

## DOMAINE 1 - LE PROCESSUS D'AUDIT DES IT

1. Pendant l'étape de planification d'un audit informatique, le but principal de l'auditeur est :
  - A. de traiter les objectifs de l'audit.
  - B. de recueillir suffisamment de preuves.
  - C. d'établir les spécifications des tests appropriés.
  - D. de minimiser les ressources de l'audit.
  
2. Lors de la sélection des procédures d'audit, l'auditeur en SI devrait utiliser son jugement professionnel pour garantir que:
  - A. Les preuves recueillies sont suffisantes.
  - B. Toutes les défaillances significatives identifiées seront corrigées dans une période raisonnable.
  - C. Toutes les faiblesses matérielles seront identifiées.
  - D. Les coûts de l'audit seront maintenus au minimum.
  
3. Un test approfondi pour vérifier la précision de l'inventaire des bandes magnétiques aurait pour objectif principal :
  - A. la détermination si les lecteurs de code à barres sont installés.
  - B. la détermination si le déplacement de bandes est autorisé.
  - C. la conduite d'un comptage physique de l'inventaire des bandes.
  - D. le contrôle si les entrées et sorties des bandes sont exactement enregistrées.
  
4. Pour déterminer le montant des chèques émis à chaque fournisseur pendant une période indiquée par rapport aux factures comptabilisées, l'auditeur en SI devrait utiliser :
  - A. une technique de simulation en parallèle.
  - B. un logiciel de vérification généralisé.
  - C. des données d'essai.
  - D. un échantillon statistique de données.
  
5. Lors de toutes les phases d'une mission d'audit, l'auditeur en SI devrait se concentrer sur:
  - A. la collection de preuve.
  - B. l'échantillonnage.
  - C. les tests approfondis.
  - D. la documentation de l'audit.
  
6. En exécutant une enquête légale informatique (expertise judiciaire), un auditeur de SI devrait être concerné, pour ce qui est des preuves rassemblées, par:
  - A. l'analyse des preuves.
  - B. l'évaluation des preuves.
  - C. la préservation des preuves.
  - D. la divulgation de preuves.
  
7. Un auditeur en SI interrogeant un employé de bureau affecté à la gestion informatisée de la paie, constate que ses réponses ne correspondent pas à sa description d'emploi ni aux procédures documentées. Dans ces circonstances, l'auditeur devrait :
  - A. conclure que les contrôles sont inadéquats.
  - B. élargir la portée pour y inclure des tests approfondis.
  - C. se fier fortement sur les audits précédents.
  - D. suspendre l'audit.

8. Un auditeur en SI publie un rapport d'audit montrant un manque de protection au niveau de la passerelle du réseau et son périmètre par l'intermédiaire du firewall utilisé ; il recommande alors le produit d'un fournisseur pour traiter cette vulnérabilité. L'auditeur en SI a échoué dans l'exercice de :
  - A. l'indépendance professionnelle.
  - B. l'indépendance d'organisation.
  - C. sa compétence technique.
  - D. sa compétence professionnelle.
  
9. La raison principale pour laquelle un auditeur en SI exécute un parcours des fonctionnalités pendant la phase préliminaire d'une mission d'audit est:
  - A. de comprendre les processus métiers supportés par le SI .
  - B. de se conformer aux normes de vérification.
  - C. d'identifier la faiblesse des contrôles.
  - D. de planifier des essais approfondis.
  
10. Dans un processus d'évaluation des contrôles des modifications de maintenance d'un programme pour lequel les codes sources initiaux ne sont plus conservés, un auditeur en SI utiliserait un logiciel de comparaison de code source pour:
  - A. examiner des changements de programme source sans informations provenant du personnel informatique.
  - B. découvrir un changement de programme source fait entre le moment de l'acquisition de la copie de programme source et l'exécution de la comparaison.
  - C. confirmer que la copie contrôlée est la version actuelle du programme en production.
  - D. garantir que tous les changements faits dans la copie source actuelle sont découverts.

## DOMAINE 2 - GOUVERNANCE IT

1. Parmi les actions suivantes, l'élément le plus important pour l'implantation réussie d'un programme de gouvernance IT serait de :
  - A. Implanter un tableau d'indicateurs informatiques.
  - B. Identifier les stratégies de l'organisation.
  - C. Exécuter une analyse des risques.
  - D. Créer une politique de sécurité formelle.
  
