RAPPORT D'EXEMPLE — informations du tenant floutées, résultats réels d'EntraGUARD

EntraGUARD
entraguard.eu

TENANT AUDITÉ

[redacted]

[redacted]

RAPPORT D'AUDIT

Sécurité Microsoft 365

Synthèse à destination de la Direction et du RSSI

DATE DU RAPPORT
27/07/2026

PÉRIMÈTRE
Entra ID, Exchange, Teams, SharePoint, OneDrive, Defender, Intune, Purview

RÉFÉRENTIEL APPLIQUÉ
Baseline « CIS — niveau 1 » — 64 contrôles exécutés

SCORE DE CONFORMITÉ PONDÉRÉ

75%

- 45 conformes
- 7 avertissements
- 10 non conformes
- 2 non évalués

Rapport généré par EntraGUARD — entraguard.eu — audit en lecture seule.

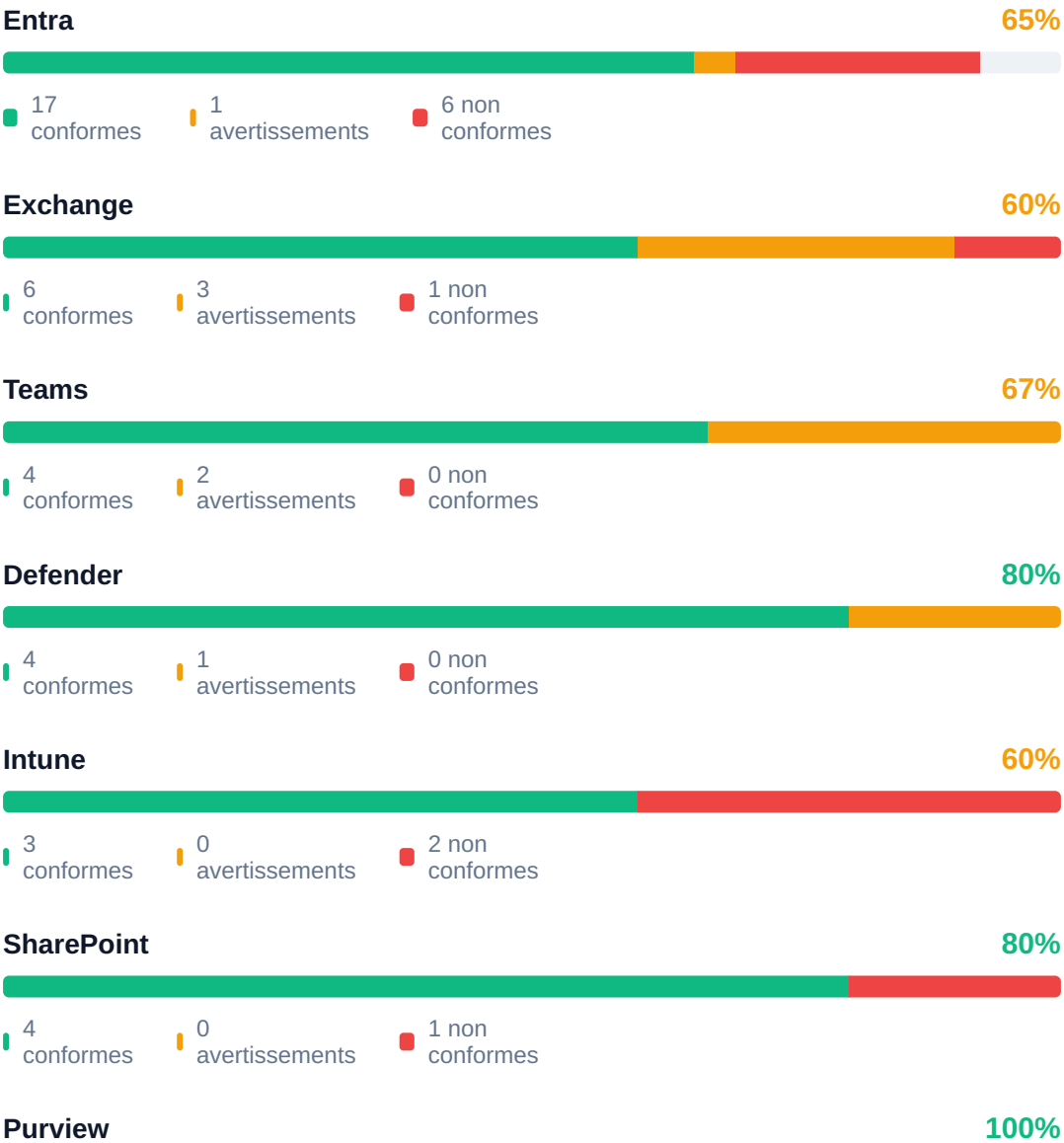
Synthèse exécutive

CONFORMITÉ	CONFORMES	AVERTIS.	NON CONF.	NON ÉVALUÉS	CONTRÔLES
75%	45	7	10	2	64

Méthodologie : score pondéré par criticité — les contrôles fondamentaux (L1) pèsent 3× plus que le renforcement (L2). Un avertissement compte pour la moitié des points. Audit réalisé en lecture seule.

Conformité par référentiel

Répartition des contrôles conformes, en avertissement et non conformes



4 conformes
0 avertissements
0 non conformes

OneDrive 100%

3 conformes
0 avertissements
0 non conformes

Priorités d’action

Les 8 non-conformités les plus critiques à traiter en premier

1 **Retirer les comptes désactivés des rôles à privilèges** ENTRA · L1

Remédiation : Retirez l'attribution de rôle des comptes désactivés.

2 **Exiger la MFA pour tous les utilisateurs** ENTRA · L1

Remédiation : Accès conditionnel : stratégie ciblant tous les utilisateurs (avec exclusions break-glass) exigeant la MFA, idéalement via une force d'authentification résistante au phishing.

3 **Exiger la MFA pour la jointure et l'enregistrement d'appareils** ENTRA · L1

Remédiation : Accès conditionnel : créez une stratégie sur l'action utilisateur « Enregistrer ou joindre des appareils » exigeant la MFA.

4 **Bloquer le flux d'authentification par code d'appareil** ENTRA · L1

Remédiation : Portail Entra > Accès conditionnel : créer une stratégie ciblant les flux d'authentification par code d'appareil avec l'octroi « Bloquer ».

5 **Contrôler les connecteurs de messagerie entrants et sortants** EXCHANGE · L1

