OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen SC-401

Administration de la sécurité de l’information Microsoft 365

Certification : Microsoft Certified — Information Security Administrator

Niveau : Associate | Public : Administrateurs sécurité de l’information / Purview

1. Présentation de la certification

L'examen **SC-401 : Administering Information Security in Microsoft 365** valide les compétences des administrateurs en charge de la planification et de l'implémentation de la sécurité de l'information pour les données sensibles via Microsoft Purview et les services associés. Cette certification atteste de votre capacité à atténuer les risques en protégeant les données dans les environnements collaboratifs gérés par Microsoft 365 contre les menaces internes et externes, et à protéger les données utilisées par les services d'IA.

Important : Le SC-401 remplace l'ancienne certification SC-400 (Information Protection and Compliance Administrator), retirée le 31 mai 2025. La réussite de cet examen unique conduit à l'obtention de la certification **Microsoft Certified : Information Security Administrator**, particulièrement valorisée pour les rôles DPO, RGPD compliance officer, administrateur Purview et consultant en protection des données.

Informations clés

Code de l'examen	SC-401
Intitulé officiel	Administering Information Security in Microsoft 365
Certification obtenue	Microsoft Certified : Information Security Administrator
Niveau	Associate
Statut	Actif (nouvelle certification — remplace SC-400 retiré le 31 mai 2025)
Différence avec SC-400	Centré sur la protection de l'information uniquement (les sujets compliance sont désormais couverts par les Microsoft Applied Skills)
Nouveautés	Data Security Posture Management (DSPM) for AI, OCR pour types d'informations sensibles, protection des données Copilot, Adaptive Protection avancée
Durée de l'examen	Environ 100 à 120 minutes (selon planification)
Nombre de questions	40 à 60 questions (QCM, études de cas Contoso, glisser-déposer, scénarios)
Score de réussite	700 / 1000
Langues disponibles	Anglais et autres langues (délai d'environ 8 semaines pour les versions localisées)

Validité	1 an, renouvellement gratuit en ligne via Microsoft Learn
Modalité	En centre agréé (OpenCertif — Pearson VUE) ou à distance (OnVUE)

2. Profil du candidat

En tant qu'administrateur sécurité de l'information, vous planifiez et implémentez la sécurité de l'information des données sensibles via Microsoft Purview et les services associés. Vous êtes responsable de :

- Atténuer les risques en protégeant les données dans les environnements collaboratifs gérés par Microsoft 365 contre les menaces internes et externes.
- Protéger les données utilisées par les services d'IA (Copilot, Azure AI).
- Implémenter l'information protection (étiquettes de confidentialité, classification).
- Implémenter la prévention de perte de données (DLP) et la rétention.
- Gérer Insider Risk Management.
- Gérer les alertes et activités de sécurité de l'information.
- Participer à la réponse aux incidents de sécurité de l'information.

Vous collaborez avec d'autres rôles en charge de la gouvernance, des données et de la sécurité pour évaluer et développer les stratégies répondant aux objectifs de sécurité de l'information et de réduction des risques. Vous devez être familier avec :

- L'ensemble des services Microsoft 365.
- PowerShell pour l'administration scriptable.
- Microsoft Entra ID.
- Le portail Microsoft Defender.
- Microsoft Defender for Cloud Apps.

3. Prérequis et public cible OpenCertif

Aucun prérequis formel n'est exigé, mais OpenCertif recommande aux candidats de disposer d'une expérience préalable dans les domaines suivants :

- Notions de Microsoft 365 Fundamentals (idéalement certification MS-900).
- Notions de Microsoft Security, Compliance and Identity Fundamentals (SC-900).
- Familiarité avec Microsoft Purview et ses portails.
- Compréhension des réglementations (RGPD, HIPAA, ISO 27001).
- Expérience pratique d'un environnement Microsoft 365 / Azure.
- Bonus : les titulaires de l'ancienne SC-400 sont parfaitement positionnés pour ce nouveau parcours.

