

Durée : 1 jour soit 7 heures

Référence : MS-4002



Public visé :

Cette formation s'adresse spécifiquement aux professionnels de l'informatique en charge de la gestion, de la sécurité et de l'architecture d'un environnement Microsoft (Tenant).

Voici le public cible principal :

- **Administrateurs Microsoft 365** : C'est le cœur de cible. Ce sont eux qui gèrent les licences, le déploiement des applications (via Intune ou Configuration Manager) et les paramètres globaux du tenant.
- **Administrateurs Sécurité (Security Administrators)** : Ceux qui ont la responsabilité de configurer et maintenir les accès sécurisés, l'authentification forte (MFA), l'accès conditionnel et la gestion des identités via Microsoft Entra ID.
- **Administrateurs de la Conformité (Compliance Administrators)** : Les profils en charge de la protection de la donnée, qui doivent configurer Microsoft Purview (règles DLP, étiquettes de confidentialité) pour s'assurer que l'IA ne génère pas de fuites d'informations sensibles.
- **Architectes Cloud et Ingénieurs Système** : Les professionnels impliqués dans la conception et la préparation technique de l'infrastructure avant le déploiement massif d'un nouvel outil comme Copilot.

Cette formation ne s'adresse absolument pas aux utilisateurs finaux de Copilot ni aux managers cherchant simplement à comprendre les usages fonctionnels de l'IA. C'est une formation purement orientée "Back-Office" et configuration technique préalable.



Pré-requis :

Prérequis obligatoires :

- Expérience pratique de l'administration générale de Microsoft 365 (navigation et utilisation du Centre d'administration Microsoft 365).
- Compréhension fondamentale des concepts de sécurité informatique en entreprise (gestion des identités, authentification, droits d'accès).
- Connaissance de base du fonctionnement des applications de la suite Microsoft (SharePoint, OneDrive).

Prérequis recommandés (les "Plus") :

- Une première exposition à Microsoft Entra ID (anciennement Azure AD) ou aux concepts de conformité des données (Microsoft Purview).
- Des notions sur la gestion des appareils ou des applications via Microsoft Intune ou Configuration Manager.



Objectifs pédagogiques :

À l'issue de cette journée de formation, le stagiaire aura atteint les objectifs opérationnels suivants :

- **Préparer** les données, les licences et les outils SharePoint Management pour l'intégration de Microsoft 365 Copilot.
- **Configurer** les stratégies d'accès conditionnel et les méthodes d'authentification forte (MFA, sans mot de passe) pour sécuriser les accès.
- **Gérer** les rôles d'administration et limiter le partage excessif de données dans SharePoint pour garantir le principe de moindre privilège.
- **Planifier et exécuter** le déploiement de Microsoft 365 Apps for enterprise selon différentes méthodes (cloud, local) tout en appliquant les bases de sécurité.
- **Créer et appliquer** des règles personnalisées de prévention des pertes de données (DLP) via Microsoft Purview.
- **Déployer** une stratégie d'étiquettes de confidentialité pour classer et protéger les fichiers dans SharePoint et OneDrive.
- **Intégrer** des sources de données tierces à Copilot en gérant les agents et les connecteurs Microsoft Graph.



Compétences acquises à l'issue de la formation :

- Être capable de préparer techniquement un environnement Microsoft 365 pour le déploiement, l'adoption et l'extensibilité de Copilot (gestion des licences, agents et connecteurs Graph).
- Être en mesure de sécuriser les identités, les accès utilisateurs et les privilèges administratifs en s'appuyant sur les outils Microsoft Entra ID (Accès conditionnel, MFA, PIM) et SharePoint.



- Savoir déployer, sécuriser et maintenir à jour la suite Microsoft 365 Apps for enterprise via des outils centralisés (Microsoft Intune, Configuration Manager) ou en libre-service.
- Maîtriser la protection des données sensibles et prévenir le partage excessif en configurant les stratégies de prévention des pertes de données (DLP) et les étiquettes de confidentialité dans Microsoft Purview.



Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure. La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz. L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration. En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Note relative au programme : Les ateliers, démonstrations, travaux pratiques et scénarios présentés dans ce programme sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation permanente avec les évolutions technologiques, le contenu pédagogique ainsi que les environnements de travaux pratiques (TP) sont susceptibles d'être adaptés, ajustés ou mis à jour au cours du temps.



Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassRoom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique



Modalités d'évaluation et de suivi :

Avant

Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice), qui valide la base de connaissances nécessaires.

Les stagiaires disposent également, depuis leur extranet, d'un **outil d'auto-positionnement** leur permettant d'évaluer leur niveau de maîtrise des compétences visées par la formation. Cette auto-évaluation est réalisée avant le démarrage de la formation à l'aide d'un curseur de positionnement allant du niveau le plus faible au niveau le plus élevé.

Pendant

Après chaque module théorique, un ou plusieurs ateliers pratiques permettent de valider progressivement l'acquisition des connaissances. Un quiz peut accompagner les ateliers pratiques afin de mesurer la compréhension des notions abordées.

Après

À l'issue de la formation, les stagiaires réalisent une nouvelle **auto-évaluation** sur les mêmes compétences que celles évaluées avant la formation. Cette comparaison permet de mesurer leur perception de la progression réalisée et de visualiser les compétences développées au cours de la formation.

Lorsque le programme de formation le prévoit, un examen de certification est organisé conformément aux modalités définies par l'éditeur ou le centre de certification (TOSA, Pearson VUE, ENI, PeopleCert...).

Le formateur réalise également une **évaluation individuelle des compétences** de chaque stagiaire sur l'ensemble des

compétences visées par la formation. Pour chacune d'elles, il indique si la compétence est :

- Acquis ;
- En cours d'acquisition ;
- Non acquise.

Lorsque la compétence est évaluée comme **en cours d'acquisition** ou **non acquise**, le formateur formule des observations précisant les difficultés rencontrées ainsi que les actions ou recommandations permettant au stagiaire de poursuivre sa montée en compétences.

Enfin

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation de formation.



Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre référente handicap certifiée :

Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr

Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.

Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- [AGEFIPH](#)
- [FIPHFP](#)
- MDPH de votre département

Description / Contenu

Important : cette formation officielle Microsoft sera retirée le 30/10/2026 puis remplacée par la formation officielle Microsoft AB-650T00 Administrer des services Microsoft 365 et IA

Module 1 : Mettre en œuvre Microsoft 365 Copilot

Ce module présente les principales tâches que les administrateurs doivent effectuer lors de la mise en œuvre de Microsoft 365 Copilot, notamment la réalisation des prérequis, la préparation des données pour les recherches, l'attribution des licences Copilot et l'extension de Copilot.

- Se préparer à Microsoft 365 Copilot
- Mettre en œuvre les outils SharePoint Advanced Management pour préparer Microsoft 365 Copilot
- Préparer vos données pour les recherches dans Microsoft 365 Copilot
- Protéger vos données Microsoft 365 Copilot avec les outils de sécurité Microsoft 365
- Attribuer vos licences Microsoft 365 Copilot
- Étendre Microsoft 365 Copilot
- Favoriser l'adoption de Microsoft 365 Copilot dans toute votre organisation

Module 2 : Gérer les accès sécurisés des utilisateurs dans Microsoft 365

Ce module présente les différentes fonctionnalités proposées dans l'écosystème Microsoft 365 pour sécuriser les accès des utilisateurs, notamment les stratégies Conditional Access, l'authentification multifacteur, la gestion des mots de passe en libre-service, les stratégies Smart Lockout et les paramètres de sécurité par défaut.

- Examiner les outils d'identité et d'accès utilisés dans Microsoft 365
- Gérer les mots de passe des utilisateurs
- Mettre en œuvre des stratégies Conditional Access
- Activer l'authentification pass-through
- Mettre en œuvre l'authentification multifacteur
- Explorer les options d'authentification sans mot de passe
- Explorer la gestion des mots de passe en libre-service
- Mettre en œuvre Microsoft Entra Smart Lockout
- Explorer les paramètres de sécurité par défaut dans Microsoft Entra ID
- Examiner les problèmes d'authentification à l'aide des journaux de connexion

Module 3 : Gérer les autorisations, les rôles et les groupes de rôles dans Microsoft 365

Ce module présente l'utilisation des rôles et des groupes de rôles dans le modèle d'autorisations de Microsoft 365, notamment la gestion des rôles, les bonnes pratiques lors de la configuration des rôles d'administrateur, la délégation des rôles et l'élévation des privilèges.

