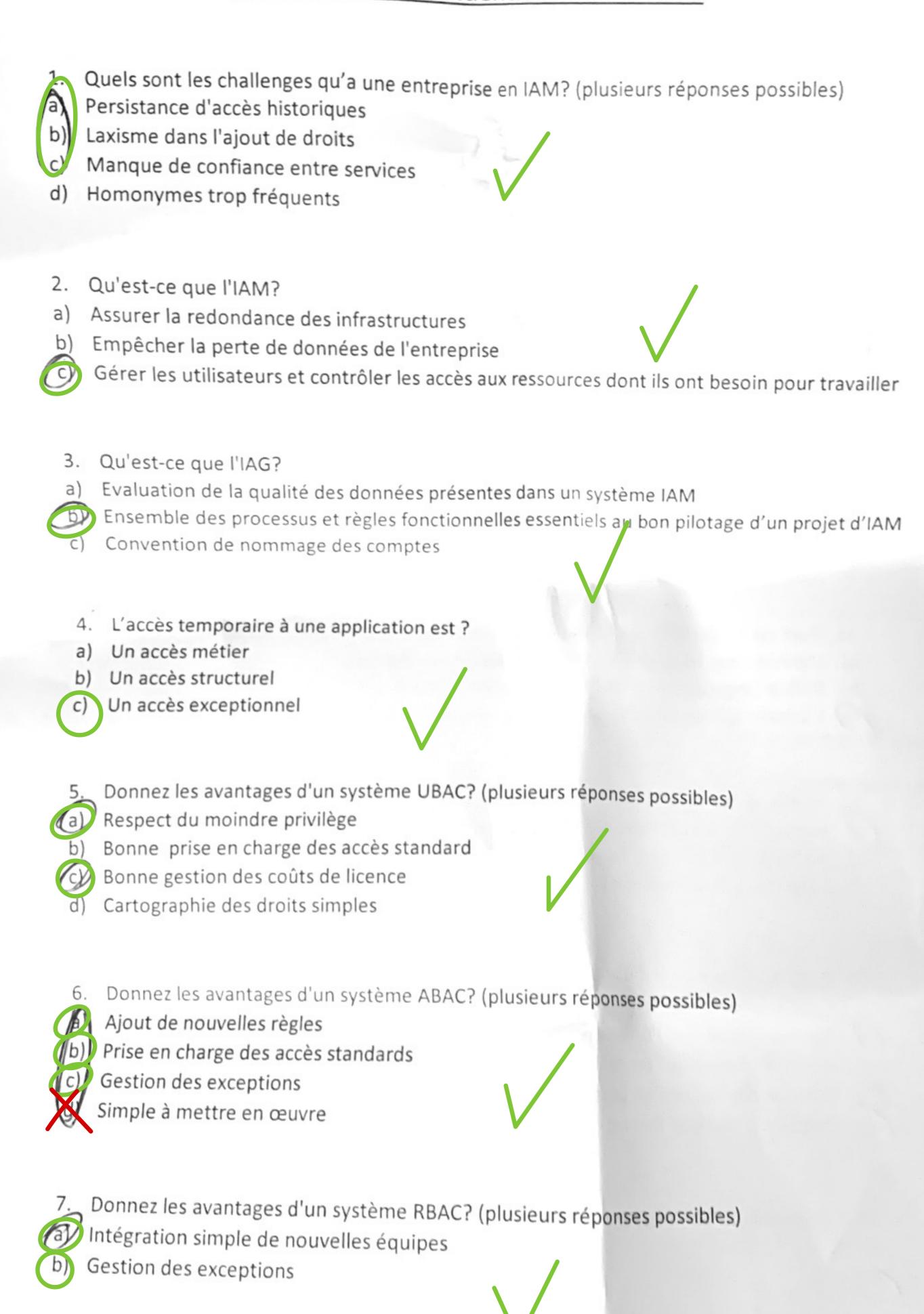


## Sujet : Gestion des identités et des accès







(c) Recommandé par l'ANSSI Facile à superviser

8. Quels sont les actions standards de gestion du cycle de vie des identités? (plusieurs réponses



Joiner

Leaver

Mover

Manager





Auditer simplement



Optimiser les coûts

Informer des modifications RHs



a) La re certification des rôles métiers



La rectification des profils techniques

La re certification des privilèges



a) S'assurer que les employés sont dans les bonnes équipes

Définir l'organigramme de l'entreprise simplement



S'assurer qu'aucune action sensible ne peut être réalisée par une seule équipe ou personne

12. Qu'est-ce que l'AM?



Authentifier les utilisateurs afin de garantir la légitimité d'un accès à une ressource.

