Voici un QCM de 60 questions entièrement revérifié avec des réponses bien réparties pour éviter les schémas répétitifs. Il couvre l’audit informatique, la gouvernance des SI, la cybersécurité et la conformité réglementaire.

# **QCM – Audit Informatique (60 Questions)**

## **Chapitre 1 : Introduction à l'Audit Informatique**

1. Quelle est la principale mission d’un audit informatique ?  
   a) Former les utilisateurs  
   b) Développer de nouveaux logiciels  
   c) Remplacer les équipements informatiques  
   d) Évaluer et améliorer la sécurité des systèmes d'information

**Réponse : d**

1. L’audit informatique permet principalement de :  
   a) Vérifier la conformité et la performance des systèmes  
   b) Optimiser la programmation des applications  
   c) Modifier les bases de données  
   d) Augmenter la rapidité d’un réseau

**Réponse : a**

1. COBIT est un référentiel qui concerne principalement :  
   a) L’optimisation des performances des applications  
   b) La gouvernance des systèmes d’information  
   c) Le développement de logiciels  
   d) La gestion des bases de données

**Réponse : b**

1. Quelle norme est couramment utilisée pour la gestion de la sécurité de l'information ?  
   a) ITIL  
   b) COBIT  
   c) ISO 27001  
   d) ISO 9001

**Réponse : c**

1. Qui est responsable du cadre de référence COBIT ?  
   a) IEEE  
   b) ISACA  
   c) ISO  
   d) W3C

**Réponse : b**

1. Un audit interne est réalisé par :  
   a) Un organisme gouvernemental  
   b) Une société de cybersécurité indépendante  
   c) Un auditeur interne appartenant à l'organisation  
   d) Un auditeur externe

**Réponse : c**

1. Un audit de conformité vise à :  
   a) Vérifier si une entreprise respecte les réglementations et normes en vigueur  
   b) Tester la performance des ordinateurs  
   c) Évaluer la productivité des employés  
   d) Identifier les bugs logiciels

**Réponse : a**

1. Quelle loi régule la protection des données personnelles en Europe ?  
   a) DMCA  
   b) HIPAA  
   c) GDPR (RGPD)  
   d) SOX

**Réponse : c**

1. Le "Due Diligence" en audit informatique fait référence à :  
   a) Une analyse approfondie avant une acquisition ou une fusion  
   b) Une technique de cryptage avancée  
   c) Un type de virus informatique  
   d) Une formation pour les utilisateurs finaux

**Réponse : a**

1. Quelle est la première étape d’un audit informatique ?  
   a) Former les employés  
   b) Définir les objectifs et le périmètre de l’audit  
   c) Installer un antivirus  
   d) Rédiger un rapport

**Réponse : b**

## **Chapitre 2 : Processus et Outils d'Audit Informatique**

1. Quel outil est utilisé pour analyser les vulnérabilités d’un système ?  
   a) Nessus  
   b) Wireshark  
   c) Notepad++  
   d) Microsoft Excel

**Réponse : a**

1. L’analyse forensique informatique vise à :  
   a) Développer des applications sécurisées  
   b) Identifier les causes d’une cyberattaque  
   c) Augmenter la vitesse du réseau  
   d) Améliorer les performances des ordinateurs

**Réponse : b**

1. Un test d’intrusion (PenTest) est utilisé pour :  
   a) Optimiser l'ergonomie d'une application  
   b) Détecter les failles de sécurité  
   c) Vérifier la compatibilité des logiciels  
   d) Mettre à jour les systèmes d’exploitation

**Réponse : b**

1. Une politique de sécurité efficace doit inclure :  
   a) Un mot de passe unique pour tous les employés  
   b) Un seul administrateur pour toute l’entreprise  
   c) Des règles claires et documentées  
   d) Des mises à jour annuelles obligatoires

**Réponse : c**

1. Quel élément fait partie des 4 piliers de la cybersécurité ?  
   a) Rapidité  
   b) Accessibilité  
   c) Confidentialité  
   d) Convivialité

