PCIe device isolation, required for VFIO device pass-through.

- Enable virtualization instructions

Enables virtualization instructions, such as Secure Virtual Machine for AMD shapes or VT-x for Intel shapes.

- Enable the input-output memory management unit (IOMMU)

Controls whether IO memory access goes through the IOMMU.

Figure 14. OCI Example

By utilizing unique identifiers, resource tags, naming conventions, and metadata labels provided by the respective cloud platforms, TOE identification can be effectively established in public cloud infrastructure deployments. These identification mechanisms aid in maintaining clear visibility, control, and management of TOE instances, enabling administrators to enforce security controls and monitor the specific security posture of each deployed TOE instance within the public cloud environment.

## Browse all shapes

A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Instance type

### Virtual machine

A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

### Bare metal machine

A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation. 

**Image:** Oracle Linux 8

Shape name	OCPUs 	Memory (GB)	Security
<input type="checkbox"/> BM.Standard.A1.160	160	1024	
<input type="checkbox"/> BM.Standard.E4.128	128	2048	  

**Network bandwidth (Gbps):** 100

**Maximum VNICs:** 256 

**Local disk:** Block storage only

 [Hide advanced BIOS settings](#)

These settings are for advanced users. They cannot be changed after you create the instance. [How do I choose the right BIOS settings?](#)

- Provision only a percentage of cores and disable the rest

Reduces licensing costs for applications that use a core-based licensing model. The instance itself is billed for the full shape. Value is rounded up to the nearest whole number.

25%  50%  75%  100%  
Use 25% of available cores Use 50% of available cores Use 75% of available cores Use 100% of available cores

- Customize the non-uniform memory access (NUMA) setting

The NUMA nodes per socket (NPS) setting configures how the memory is interleaved between cores and memory channels in the CPU.

NPS0  NPS1  NPS2  NPS4

- Enable simultaneous multithreading (SMT)

Allows multiple independent hardware execution threads per core (OCPUs). When disabled, only one thread can run on each core.

- Enable access control service

Allows the platform to enforce PCIe device isolation, required for VFIO device pass-through.

- Enable virtualization instructions

Enables virtualization instructions, such as Secure Virtual Machine for AMD shapes or VT-x for Intel shapes.

- Enable the input-output memory management unit (IOMMU)

Controls whether IO memory access goes through the IOMMU.

Figure 14. OCI Example

By utilizing unique identifiers, resource tags, naming conventions, and metadata labels provided by the respective cloud platforms, TOE identification can be effectively established in public cloud infrastructure deployments. These identification mechanisms aid in maintaining clear visibility, control, and management of TOE instances, enabling administrators to enforce security controls and monitor the specific security posture of each deployed TOE instance within the public cloud environment.

# Cloud Equivalence Considerations

Common Criteria is about products not systems or services. This guidance operates on the principle that products must be tested individually on each desired cloud service offering.

When writing Security Targets, the Cloud Service Offering (including the cloud region or datacenter) must be detailed in the TOE evaluated configuration details. CSOs cannot inherently be assumed to be equivalent. For instance, CSPs may have separate environments between government or commercial customers. However, if existing cloud authorizations exist for multiple regions or datacenters this may inform equivalency claims. Especially if the Trusted Platform meets the assumptions and objectives of the PP and is consistent across multiple cloud regions. Each CC scheme has the option to define a policy for acceptance criteria.

## CPU Equivalency

Applicable guidance shall be followed when labeling Operational Environments. Such as:

For a Type 1 (or native) hypervisor, where the hypervisor runs directly on the hardware, the OE listing shall include the guest OS, hypervisor, and processor using the following format: “Guest OS on hypervisor on Processor.” An example is “Microsoft Windows 11 on VMWare ESXi 7.0 on Intel Xeon W (Rocket Lake).”

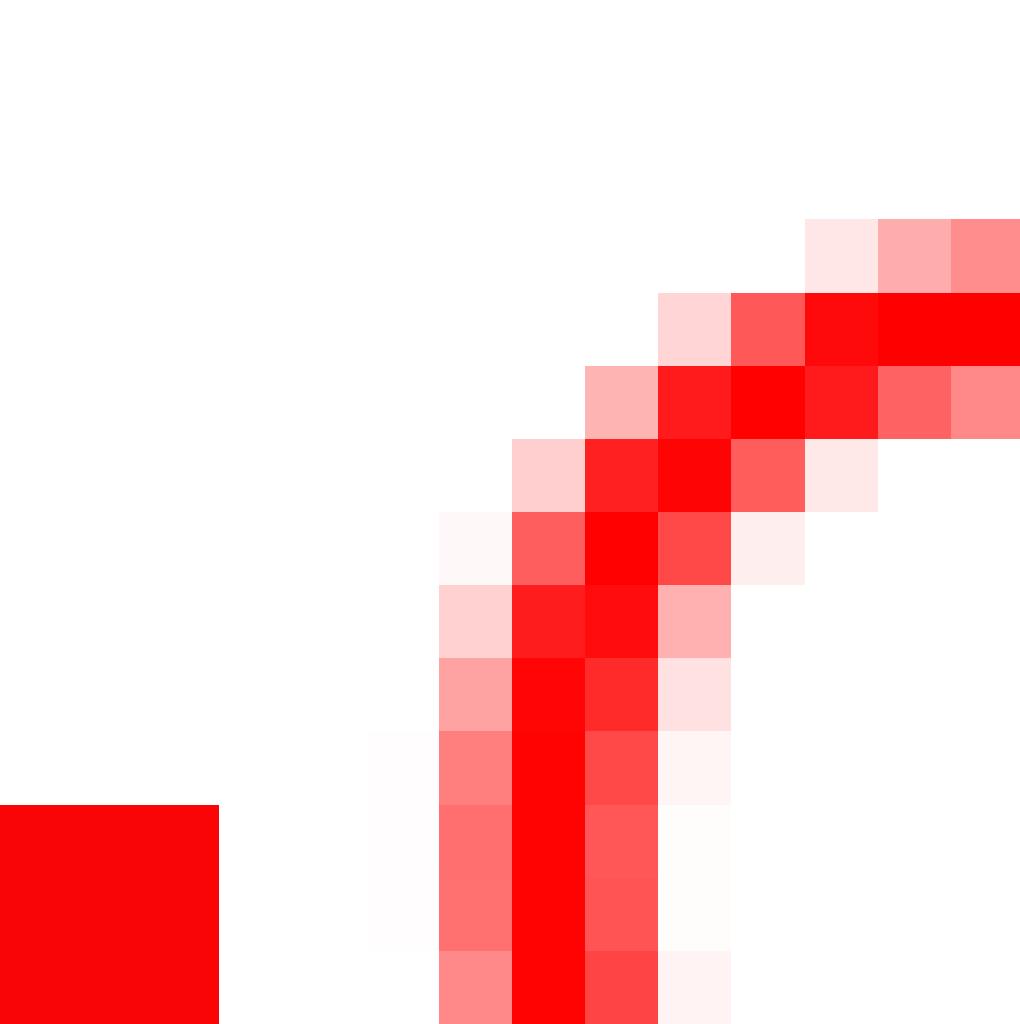
For a Type 2 (or hosted) hypervisor, where the hypervisor runs on a host operating system (OS), the OE listing shall include the guest OS, hypervisor, host OS, and processor using the following format: “Guest OS on hypervisor on Host OS on Processor.” An example is “Microsoft Windows 11 on Parallels Desktop 17 on macOS Monterey on Intel Core i7 (Kaby Lake).”

Algorithm tests may also be performed using containers. The OE listing shall include the container, runtime, host OS, and processor using the following format: “container on runtime on host OS on processor.” An example is “Ubuntu 20.04 Docker Image on Docker Engine 20 on Ubuntu 20.04 on Intel Xeon W (Rocket Lake).”

TOE’s that are being evaluated in a cloud context are expected to be able to conclusively demonstrate knowledge of the underlying TOE Platform for these specifics. If SFR enforcing functionality is agnostic to the TOE platform, such equivalency claims may be made.

E.g. CPU model / OS / Hypervisor / Guest OS / Container shall be defined where appropriate.

At this time, if a TOE is reliant on the OE for cryptographic operations, there is no need to leverage the related collateral that explicitly states operation for a given Cloud Provider. This equivalence rationale should also be considered when a TOE vendor is reliant upon a CSP for algorithm certification and many TOE platforms are claimed.



# Contributors Roles in Product Evaluations

## Roles Clarification

### **Administrator**

Entity that has a level of trust with respect to all policies implemented by the TOE security functionality [CC:2022 Part 1]

### **Customer**

A customer of the Cloud Service Provider. Also may be the administrator for the TOE

### **Developer**

Organization responsible for the development of the TOE [CC:2022 Part 1]

### **Cloud Service Provider (CSP)**

A cloud service provider, or CSP, is an entity that offers some component of cloud computing; typically infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS) to other businesses or individuals.

