Cloud Security
Compliance

pyxis

Pyxis Cloud Security Compliance

Today the corporate environment often requires quality depth and different standards to comply with regulations on the business they develop, for example, PCI-DSS, HIPAA, and SOX. These requirements are focused on the protection of information assets, so it is necessary to add an additional specific analysis to good cloud security practices.

The Compliance service (CSC) includes Approach (CSA) and Deployment (CSD) services and complements them from the beginning considering compliance with the standard that the client requires.

CSC allows explicit confirmation of compliance with the norm or standard through the execution of tests on the solutions to be certified.

- Cloud Security Approach
- Cloud Security Deployment

The phases of the Compliance services are described below :

Scope and Standard
The first phase that must be established is the required regulatory framework (standard to be met) and the scope that it will have in the customer's new Cloud infrastructure. Compliance is generally applied to information assets in relation to the standard that is followed, therefore in this phase the scope of compliance of the solutions to be deployed in the new infrastructure must be agreed upon with the customer.

Compliance
The second phase of this service is the empirical confirmation of compliance with the standard, in the implemented infrastructure with the operational solutions. For this, configuration check activities, accesses, and important procedures for the audit processes will be carried out.

Microsoft Partner

Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions

Powered By:

View in:
Azure Marketplace

More Information:
www.pyxis.com.uy/cloud-security