

Enclave Overview

Automation with Human Insight

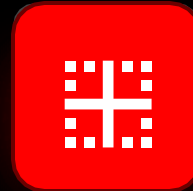


What is an Enclave in CMMC?

Think of it like a secure room in a building that hosts secure information where only authorized users are allowed

An enclave is not just a cloud environment – can be physical too

The cage code associated with a CUI contract will be linked to the enclave where CUI is stored, transmitted



A segregated environment with only users, apps, workloads that store, process, or transmit CUI data

Can be your CUI authorized boundary for CMMC Level 2 Certification

Benefits of CMMC Enclave



Reduce CUI footprint



Smaller the CUI footprint

- Reduced Cost
- Faster to set up
- Easier to achieve CMMC Compliance
- Simpler to maintain compliance

Common CMMC Enclaves



Azure GCC / GCCH



AWS Gov



Google GCP for
Government



Hybrid
Environment

Exploring Microsoft GCCH

Cloud Providers have invested in building FedRAMP compliant clouds authorized to handle CUI securely

Common Government Cloud Options from Microsoft

- **GCC** – Government Community Cloud
- **GCCH** – Government Community Cloud High

Microsoft cloud will vary on the IT services

- O365
- Azure Computing Environment – VM's, Storage, Kubernetes, SQL database, App Services, etc.

GCC

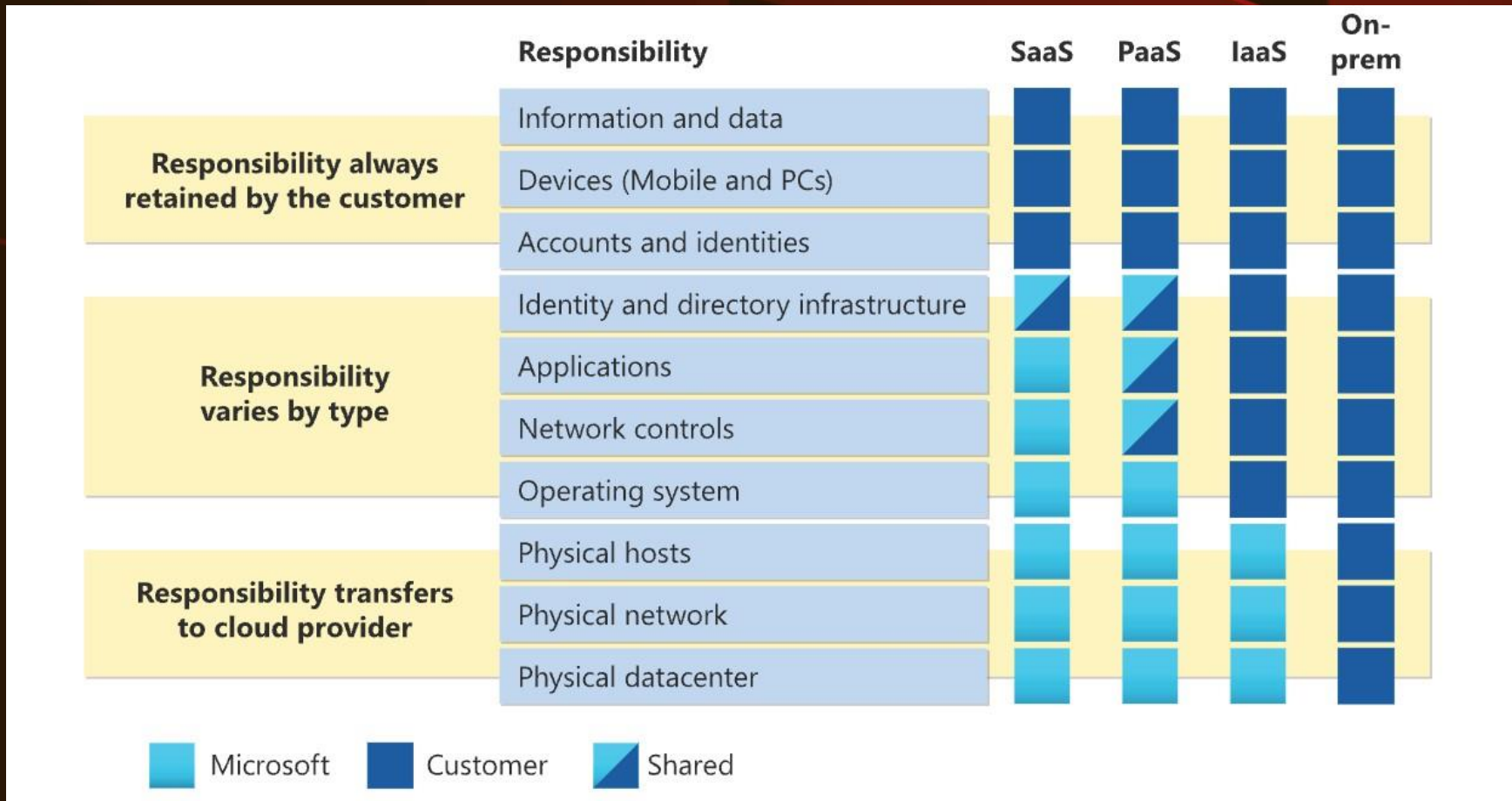
- Identical to a commercial environment except that Government data is segregated
- Less inherited controls

VS

GCCH

- Hosted in the United States and is authorized to handle ITAR data
- More inherited controls

Shared Responsibility Model



Scan to Download

FedRAMP Body of Evidence – O365 & Azure



CIS - Control Implementation Summary: report includes control implementation responsibility and implementation status of the FedRAMP security controls.

CRM - Customer Responsibility Matrix: An excel file included in the CIS that identifies what controls are inherited from the cloud service provider (CSP) versus what controls you own (the customer), and which controls are shared between the 2 of you.

SAR - The Security Assessment Report: generated by the 3PAO during the annual assessment.

SAP - The Security Assessment Plan: lists scope and security controls selected for annual assessment by the 3PAO.

Penetration Testing Report: Cloud penetration testing report produced by Azure FedRAMP High and DoD SRG compliance program.

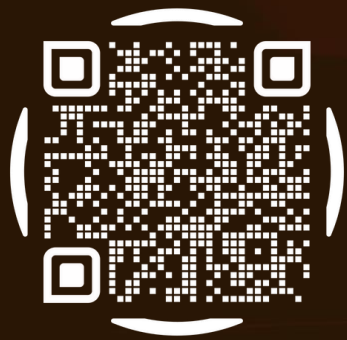
Accessing the FedRAMP Body of Evidence

Service Trust Portal (STP)

The Service Trust portal has the BoE for Azure Commercial and for Office 365 GCC.

Government BoE

The Government BoE is considered highly sensitive and confidential information. Microsoft will allow customers to access under an NDA.



Scan Me

Request the BoE, you must be a customer. Send an email request to:



Office 365 GCC High: O365FedRAMP@microsoft.com

Azure Government: AzFedDoc@microsoft.com

Thank You.



Powered by Aprio[®]