### **Evaluation Authority (EA)**

Body operating an evaluation scheme [CC:2022 Part 1]

### **Evaluator**

Individual assigned to perform evaluations in accordance with a given evaluation standard and associated evaluation methodology [CC:2022 Part 1]

### **Evaluator Guidance**

Placeholder for Issue #74

## **Contributors Involvement**

This section would be useful for explaining the relationships possible between the TOE Vendor, CSP and Trusted Platform

# Contributors Roles in Product Evaluations

## Roles Clarification

### **Administrator**

Entity that has a level of trust with respect to all policies implemented by the TOE security functionality [CC:2022 Part 1]

### **Customer**

A customer of the Cloud Service Provider. Also may be the administrator for the TOE

### **Developer**

Organization responsible for the development of the TOE [CC:2022 Part 1]

### **Cloud Service Provider (CSP)**

A cloud service provider, or CSP, is an entity that offers some component of cloud computing; typically infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS) to other businesses or individuals.

### **Evaluation Authority (EA)**

Body operating an evaluation scheme [CC:2022 Part 1]

### **Evaluator**

Individual assigned to perform evaluations in accordance with a given evaluation standard and associated evaluation methodology [CC:2022 Part 1]

### **Evaluator Guidance**

Placeholder for Issue #74

# Steps to optimize a PP for TOEs in a cloud environment.

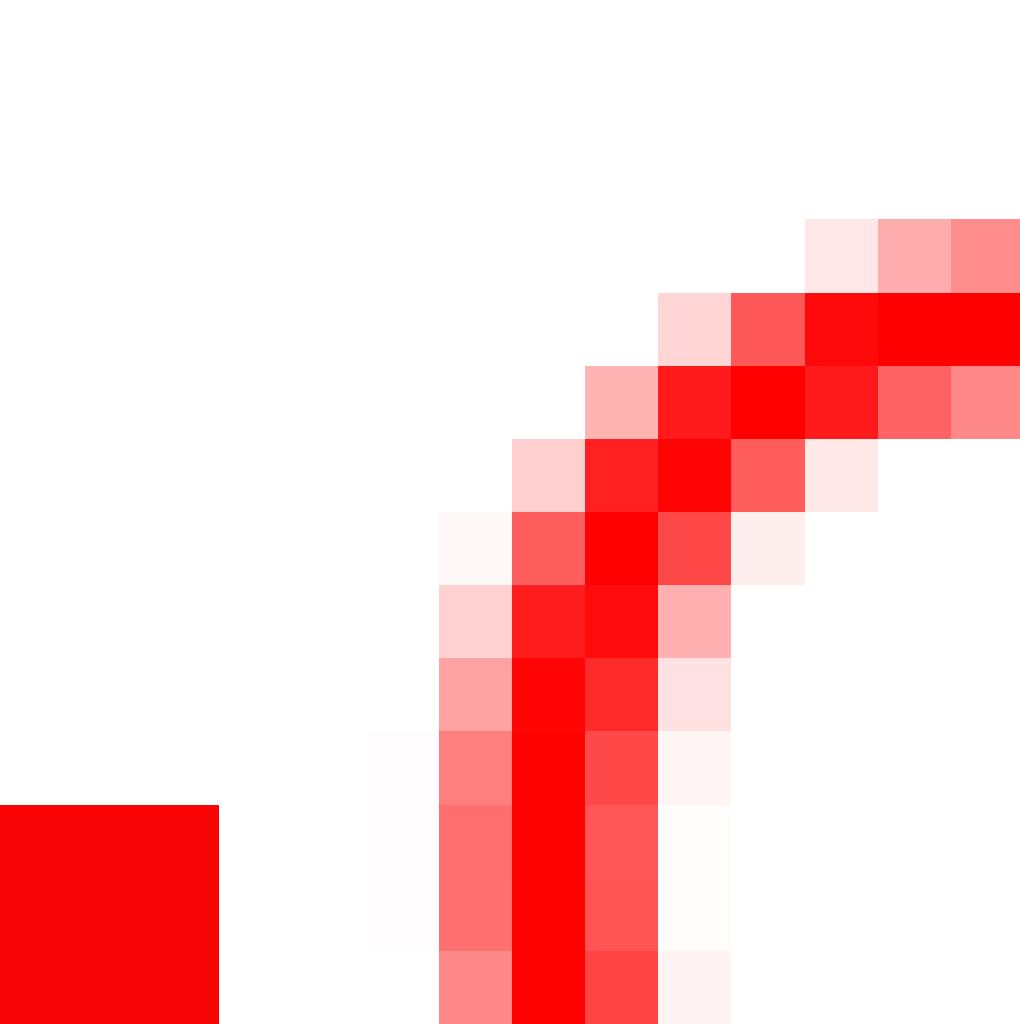
A PP comprises of a number of sections and each should be reviewed and updated in order to give directions to ST authors for TOEs in a cloud environment:

## Process Overview

- Review this guidance document and associated instructions
- Map Assumptions, Security Objections for the Operational Environment, and Organizational Security Policies to applicable authorization scheme(s) as a reference implementation (FedRamp, C5, etc)
  - Summarize this mapping in generic language for wider Cloud Authorization adoption i.e. consideration in other authorization schemes
    - Determine the extent to which SFRs and SARs in the PP can rely on the OE to be satisfied so that the extent to which the TSF may need to rely on cloud services can be determined.
  - Identify SFR challenges in a cloud operational environment
    - For example certain requirements collecting test evidence may be complicated by the cloud operational environment and may not be directly accessible due to cloud isolation.
      - Many TOEs that will operate in a cloud environment will utilize object storage as provided by the CSP. These objects will often be encrypted either by the TOE itself or by the CSP. For instances in which the CSP is providing encryption of the storage object, it is expected that the TOE vendor or evaluator will not be able to perform assurance activity tests with regards to Key Destruction. PP authors will be expected to make modifications to related SFRs to allow for CSP Key Destruction or Zeroization as additional selections.
      - Such modifications may be made by iterating the underlying SFR in a base PP into a "Cloud" PP module which provides the cloud-specific selections and assurance activities.
  - Identify SAR challenges with either new/updated SAR's and/or determine if applicable
    - For example AVA may have different considerations for a cloud operating environment depending on the TOE or PP. See [Vulnerability Assessment Methodology](#) for more information.
- Edit cPP/PP and add new optional or selection based SFRs/SARs for cloud evaluations
- Update cPPs supporting documents with new cloud requirements and applicable assurance activities.

## Conformance Claims

It is not expected that changes would be required to the Conformance Claims chapter.



PP editors may consider including a reference to this guidance document within the updated PP.

## Security Problem Definition

This chapter describes security problems in terms of threats, assumptions and organizational security policies.

Appendix A details the Threats, Assumptions, Security Objectives for the TOE, and Security Objectives for the operational environment for a number of PP's of interest.

Generally within the PP's proposed, the Network Device and Application Software PPs are used the most.

In Appendix B specific aspects of the Assumptions and Security Objectives for the Operational Environment were considered to determine whether assumptions made for each PP of interest are consistent and could be satisfied by a cloud environment. The analysis found that the assumptions and Security Objectives of the Operating Environment for PP's of interest are consistent: There are generally only three categories: Platform Integrity, Proper (Non-Malicious User) and Proper (Trusted) Admin. The virtualization PP considers also Physical Security but this not considered by the other PPs.

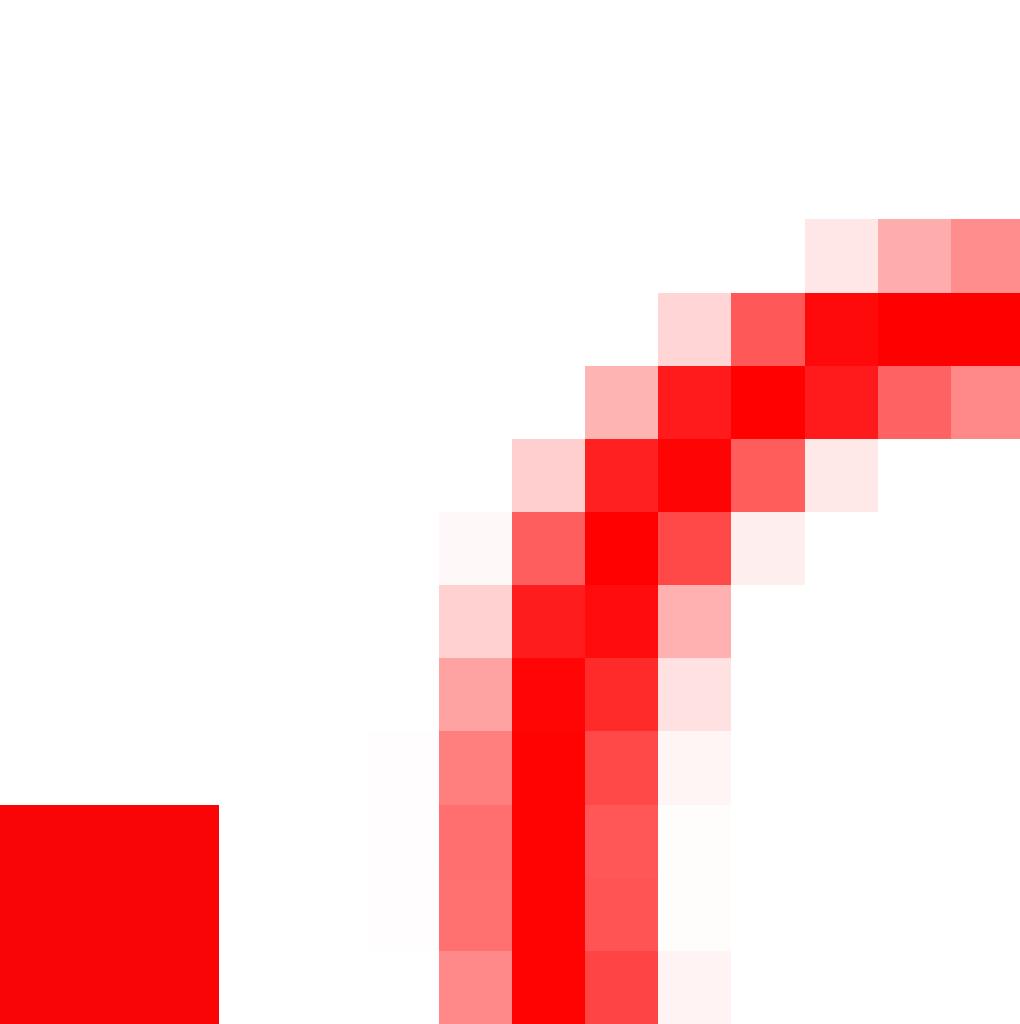
It is not necessarily expected that a cloud environment will introduce new threats, assumptions or organizational security policies, although the PP writers may wish to consider whether existing threats, assumptions and organization security policies should be refined to provide more explanation in the case of cloud. For example, threat models may consider the impact of potential ubiquitous access and multi-tenancy to either add to existing threats, assumptions and organizational security policies or refine them.

