Understanding the implications of not independently backing up and archiving your Microsoft 365 data in the cloud

We believe that moving to the cloud has numerous benefits, however we have noticed that the **"Shared Responsibility Model"** has caught out a number of our Clients with regards to their own data management. We therefore produced this infosheet to help you locate the relevant information in your **Microsoft Service Agreement** with regards to data responsibilities and roles when using **Microsoft Cloud Services,** for example the Backup and Archiving of M365 and Azure.

Weblinks to full content:

1. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
2. https://www.microsoft.com/en-us/servicesagreement
3. https://azure.microsoft.com/en-gb/resources/shared-responsibility-for-cloud-computing/

Extracted content:

1 Microsoft Service Agreement

Section 6b

"*We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services*."

2 Shared Responsibility in the Cloud

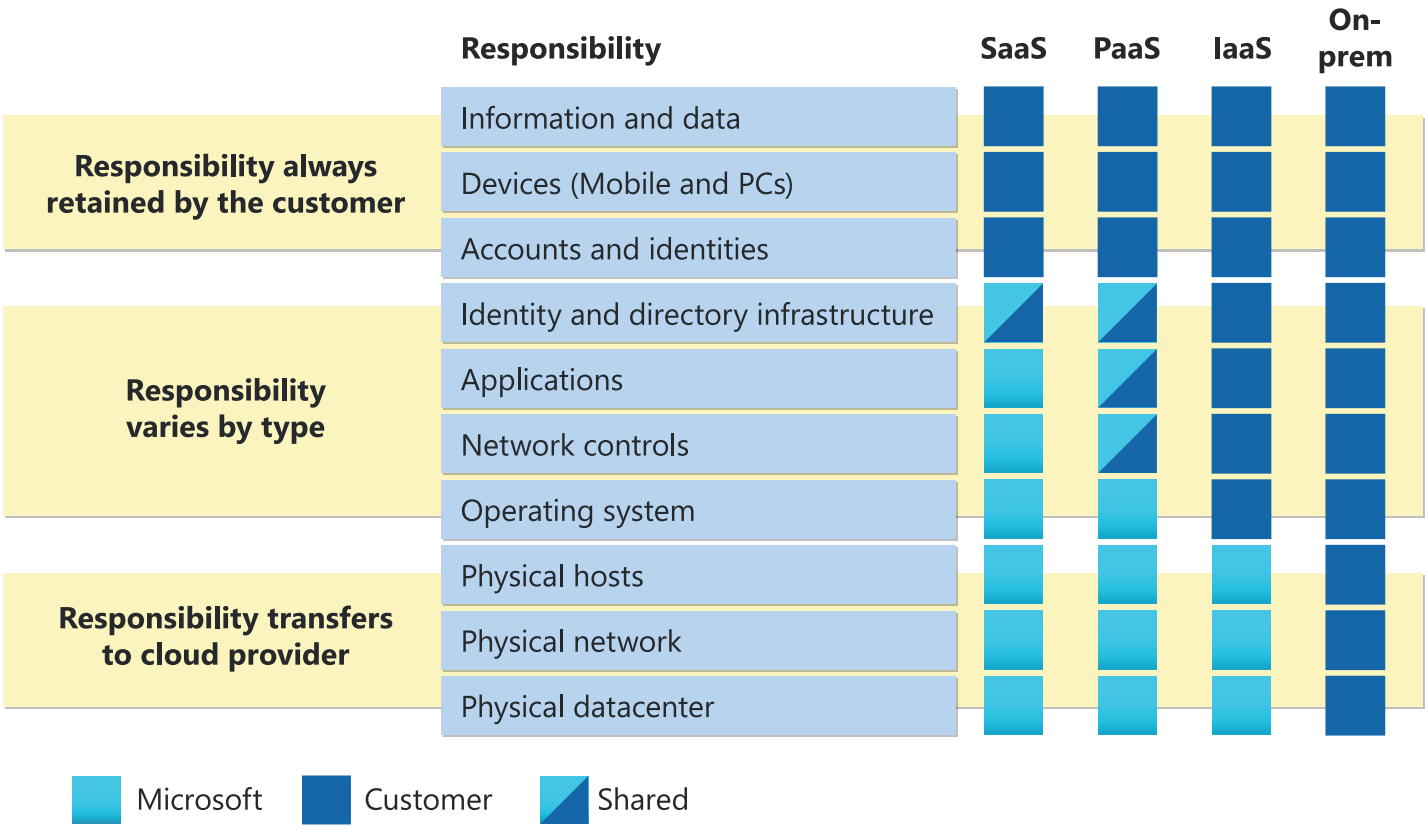
As you consider and evaluate public-cloud services, it's critical to understand the shared responsibility model: which security tasks are handled by the cloud provider and which tasks are handled by you. The workload responsibilities vary depending on whether the workload is hosted on Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) or within an on-premise data centre.

Division of responsibility

In an on-premise data centre, you own the whole stack. As you move to the cloud some responsibilities transfer to Microsoft. **The diagram overleaf** illustrates the areas of responsibility between you and Microsoft, according to the type of deployment of your stack.

For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources and the cloud components you control (which varies by service type). Regardless of the type of deployment, the following responsibilities are **always** retained by you:

- **Data**
- **Endpoints**
- **Account**
- **Access Management**



3 Shared Responsibilities for Cloud Computing

Conclusion

For on-premise solutions, the customer is both accountable and responsible for all aspects of security and operations:

- **For IaaS solutions**, the elements such as buildings, servers, networking hardware, and the hypervisor should be managed by the platform vendor. The customer is responsible or has a shared responsibility for securing and managing the operating system, network configuration, applications, identity, clients, and data.
- **For PaaS solutions built on IaaS deployments**, the provider is additionally responsible to manage and secure the network controls. The customer is still responsible or has a shared responsibility for securing and managing applications, identity, clients and data.
- **For SaaS solutions**, a vendor provides the application and abstracts customers from the underlying components. Nonetheless, the customer continues to be accountable; they must ensure that data is classified correctly and share a responsibility to manage their users and endpoint devices.

The importance of understanding this shared responsibility model is essential for customers who are moving to the cloud. Cloud providers offer considerable advantages for security and compliance efforts, but these advantages do not absolve the customer from protecting their users, applications and service offerings.

TO GET STARTED ON YOUR CLOUD BACKUP JOURNEY:

CLICK HERE FOR MORE INFORMATION ABOUT CLOUDLAKE® SAAS BACKUP

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. sales@autodata.co.uk