Authentifier fortement les utilisateurs (double facteur)

Avoir une identité unique sur toutes les applications

13. Quels sont les moyens d'authentification composant une authentification forte? (plusieurs réponses possibles)

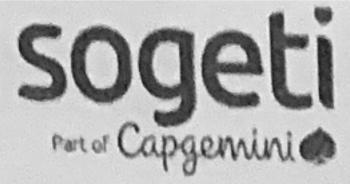
Quelque chose que l'on sait

Quelque chose que l'on comprend Quelque chose que l'on possède

Quelque chose que l'on est









- c) 3
- d) 4
- 15. Qu'est-ce que l'authentification out of band?
- a) C'est une authentification qui s'adapte à l'utilisateur connecté en fonction du contexte
- b) Elle consiste à comparer le comportement de l'utilisateur par rapport à son « empreinte comportementale ».
- c) C'est une authentification qui s'adapte à l'utilisateur connecté en fonction du risque

  Elle consiste à recourir, pour un facteur d'authentification, à un canal différent de celui utilisé pour accéder à l'application.
  - 16. Quel est l'objectif du eSSO?
  - a) Le principe de base est d'intercepter les requêtes entre le client et le serveur, et indiquer au serveur que le client est bien authentifié
    - Cela consiste à entrer à la place de l'utilisateur, ses informations de connexion préalablement connues.
  - 17. Quels sont les intérêts de la fédération d'identité? (plusieurs réponses possibles)

    a) La protection de la vie privée
  - b) Le fournisseur de service (SP) ne gère plus les identités, il fait confiance à l'IDP.
  - L'accès transparent aux fournisseurs de service d) Chiffrer les mots de passe
  - 18. Quelle est la version du SAML déployée aujourd'hui ?
  - a) SAML 1.0
  - by SAML 2.0
    - SAML 2.1
    - 19. Quel est le rôle de l'Identity Provider ?
    - C'est celui qui construit et transmet une assertion à destination de l'application cible
    - b) C'est celui qui protège l'application cible contre les accès non authentifiés ;
    - c) C'est celui qui crée une session pour l'utilisateur sur l'application cible.
    - 20. Quelle est la bonne cinématique SAML?
    - a) L'utilisateur accède au Service Provider, est redirigé vers l'Identity Provider, s'authentifie à l'Identity Provider, est redirigé vers le Service Provider avec une réponse SAML;
    - b) L'utilisateur accède à l'Identity Provider, est redirigé vers le SP, s'authentifie au Service Provider, est redirigé vers l'Identity Provider avec une réponse SAML;
      - c) L'utilisateur s'authentifie sur l'application, est redirigé vers le Service Provider, reçoit une réponse SAML et la transmet à l'Identity Provider pour validation.

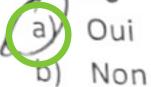


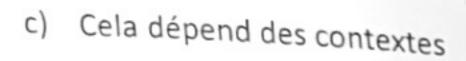


- 21. A l'état de l'art, toutes les applications internes en entreprise :
- a) Ont un référentiel d'identité uniques pour simplifier la gestion ;
- b) S'authentifient avec des mots de passe différents par application pour diminuer le risque ;
- c) Ont un référentiel par application pour être indépendantes.
- 22 Quel est l'objectif du cIAM ?
- (a) Avoir une vision unifiée des clients, partenaires et grand public à la fois sécurité et métier ;
- b) Avoir un mot de passe unique pour tous les clients ;
- c) Permettre un audit simple des comptes à privilèges.
- 23. Quelles sont les briques couvertes par le cIAM? (plusieurs réponses possibles)
- Enregistrement et Accès Stockage et Traitement
- c) Offrir un service de SSO sur les périphériques mobiles tels que les smartphones et les tablettes.
  - 24. Quelle affirmation est vraie?
- a) Il est plus important d'avoir des performances sur les applications internes que cIAM;
  (b) Il y a plus d'utilisateurs gérés dans des projets cIAM que IAM;
  - c) Les RHs sont la source d'information unique des données pour les comptes clients.
  - 25. Quels comptes sont des comptes à privilèges? (plusieurs réponses possibles)
- (a) Un compte bancaire
  - Un compte réseau social d'entreprise
  - Un compte d'administration Un compte royal canin
- 26. Quels sont les standards les plus connus en fédération d'identités? (plusieurs réponses possibles)
- (a) OAuth2
  - b) SSH
- OpenIDConnect
  - 27. Les comptes applicatifs sont-ils des comptes à privilèges?
  - a) Oui
- b) Non
- (c) Cela dépend des contextes

28. Les comptes d'administration sont-ils des comptes à privilèges?

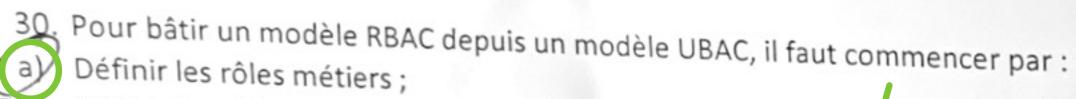








- 29. Quelle affirmation est vraie?
- A l'état de l'art du modèle RBAC, chaque utilisateur bénéficie d'un seul rôle métier ;
  - Dans un modèle RBAC, les utilisateurs qui ont le même rôle métier n'ont pas les mêmes
  - c) Le modèle RBAC est le modèle le plus mature sur le marché.



- Définir les rôles techniques ;
  - Définir le niveau de confiance dans l'authentification.