Physical Security

Cloud service provider must enforce the physical security as per the ISO27001 controls and it must be implemented and followed in a professional manner and the detailed control mapping is mentioned in the Annex A.

In a cloud environment, Individual entity environments should be physically and administratively separate from each other.

Customers utilizing a public or otherwise shared cloud must ensure that their environments are adequately isolated from the other cloud tenants.

In addition to enforcing separation between Customer environments, segmentation may also be recommended within a Customer’s environment to isolate its sensitive servers as per ISO 27001 and cloud security alliance standards.

Segmentation on a cloud computing infrastructure must provide a level of isolation equivalent to that feasible through physical network separation.

Proper mechanism and process should be in place to ensure appropriate isolation may be required at the network, operating system and application layers; and most importantly, there should be guaranteed isolation of data that is stored.

Cloud tenant environments must be isolated from each other such that they can be considered separately managed entities with no connectivity between them.

Providers should test segmentation between all entities within their control at least biannually and demonstrate results.

Any systems or components shared by the Customers in multi-tenant environments, including the Hypervisor and underlying systems, must not provide an access path between environments.

The cloud service provider needs to take ownership of the segmentation between Customers and verify that it is effective and provides adequate isolation between individual Customer environments.

The cloud service provider must ensure the segmentation between customer environments and the Provider’s own environment, and between client environments and other untrusted environments.

The Customer is responsible for the proper configuration of any segmentation controls implemented within its own environment and for ensuring that effective isolation is maintained components.

Cloud services involve physical resources located within the Provider environment (including DR Infrastructure) that are accessed remotely from the Customer’s environment.

Physical security controls need to be implemented which will protect the provider’s infrastructure as well
as the customer infrastructure.

Cloud service provider ensure the segmentation where Cloud service Providers shared clouds provide services to multiple Customers whose data and virtual components co-exist in the same physical location and are managed by the same physical systems as those of other Customers.

Revision #1
Created 6 October 2025 09:39:28 by RISA
Updated 6 October 2025 09:39:51 by RISA