Public cible OpenCertif

- Administrateurs Microsoft Purview et Information Protection.
- DPO (Délégués à la Protection des Données) RGPD.
- Compliance officers et risk managers.
- Consultants en protection des données et classification de l'information.
- Administrateurs Microsoft 365 spécialisés sur DLP et rétention.
- Anciens titulaires SC-400 souhaitant migrer vers la nouvelle certification.

4. Domaines de compétences mesurées

L'examen est structuré autour de 3 grands domaines de compétences. Le tableau ci-dessous indique le poids relatif de chaque domaine dans l'évaluation finale (version d'avril 2026).

Domaine	Intitulé	Pondération
1	Implémenter l'information protection	30 — 35 %
2	Implémenter la DLP et la rétention	30 — 35 %
3	Gérer les risques, alertes et activités	30 — 35 %

Remarque : la majorité des questions concernent des fonctionnalités en disponibilité générale (GA). Certaines questions peuvent porter sur des fonctionnalités en préversion couramment utilisées.

5. Détail des compétences mesurées

Cette section détaille de manière exhaustive l'ensemble des compétences couvertes par l'examen SC-401, conformément au guide d'étude officiel Microsoft (version d'avril 2026).

1 Implémenter l'information protection — 30 — 35 %

1.1 Implémenter et gérer la classification des données

- Identifier les exigences de l'organisation en matière d'informations sensibles.
- Traduire les exigences d'informations sensibles en types d'info sensibles intégrés ou personnalisés.
- Créer et gérer des types d'info sensibles personnalisés.
- Implémenter document fingerprinting.
- Créer et gérer des classifieurs Exact Data Match (EDM).
- Créer et gérer des classifieurs entraînés (trainable classifiers).
- Superviser la classification des données et l'usage des étiquettes via data explorer et content explorer.
- Configurer la prise en charge de l'OCR (reconnaissance optique de caractères) pour les types d'info sensibles.

1.2 Implémenter et gérer les sensitivity labels dans Microsoft Purview

- Implémenter les rôles et permissions pour administrer les sensitivity labels.
- Définir et créer des sensitivity labels pour les éléments et les conteneurs.
- Configurer les paramètres de protection et le marquage de contenu pour les sensitivity labels.
- Configurer et gérer les stratégies de publication pour les sensitivity labels.
- Configurer et gérer les stratégies d'auto-labeling pour les sensitivity labels.
- Appliquer un sensitivity label aux conteneurs : Microsoft Teams, Microsoft 365 Groups, Microsoft Power BI et Microsoft SharePoint.
- Appliquer des sensitivity labels via Microsoft Defender for Cloud Apps.

1.3 Implémenter l'information protection pour Windows, partages de fichiers et Exchange

- Planifier et implémenter le client Microsoft Purview Information Protection.
- Gérer les fichiers via le client Microsoft Purview Information Protection.
- Appliquer la classification en masse aux données on-premises via le scanner Microsoft Purview Information Protection.
- Concevoir et implémenter Microsoft Purview Message Encryption.
- Concevoir et implémenter Microsoft Purview Advanced Message Encryption.

2 Implémenter la DLP et la rétention — 30 — 35 %

2.1 Créer et configurer les stratégies DLP (Data Loss Prevention)

- Concevoir des stratégies DLP basées sur les exigences de l'organisation.
- Implémenter les rôles et permissions pour la DLP.
- Créer et gérer des stratégies DLP.
- Configurer les stratégies DLP pour Adaptive Protection.
- Interpréter la précédence des stratégies et règles dans la DLP.
- Créer des stratégies de fichiers dans Microsoft Defender for Cloud Apps via une stratégie DLP.

2.2 Implémenter et superviser Microsoft Purview Endpoint DLP

- Spécifier les exigences d'appareils pour Endpoint DLP, y compris les extensions.
- Configurer les règles DLP avancées pour les appareils dans les stratégies DLP.
- Configurer les paramètres Endpoint DLP.
- Configurer la protection just-in-time.
- Superviser les activités endpoint.