## Security Objectives

Security Objectives for the TOE map to security functionalities/services of the TOE itself so it is not expected that changes would be required.

As described in Appendix B of this document, the Security Objectives of the Operating Environment provide the general requirements that should be satisfied by the cloud environment. It is proposed that PP's should include an appendix as guidance for an evaluator to assess whether the cloud environment for the TOE satisfies the Security Objectives of the Operating Environment of the PP. In the context of the PP's highlighted, where the assurance level is low (no development security requirements, vulnerability requirements at AVA\_VAN.1: public search), the assumptions and Security Objectives of the Operating Environment should be sufficiently satisfied by any suitable cloud security certification process recognized by a national government supporting Common Criteria, that addresses the environment being used(e.g. lowest level Fedramp, BSI C5 baseline, ISO27017).

The Security Objectives rationale is not expected to change, unless additional threats, assumptions or security objectives have been added.



# Security Requirements.

It is expected that some additional application notes would be appended to a PP regarding Security Requirements.

Security Functional Requirements should be each considered carefully as to whether there may be dependency on the cloud platform.

For example, Cryptographic Support (FCS) may include cryptographic operations using services of the platform, or random number generation derived from platform entropy sources. Others example would be any SFRs around boot integrity and maybe key destruction.

Depending on the type of technology and the associated test scenarios some modification to SFRs will be necessary.

A product that operates identically outside of a cloud operating environment may not require changes.

A product that is only designed to operate in a cloud-native context may need refinements to requirements to the PP.

*MDM Example*

Place example here

# Security Assurance Requirements.

Classes ASE and ADV are not expected to require change.

Class AGD will be evaluated similarly but the developer must provide guidance both the AGD\_PRE and AGD\_OPE that work for the cloud platform.

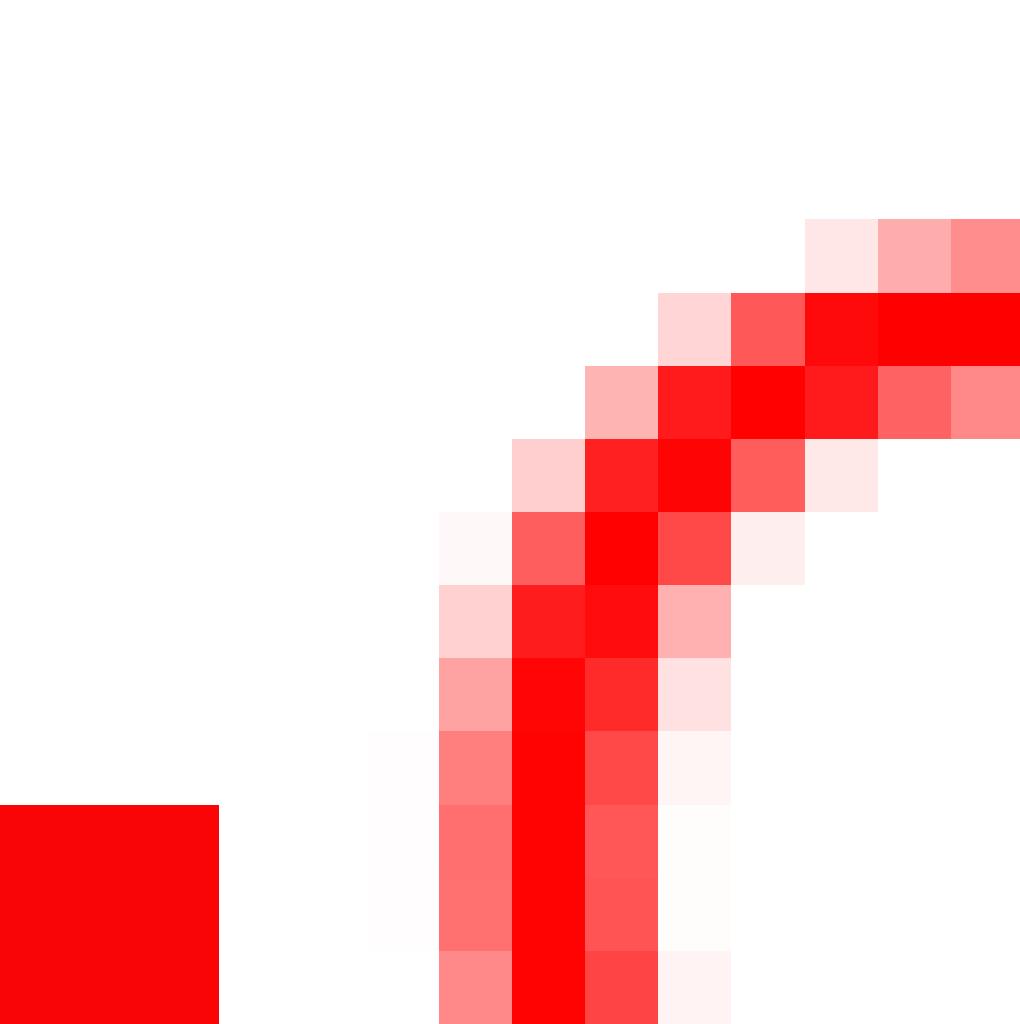
There also may be two scenarios for guidance:

- i. A developer providing guidance for their TOE to be installed and operated in a cloud environment. This may look very similar to the guidance for a typical ‘on-prem’ installation.
- ii. A developer providing guidance for their TOE to be installed and operated on their own cloud environment. In this case the developer may provide installation and operational instructions specific to their cloud platform.

Class ALC changes expected to be minimal and should be resolved with minor adjustments. However, it is likely that care will be required around Flaw remediation and similar ALC aspects (including ALC\_TSU\_EXT.1.1 Timely Security Updates) as how they would work in a cloud platform.

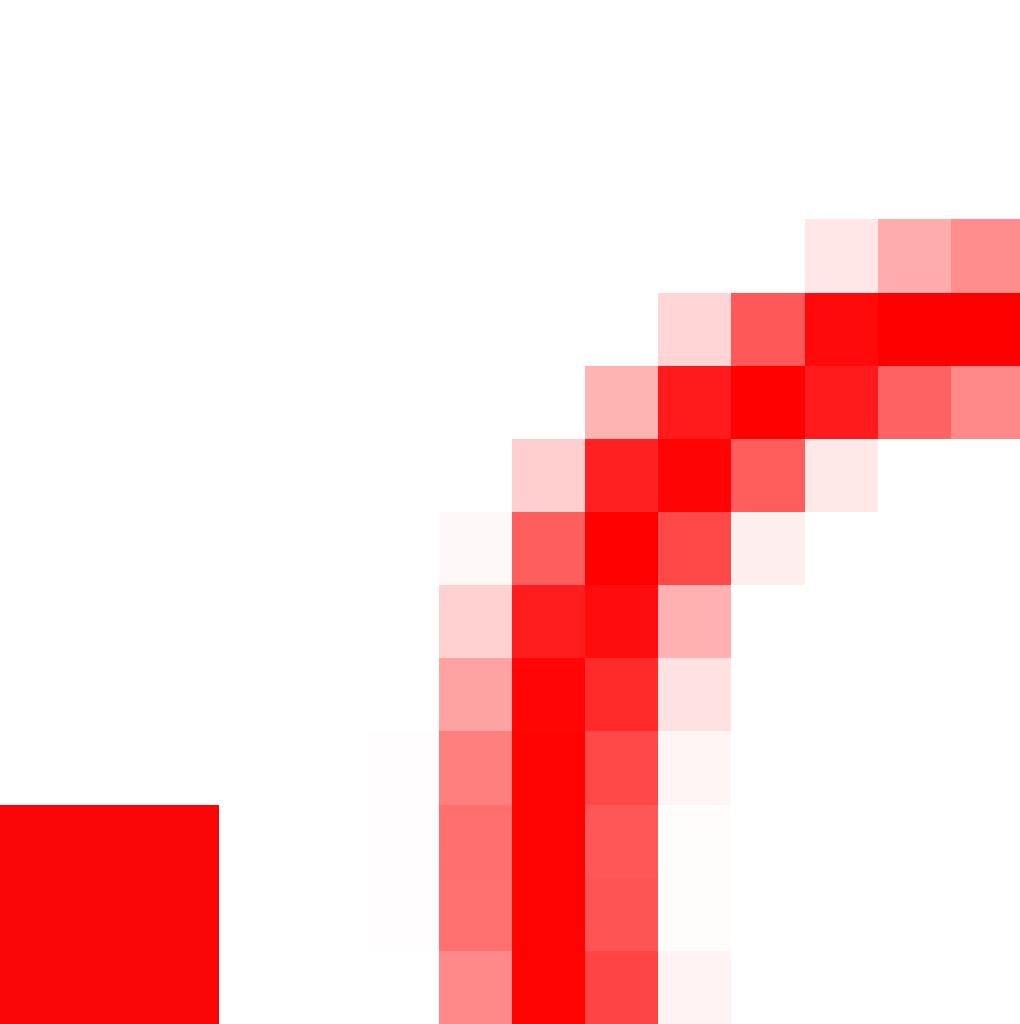
Class ATE will require some additional application notes required around ‘provide the OS for testing’ for a cloud environment.