2. Pour aider les gestionnaires dans l'accomplissement de l'alignement des systèmes IT sur les objectifs métiers, un auditeur en SI devrait recommander l'utilisation de:
  - A. une auto-évaluation des contrôles.
  - B. une analyse d'impact sur les affaires.
  - C. un tableau de bord TI équilibré,
  - D. une réingénierie de processus d'affaires.
  
3. Pendant le déroulement d'une mission d'audit, un auditeur en SI remarque que le principe de séparation des tâches n'est pas respecté dans un service. Dans une telle circonstance, l'auditeur devrait chercher:
  - A. des contrôles de chevauchement.
  - B. des contrôles préventifs,
  - C. des contrôles compensatoires.
  - D. des contrôles d'accès logiques.
  
4. Parmi les activités suivantes, laquelle devrait être exécutée par une autre personne que l'administrateur de la base de données (DBA)?
  - A. Le fait d'effacer journaux d'activité de la base de données
  - B. Le fait d'implanter des outils d'optimisation de la base de données
  - C. Surveiller l'usage de base de données
  - D. Le fait de définir les procédures d'archivage et de récupération
  
5. Pour traiter le risque d'échec du personnel des opérations à exécuter la procédure d'archivage quotidien, le gestionnaire exige que l'administrateur des systèmes termine avec l'archivage quotidien. C'est un exemple de risque:
  - A. évité.
  - B. transféré.
  - C. atténué
  - D. accepté;

6. Un choix de mots de passe faible et la transmission de données sur des réseaux de communication non protégés sont des exemples de:
- A. vulnérabilités.
  - B. menaces.
  - C. probabilités.
  - D. impacts.
7. On a désigné un auditeur en SI pour analyser l'organisation d'un service d'un service IT ainsi que les activités récemment sous-traitées à des fournisseurs externes différents. Laquelle des actions suivantes, l'auditeur devrait-il déterminer en PREMIER?
- A. Qu'une clause d'audit soit présente dans tous les contrats
  - B. Que le contrat de niveau de service (SLA) de chaque contrat soit justifié par un indicateur clé de performance(KPI) approprié
  - C. Que les garanties contractuelles des fournisseurs soutiennent les objectifs business de l'organisation
  - D. qu'à la résiliation de contrat du actuel fournisseur, celui-ci garantit son soutien au nouveau fournisseur qui reprendrait le contrat
8. Pour obtenir une compréhension de l'efficacité de la planification et de gestion d'une organisation et de ses investissements dans des systèmes d'information, un auditeur en SI devrait revoir :
- A. le modèle de données d'entreprise.
  - B. le tableau de bord équilibré des TI (IT Balanced Scorecard).
  - C. la structure organisationnelle des TI.
  - D. l'historique des états financiers.
9. En ce qui concerne l'externalisation des services IT, laquelle de conditions suivantes devraient avoir de la plus grande importance aux yeux d'un auditeur en SI ?
- A. Les activités imparties (externalisées) sont au cœur des activités métiers et fournissent un avantage appréciable à l'organisation.
  - B. La renégociation périodique est spécifiée dans le contrat d'externalisation.
  - C. Le contrat d'externalisation ne couvre pas toutes les actions requises durant la réalisation des services.
  - D. Les activités semblables sont externalisées à plus d'un fournisseur.
10. Un exemple d'un avantage direct provenant des retombées d'un investissement IT concernant les affaires est:
- A. l'amélioration de la réputation de l'entreprise.
  - B. le moral du personnel est amélioré.
  - C. l'utilisation de nouvelles technologies.
  - D. le niveau pénétration du marché est amélioré.

---

DOMAINE 3 - GESTION DU CYCLE DE VIE DES SYSTÈMES ET DES INFRASTRUCTURES

1. Un auditeur en SI impliqué dans la phase d'analyse préliminaire d'un projet de développement d'une nouvelle application devra s'assurer que:
  - A. les programmeurs fournissent les solutions aux exigences fonctionnelles.
  - B. les exigences de sécurité ont été définies.
  - C. le coût pour l'entretien du système est dans une marge acceptable.
  - D. une solution clés en main pour couvrir les besoins du système est disponible.
  
2. Pour garantir l'identification des erreurs d'interface internes d'application le plus tôt possible, l'approche la plus appropriée pour les essais serait:
  - A. une approche du bas vers le haut (bottom up).
  - B. des essais avec les utilisateurs.
  - C. une approche du haut vers le bas (top down).
  - D. des essais de système.
  
