Security and Compliance

Proactive testing, identification and mitigation of vulnerabilities are an important part of achieving and maintaining compliance ISO 27001 and cloud security alliance standards that utilize cloud services and systems.

Cloud service provider must ensure that the proper controls requirements is in place to protect the Data
Breaches, unavailability, Account hijacking, malicious code.

There are six distinct areas of vulnerability management: web application vulnerability testing, internal network vulnerability scanning, external network vulnerability scanning, external penetration internal penetration testing and segmentation testing and Scoping is a critical element of vulnerability management.

Customers need to ensure that they have properly identified all in - scope systems and services, including those provided by the Provider, those for which the Customer and Provider have shared responsibility and those that fall uniquely to the Customer (e.g., on - premises, private cloud, hybrid systems, or applications or systems that the Customer maintains). Penetration testing is used to confirm segmentation controls intended to constrain scope, and to proactively identify vulnerabilities that could be exploited to allow an attacker to breach these boundaries.

Testing vulnerabilities in the cloud also requires an in - depth understanding of the cloud deployment model to determine responsibility when it comes to performing the appropriate testing exercise.

It is critical to understand the aspects of the environment that will be tested by the Provider and those that will be required to be tested by the Customer. It is not enough to identify responsibility by physical system, as each entity may have distinct or shared responsibility for aspects of a physical system (e.g., physical hardware, hypervisor, guest OS, application, configuration).

These responsibilities will vary depending on cloud service delivery model (i.e., IaaS, SaaS, and PaaS) or other division of control.

Where shared responsibility exists for vulnerability testing activities, the Customer and Provider should cooperate to ensure that these tests are performed, and vulnerabilities are resolved. It is ultimately the Customer’s responsibility to provide evidence that all required tests have been performed.

All public - facing web applications must be protected, either by deploying an automated technical solution that detects and prevents web - based attacks or by employing application vulnerability security testing in accordance with ISO 27001 control requirements.

If a Provider is providing a web application, the application should be either protected by a web application Firewall (or similar solution) or tested by the Provider. Providers that expose APIs

to their Customers should also perform testing and reporting on those APIs.

If it is the Customer’s hosting web application, the customer should perform the web application vulnerability security testing as part of its ISO27001 and cloud security alliance standards.

Providers should recognize this requirement and support these required testing activities (e.g., by supporting the ability to disable controls that would impede controlled testing, by supporting applications that may perform these operations or offering a service to perform these services).

Revision #1
Created 6 October 2025 09:40:50 by RISA
Updated 6 October 2025 09:41:16 by RISA