Class AVA would not be expected to require significant additional application notes.



## Other considerations

A text search of the term ‘platform’ is likely to highlight areas of a PP that will require modification in order to support evaluations in a Cloud environment (if not already resolved with the activities in sections 3.1-3.6)



# 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.

Threats are not considered here, since they map to Security Objectives for the TOE rather than Assumptions and Security Objectives for the Operating Environment. A threat, as an adverse action performed by a threat agent on an asset, is not contextual to the operating environment of the TOE. However, an author may choose to review the listed threats detailed in a PP in the context of cloud evaluations.

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.

# 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.

Threats are not considered here, since they map to Security Objectives for the TOE rather than Assumptions and Security Objectives for the Operating Environment. A threat, as an adverse action performed by a threat agent on an asset, is not contextual to the operating environment of the TOE. However, an author may choose to review the listed threats detailed in a PP in the context of cloud evaluations.

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\_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*

## **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**

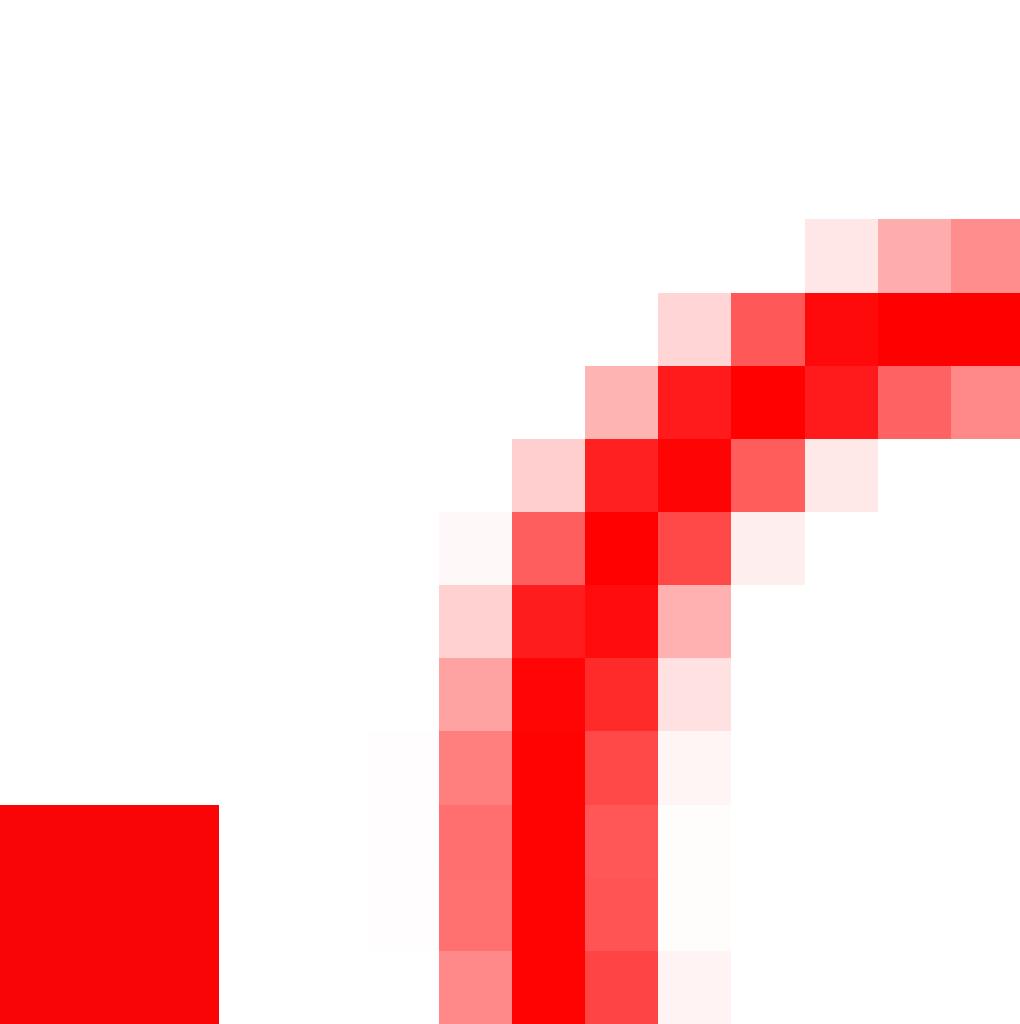
The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE. The Trusted Platform service shall be managed according to known, accepted and trusted policies. Any information provided by 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*

<b>Assumption</b>	<b>Environmental Objective Addressing the Assumption</b>	<b>Cloud Authorization Scheme Controls - Cisco CCF v2.0</b>
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
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



# Cloud Sub-Processes

## Introduction

This section in the JIL guidance is meant to help vendors "anticipate their development capability to comply to the requirements of CC". For the CCiTC purposes, this should provide guidance to PP authors and Evaluators how to augment CC deliverables for cloud evaluations.

## Development Environment Sub-Process

It may be necessary for the iTC to provide additional assurance strategies for PP authors to incorporate more development environment review. The goal of which is to support Dev Ops practices and facilitate cloud evaluations that allow the customer some assurance apart from fixed version evaluations.

For example if a TOE vendor is leveraging a cloud providers container images to deploy a software product, the Development Environment sub-process should require additional collateral to demonstrate that the cloud provider is providing assurance to the TOE vendor for the image that it is appropriately signed and/or updated.

FEDRamp PaaS OS images can be assumed to receive continuous vulnerability patching to maintain authorization and that collateral can be extended to CCiTC.

---

Place output from TP group here ---

## Security Target (TSS) Sub-Process

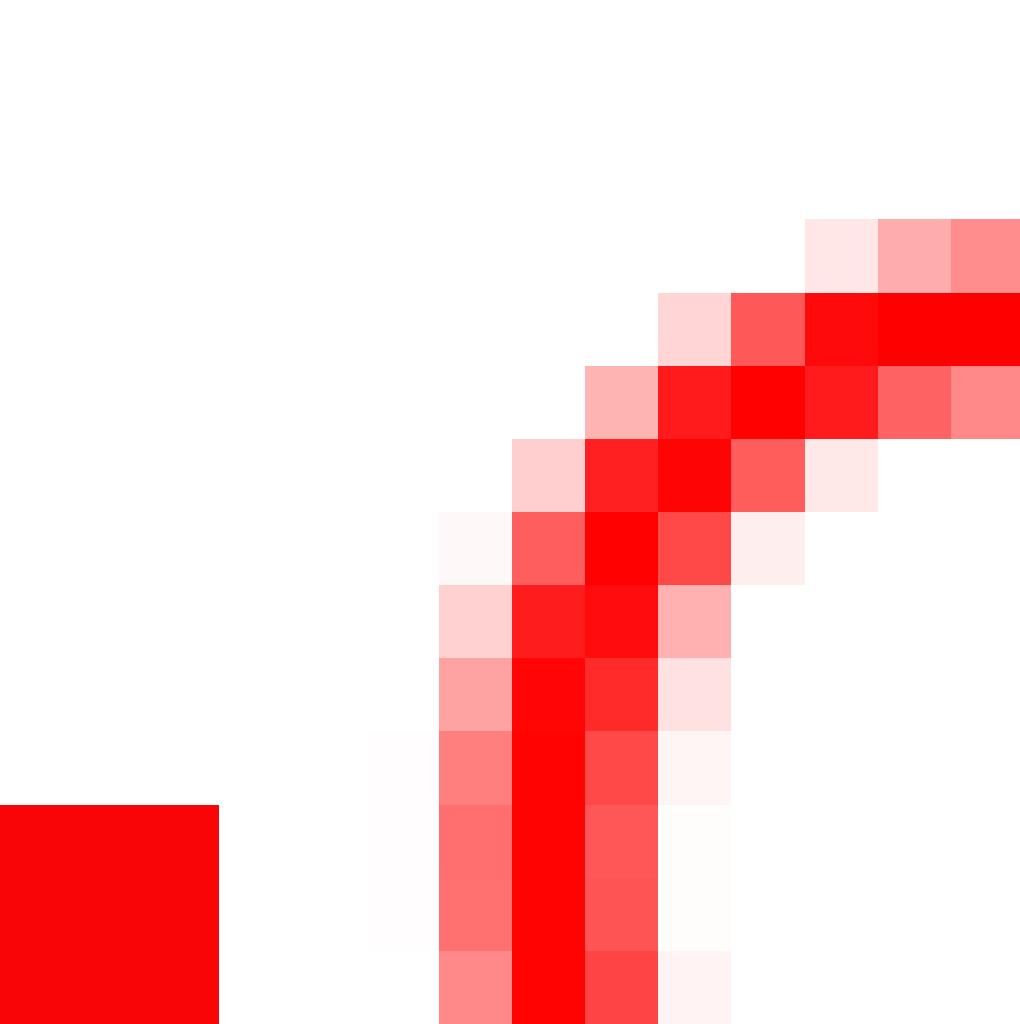
This section shall discuss the expected changes to a Security Target for cloud evaluations. This also may be better suited to address SFR changes needed in a PP. For example, changes need to address SFRs that deal with credential management:

For example, for all Assurance Activities that extend TOE Summary Specification (TSS) requirements in a ST will need to be modified such that Cloud Operating Environments are captured.

