How Data Compliance in the Cloud Happens

By Greg Smith

As the current work from home paradigm motivates organizations to move all or part of their infrastructure to the cloud, data compliance in the cloud becomes a critical concern.

> *Is our data safe from unauthorized access and disclosure in the cloud? Are we in compliance with all the government and industry regulations?*

Answering these questions means looking at both cloud data center compliance and the organizational processes and controls relating to data stored in the cloud.

Data Center Compliance

"Who can access our data in the cloud?" is a valid question. Organizations want to be sure that their data is seen only by those they designate and not by unauthorized technicians, data center employees or others.

Fortunately, the major public cloud companies provide well-documented control over their physical data center infrastructure and over the people that access it. From an auditing and physical access perspective, data center compliance is covered.

Organizational Compliance in the Cloud

On the other hand, organizations still must control logical access to their own data. It's not much different than if the data center were located on-site. How you handle information governance (IG), data backup, data deletion and retention, and access controls has much more of a bearing on data compliance that the physical location of the data.

Indeed, bad actors have a much better chance of hacking your data through front-end access points within the organization using social engineering and stolen passwords than from a back-end attack on the cloud data center.

> *Put another way, compliance in the cloud is your responsibility.*

Happily, cloud providers like Microsoft provide access to all the tools necessary to achieve ongoing compliance. Then, it becomes a matter of your configuration and setup of the appropriate front-end data access, storage, sharing and retention controls. Multi-factor authentication serves as a good example.

Cloud Compliance Laws

No laws prevent organizations from adopting the cloud. However, moving data to the cloud does have a significant impact on compliance. For example, it is important to know in which countries your data will be processed, which local laws apply, and how they impact your data. Then the organization should pursue a risk-based approach to comply with the regulations.

With a variety of laws, like data protection regulations, data localization and data sovereignty laws, and government access to information provisions, laws in many countries could apply. Organizations also need to know which security measures are required.

Cloud Compliance Tools

Those with compliance responsibilities should take the time necessary to become familiar with the tools. Resources such as the Microsoft 365 Compliance Center, show users how their organization is doing with data compliance, what solutions are available, and a summary of any active alerts.

From the Microsoft 365 Compliance Center users can:

- Review the **Microsoft Compliance Manager** solution. Compliance Manager helps simplify the way organizations manage compliance. It calculates a risk-based score measuring their progress toward completing recommended actions that help reduce data protection and regulatory risks.
- Review **integrated solutions** to help manage end-to-end compliance scenarios. A solution's capabilities and tools might include a combination of policies, alerts, reports, and other controls.
- Review **Active alerts**, including a summary of the most active alerts and view more detailed information, such as severity, status, and category.
- **Customize the view** with information showing the organization's cloud app compliance, data about users with shared files, or other tools to explore data.

Microsoft offers a comprehensive set of compliance offerings related to both Microsoft 365 and Azure Cloud solutions. They help organizations comply with national, regional, and industry-specific requirements governing the collection and use of data.

The Microsoft offerings to aid compliance in the cloud are listed and accessible by global, US government, regional and industry regulations such as ISO 9001, CJIS, GDPR, and PCI DSS.

Compliance in the Cloud Next Steps

To improve compliance in the cloud, Microsoft recommends that organizations:

- Visit the **Microsoft Compliance Manager** to see their compliance score and start managing compliance for the organization.
- Configure **insider risk management policies** to help minimize internal risks and enable managers to detect, investigate, and act or risky activities within the organization.
- Review the organization's **data loss prevention policies** and make changes as necessary.
- Get acquainted with and set up **Microsoft Cloud App Security**.
- Learn about and create **communication compliance policies** to quickly identify and remediate corporate code-of-conduct policy violations.
- Visit the **Microsoft 365 Compliance Center** often, and make sure to review any alerts or potential risks that arise. Go to https://compliance.microsoft.com and sign in.

Azure Cloud Training

The current work from home environment has required organizations to move all or part of their infrastructure to the Cloud. Hence, training in the Azure Cloud environment is in big demand.

Interested parties may join an upcoming eMazzanti Technologies’ Azure Customer Immersion Experience (CIE) for valuable Azure education.

Attendees will walk through a virtual tour of the Azure Portal and receive hands-on training on Windows Server Data Center. They’ll learn how to deploy virtual machines, create availability sets and resource groups, understand Azure disk storage and more.

Working with Microsoft Certified CIE Facilitators, each attendee gets their own Azure Tennant to work through creating their cloud environment in Azure.