2.3 Implémenter et gérer la rétention

- Planifier la rétention et l'élimination de l'information via les retention labels.
- Créer, configurer et gérer des adaptive scopes.
- Créer des retention labels pour la gestion du cycle de vie des données.
- Configurer une stratégie de retention label pour publier des étiquettes.
- Configurer une stratégie de retention label pour auto-appliquer des étiquettes.
- Interpréter les résultats de la précédence des stratégies via Policy lookup.
- Créer et configurer des stratégies de rétention.
- Récupérer le contenu retenu dans Microsoft 365.

3 Gérer les risques, alertes et activités — 30 — 35 %

3.1 Implémenter et gérer Microsoft Purview Insider Risk Management

- Implémenter les rôles et permissions pour Insider Risk Management.
- Planifier et implémenter les connecteurs Insider Risk Management.
- Planifier et implémenter l'intégration avec Microsoft Defender for Endpoint.
- Configurer et gérer les paramètres d'Insider Risk Management.
- Configurer les indicateurs de stratégie.
- Sélectionner un modèle de stratégie approprié.
- Créer et gérer les stratégies Insider Risk Management.
- Gérer les paramètres de forensic evidence.
- Activer et configurer les niveaux de risque interne pour Adaptive Protection.
- Gérer les alertes et cas Insider Risk Management.
- Gérer le workflow Insider Risk Management, y compris les modèles de notice.

3.2 Gérer les alertes et activités de sécurité de l'information

- Attribuer les licences utilisateur Microsoft Purview Audit (Premium).
- Enquêter sur les activités via Microsoft Purview Audit.
- Configurer les stratégies de rétention d'audit.
- Analyser les activités Purview via activity explorer.
- Répondre aux alertes DLP dans le portail Microsoft Purview.
- Enquêter sur les activités Insider Risk via le portail Microsoft Purview.
- Répondre aux alertes Purview dans Microsoft Defender XDR.
- Répondre aux alertes de stratégie de fichier Defender for Cloud Apps.
- Effectuer des recherches via Content Search.

3.3 Protéger les données utilisées par les services d’IA

- Implémenter des contrôles dans Microsoft Purview pour protéger le contenu dans un environnement utilisant des services d’IA.
- Implémenter des contrôles dans les workloads de productivité Microsoft 365 pour protéger le contenu dans un environnement utilisant des services d’IA.
- Implémenter les prérequis pour Data Security Posture Management (DSPM) for AI.
- Gérer les rôles et permissions pour DSPM for AI.
- Configurer les stratégies DSPM for AI.
- Superviser les activités dans DSPM for AI.

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au SC-401 à travers un parcours blended-learning complet, combinant ressources e-learning interactives, sessions tutorées et ateliers techniques pratiques sur les technologies Microsoft Purview, sensitivity labels, DLP, retention, Insider Risk Management, DSPM for AI et Microsoft Defender for Cloud Apps.

Format de la formation

Durée recommandée	45 à 60 heures de formation (selon profil et niveau d'entrée)
Modalité	100 % distanciel asynchrone, ou blended (distanciel + classes virtuelles)
Support pédagogique	Modules interactifs Articulate Rise 360, scénarios immersifs VTS, ateliers techniques
Plateforme LMS	lmsopencertif.fr (Moodle) — accès 24/7 pendant 12 mois
Encadrement	Tutorat asynchrone par expert certifié + classes virtuelles bimensuelles
Évaluations	Quiz formatifs par module, ateliers pratiques, examen blanc final, simulation OnVUE
Certification finale	Passage de l'examen SC-401 en centre OpenCertif (Pearson VUE) ou OnVUE