3. Dans un projet de développement de système où il est difficile de fixer et stabiliser les exigences de base du système, la méthode recommandée pour le développement serait:
  - A. la programmation en ligne.
  - B. le développement classique des systèmes
  - C. la méthode du temps fixe (Timebox).
  - D. la programmation agile,
  
4. En analysant les contrôles liés à la saisie, un auditeur en SI remarque que conformément à la politique d'entreprise, les procédures de supervision permettent de rectifier des données après leur validation à la saisie. L'auditeur doit auditer:
  - A. qu'il peut y avoir des contrôles compensatoires pour atténuer les risques.
  - B. garantir que les modifications sont automatiquement journalisées pour être revues ultérieurement
  - C. s'assurer que tout changement est référé aux gestionnaires pour approbation.
  - D. recommander que ces modifications ne soient pas autorisées.
  
5. Lors de la mise en place d'infrastructure d'essais intégrée (I TF), l'auditeur devrait s'assurer que:
  - A. ses données de production sont utilisées pour les essais.
  - B. les données d'essai sont isolées des données de production.
  - C. un générateur de données de test est utilisé.
  - D. les fichiers maîtres sont mis à jour avec les données d'essai.

- 
6. La description la plus exacte du modèle de boîte noire d'essai est liée au fait qu'il:
- A. permet d'obtenir la preuve de conformité avec les spécifications, en garantissant que les résultats obtenus à la sortie ont été obtenus uniquement à partir de ce qui a été défini à l'entrée.
  - B. permet de vérifier l'exactitude de la logique du programme et des flux de donnée.
  - C. préconise des essais non documentés entrepris par les utilisateurs pour confirmer que le système est testé dans des conditions réelles.
  - D. permet de démontrer la performance des nouveaux équipements.
7. Pour minimiser le coût d'un projet de développement de système, les techniques de gestion de la qualité devraient être appliquées:
- A. au stade le plus près possible de sa réalisation des activités concernées.
  - B. essentiellement lors du démarrage du projet pour garantir que le projet est aligné sur les normes de gouvernance de l'organisation.
  - C. de façon continue durant tout le projet avec plus d'efforts vers la fin pour identifier les erreurs et les mesures correctives pendant les essais et ce, dans le but de maximiser le taux de détection des anomalies.
  - D. particulièrement à la fin du projet pour détecter les leçons apprises pour pouvoir les appliquer aux projets futurs.
8. Un employé de bureau a changé le taux d'intérêt d'un crédit dans le fichier principal. Le taux saisi n'est pas compris dans la plage normale pour un tel crédit. Laquelle des mesures suivantes est la plus appropriée pour garantir une assurance raisonnable que le changement a été autorisé ?
- A. Le système ne traitera pas le changement tant que le directeur de l'employé de bureau n'a pas confirmé le changement en saisissant un code d'approbation.
  - B. Le système produit un rapport hebdomadaire qui liste tous les taux exceptionnels et ce rapport est analysé par le directeur de l'employé de bureau.
  - C. Le système exige à l'employé de bureau de saisir un code d'approbation.
  - D. Le système affiche un message d'avertissement à l'employé de bureau.
9. Lequel des énoncés suivants est le plus important pour un auditeur de système d'information analysant un processus de sélection d'un fournisseur ?
- A. Le fournisseur qui a été choisi propose le plus bas prix.
  - B. Le fournisseur qui a été choisi propose le prix le plus élevé.
  - C. Le fournisseur a été choisi avant la définition des critères de sélection.
  - D. Certains fournisseurs n'ont pas répondu à la demande d'offre.
10. Dans une stratégie de veille stratégique (Business Intelligence), lequel de ces éléments est indispensable?
- A. Gestion de la relation client (CRM)
  - B. Entrepôt de données
  - C. Intelligence artificielle
  - D. Systèmes de gestion de la qualité

#### DOMAINE 4 - LIVRAISON ET SOUTIEN DES SERVICES I

1. En analysant un programme de maintenance d'une infrastructure, l'auditeur en SI devrait évaluer si:
  - A. le calendrier de toute la maintenance non planifiée est maintenu,
  - B. il est conforme aux tendances historiques.
  - C. il a été approuvé par un comité directeur.
  - D. le programme est validé par rapport aux spécifications des fournisseurs.
  