Remédiation : Centre d'administration Exchange > Flux de messagerie > Connecteurs : imposer TLS et restreindre les domaines ou adresses IP d'origine.

6 **Recenser les appareils non conformes** INTUNE · L1

Remédiation : Configurez ce point dans le centre d'administration Microsoft Intune.

7 **Analyser l'affectation des profils de configuration** INTUNE · L2

Remédiation : Configurez ce point dans le centre d'administration Microsoft Intune.

8 **Contrôler les relations de fédération et la configuration ADFS** ENTRA · L2

Remédiation : Auditez les domaines fédérés (authenticationType) et migrez vers l'authentification cloud (PHS/PTA + SSO fluide) lorsque c'est possible.

Détail des contrôles

RÉFÉRENTIEL	CONTRÔLE	NIV.	STATUT
Defender	**Activer Liens fiables pour les applications Office et Teams** CIS Microsoft 365 2.1.1 · NIST SI-3 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b)	L1	Conforme
Defender	**Bloquer les comptes dépassant les limites d'envoi sortant** CIS Microsoft 365 2.1.3 · NIST SI-4 · ISO 27001 A.8.16 · DORA Art. 10 · NIS2 21.2(b)	L1	Conforme
Defender	**Ne tolérer aucun incident actif de sévérité haute** → Portail Defender > Incidents : mobiliser la réponse sur tout incident de sévérité haute (confinement, éradication, post-mortem). NIST IR-4 · ISO 27001 A.5.26 · DORA Art. 10 · NIS2 21.2(b)	L1	Avertissement
Defender	**Résorber les incidents actifs anciens** NIST IR-4 · ISO 27001 A.5.26 · DORA Art. 10 · NIS2 21.2(b)	L2	Conforme
Defender	**Renforcer les contrôles Applications du score de sécurité** Microsoft Secure Score · NIST · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Entra	**Retirer les comptes désactivés des rôles à privilèges** → Retirez l'attribution de rôle des comptes désactivés. NIST AC-2 · ISO 27001 A.5.18 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Non conforme
Entra	**Exiger la MFA pour tous les utilisateurs** → Accès conditionnel : stratégie ciblant tous les utilisateurs (avec exclusions break-glass) exigeant la MFA, idéalement via une force d'authentification résistante au phishing. CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.2 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Non conforme

