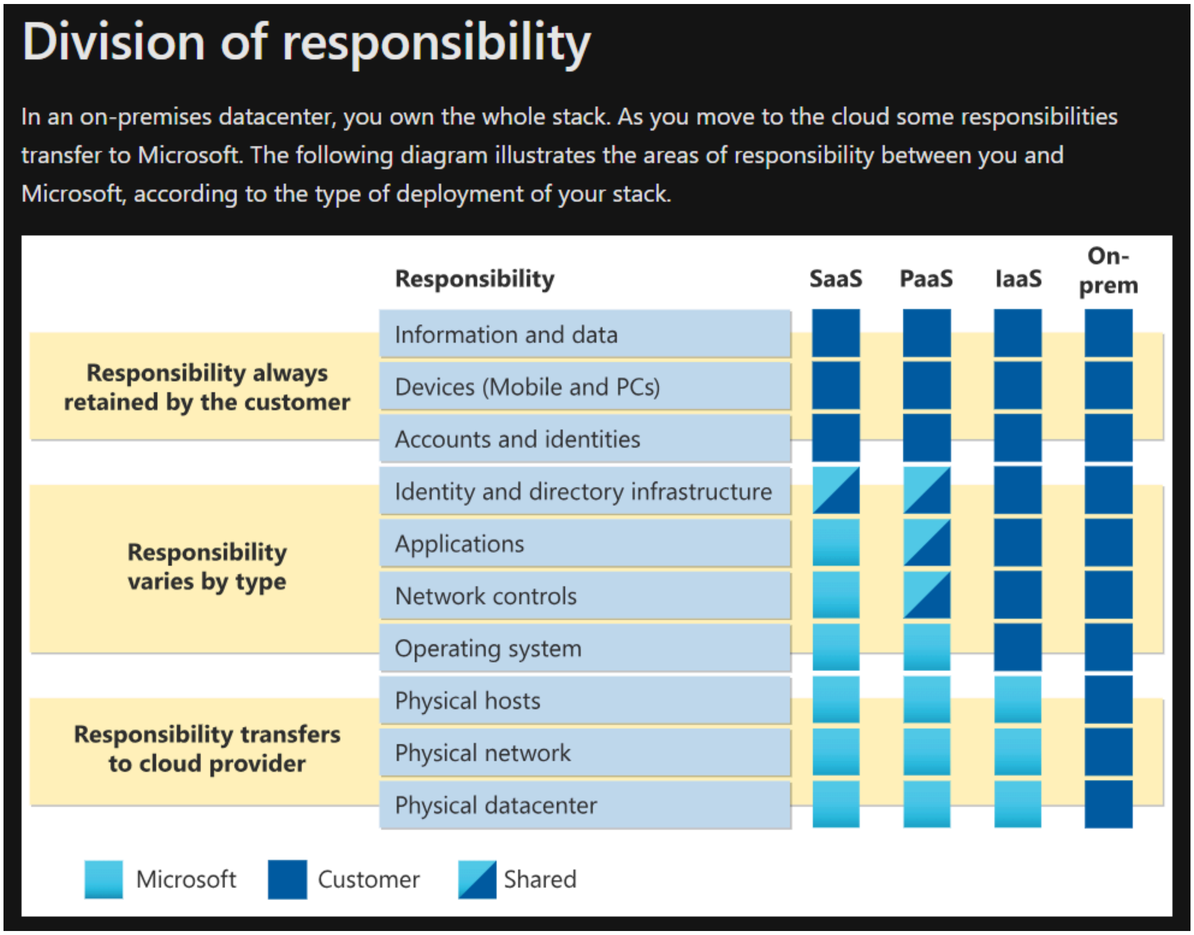
Shared Responsibility

Shared responsibility for a PaaS application is shown in this chart distributed by Microsoft.

-



Division of responsibility

In an on-premises datacenter, you own the whole stack. As you move to the cloud some responsibilities transfer to Microsoft. The following diagram illustrates the areas of responsibility between you and Microsoft, according to the type of deployment of your stack.

	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

The responsibility elements in the diagram constitute an integrated system. The parts rely on one another for reliability and security. An auditor would need to understand which control groupings are assigned to the client or the cloud vendor. Further, the client needs to understand how to configure its controls to avoid cloud vulnerabilities. The characterizations on this chart suggest that some network controls are managed by the cloud provider while others are managed by the client. As noted in an appendix, some other PaaS shared responsibility diagrams divide things differently, for example assign “all” network controls to the cloud provider.

The reality for BigU, and for most medium to large organizations, is that special connections are made into and out of the PaaS environment. To facilitate protected administrative access and because of interactions with other systems, most client organizations need to have some solid network controls in place if the PaaS environment is to be secure. This illustrates an important reality for an IT auditor assigned to provide assurance that controls over cloud systems are effective. They need to understand the client’s use of a cloud platform so that they can see if management assertions about the effectiveness of controls are true. Numerous impactful incidents have happened when a client uses a well-regarded cloud provider but fails to properly secure relevant controls on the client side.