2. Un auditeur de système d'information devrait recommander l'utilisation d'un logiciel de contrôle de bibliothèque de programmes pour fournir une assurance raisonnable que:
  - A. les changements de programme ont été autorisés.
  - B. seuls, les programmes testés disposeront d'une version.
  - C. les programmes modifiés sont automatiquement déplacés à la production.
  - D. l'intégrité du code source et de son exécutable est maintenue.
  
3. En auditant un coupe-feu de type proxy, l'auditeur doit:
  - A. vérifier que le coupe-feu ne perd pas de paquets transférés.
  - B. reconsidérer les tables de résolution d'adresses (ARP—Address Resolution Protocol) et la correspondance entre les adresses (IP) et les adresses (MAC).
  - C. vérifier que les filtres appliqués aux services comme HTTP sont efficaces.
  - D. évaluer si l'acheminement des informations est effectué correctement par le coupe-feu.
  
4. Laquelle des énoncés suivants décrit une similitude entre le Protocole (TCP) et le Protocole (UDP) ? Les deux protocoles :
  - A. sont liés à la connectivité.
  - B. garantissent la livraison des paquets.
  - C. confirment chaque paquet reçu.
  - D. utiliser des numéros de port pour identifier des applications.
  
5. Quelle configuration de protocole devrait revoir un auditeur en SI pour découvrir un mappage non autorisé entre des adresses (IP) et des adresses (MAC)?
  - A. Le protocole (SOAP)
  - B. Le protocole (ARP)
  - C. Le protocole (RIP)
  - D. Le protocole(TCP)
  
6. L'objectif principal d'un contrat de services (SLA) pour des services SI est :
  - A. définir, s'entendre, enregistrer et diriger les niveaux de service voulus.
  - B. garantir que les services sont organisés pour livrer le plus haut niveau de disponibilité possible.
  - C. garder les prix associés à chaque service au minimum.
  - D. contrôler et signaler toute non-conformité juridique à l'administration d'entreprise.

7. Lequel des énoncés suivants devrait avoir un intérêt **principal** pour un auditeur qui audite l'administration des services TI assurés par un fournisseur externe?
- A. Le fait de minimiser le coût des services fournis
  - B. Le fait d'interdire au fournisseur de sous-traiter à son tour
  - C. Le fait d'évaluer le processus de transférer de la connaissance au département des TI
  - D. La détermination si les services ont été fournis selon les ententes
8. Les meilleures pratiques TI pour la disponibilité et la continuité des services devrait :
- A. minimiser les coûts associés aux bris de composantes en cas de désastre.
  - B. prévoir une capacité suffisante pour satisfaire les demandes convenues des lignes d'affaires.
  - C. fournir l'assurance raisonnable que les obligations convenues avec les clients peuvent être rencontrées.
  - D. produire des rapports et métriques sur la performance.
9. Une organisation a récemment installé un correctif de sécurité, qui a provoqué un arrêt du serveur de production. Pour réduire les chances que cela se reproduise de nouveau, l'auditeur doit recommander:
- A. d'appliquer le correctif selon les notes documentaires du correctif.
  - B. de s'assurer qu'un bon processus de gestion du changement est place.
  - C. d'évaluer correctement le correctif avant sa migration en production.
  - D. d'approuver le correctif après une analyse des risques.
10. Durant la maintenance d'une base de données relationnelle, plusieurs valeurs de la clé étrangère d'une table transactionnelle d'une base de données relationnelle ont été corrompues. La conséquence est que:
- A. le détail des transactions impliquées ne peut plus être associé aux données principales, provoquant ainsi des erreurs lorsque ces transactions sont complétées.
  - B. il n'y a aucune façon de reconstruire les informations perdues, sauf en effaçant les références perdues et en réentrant dans les transactions.
  - C. la base de données s'arrêtera immédiatement et perdra plus d'informations.
  - D. la base de données n'acceptera plus de données saisies.
11. Dans une base de données relationnelle avec gestion de l'intégrité référentielle, laquelle des clés suivantes, préviendrait l'effacement d'une rangée de la table client tant que le nombre de clients est mémorisé avec les commandes en ligne dans une table des commandes ?
- A. Clé étrangère
  - B. Clé primaire
  - C. Clé secondaire
  - D. Clé publique
12. L'objectif principal de réaliser une révision post-incident consiste dans l'opportunité:
- A. d'améliorer des procédures de contrôle internes.
  - B. d'endurcir le réseau selon les meilleures pratiques de l'industrie.
  - C. de faire ressortir l'importance de la gestion de la réaction aux incidents à l'administration.
  - D. d'augmenter la sensibilité des employés au processus de réaction aux incidents.



