

Azure successfully completed a formal assessment by the Motion Picture Association of America.

Microsoft and MPAA

Microsoft Azure was the first hyperscale, multitenant cloud service to successfully complete a formal assessment by independent MPAA auditors and comply with all three of the MPAA content security best practices frameworks: Common, Application, and Cloud Security Guidelines.

The MPAA assessment covers 48 security topics in the Common Guidelines, and an additional six in the Application and Cloud Security Guidelines. These are built on industry-accepted security standards such as ISO/IEC 27001 and NIST 800-53, and are aligned to best practices, such as the Cloud Security Alliance (CSA) Cloud Controls Matrix.

The formal assessment of Azure compliance means that companies who do business with major studios can use Azure to help reduce the IT costs that are normally associated with the secure creation, management, storage, and distribution of content—all while complying with MPAA requirements. Azure Media Services, Storage, Virtual Networks, and more than 30 other services provide a content workflow engine in the cloud that is more secure and scalable than traditional on-premises production processes and more effective at protecting media assets downstream.

Microsoft in-scope cloud services

- Azure
[Learn more](#)

Audits, reports, and certificates

- [Azure MPAA Common Guidelines](#)
- [Azure MPAA Application and Cloud Security Guidelines](#)

How to implement

- [Azure Media Services overview](#)
Quickstarts, tutorials, and how-to guides help you get started with version 3.
[Learn more](#)

About MPAA

The [Motion Picture Association of America](#) (MPAA) provides best practices guidance and control frameworks to help major studio partners and vendors design infrastructure and solutions to ensure the security of digital film assets. The MPAA also performs content security assessments on behalf of its member companies: Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc.

Frequently asked questions

How can I get copies of Microsoft responses to the MPAA audit?

The [Service Trust Portal](#) provides access to Microsoft responses to the Common Guidelines and the Application and Cloud Security Guidelines. You can also review copies of the Azure ISO/IEC 27001 Audit Report and the CDSA CPS Audit Report and Statement of Applicability in the portal.

Why is the MPAA important?

Content security is critical for feature film development, as there are multiple points along the workflow where digital assets could be compromised or stolen. Dailies, rough cuts, and visual effects are just some of the materials exposed during a normal production cycle, and the box office impacts of a security breach on a blockbuster project can reach tens of millions of dollars.

MPAA guidelines provide major studio vendors and partners with a set of best practices for creating, processing, storing, and distributing digital assets. Service providers such as Azure who undergo the formal assessment can provide an additional layer of assurance that content uploaded to the cloud will be managed in accordance with established industry requirements for encryption, authentication, access control, and resiliency, among others.

Does my organization still need to undergo an MPAA audit, or can we just use the Azure audit?

Production facilities, visual effects houses, and other service partners should work with their executive producers and directors to understand the new security requirements, and whether a formal MPAA audit is necessary. Compliance with MPAA guidelines is voluntary, but Microsoft elected to carry out an independent assessment so that media customers can be confident in the content security and protection capabilities of Azure. However, Azure does not manage the individual cloud environments of customers, which may be subject to additional MPAA regulation that is best addressed by your own audit of your environment.

Additional resources

- [MPAA Common Guidelines](#)
- [MPAA Application and Cloud Security Guidelines](#)
- [Microsoft and CSA STAR Self-Assessment](#)
- [Azure Responses to CSA CAIQ v3.0.1](#)