Due to the fungible nature of compute resourcing in a Cloud Environment, traditional methods of credential storage to a local operating environment are not viable. Cloud IAM, Token, and Key management are often adapted to Cloud Products and these changes must be reflected in the associated TSS requirements.

---

Put TP SFR details here ---



## Guidance Documentation Sub-Process

If existing documentation exists for a CSP it should be leveraged. Each CSP that is tested shall provide instructions for deployment of the TOE. Consultants and vendors shall provide necessary supplemental guidance as it supports deploying the TOE as evaluated in the cloud. In addition, functionality that is included but not evaluated shall be clearly identified.

It is important to distinguish here that not all expected elements of a traditional AGD document can be translated for Cloud Environments. It may be necessary to exclude or supplement these guidance requirements depending on the topology of the product and the cloud service provider. In some circumstances, the Cloud Provider is the only entity that may fulfill these guidance requirements to ensure that the TOE is deployed in the tested configuration.

## Development / Tests Sub-Process

This section shall discuss augmentations needed for assurance activities that are targeting cloud evaluations.

Depending on the type of technology and the associated test scenarios some modification of test methodology will be necessary.

A product that operates identically outside of a cloud operating environment may not require changes.

A product that is only designed to operate in a cloud-native context may need refinements to test cases to be accommodated by the appropriate Technical Community.

## Guidance For Establishing Test Environments on Cloud Infrastructure

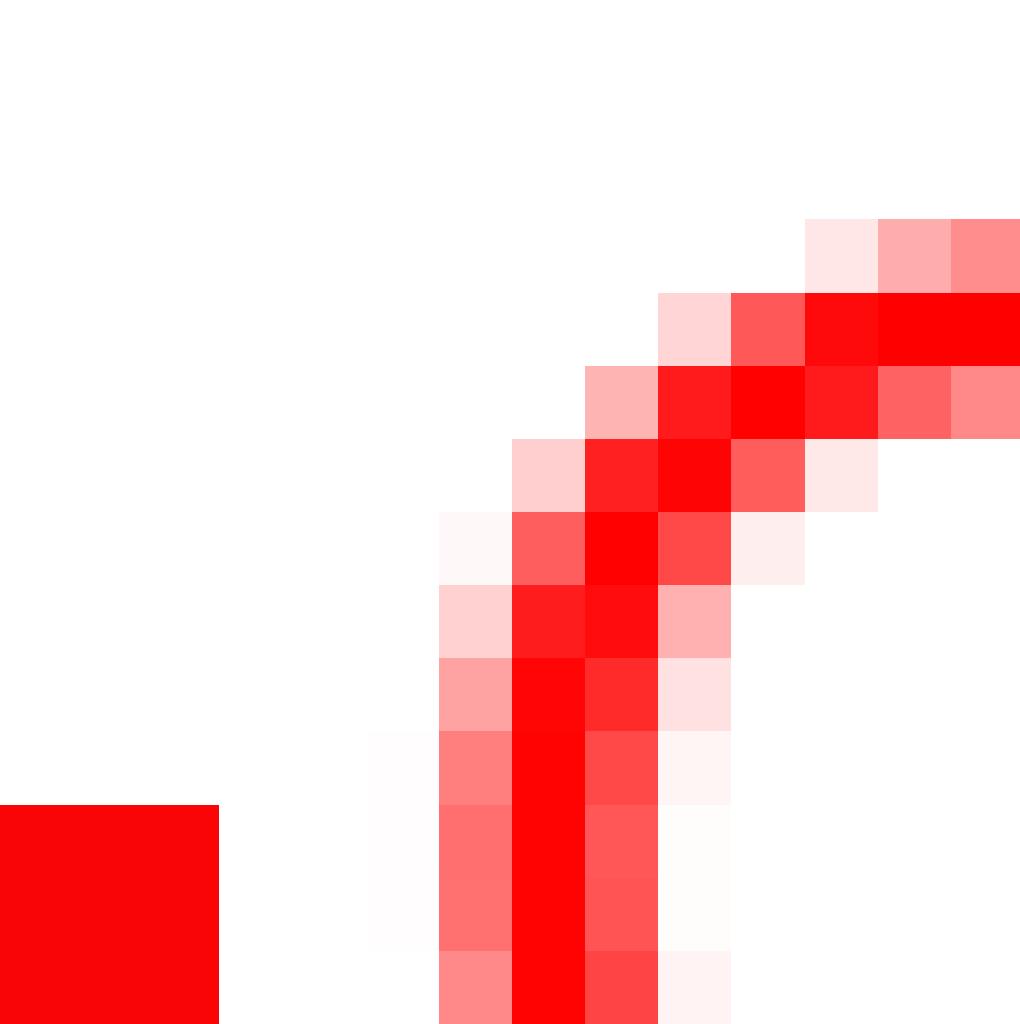
As Common Criteria testing requires unique test environments for each TOE that are isolated to prevent contamination of test results, testing on Public Cloud infrastructure raises some initial concerns.

In general, the necessity to abstract from underlying hardware layers is dictated by the TOE type in Protection Profiles. For instance, the cPP for Application Software relies only on the underlying OS and makes no distinction on whether that OS is virtualized or not. In this scenario bare metal isolation in the cloud testing would be unnecessary and a multi-tenancy environment is acceptable.

An evaluator should be prepared to create and offer cloud testing infrastructure to TOE developers. This environment must establish controls provided by the CSP to establish effective isolation equivalent to on-prem testing to ensure the integrity of results. This may involve isolated VLANs, ACLs, Compute Resources, etc on multi-tenant infrastructure. This information will need to be captured and presented to Evaluation Authorities as evaluation deliverables.

### *ExamplesFromMDM*

PlaceHolder for Example AA modification



# Vulnerability Assessment Methodology

In general, the AVA methodology shall be sufficient for most TOE types. However, certain edge cases may present themselves.

As we have introduced a trusted platform concept, underlying vulnerabilities in the cloud operating environment can be treated as they are in traditional OE analysis.

However, when applicable vulnerabilities are discovered or suspected for TOEs operating in a cloud environment the means in which evaluators are expected to shift negative test coverage must utilize cloud attack vectors. I.e. service portal, management plane, etc.

## List of potential vulnerabilities

Since a cloud stack will inherently contain many vulnerabilities, it would be useful for the iTC to provide guidance on risk management practices to minimize these factors.

## Defining penetration tests

The JII Guidance uses this section on how to compose the penetration testing coverage needed. This may need to be expanded given the content above or removed entirely from the CCiTC guidance.

## List of attacks and strategies

The JII Guidance uses this section to allow for attacker potential mitigation. The iTC will need to provide some language here to adapt for cloud evaluations.