## DOMAINE 5 - PROTECTION DES ACTIFS INFORMATIIONNELS

1. Lors de la vérification d'un serveur Web, un auditeur en SI devrait estimer le risque d'accès non autorisé à de l'information confidentielle à un plus haut niveau, s'il y a utilisation de:
  - A. scripts utilisant des composants (CGI).
  - B. composants java d'entreprise (EJBs).
  - C. applets.
  - D. services Web.
  
2. D'une perspective de contrôle, l'objectif principal de classier les actifs informationnels est:
  - A. d'établir des directives pour le niveau de contrôles d'accès qui devraient être accordé.
  - B. de garantir que les contrôles d'accès sont accordés à tous les actifs informationnels.
  - C. d'aider l'administration et les auditeurs dans l'appréciation des risques.
  - D. d'identifier que les actifs qui doivent être assurés contre les pertes.
  
3. Une organisation a récemment subi des compressions de personnel. Dans ce cadre, un auditeur en SI décide d'évaluer des contrôles d'accès logiques. Quelle est la préoccupation principale de l'auditeur :
  - A. tout accès logique est autorisé et approprié pour le rôle d'un individu et ses responsabilités.
  - B. les gestionnaires ont autorisés des accès logiques appropriés pour tous les individus nouvellement embauchés.
  - C. seulement l'administrateur du système possède les privilèges pour accorder ou modifier les accès logiques.
  - D. des formulaires d'autorisation d'accès sont utilisés pour accorder ou modifier l'accès aux individus.
  
4. Un auditeur en SI analysant les contrôles d'accès pour un environnement client-serveur devrait d'abord :
  - A. évaluer la technique de cryptage.
  - B. identifier les points d'accès au réseau.
  - C. reconsidérer le système de gestion d'identité.
  - D. reconsidérer les contrôles d'accès au niveau de l'application.
  
5. Pour prévenir des attaques de mystification (IP spoofing), un coupe-feu devrait être configuré pour bloquer un paquet si:
  - A. le champ source ou origine du routage est permis.
  - B. il a une adresse de diffusion dans le champ destination.
  - C. un indicateur de mise à jour (RST) est activé pour la connexion TCP.
  - D. un routage dynamique est utilisé au lieu du routage statique,

6. Lequel des aspects suivants du cryptage avec une clé symétrique, a influencé le développement du cryptage asymétrique?
- A. Capacité de traitement
  - B. Volume de données
  - C. Distribution des clés
  - D. Complexité de l'algorithme
7. L'exposition logique associée à l'utilisation d'une procédure de relance au point de reprise est :
- A. un déni de service.
  - B. une attaque asynchrone.
  - C. de l'espionnage électronique.
  - D. une fermeture des ordinateurs.
8. Lequel des moyens biométriques suivants présente la plus haute fiabilité et le plus bas taux de faux-positifs ?
- A. Scanner de la paume
  - B. Reconnaissance faciale
  - C. Scanner de rétine
  - D. Géométrie de mains
9. Un auditeur en SI qui effectue une revue de l'implantation d'un système de détection d'intrusion (IDS) devrait être le plus concerné par le fait que:
- A. les sondes d'IDS sont placées à l'extérieur du coupe-feu.
  - B. l'IDS est de type comportemental provoque beaucoup fausses alarmes (faux positifs).
  - C. l'IDS à base de signature est faible contre les nouveaux types d'attaques.
  - D. l'IDS est utilisé pour découvrir le trafic crypté.
10. Lequel des énoncés est le meilleur pour décrire le rôle d'un serveur de répertoire dans une infrastructure clé publique (PKI)?
- A. Crypte les informations transmises sur le réseau
  - B. Rend les certificats des utilisateurs disponibles pour les applications
  - C. Facilite l'application d'une politique de mot de passe
  - D. Listes de suspensions de certificats de réserves (CRLs)
11. Une organisation utilise le cryptage symétrique. Laquelle des énoncés suivants serait une raison valide pour changer vers le au cryptage asymétrique? Le cryptage symétrique :
- A. fournit l'authenticité.
  - B. est plus rapide que le cryptage asymétrique.
  - C. peut rendre l'administration des clés difficile.
  - D. exige un algorithme relativement simple.

