Microsoft 365 Compliance Licensing Comparison

©2020 Microsoft Corporation. All rights reserved. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. Some information relates to pre-released

Note: A dot (●) indicates that the rights to benefit from the feature are specifically conveyed through the license. Microsoft 365 E5 Compliance, Microsoft 365 E5 Information Protection and Governance, Microsoft 365 E5 Insider Risk Management, and Microsoft 365 E5 eDiscovery and Audit are supplemental (add-on) licenses that have pre-requisite license requirements and convey only the rights to benefit from advanced (E5) features only, and not the rights to benefit from underlying features (e.g. Microsoft 365 E3 features), which must be licensed separately.

Solution	Feature	Microsoft 365 E5[1]	Microsoft 365 E5 Compliance[2] (See footnote 2	Microsoft 365 E5/A5 Info Protection & Governance[3]	Microsoft 365 E5 Insider Risk Management[4]	Microsoft 365 E5 eDiscovery and Audit[4]	Microsoft 365 E3	Microsoft 365 F3	Microsoft 365 F1	Microsoft 365 F2	Office 365 E5	Office 365 E3	Office 365 E1	Office 365 F3	Office 365 Advanced Compliance	Office 365 Data Loss Prevention (DLP)	Exchange Online Archiving	Enterprise Mobility + Security (EMS) E5	EMS E3	Azure Info Protection (AIP) Plan 1	AIP Plan 2 (No longer available for new
Information Protection & Governance	Apply sensitivity labels manually in Microsoft 365 Apps (Office 365 ProPlus/Business client apps) using built-in labeling	●					●	●[3]	●[3]	●	●	●						●[3]	●[3]	●[3]	●[3]
	Apply sensitivity labels manually in Microsoft 365 Apps (Office 365 ProPlus/Business client apps) on Windows using AIP plug-in	●					●	●[3]	●[3]	●								●[3]	●[3]	●[3]	●[3]
	Apply sensitivity labels manually in Office for the Web and Office Mobile	●					●	●		●	●	●									
	Apply sensitivity labels manually for SharePoint sites, Teams, and Microsoft 365 Groups (Preview)	●					●				●[3]	●[3]									
	Apply sensitivity labels manually to data in 3rd party clouds	●					●[3]	●[3]	●[3]	●[3]								●	●[3]	●[3]	●[3]
	Apply sensitivity labels automatically in Microsoft 365 Apps (Office 365 ProPlus/Business client apps), Office for the Web, and Office Mobile based on sensitive information types	●	●	●							●				●						
	Apply sensitivity labels automatically to data in Office perpetual and SharePoint Server on-premises using AIP client (incl. AIP scanner)	●	●	●														●			●
	Apply sensitivity labels automatically to files in SPO or to EXO email (Preview)	●	●	●							●				●						
	Auto-labeling policy simulation (Preview)	●	●	●							●										
	Apply sensitivity labels automatically to data in 3rd party clouds	●	●	●														●			●[3]
	Classify data automatically based on Exact Data Match	●	●	●							●										
	Classify data automatically based on Machine Learning (trainable classifiers) (Preview)	●	●	●																	
	Enable 3rd party integration into Microsoft Information Protection (MIP) using MIP SDK	●					●	●	●	●								●	●	●	●
	Apply non-record retention labels manually	●					●	●	●	●	●	●	●	●							
	Apply a default retention label for SharePoint/Teams/OneDrive for business libraries, folders, and document sets and Microsoft 365 Groups	●	●	●							●				●						
	Apply a basic retention policy to the entire organization, specific locations or users	●					●				●	●									
	Apply retention policies automatically based on specific conditions (e.g., keywords or sensitive information)	●	●	●							●				●						
	Apply retention policies automatically based on Machine Learning (trainable classifiers)	●	●	●																	
	Apply retention policies automatically based on an event	●	●	●							●				●						
	Retention labels disposition review	●	●	●							●				●						
	Records Management (record labels, file plan manager, records versioning) (Preview)	●	●	●							●				●						
