Microsoft Administering Information Protection and Compliance in Microsoft 365 (Microsoft SC-400)

Cours officiel SC-400, préparation à l'examen

Cours Pratique de 4 jours - 28h
Réf : SC4 - Prix 2024 : 2 890€ HT

Avec cette formation, vous bénéficierez des connaissances et des compétences nécessaires pour protéger les informations dans votre déploiement Microsoft 365. La formation se concentre sur la gestion du cycle de vie des données, la protection des informations et la conformité au sein de votre organisation. Vous aborderez, entre autres, la mise en œuvre des politiques de prévention des pertes de données, les types d'informations sensibles, les étiquettes de sensibilité, les politiques de conservation des données, le chiffrement des messages Microsoft Purview, l'audit et l'eDiscovery.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Implémenter la protection des informations

Implémenter la protection contre la perte de données (DLP)

Implémenter la gestion des enregistrements et du cycle de vie des données

Superviser et examiner des données et des activités à l'aide de Microsoft Purview

Gérer les risques internes et de confidentialité dans Microsoft 365

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel en anglais. Bonne compréhension de l'anglais à l'écrit.

CERTIFICATION

La réussite de l'examen permet d'obtenir la certification Microsoft Microsoft Certified: Information Protection and Compliance Administrator Associate.

PARTICIPANTS

Administrateur de la protection des informations.

PRÉREQUIS

Connaissances de base des technologies de sécurité et de conformité de Microsoft, des concepts de protection de l'information. Compréhension du cloud computing, des produits et services Microsoft 365.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 10/2023

1) Créer et gérer les types d'informations sensibles

- Identifier les exigences en matière d'informations sensibles pour les données d'une organisation.
- Traduire les exigences en matière d'informations sensibles en types d'informations sensibles intégrés ou personnalisés.
- Créer et gérer des types d'informations sensibles personnalisés.
- Créer des classifieurs basés sur la correspondance exacte des données (EDM).
- Implémenter l'empreinte digitale du document.

2) Créer et gérer des classifieurs entraînables

- Identifier les cas d'utilisation des classifieurs entraînables.
- Concevoir et créer un classifieur entraînable.
- Tester un classifieur entraînable.
- Réentraîner un classifieur entraînable.

3) Implémenter et gérer des étiquettes de confidentialité

- Implémenter des rôles et des autorisations pour administrer des étiquettes de confidentialité.

- Définir et créer des étiquettes de confidentialité.
- Configurer et gérer des stratégies d'étiquettes de confidentialité.
- Superviser la classification des données et l'utilisation des étiquettes
- Appliquer la classification en bloc aux données locales à l'aide du scanneur Microsoft Purview Information Protection.
- Gérer les paramètres de protection et le marquage des étiquettes de confidentialité appliquées.

4) Concevoir et implémenter le chiffrement pour les e-mails

- Concevoir une solution de chiffrement d'e-mails basée sur les méthodes disponibles dans Microsoft 365.
- Implémenter le chiffrement des messages Microsoft Purview.
- Implémenter le chiffrement avancé des messages Microsoft Purview.

5) Créer et configurer des stratégies de protection contre la perte de données

- Concevoir des stratégies DLP en fonction des exigences d'une organisation.
- Configurer des autorisations pour DLP.
- Créer et gérer les stratégies DLP.
- Traduire la priorité des stratégies et des règles dans DLP.
- Configurer une stratégie de fichier dans Microsoft Defender for Cloud Apps pour utiliser des stratégies DLP.

6) Implémenter et superviser la protection contre la perte de données (DLP)

- Configurer des règles DLP avancées pour les appareils.
- Configurer les paramètres DLP pour les points de terminaison.
- Recommander une méthode de déploiement pour l'intégration d'appareils.
- Identifier les exigences de point de terminaison pour l'intégration des appareils.
- Superviser les activités du point de terminaison.
- Implémenter l'extension Microsoft Purview.

7) Superviser et gérer les activités DLP

- Analyser les rapports DLP.
- Analyser les activités DLP à l'aide de l'Explorateur d'activités.
- Corriger les alertes DLP dans le portail de conformité Microsoft Purview.
- Corriger les alertes DLP générées par Defender for Cloud Apps.

8) Conserver et supprimer des données à l'aide d'étiquettes de rétention

- Planifier la conservation et la destruction des informations à l'aide d'étiquettes de rétention.
- Créer des étiquettes de rétention pour la gestion du cycle de vie des données.
- Configurer et gérer les requêtes d'appartenance.
- Configurer une stratégie d'étiquette de rétention pour publier des étiquettes.
- Configurer une stratégie d'étiquette de rétention pour l'application automatique des étiquettes.
- Traduire les résultats de la stratégie de priorité, notamment à l'aide de Policy Lookup.