12. Une mauvaise programmation et des pratiques de codification inadéquates présentent un risque de :
- A. hameçonnage (phishing).
  - B. débordement de mémoire tampon
  - C. attaques de type SYN flood.
  - D. attaques par force brute.
13. Lequel des énoncés suivants, préviendrait les changements effectués sans autorisation aux informations mémorisées dans le journal d'un serveur?
- A. La protection contre l'écriture du répertoire contenant le journal du système
  - B. L'écriture d'un journal en duplicata sur un autre serveur
  - C. Tous les jours, le journal de système est imprimé
  - D. Le fait de copier le journal du système dans un média protégé contre la réécriture
14. Parmi ces choix, lequel fournirait la meilleure protection contre le piratage d'un ordinateur connecté à Internet?
- A. Un serveur d'accès distant
  - B. Un serveur proxy
  - C. Un pare-feu personnel
  - D. Un jeton produisant un mot de passe
15. Dans le processus d'installation d'un système de détection d'intrusion (IDS), qu'est ce qui est le plus important?
- A. localiser correctement l'IDS dans l'architecture de réseau
  - B. prévenir contre les attaques de déni de service (Dos)
  - C. identifier les messages qui doivent être mis en quarantaine
  - D. minimiser les erreurs dans les rejets

## DOMAINE 6 - CONTINUITÉ DES AFFAIRES ET RECOUVREMENT APRÈS SINISTRE

1. Parmi les suivantes, laquelle correspond à la **première** phase dans le développement d'un plan de continuité d'activité:
  - A. identifier des sites externes d'alternatives/endroits de récupération.
  - B. obtenir l'approbation de budget pour un plan de continuité d'affaires.
  - C. préparer une analyse d'impact d'affaires.
  - D. déterminer des exigences technologiques pour de la haute disponibilité (HA).
  
2. Les gestionnaires d'une entreprise ont considéré deux scénarios pour le plan de continuité d'activité ; le plan A avec deux mois pour le rétablissement et le plan B avec huit mois. Les objectifs de récupération sont les mêmes dans les deux plans. Il est raisonnable de s'attendre à ce que le plan B ait surestimé :
  - A. le prix du temps mort.
  - B. le prix de reprise.
  - C. le prix de récupération.
  - D. le survol des coûts.
  
3. Des alternatives suivantes, la **première** étape dans le développement d'une stratégie de reprise après sinistre serait d'évaluer si :S
  - A. toutes les menaces peuvent être complètement enlevées.
  - B. une résilience intégrée peut être implantée à coût optimal :
  - C. l'objectif de temps de récupération peut être optimisé.
  - D. le prix de récupération peut être minimisé.
  
4. Une organisation possède un certain nombre d'unités à travers une large région géographique. Pour garantir que tous les aspects du plan de reprise après sinistre sont évalués selon un coût optimal, l'auditeur en SI devrait recommander l'utilisation de:
  - A. test de récupération de données.
  - B. test opérationnel complet.
  - C. post-test.
  - D. test de préparation.
  
5. Un auditeur en SI devrait recommander l'utilisation d'une salle de secours équipée (hot site) plutôt qu'un accord de services croisés quand:
  - A. l'objectif de temps de récupération est bas.
  - B. la fenêtre d'interruption est haute.
  - C. l'objectif de temps de récupération (RTO) est haut,
  - D. le coût limite de récupération est bas.

6. La stratégie optimale de continuité des activités pour une entité, est déterminée par le:
- A. le coût de temps mort le plus bas et le plus haut coût de récupération,
  - B. la somme la plus basse de coût de temps mort et le coût de récupération.
  - C. coût de récupération le plus bas et le plus haut coût de temps mort.
  - D. la moyenne du temps mort combiné avec le coût de récupération.
7. Dans l'éventualité d'un sinistre au sein d'un centre de données, quelle serait la stratégie la plus appropriée pour permettre une récupération complète d'une base de données critique ?
- A. Les données quotidiennes sauvegardées sur bande et archivage sur un site distant.
  - B. Réplication en temps réel sur un site à distance.
  - C. les disques durs sont en miroir avec un serveur local.
  - D. Les données sont archivées en temps réel dans un réseau de stockage SAN .
8. L'objectif **premier** du test d'un plan de continuité des activités est:
- A. de familiariser des employés avec le plan de continuité d'affaires.
  - B. garantir que tous les risques restants sont traités.
  - C. se préparer à tous les scénarios de désastre possibles.
  - D. identifier les limites du plan de continuité d'affaires.