	Protection for on-premises Exchange and SharePoint content via Rights Management connector	●					●	●	●	●	●	●	●	●				●	●	●	●
	Set labels to automatically apply pre-configured S/MIME protection in Outlook	●	●	●														●			●
	Control oversharing of information when using Outlook (warn, justify or block emails)	●	●	●														●			●
	3rd-party data connectors	●	●	●							●				●						
	Preservation Lock	●	●	●							●				●						
	Email archiving	●					●			●[10]	●[3]	●[3]	●[10]				●[10]				
	Import PST	●					●				●[3]	●[3]	●[10]								
	Content and Activity Explorer (Preview)	●	●	●							●				●						
	Analytics Overview (Preview)	●					●				●	●									
	Basic Office 365 Message Encryption	●					●	●		●	●	●						●	●	●	●
	Advanced Office 365 Message Encryption	●	●	●							●				●						
	Office 365 DLP for files and email	●					●				●	●				●					
	Communication DLP (Teams chat and channel conversations)	●	●	●							●				●						
	Cloud App Security	●	●	●							●[11]							●			
	Customer Key for Office 365	●	●	●							●				●						
	Bring Your Own Key (BYOK) for customer-managed key provisioning life cycle[12]	●					●	●	●	●								●	●	●	●
	Hold Your Own Key (HYOK) that spans Azure Information Protection and Active Directory (AD) Rights Management for highly regulated scenarios (Preview)	●	●	●														●			●
Insider Risk Management	Insider Risk Management	●	●		●																
	Communication Compliance (incl. Supervision policies)	●	●		●						●				●						
	Information Barriers	●	●		●						●				●						
	Customer Lockbox	●	●		●						●				●						
	Privileged Access Management	●	●		●						●				●						
Discover & Respond	Content Search	●					●	●	●	●	●	●	●	●							
	Core eDiscovery (incl. Hold and Export)	●					●				●	●					●[11]				
	Advanced eDiscovery	●	●			●					●				●						
	Custodian management (mapping content to custodian)	●	●			●					●										
	Custodian communications	●	●			●					●										
	Deep crawling/indexing	●	●			●					●										
	Review data (query data, tags, smart tags, dashboard) and annotate (redact)	●	●			●					●										
	Analyze data (near duplicate identification, email threading, themes)	●	●			●					●										
	Non-Office 365 ingestion and processing (e.g. OCR)	●	●			●					●										
	Advanced eDiscovery Export (download, export, add to another review set)	●	●			●					●										
	Basic Audit	●					●	●	●	●	●	●	●	●							
	Advanced Audit	●	●			●					●										
Compliance Management	Compliance Manager (Preview)	●					●	●	●	●	●	●	●	●							
	Compliance Score (Preview)	●					●	●	●	●	●	●	●	●							

[1] E5 Compliance value shown. Includes additional value.

[2] Requires Microsoft 365 E3 or [Office 365 E3 + EMS E3]. All listed features with blank cells are not specifically included in Microsoft 365 E5 Compliance, but are included in the pre-requisite licenses. For example, the combination of Microsoft 365 E3 + Microsoft 365 E5 Compliance includes all of the listed features.

[3] Requires [AIP Plan 1 or EMS E3] + [Exchange Online, SharePoint Online or OneDrive for business]

[4] Requires Exchange Online, SharePoint Online or OneDrive for business

[5] Requires EMS E5, E5 Security, Windows 10 E5, Microsoft Defender ATP, or Microsoft Cloud App Security.

[6] Microsoft 365 Apps must be licensed separately.

[7] Requires Azure Active Directory Premium Plan 1

[8] Requires Microsoft Cloud App Security

[9] Each user initially receives 100 GB of storage in the archive mailbox. When auto-expanding archiving is turned on, additional storage is automatically added when the 100 GB storage capacity is reached.

[10] Archive mailbox limited to 50 GB

[11] Office 365 Cloud App Security only

[12] Azure subscription required to use configured key for Bring Your Own Key (BYOK).