Corrigé Activité P1C4

Pour résoudre cette situation, il faut appliquer les principes du Zero Trust (Vérification explicite, Moindre privilège, etc.) en les adaptant à la surface de contrôle que vous offre chaque modèle de service :

- **Environnement On-premise (Application de production héritée)**
    - *Exigence Zero Trust* : Les accès administratifs au serveur On-premise doivent être micro-segmentés et opérés via un bastion (PAM).
    - *Preuve de vérification* : Extraction des journaux d'audit du bastion démontrant que 100 % des connexions d'administration RDP/SSH sont enregistrées et proviennent du réseau dédié.
    - *RACI* : La **Sécurité est (R)** (elle prescrit la règle du bastion et vérifie les logs), l'**Équipe IT / Infra est (A)** (elle configure le serveur pour n'accepter que l'IP du bastion).
    - *Raisonnement* : Sur le On-premise, vous maîtrisez le réseau. Face au risque de mouvement latéral, vous forcez le passage par un point de contrôle unique et auditable.
- **Environnement SaaS (CRM)**
    - *Exigence Zero Trust* : L'authentification au CRM doit être exclusivement déléguée à l'IdP central de l'entreprise avec application d'une politique d'accès conditionnel (MFA obligatoire et appareil conforme).
    - *Preuve de vérification* : Fiche de configuration du SSO (SAML/OIDC) validée, et logs de l'IdP prouvant que les connexions au CRM sont soumises à la vérification des appareils.
    - *RACI* : La **Sécurité est (R)** (elle impose l'intégration IdP), l'**Équipe IAM / IT est (A)** (elle paramètre le connecteur SSO avec le fournisseur SaaS).
    - *Raisonnement* : Sur le SaaS, vous ne maîtrisez ni le réseau ni l'OS. Votre seul périmètre de défense face au risque de fuite de données est l'Identité. Vous appliquez donc la vérification explicite avant d'accorder l'accès aux données.