9) Gérer la rétention des données dans les charges de travail Microsoft 365

- Créer et appliquer des stratégies de rétention pour SharePoint et OneDrive.
- Créer et appliquer des stratégies de rétention pour les groupes Microsoft 365.
- Créer et appliquer des stratégies de rétention pour Teams.
- Créer et appliquer des stratégies de rétention pour Yammer.
- Créer et appliquer des stratégies de rétention pour Exchange Online.
- Appliquer la rétention des mails dans Exchange Online.
- Implémenter des stratégies d'archivage dans Exchange Online.
- Configurer des verrous de conservation pour les stratégies de rétention et les stratégies d'étiquette de rétention.
- Récupérer les contenus conservés dans Microsoft 365.

10) Implémenter Microsoft Purview Records Management

- Créer et configurer des étiquettes de rétention pour la gestion des enregistrements.
- Gérer les étiquettes de rétention à l'aide d'un plan de fichiers, y compris des descripteurs de plan de fichiers.
- Classifier des enregistrements à l'aide d'étiquettes de rétention et de stratégies d'étiquette de rétention.
- Gérer la rétention basée sur les événements.
- Gérer la disposition du contenu dans Records Management.
- Configurer les paramètres de gestion des enregistrements.

11) Planifier et gérer les exigences réglementaires à l'aide du Gestionnaire de conformité Microsoft Purview

- Planifier la conformité réglementaire dans Microsoft 365.
- Créer et gérer des évaluations.
- Créer et modifier des modèles personnalisés.
- Interpréter et gérer les actions d'amélioration.
- Créer et gérer des stratégies d'alerte pour les évaluations.

12) Planifier et gérer eDiscovery et la recherche de contenu

- Choisir entre eDiscovery (Standard) et eDiscovery (Premium) en fonction des exigences d'une organisation.
- Planifier et implémenter eDiscovery.
- Déléguer des autorisations pour utiliser eDiscovery et la recherche de contenu.
- Effectuer des recherches et répondre aux résultats d'eDiscovery.
- Gérer les tickets eDiscovery.
- Effectuer des recherches à l'aide de Content Search.

13) Gérer et analyser les rapports et les journaux d'audit dans Microsoft Purview

- Choisir entre Audit (Standard) et Audit (Premium) en fonction des exigences d'une organisation.
- Planifier et configurer l'audit.
- Examiner les activités à l'aide du journal d'audit unifié.
- Passer en revue et interpréter les rapports et tableaux de bord de conformité.
- Configurer des stratégies d'alerte.
- Configurer des stratégies de conservation d'audit.

14) Implémenter et gérer Microsoft Purview Communication Compliance

- Préparer l'implémentation de Communication Compliance.
- Créer et gérer des stratégies dans Communication Compliance.
- Examiner et corriger les alertes et les rapports dans Communication Compliance.

15) Implémenter et gérer Microsoft Purview Insider Risk Management

- Préparer l'implémentation d'Insider Risk Management.
- Créer et gérer des stratégies dans Insider risk management policies
- Examiner et corriger les activités, les alertes et les rapports dans Insider Risk Management.
- Gérer des tickets dans Insider Risk Management.
- Gérer le paramétrage de Forensic Evidence.
- Gérer les modèles de notification.

16) Implémenter et gérer Microsoft Purview Information Barriers (IBs)

- Préparer l'implémentation de Microsoft Purview Information Barriers.
- Créer et gérer des stratégies et des segments dans Microsoft Purview Information Barriers.
- Configurer Teams, SharePoint et OneDrive pour pour appliquer les stratégies de cloisonnement de l'information.
- Examiner les problèmes liés aux stratégies de cloisonnement de l'information (IB).

17) Implémenter et gérer les exigences de confidentialité à l'aide de Microsoft Priva
- Configurer et tenir à jour la gestion des risques de confidentialité.
- Créer et gérer des stratégies de gestion des risques de confidentialité.
- Identifier et superviser les risques potentiels impliquant des données personnelles.
- Évaluer et corriger les alertes et les problèmes.
- Implémenter et gérer les demandes de droits des personnes concernées.

LES DATES

CLASSE À DISTANCE
2024 : 03 juin, 10 juil., 23 oct.

PARIS
2024 : 03 juil., 16 oct.