





### 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 BACKUP JOURNEY [PLEASE CLICK HERE](#) TO ACCESS OUR CLOUDLAKE PLATFORM WITH INTEGRATED BACKUP SOLUTIONS.**