Network and Infrastructure Security

Cloud service provider must enforce the network 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.

Cloud service provider must ensure the network security by implementing either virtual or physical firewall network segmentation at the infrastructure level and the firewalls at the hypervisor and VM level.

Cloud service provider must ensure the network segmentation by implementing either virtual or physical switch with the provision of VLAN tagging or zoning in addition to firewalls.

Cloud service provider must ensure the implementation of Intrusion prevention systems at the hypervisor level, VM level or both, to detect and block unwanted traffic.

A segmented cloud environment exists when the Provider enforces isolation between Customers in multitenant environments. Environments where Customers run their applications in separate logical partitions using separate database management system images and do not share disk storage or other resources.

As per ISO 27001 and cloud security alliance standards, the environments where organizations use the same application image on the same server and are only separated by the access control system of the operating system or the application.

Strong, two - factor authentication should be implemented as per ISO 27001 standards and cloud security alliance standards.

Virtualized servers that are individually dedicated to a particular Customer, including any virtualized storage such as Storage Area Networks (SANs), Network Attached Storage (NAS) or virtual database servers.

Environments where organizations use different images of an application on the same server and are only separated by the access control system of the operating system or the application.

Revision #1
Created 6 October 2025 09:40:01 by RISA
Updated 6 October 2025 09:40:20 by RISA