RÉFÉRENTIEL	CONTRÔLE	NIV.	STATUT
Entra	**Exiger la MFA pour la jointure et l'enregistrement d'appareils** → Accès conditionnel : créez une stratégie sur l'action utilisateur « Enregistrer ou joindre des appareils » exigeant la MFA. CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Non conforme
Entra	**Bloquer le flux d'authentification par code d'appareil** → Portail Entra > Accès conditionnel : créer une stratégie ciblant les flux d'authentification par code d'appareil avec l'octroi « Bloquer ». NIST AC-3 · ISO 27001 A.5.15 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Non conforme
Entra	**Contrôler les relations de fédération et la configuration ADFS** → Auditez les domaines fédérés (authenticationType) et migrez vers l'authentification cloud (PHS/PTA + SSO fluide) lorsque c'est possible. CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L2	Non conforme
Entra	**Limiter la durée maximale d'activation des rôles PIM** → Entra > PIM > Paramètres du rôle > Activation : réduire « Durée maximale d'activation » à 8 heures ou moins. CIS Entra ID · NIST AC-6 · ISO 27001 A.5.15 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L2	Non conforme
Entra	**Exiger des appareils conformes ou hybrid joined** CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A. 8.2, A.8.5 · CISA SCuBA MS.AAD.3.7 · DORA Art. 9 · NIS2 21.2(h)	L2	Conforme
Entra	**Exiger une application approuvée ou une stratégie de protection d'application** CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A. 8.2, A.8.5 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Entra	**Bloquer l'authentification héritée** → Accès conditionnel : créez une stratégie ciblant les clients d'authentification héritée (Exchange ActiveSync et autres) avec l'octroi « Bloquer ». CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A. 8.2, A.8.5 · CISA SCuBA MS.AAD.1.1 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Non évalué
Entra	**Activer la correspondance de numéro dans Microsoft Authenticator** CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.3 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Conforme
Entra	**Prévoir des comptes d'accès d'urgence (break-glass)**	L1	Conforme

RÉFÉRENTIEL	CONTRÔLE	NIV.	STATUT
	CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)		
Entra	**Éliminer les attributions de rôles privilégiés permanentes** CIS Entra ID 1.1.4 · NIST AC-6(1) · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.4 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Entra	**Interdire les URI de redirection non sécurisés (HTTP)** CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Entra	**Configurer des alertes sur les modifications de stratégies d'accès conditionnel** CIS Entra ID · NIST AU-6 · ISO 27001 A.8.15 · ANSSI MFA · DORA Art. 10 · NIS2 21.2(b)	L2	Conforme
Entra	**Interdire les comptes invités dans les rôles à privilèges** → Retirez les comptes invités des rôles à privilèges et créez des comptes internes dédiés. CIS Entra ID 1.1.3 · NIST AC-6 · ISO 27001 A.5.15 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Avertissement
Entra	**Activer le signalement d'activité suspecte** CIS Entra · NIST IR-6 · ISO 27001 A.6.8 · DORA Art. 10 · NIS2 21.2(b)	L1	Conforme
Entra	**Restreindre la création de groupes Microsoft 365** CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Entra	**Configurer les paramètres de diagnostic Entra vers Azure Monitor** CIS Entra ID · NIST AU-2 · ISO 27001 A.8.15 · CISA SCuBA MS.AAD.4.1 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b)	L1	Conforme
Entra	**Utiliser des unités administratives à gestion restreinte** NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Entra	**Éliminer les méthodes d'authentification faibles sur les comptes à privilèges** CIS Entra ID 1.1.6 · NIST IA-2(8) · ISO 27001 A.8.5 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(j)	L2	Conforme
Entra	**Limiter le nombre d'administrateurs généraux entre deux et quatre** → Portail Entra > Rôles et administrateurs > Administrateur général : retirez les comptes superflus pour ne conserver que 2 à 4 titulaires,	L1	Non évalué