- Examiner l'utilisation des rôles dans le modèle d'autorisations de Microsoft 365
- Gérer les rôles dans l'ensemble de l'écosystème Microsoft 365
- Explorer les rôles d'administrateur dans Microsoft 365
- Examiner les bonnes pratiques lors de la configuration des rôles d'administration
- Attribuer des rôles d'administrateur aux utilisateurs dans Microsoft 365
- Déléguer des rôles d'administrateur à des partenaires
- Mettre en œuvre des groupes de rôles dans Microsoft 365
- Gérer les autorisations à l'aide des unités administratives dans Microsoft Entra ID
- Gérer les autorisations SharePoint pour empêcher le partage excessif de données
- Élever les privilèges à l'aide de Microsoft Entra Privileged Identity Management

Module 4 : Déployer Microsoft 365 Apps for enterprise

Ce module présente comment mettre en œuvre la suite de productivité Microsoft 365 Apps for enterprise, à la fois dans le cadre de déploiements pilotés par les utilisateurs et de déploiements centralisés.

- Explorer les fonctionnalités de Microsoft 365 Apps for enterprise
- Effectuer une installation en libre-service de Microsoft 365 Apps for enterprise
- Déployer Microsoft 365 Apps for enterprise avec Microsoft Configuration Manager
- Déployer Microsoft 365 Apps for enterprise depuis le cloud
- Déployer Microsoft 365 Apps for enterprise depuis une source locale
- Gérer les mises à jour de Microsoft 365 Apps for enterprise
- Explorer les canaux de mise à jour de Microsoft 365 Apps for enterprise
- Gérer vos applications cloud à l'aide du Centre d'administration Microsoft 365 Apps
- Ajouter Microsoft 365 Apps for enterprise à Microsoft Intune

- Déployer la baseline de sécurité de Microsoft 365 Apps for enterprise

Module 5 : Mettre en œuvre Microsoft Purview Data Loss Prevention

Ce module présente comment les organisations peuvent utiliser Microsoft Purview Data Loss Prevention pour contribuer à la protection des données sensibles et définir les actions de protection qu'elles peuvent mettre en œuvre lorsqu'une règle DLP est enfreinte.

- Planifier la mise en œuvre de Microsoft Purview Data Loss Prevention
- Mettre en œuvre les stratégies DLP par défaut de Microsoft Purview
- Concevoir une stratégie DLP personnalisée
- Créer une stratégie DLP personnalisée à partir d'un modèle
- Configurer les notifications par e-mail pour les stratégies DLP
- Configurer les conseils de stratégie pour les stratégies DLP

Module 6 : Mettre en œuvre les étiquettes de confidentialité

Ce module présente le processus de mise en œuvre des étiquettes de confidentialité, notamment l'attribution des autorisations d'administration appropriées, la détermination d'une stratégie de déploiement, la création, la configuration et la publication des étiquettes, ainsi que leur suppression et leur effacement.

- Planifier votre stratégie de déploiement des étiquettes de confidentialité
- Activer les étiquettes de confidentialité pour les fichiers dans SharePoint et OneDrive
- Examiner les prérequis pour créer une étiquette de confidentialité
- Créer des étiquettes de confidentialité
- Publier des étiquettes de confidentialité
- Supprimer et effacer des étiquettes de confidentialité

Module 7 : Gérer l'extensibilité de Microsoft 365 Copilot

Ce module présente les tâches que les administrateurs doivent effectuer pour gérer l'extensibilité de Microsoft 365 Copilot, notamment la gestion des agents Copilot ainsi que la création et la supervision des connecteurs.

- Gérer les agents Copilot dans les applications intégrées
- Créer une connexion entre une source de données et un connecteur Microsoft Graph

- Superviser vos connecteurs Microsoft Graph
- Gérer l'affichage du contenu des connecteurs Microsoft Graph dans Microsoft 365 Copilot