# Vulnerability Assessment Methodology

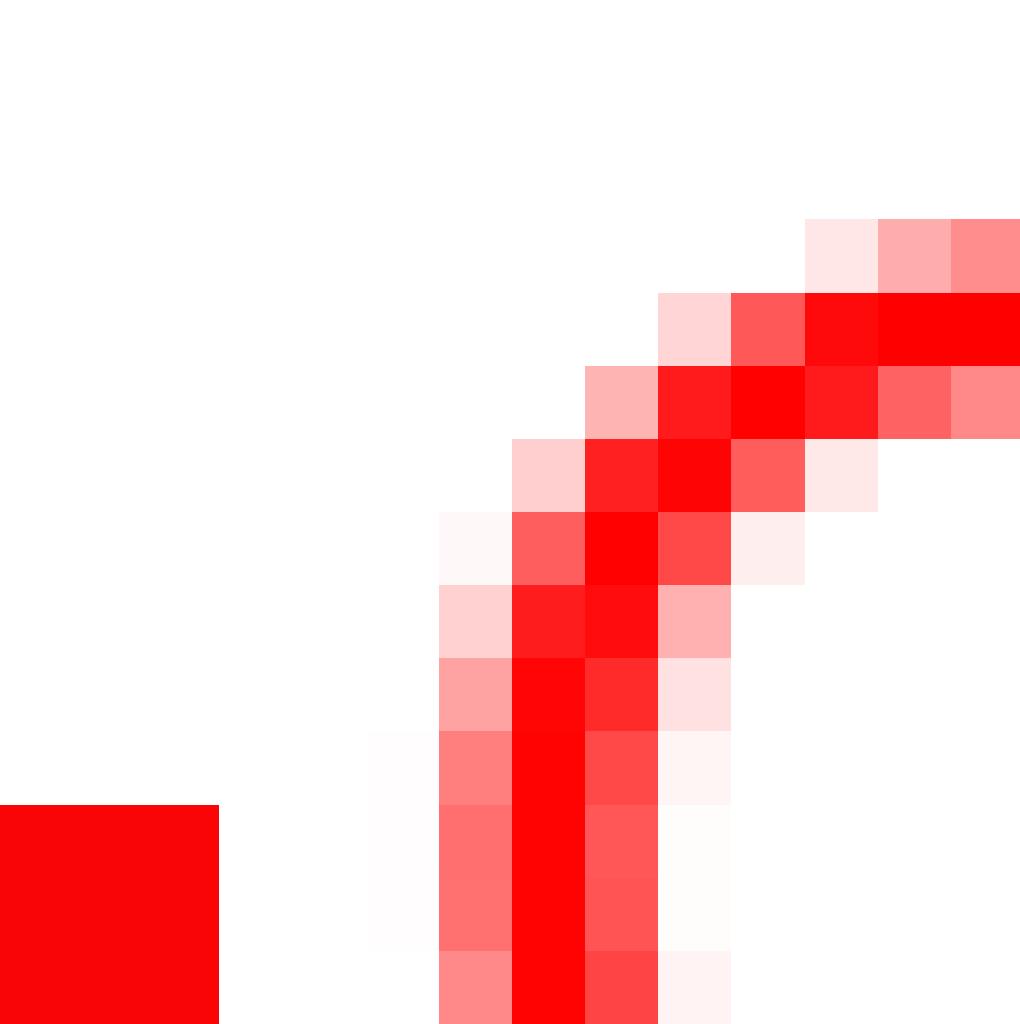
In general, the AVA methodology shall be sufficient for most TOE types. However, certain edge cases may present themselves.

As we have introduced a trusted platform concept, underlying vulnerabilities in the cloud operating environment can be treated as they are in traditional OE analysis.

However, when applicable vulnerabilities are discovered or suspected for TOEs operating in a cloud environment the means in which evaluators are expected to shift negative test coverage must utilize cloud attack vectors. I.e. service portal, management plane, etc.

# References

- [nist\_cloud] NIST SP 800-145 "The NIST Definition of Cloud
- [CC\_2022] Common Criteria for Information Technology Security Evaluation, November 2022



# Appendix A: Threats, Assumptions and Security Objectives for each PP.

## Protection Profile for General Purpose Computing Platform, Version 1.0

### Use Cases

[USE CASE 1]: Server-Class Platform, Basic

This use case encompasses server-class hardware in a data center. There are no additional physical protections required because the platform is assumed to be protected by the operational environment as indicated by A.PHYSICAL\_PROTECTION. The platform is administered through a management controller that accesses the MC through a console or remotely.

This use case adds audit requirements and Administrator authentication requirements to the base mandatory requirements.

For changes to included SFRs, selections, and assignments required for this use case, see G.1 Server-Class Platform, Basic.

### Threats

- T.PHYSICAL
- T.SIDE\_CHANNEL\_LEAKAGE
- T.PERSISTENCE
- T.UPDATE\_COMPROMISE
- T.SECURITY\_FUNCTIONALITY\_FAILURE
- T.TENANT\_BASED\_ATTACK
- T.NETWORK\_BASED\_ATTACK
- T.UNAUTHORIZED\_RECONFIGURATION
- T.UNAUTHORIZED\_PLATFORM\_ADMINISTRATOR

### Assumptions

- A.PHYSICAL\_PROTECTION
- A.ROT\_INTEGRITY
- A.TRUSTED\_ADMIN
- A.MFR\_ROT
- A.TRUSTED\_DEVELOPMENT\_AND\_BUILD\_PROCESSES
- A.SUPPLY\_CHAIN\_SECURITY
- A.CORRECT\_INITIAL\_CONFIGURATION
- A.TRUSTED\_USERS
- A.REGULAR\_UPDATES

# Appendix A: Threats, Assumptions and Security Objectives for each PP.

## Protection Profile for General Purpose Computing Platform, Version 1.0

### Use Cases

[USE CASE 1]: Server-Class Platform, Basic

This use case encompasses server-class hardware in a data center. There are no additional physical protections required because the platform is assumed to be protected by the operational environment as indicated by A.PHYSICAL\_PROTECTION. The platform is administered through a management controller that accesses the MC through a console or remotely.

This use case adds audit requirements and Administrator authentication requirements to the base mandatory requirements.

For changes to included SFRs, selections, and assignments required for this use case, see G.1 Server-Class Platform, Basic.

### Threats

- T.PHYSICAL
- T.SIDE\_CHANNEL\_LEAKAGE
- T.PERSISTENCE
- T.UPDATE\_COMPROMISE
- T.SECURITY\_FUNCTIONALITY\_FAILURE
- T.TENANT\_BASED\_ATTACK
- T.NETWORK\_BASED\_ATTACK
- T.UNAUTHORIZED\_RECONFIGURATION
- T.UNAUTHORIZED\_PLATFORM\_ADMINISTRATOR

### Assumptions

- A.PHYSICAL\_PROTECTION
- A.ROT\_INTEGRITY
- A.TRUSTED\_ADMIN
- A.MFR\_ROT
- A.TRUSTED\_DEVELOPMENT\_AND\_BUILD\_PROCESSES
- A.SUPPLY\_CHAIN\_SECURITY
- A.CORRECT\_INITIAL\_CONFIGURATION
- A.TRUSTED\_USERS
- A.REGULAR\_UPDATES

## Security Objectives for the TOE

O.PHYSICAL\_INTEGRITY  
O.ATTACK\_DECEPTION\_AND\_RESPONSE  
O.MITIGATE\_FUNDAMENTAL\_FLAWS  
O.PROTECTED\_FIRMWARE  
O.UPDATE\_INTEGRITY  
O.STRONG\_CRYPTOGRAPHY  
O.SECURITY\_FUNCTIONALITY\_INTEGRITY  
O.TENANT\_SECURITY  
O.TRUSTED\_CHANNELS  
O.CONFIGURATION\_INTEGRITY  
O.AUTHORIZED\_ADMINISTRATOR

## Security Objectives for the Operational Environment

OE.PHYSICAL\_PROTECTION  
OE.SUPPLY\_CHAIN  
OE.TRUSTED\_ADMIN

## Base PP for Virtualization Version 1.1

### Use Cases

None for Cloud

### Threats

T.DATA\_LEAKAGE  
T.UNAUTHORISED\_UPDATE  
T.UNAUTHORIZED\_MODIFICATION  
T.USER\_ERROR  
T.3P\_SOFTWARE  
T.VMM\_COMPROMISE  
T.PLATFORM\_COMPROMISE  
T.UNAUTHORIZED\_ACCESS  
T.WEAK\_CRYPTO  
T.UNPATCHED\_SOFTWARE  
T.MISCONFIGURATION  
T.DENIAL\_OF\_SERVICE

### Assumptions

A.PLATFORM\_INTEGRITY  
A.PHYSICAL  
A.TRUSTED\_ADMIN

## Security Objectives for the TOE

O.PHYSICAL\_INTEGRITY  
O.ATTACK\_DECEPTION\_AND\_RESPONSE  
O.MITIGATE\_FUNDAMENTAL\_FLAWS  
O.PROTECTED\_FIRMWARE  
O.UPDATE\_INTEGRITY  
O.STRONG\_CRYPTOGRAPHY  
O.SECURITY\_FUNCTIONALITY\_INTEGRITY  
O.TENANT\_SECURITY  
O.TRUSTED\_CHANNELS  
O.CONFIGURATION\_INTEGRITY  
O.AUTHORIZED\_ADMINISTRATOR

## Security Objectives for the Operational Environment

OE.PHYSICAL\_PROTECTION  
OE.SUPPLY\_CHAIN  
OE.TRUSTED\_ADMIN

## Base PP for Virtualization Version 1.1

### Use Cases

None for Cloud

### Threats

T.DATA\_LEAKAGE  
T.UNAUTHORISED\_UPDATE  
T.UNAUTHORIZED\_MODIFICATION  
T.USER\_ERROR  
T.3P\_SOFTWARE  
T.VMM\_COMPROMISE  
T.PLATFORM\_COMPROMISE  
T.UNAUTHORIZED\_ACCESS  
T.WEAK\_CRYPTO  
T.UNPATCHED\_SOFTWARE  
T.MISCONFIGURATION  
T.DENIAL\_OF\_SERVICE

### Assumptions

A.PLATFORM\_INTEGRITY  
A.PHYSICAL  
A.TRUSTED\_ADMIN

A.NON\_MALICIOUS\_USER

## Security Objectives for the TOE

O.VM\_ISOLATION  
O.VMM\_INTEGRITY  
O.PLATFORM\_INTEGRITY  
O.DOMAIN\_INTEGRITY  
O.MANAGEMENT\_ACCESS  
O.PATCHED\_SOFTWARE  
O.VM\_ENTROPY  
O.AUDIT  
O.CORRECTLY\_APPLIED\_CONFIGURATION  
O.RESOURCE\_ALLOCATION

## Security Objectives for the Operational Environment

OE.CONFIG  
OE.PHYSICAL  
OE.TRUSTED\_ADMIN  
OE.NON\_MALICIOUS\_USER

# Protection Profile for General Purpose Operating Systems Version 4.3

## [USE CASE 3] Cloud Systems

The OS provides a platform for providing cloud services running on physical or virtual hardware. An OS is typically part of offerings identified as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

This use case typically involves the use of virtualization technology which should be evaluated against the Protection Profile for Server Virtualization.