RÉFÉRENTIEL	CONTRÔLE	NIV.	STATUT
	et remplacez les affectations permanentes par de l'éligible PI CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.1 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)		
Entra	**Auditer les principaux de service à forte permission avec identifiants actifs** CIS Entra · NIST IA-5 · ISO 27001 A.8.2 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b)	L2	Conforme
Entra	**Utiliser des comptes d'administration dédiés et cloud-only** CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.3 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Conforme
Entra	**Empêcher les utilisateurs non administrateurs de créer des tenants** CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Conforme
Entra	**Exiger la MFA pour les utilisateurs externes et invités** CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A. 8.2, A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Conforme
Entra	**Empêcher les utilisateurs de récupérer les clés BitLocker** CIS Entra · NIST AC-6 · ISO 27001 A.8.2 · DORA Art. 9 · NIS2 21.2(h)	L2	Conforme
Exchange	**Contrôler les connecteurs de messagerie entrants et sortants** → Centre d'administration Exchange > Flux de messagerie > Connecteurs : imposer TLS et restreindre les domaines ou adresses IP d'origine. CIS Microsoft 365 6.x · NIST SC-8 · ISO 27001 A. 8.20 · DORA Art. 9 · NIS2 21.2(i)	L1	Non conforme
Exchange	**Activer Pièces jointes fiables (Safe Attachments)** CIS Microsoft 365 · NIST SI-3 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b)	L1	Conforme
Exchange	**Interdire les règles de flux qui autorisent des domaines ou IP** CIS Microsoft 365 · NIST SI-8 · ISO 27001 A.8.12 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Exchange	**Désactiver le transfert automatique via les domaines distants** CIS Microsoft 365 · NIST AC-4 · ISO 27001 A.8.12 · DORA Art. 9 · NIS2 21.2(i)	L1	Conforme
Exchange	**Recenser les boîtes aux lettres avec transfert configuré** CIS Microsoft 365 · NIST AC-4 · ISO 27001 A.8.12 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme

RÉFÉRENTIEL	CONTRÔLE	NIV.	STATUT
Exchange	**Activer les MailTips pour les utilisateurs** → Set-OrganizationConfig -MailTipsAllTipsEnabled $true -MailTipsExternalRecipientsTipsEnabled $true. CIS Microsoft 365 · NIST AT-2 · ISO 27001 A.6.3 · DORA Art. 9 · NIS2 21.2(i)	L2	Avertissement
Exchange	**Déployer une politique d'authentification bloquant l'authentification héritée** CIS Microsoft 365 · NIST IA-2 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(j)	L1	Conforme
Exchange	**Désactiver les protocoles hérités boîte par boîte** CIS Microsoft 365 6.5.x · NIST IA-2 · ISO 27001 A.5.17 · DORA Art. 9 · NIS2 21.2(i)	L1	Conforme
Exchange	**Marquer les messages provenant de l'extérieur** → Exchange Online PowerShell : Set-ExternalInOutlook -Enabled $true. CIS Microsoft 365 6.2.3 · NIST SI-8 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L1	Avertissement
Exchange	**Activer la conservation inaltérable sur les boîtes sensibles** → Centre d'administration Exchange > Boîtes aux lettres > Fonctionnalités : activer la conservation inaltérable sur les comptes sensibles. NIST SI-12 · ISO 27001 A.5.33 · DORA Art. 9 · NIS2 21.2(i)	L2	Avertissement
Intune	**Analyser l'affectation des profils de configuration** → Configurez ce point dans le centre d'administration Microsoft Intune. CIS Intune · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i)	L2	Non conforme
Intune	**Recenser les appareils non conformes** → Configurez ce point dans le centre d'administration Microsoft Intune. CIS Intune · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(h)	L1	Non conforme
Intune	**Exiger l'approbation multi-administrateur pour les actions destructrices** CIS Intune · NIST AC-6 · ISO 27001 A.8.2 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Intune	**Déployer des politiques de protection des applications** CIS Intune · NIST AC-19 · ISO 27001 A.8.1 · DORA Art. 9 · NIS2 21.2(i)	L1	Conforme
Intune	**Contrôler les scripts PowerShell déployés**	L2	Conforme