Parcours d'apprentissage proposé

- **Module 1 :** Vue d'ensemble de la sécurité de l'information dans Microsoft Purview.
- **Module 2 :** Classification des données — types d'info sensibles intégrés et custom.
- **Module 3 :** Document fingerprinting, EDM et trainable classifiers.
- **Module 4 :** OCR et content explorer pour la classification visuelle.
- **Module 5 :** Sensitivity labels — conception, publication, auto-labeling.
- **Module 6 :** Labels pour conteneurs — Teams, M365 Groups, Power BI, SharePoint.
- **Module 7 :** Information protection client et scanner on-premises.
- **Module 8 :** Message Encryption et Advanced Message Encryption.
- **Module 9 :** Stratégies DLP — conception, rôles, Adaptive Protection.
- **Module 10 :** Endpoint DLP et just-in-time protection.
- **Module 11 :** Rétention — retention labels, adaptive scopes, Policy lookup.
- **Module 12 :** Insider Risk Management — stratégies, indicateurs, forensic evidence.
- **Module 13 :** Adaptive Protection avec Insider Risk Management.
- **Module 14 :** Microsoft Purview Audit (Premium) et investigation.

- **Module 15 :** Defender for Cloud Apps pour la protection des données.
- **Module 16 :** DSPM for AI — protection des données utilisées par Copilot.
- **Module 17 :** Examen blanc et préparation finale.

7. Ressources d’étude officielles

En complément du parcours OpenCertif, les ressources Microsoft Learn suivantes sont fortement recommandées :

- Documentation sécurité Microsoft (learn.microsoft.com/security).
- Documentation Microsoft Purview (learn.microsoft.com/purview).
- Documentation Data Loss Prevention (DLP).
- Documentation Insider Risk Management.
- Documentation Microsoft Purview Information Protection.
- Documentation Microsoft Defender for Cloud Apps.
- Documentation Data Security Posture Management for AI.
- Documentation Microsoft Purview Audit (Standard et Premium).
- Documentation Microsoft Purview Message Encryption.
- Zero Trust Guidance Center.
- Parcours d’apprentissage Microsoft Learn dédiés au SC-401.
- Microsoft Applied Skills associées (Information Protection, DLP, Retention).
- Évaluation pratique gratuite proposée par Microsoft.
- Espace de simulation d’examen (aka.ms/examdemo).
- Security, compliance, and identity community hub.
- Chaînes vidéo : Exam Readiness Zone.

8. Modalités de passage de l’examen

Inscription	Via OpenCertif ou directement sur learn.microsoft.com
Centre d’examen	OpenCertif — Centre agréé Pearson VUE
Examen à distance	Mode OnVUE (surveillance en ligne, conditions strictes)
Pièce d’identité	2 pièces d’identité obligatoires le jour de l’examen
Aménagements	Demande possible (temps additionnel, assistance) sur Microsoft Learn
Résultat	Score communiqué immédiatement à la fin de l’examen
Renouvellement	Annuel, via évaluation gratuite en ligne sur Microsoft Learn
Politique de reprise	Délai d’attente de 24 heures pour la 1re reprise, puis 14 jours entre les tentatives suivantes (maximum 5 tentatives sur 12 mois)

9. Contact et inscription

Pour toute information complémentaire, demande de devis ou inscription à la formation préparatoire au SC-401, l'équipe OpenCertif reste à votre disposition.

OpenCertif
Centre de formation et de certification

app.opencertif.fr
lmsopencertif.fr

Centre agréé Certiport / Pearson VUE
Certifié Qualiopi — Actions de formation

10. Mentions légales et version

Ce syllabus est établi par OpenCertif sur la base du guide d'étude officiel Microsoft SC-401, dans sa version applicable (version d'avril 2026). Les compétences mesurées, les pondérations et les objectifs présentés reflètent fidèlement la structure de l'examen telle que publiée par Microsoft.

Version du syllabus : 2026.05 — Édition mai 2026
Source officielle : learn.microsoft.com/credentials/certifications/resources/study-guides/sc-401