## Threats

T.NETWORK\_ATTACK  
T.NETWORK\_EAVESDROP  
T.LOCAL\_ATTACK  
T.LIMITED\_PHYSICAL\_ACCESS

## Assumptions

A.PLATFORM  
A.PROPER\_USER  
A.PROPER\_ADMIN

A.NON\_MALICIOUS\_USER

## **Security Objectives for the TOE**

- O.VM\_ISOLATION
- O.VMM\_INTEGRITY
- O.PLATFORM\_INTEGRITY
- O.DOMAIN\_INTEGRITY
- O.MANAGEMENT\_ACCESS
- O.PATCHED\_SOFTWARE
- O.VM\_ENTROPY
- O.AUDIT
- O.CORRECTLY\_APPLIED\_CONFIGURATION
- O.RESOURCE\_ALLOCATION

## **Security Objectives for the Operational Environment**

- OE.CONFIG
- OE.PHYSICAL
- OE.TRUSTED\_ADMIN
- OE.NON\_MALICIOUS\_USER

# **Protection Profile for General Purpose Operating Systems Version 4.3**

## **[USE CASE 3] Cloud Systems**

The OS provides a platform for providing cloud services running on physical or virtual hardware. An OS is typically part of offerings identified as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

This use case typically involves the use of virtualization technology which should be evaluated against the Protection Profile for Server Virtualization.

## **Threats**

- T.NETWORK\_ATTACK
- T.NETWORK\_EAVESDROP
- T.LOCAL\_ATTACK
- T.LIMITED\_PHYSICAL\_ACCESS

## **Assumptions**

- A.PLATFORM
- A.PROPER\_USER
- A.PROPER\_ADMIN

## Security Objectives for the Operational Environment

OE.PLATFORM  
OE.PROPER\_USER  
OE.PROPER\_ADMIN

# Protection Profile for Application Software Version 1.4

## Use Cases

None for Cloud

## Threats

T.NETWORK\_ATTACK  
T.NETWORK\_EAVESDROP  
T.LOCAL\_ATTACK  
T. PHYSICAL\_ACCESS

## Assumptions

A.PLATFORM (+ time clock)  
A.PROPER\_USER  
A.PROPER\_ADMIN

## Security Objectives for the TOE

O.INTEGRITY  
O.QUALITY  
O.MANAGEMENT  
O.PROTECTED\_STORAGE  
O.PROTECTED\_COMMS

## Security Objectives for the Operational Environment

OE.PLATFORM  
OE.PROPER\_USER  
OE.PROPER\_ADMIN

## Security Objectives for the Operational Environment

OE.PLATFORM  
OE.PROPER\_USER  
OE.PROPER\_ADMIN

# Protection Profile for Application Software Version 1.4

## Use Cases

None for Cloud

## Threats

T.NETWORK\_ATTACK  
T.NETWORK\_EAVESDROP  
T.LOCAL\_ATTACK  
T. PHYSICAL\_ACCESS

## Assumptions

A.PLATFORM (+ time clock)  
A.PROPER\_USER  
A.PROPER\_ADMIN

## Security Objectives for the TOE

O.INTEGRITY  
O.QUALITY  
O.MANAGEMENT  
O.PROTECTED\_STORAGE  
O.PROTECTED\_COMMS

## Security Objectives for the Operational Environment

OE.PLATFORM  
OE.PROPER\_USER  
OE.PROPER\_ADMIN

# Appendix B. Analysis of the Assumptions and Security Objectives of the Operating Environment for an example stack of PP's

As a way of gaining understanding of how existing PP's may work within the cloud environment, a 'composition stack' of PP's is considered.

As an example,

An Application,

**(PP for Application Software)**

or Network Device

**(Network Device cPP)**

running on an Operating System,

**(PP for General Purpose Operating System)**

running in a VM,

**(Base PP for Virtualization)**

on a Server.

**(PP for General Purpose Computing Platform)**

It can be observed that for each PP higher in the stack, it may rely on security services that may or may not be provided by PP's lower in the stack. It can also generally be observed that the 'Platform' for any PP tends to be PP immediately below in the stack.

# Appendix B. Analysis of the Assumptions and Security Objectives of the Operating Environment for an example stack of PP's

As a way of gaining understanding of how existing PP's may work within the cloud environment, a 'composition stack' of PP's is considered.

As an example,

An Application,

**(PP for Application Software)**

or Network Device

**(Network Device cPP)**

running on an Operating System,

**(PP for General Purpose Operating System)**

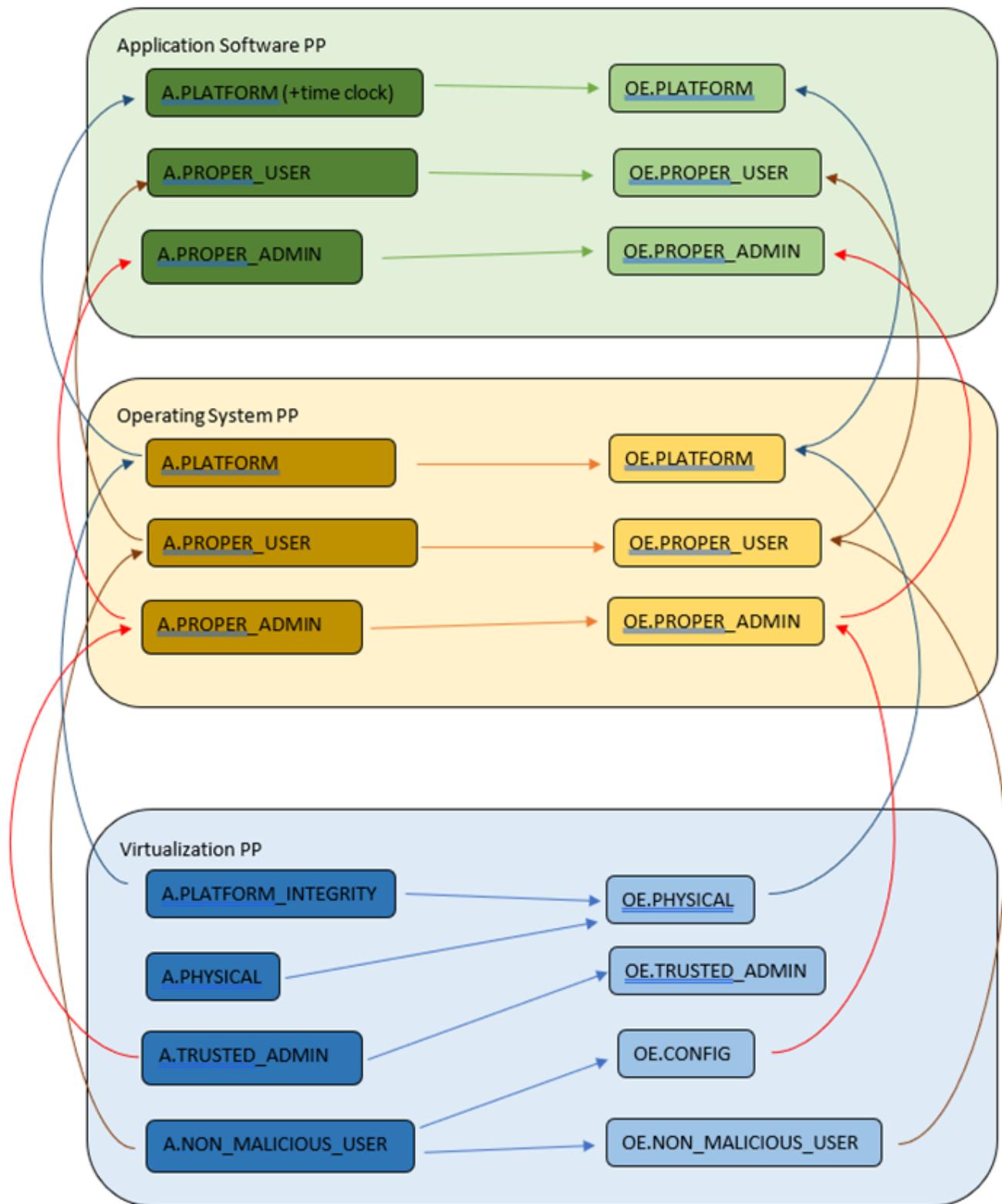
running in a VM,

**(Base PP for Virtualization)**

on a Server.