RÉFÉRENTIEL	CONTRÔLE	NIV.	STATUT
	CIS Intune · NIST CM-7 · ISO 27001 A.8.19 · DORA Art. 9 · NIS2 21.2(i)		
OneDrive	**Appliquer les restrictions imposées par l'application aux appareils non gérés** CIS Microsoft 365 · CISA SCuBA · NIST AC-3 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(h)	L2	Conforme
OneDrive	**Notifier les propriétaires OneDrive des partages externes** CIS Microsoft 365 · NIST AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
OneDrive	**Définir une limite de stockage OneDrive par défaut** CIS Microsoft 365 · NIST PM-1 · ISO 27001 A.5.1 · DORA Art. 10 · NIS2 21.2(b)	L2	Conforme
Purview	**Activer le journal d'audit unifié** CIS Microsoft 365 · NIST AU-2 · ISO 27001 A.8.15 · CISA SCuBA MS.DEFENDER.6.1 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b)	L1	Conforme
Purview	**Activer l'étiquetage automatique des documents sensibles** CIS Microsoft 365 3.5 · NIST MP-3 · ISO 27001 A.5.12 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Purview	**Publier des étiquettes de rétention** CIS Microsoft 365 · NIST SI-12 · ISO 27001 A.5.33 · DORA Art. 9 · NIS2 21.2(h)	L2	Conforme
Purview	**Définir une action de blocage sur les règles DLP** CIS Microsoft 365 3.2 · NIST AC-4 · ISO 27001 A.8.12 · CISA SCuBA MS.DEFENDER.4.2 · DORA Art. 9 · NIS2 21.2(h)	L1	Conforme
SharePoint	**Masquer l'interface de création de sites** → Centre d'administration SharePoint > Paramètres > Création de sites : masquer la commande « Créer un site » pour les utilisateurs. Microsoft Secure Score · NIST PM-1 · ISO 27001 A.5.1 · DORA Art. 9 · NIS2 21.2(i)	L2	Non conforme
SharePoint	**Limiter l'accès SharePoint depuis les appareils non gérés** CIS Microsoft 365 · NIST AC-3 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(h)	L2	Conforme
SharePoint	**Définir une limite de stockage par défaut des nouveaux sites** Microsoft Secure Score · NIST PM-1 · ISO 27001 A.5.1 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
SharePoint	**Déconnecter les sessions inactives** CIS Microsoft 365 · NIST AC-12 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(i)	L1	Conforme

RÉFÉRENTIEL	CONTRÔLE	NIV.	STATUT
SharePoint	**Restreindre les domaines de partage externe** CIS Microsoft 365 · NIST AC-21 · ISO 27001 A.5.14 · CISA SCuBA MS.SHAREPOINT.1.3 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Teams	**Limiter les équipes publiques** → Passer en revue les équipes publiques et basculer celles non légitimes en « Privé » (paramètres d'équipe ou Set-Team -Visibility Private). CIS Microsoft 365 · NIST AC-3 · ISO 27001 A.5.15 · DORA Art. 9 · NIS2 21.2(i)	L2	Avertissement
Teams	**Maîtriser le partage de canaux avec des utilisateurs externes** CIS Microsoft 365 · NIST AC-3 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Teams	**Bloquer le consentement RSC personnel des applications Teams** CIS Microsoft 365 · NIST AC-6 · ISO 27001 A.8.2 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Teams	**Bloquer l'accès des invités au contenu des groupes** CIS Microsoft 365 · NIST AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme
Teams	**Définir des directives d'utilisation pour les invités** → Paramètre de répertoire Group.Unified : renseigner GuestUsageGuidelinesUrl vers la page de directives destinée aux invités. CIS Microsoft 365 · NIST AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L2	Avertissement
Teams	**Contrôler l'accès des utilisateurs anonymes aux réunions** CIS Microsoft 365 · NIST AC-14 · ISO 27001 A.8.3 · DORA Art. 9 · NIS2 21.2(i)	L2	Conforme