


CISO cloud readiness guide

10/03/2018 • 3 minutes to read • Contributors 

In this article

[How can a CISO prepare for the cloud?](#)

[Resources for the Chief Information Security Officer](#)

[Next steps](#)

Microsoft guidance like the Cloud Adoption Framework is not positioned to determine or guide the unique security constraints of the thousands of enterprises supported by this documentation. When moving to the cloud, the role of the chief information security officer or chief information security office (CISO) isn't supplanted by cloud technologies. Quite the contrary, the CISO and the office of the CISO, become more engrained and integrated. This guide assumes the reader is familiar with CISO processes and is seeking to modernize those processes to enable cloud transformation.

Cloud adoption enables services that weren't often considered in traditional IT environments. Self-service or automated deployments are commonly executed by application development or other IT teams not traditionally aligned to production deployment. In some organizations, business constituents similarly have self-service capabilities. This can trigger new security requirements that weren't needed in the on-premises world. Centralized security is more challenging. Security often becomes a shared responsibility across the business and IT culture. This article can help a CISO prepare for that approach and engage in incremental governance.

How can a CISO prepare for the cloud?

Like most policies, security and governance policies within an organization tend to grow organically. When security incidents happen, they shape policy to inform users and reduce the likelihood of repeat occurrences. While natural, this approach creates policy bloat and technical dependencies. Cloud transformation journeys create a unique opportunity to modernize and reset policies. While preparing for any transformation journey, the CISO can create immediate and measurable value by serving as the primary stakeholder in a [policy review](#).

In such a review, the role of the CISO is to create a safe balance between the constraints of existing policy/compliance and the improved security posture of Cloud providers. Measuring this progress can take many forms, often it is measured in the number of security policies that can be safely offloaded to the cloud provider.

Transferring security risks: As services are moved into infrastructure as a service (IaaS) hosting models, the business assumes less direct risk regarding hardware provisioning. The risk isn't removed, instead it is transferred to the cloud vendor. Should a cloud vendor's approach to hardware provisioning provide the same level of risk mitigation, in a secure repeatable process, the risk of hardware provisioning execution is removed from corporate IT's area of responsibility and transferred to the cloud provider. This reduces the overall security risk corporate IT is responsible for managing, although the risk itself should still be tracked and reviewed periodically.

As solutions move further "up stack" to incorporate platform as a service (PaaS) or software as a service (SaaS) models, additional risks can be avoided or transferred. When risk is safely moved to a cloud provider, the cost of executing, monitoring, and enforcing security policies or other compliance policies can be safely reduced as well.

Growth mindset: Change can be scary to both the business and technical implementors. When the CISO leads a growth mindset shift in an organization, we've found that those natural fears are replaced with an increased interest in safety and policy compliance. Approaching a [policy review](#), a transformation journey, or simple implementation reviews with a growth mindset, allows the team to move quickly but not at the cost of a fair and manageable risk profile.

Resources for the Chief Information Security Officer

Knowledge about the cloud is fundamental to approaching a [policy review](#) with a growth mindset. The following resources can help the CISO better understand the security posture of Microsoft's Azure platform.

Security platform resources:

- [Security Development Lifecycle, internal audits](#)
- [Mandatory security training, background checks](#)
- [Penetration testing, intrusion detection, DDoS, audits, and logging](#)
- [State-of-the-art datacenter, physical security, secure network](#)
- [Microsoft Azure Security Response in the Cloud \(PDF\)](#)

Privacy and controls:

- [Manage your data all the time](#)
- [Control on data location](#)
- [Provide data access on your terms](#)
- [Responding to law enforcement](#)
- [Stringent privacy standards](#)

Compliance:

- [Microsoft Trust Center](#)
- [Common controls hub](#)
- [Cloud Services Due Diligence Checklist](#)
- [Compliance by service, location, and industry](#)

Transparency:

- [How Microsoft secures customer data in Azure services](#)
- [How Microsoft manages data location in Azure services](#)
- [Who in Microsoft can access your data on what terms](#)
- [How Microsoft secures customer data in Azure services](#)
- [Review certification for Azure services, transparency hub](#)

Next steps

The first step to taking action in any governance strategy, is a [policy review](#). [Policy and compliance](#) could be a useful guide during your policy review.

[Prepare for a policy review](#)