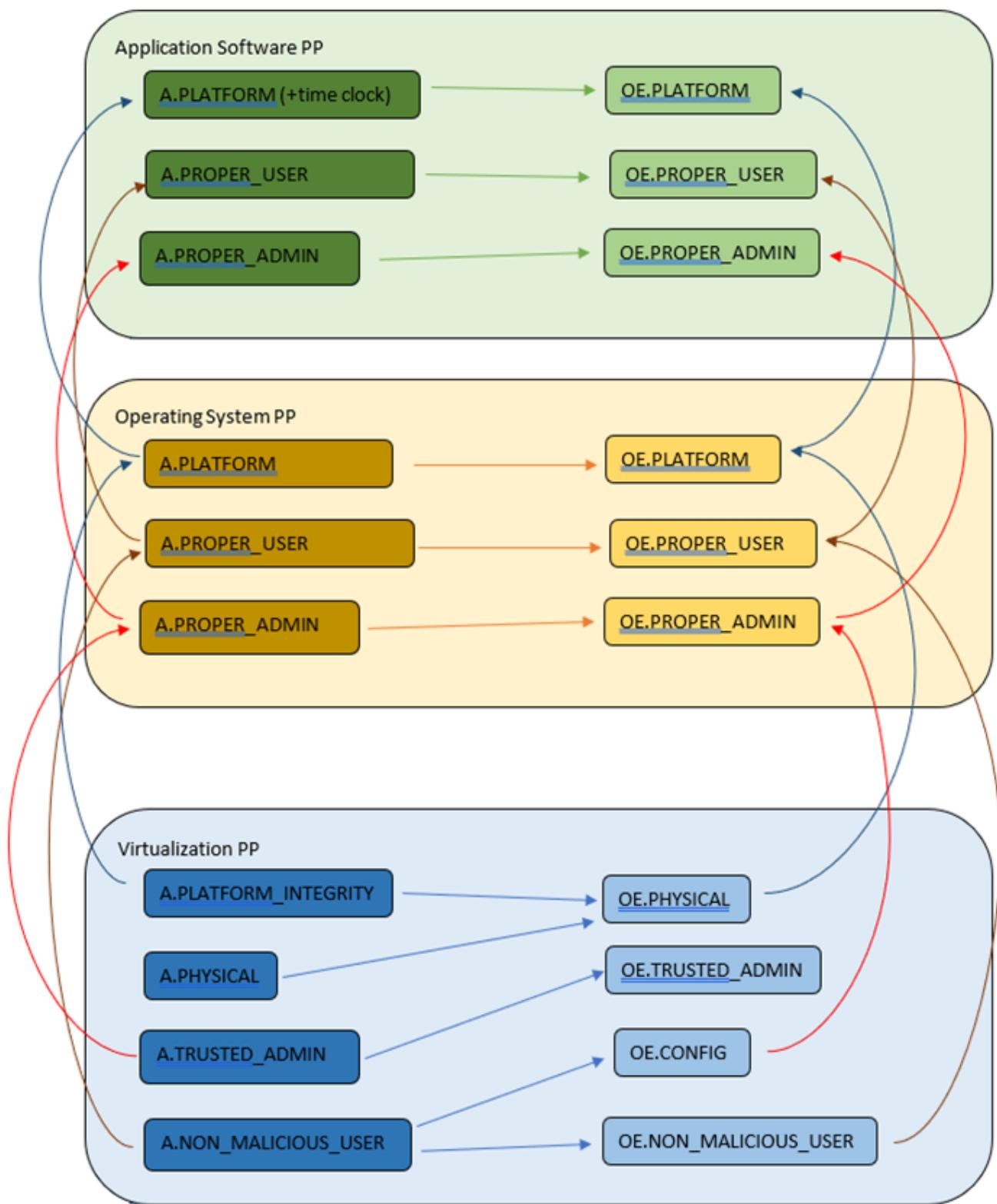
**(PP for General Purpose Computing Platform)**

It can be observed that for each PP higher in the stack, it may rely on security services that may or may not be provided by PP's lower in the stack. It can also generally be observed that the 'Platform' for any PP tends to be PP immediately below in the stack.



The assumptions and Security Objectives of the Operating Environment for the three PP's map in this example map well to each other. There are generally only three categories: Platform Integrity, Proper (Non-Malicious User) and Proper (Trusted) Admin. The virtualization PP considers also Physical Security but this not considered by the other PP's.

In the context of these PP's, where the assurance level is low (no development security requirements, vulnerability requirements at AVA\_VAN.1: public search), the assumptions and Security Objectives of the Operating Environment should be sufficiently satisfied by any suitable cloud security certification process recognized by a national government supporting Common

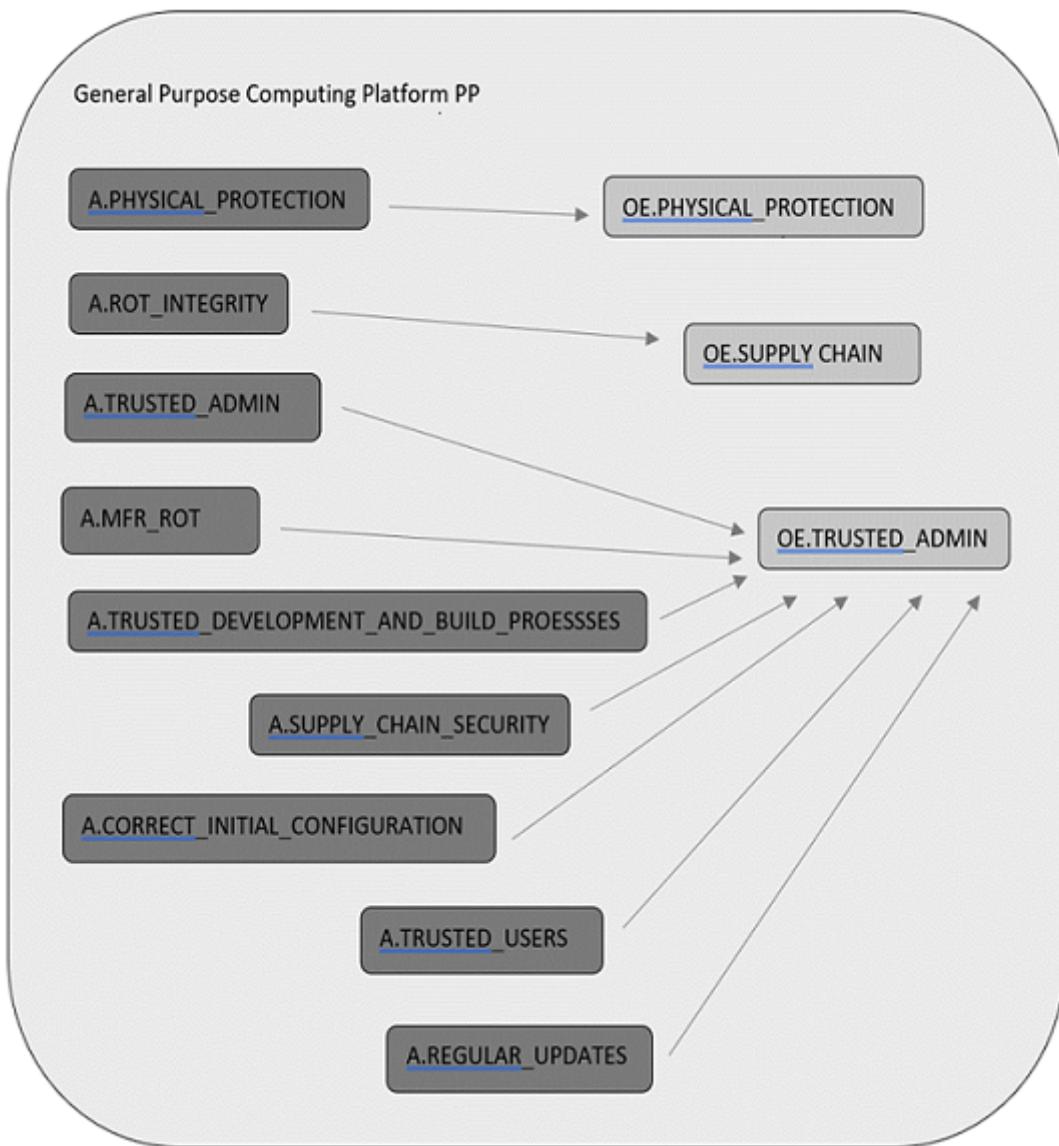


The assumptions and Security Objectives of the Operating Environment for the three PP's map in this example map well to each other. There are generally only three categories: Platform Integrity, Proper (Non-Malicious User) and Proper (Trusted) Admin. The virtualization PP considers also Physical Security but this not considered by the other PP's.

In the context of these PP's, where the assurance level is low (no development security requirements, vulnerability requirements at AVA\_VAN.1: public search), the assumptions and Security Objectives of the Operating Environment should be sufficiently satisfied by any suitable cloud security certification process recognized by a national government supporting Common

Criteria that addresses the environment being used. (e.g. lowest level Fedramp, BSI C5 baseline, ISO27017).

If the General Purpose Computing Platform PP is adopted by vendors for cloud infrastructure, then this could be added to the model since it is a number of additional assumptions around root-of-trust and supply chain security that could provide additional assurance.



Criteria that addresses the environment being used. (e.g. lowest level Fedramp, BSI C5 baseline, ISO27017).

If the General Purpose Computing Platform PP is adopted by vendors for cloud infrastructure, then this could be added to the model since it is a number of additional assumptions around root-of-trust and supply chain security that could provide additional assurance.