**Réponse : c**

1. Un IDS (Intrusion Detection System) sert à :  
   a) Détecter les intrusions sur un réseau  
   b) Gérer les bases de données  
   c) Accélérer le fonctionnement d’un serveur  
   d) Rendre les fichiers plus accessibles aux utilisateurs

**Réponse : a**

1. Un firewall est utilisé pour :  
   a) Supprimer les virus d’un ordinateur  
   b) Protéger le réseau contre les accès non autorisés  
   c) Accélérer les téléchargements  
   d) Modifier les fichiers systèmes

**Réponse : b**

1. Un honeypot est :  
   a) Une base de données sécurisée  
   b) Un système conçu pour attirer et piéger les attaquants informatiques  
   c) Un antivirus  
   d) Un pare-feu avancé

**Réponse : b**

1. L’authentification à deux facteurs (2FA) permet de :  
   a) Ajouter une couche supplémentaire de sécurité  
   b) Créer automatiquement des comptes sécurisés  
   c) Simplifier la connexion des utilisateurs en supprimant les mots de passe  
   d) Accélérer le processus d’audit

**Réponse : a**

1. Un DDoS (Distributed Denial of Service) vise à :  
   a) Optimiser la vitesse des requêtes réseau  
   b) Corriger automatiquement les erreurs des serveurs  
   c) Saturer un service en ligne pour le rendre indisponible  
   d) Mettre à jour les logiciels de cybersécurité

**Réponse : c**

Voici la suite du QCM avec les 40 dernières questions. J'ai bien fait attention à ce que l'ordre des réponses ne soit pas répétitif.

## **Chapitre 2 : Processus et Outils d'Audit Informatique (Suite)**

1. Un SIEM (Security Information and Event Management) est utilisé pour :  
   a) Collecter, analyser et surveiller les journaux d'événements de sécurité  
   b) Accélérer la vitesse du réseau  
   c) Gérer les bases de données  
   d) Optimiser le stockage des serveurs

**Réponse : a**

1. Un audit informatique préventif sert à :  
   a) Vérifier uniquement les mots de passe des employés  
   b) Identifier et corriger les vulnérabilités avant qu’elles ne soient exploitées  
   c) Changer régulièrement les équipements informatiques  
   d) Tester la rapidité du réseau

**Réponse : b**

1. Une attaque Man-in-the-Middle (MITM) consiste à :  
   a) Intercepter et modifier les communications entre deux parties sans leur consentement  
   b) Effectuer un test de charge sur un site web  
   c) Envoyer des spams à des utilisateurs ciblés  
   d) Supprimer les fichiers sensibles d’un ordinateur distant

**Réponse : a**

1. Quelle est l'étape finale d’un audit informatique ?  
   a) Installer un nouvel antivirus  
   b) Rédiger le rapport d’audit avec recommandations  
   c) Supprimer les fichiers suspects  
   d) Arrêter les serveurs de l’entreprise

**Réponse : b**

1. Le phishing est une technique qui consiste à :  
   a) Tromper un utilisateur pour lui voler des informations sensibles  
   b) Protéger les fichiers contre la corruption  
   c) Créer un accès sécurisé aux bases de données  
   d) Réparer un système corrompu

**Réponse : a**

1. Un ransomware est un logiciel malveillant qui :  
   a) Optimise la performance des serveurs  
   b) Chiffre les fichiers et exige une rançon pour les débloquer  
   c) Protège les mots de passe des utilisateurs  
   d) Répare automatiquement les fichiers corrompus

**Réponse : b**

1. L’analyse des risques en audit informatique permet de :  
   a) Identifier les menaces potentielles sur le système d’information  
   b) Supprimer automatiquement tous les virus détectés  
   c) Identifier les employés qui utilisent trop Internet  
   d) Remplacer tous les équipements informatiques obsolètes

**Réponse : a**

1. Un test de boîte noire (Black Box Testing) signifie que l’auditeur :  
   a) Travaille uniquement avec des outils automatisés  
   b) N’a aucune information préalable sur le système testé  
   c) A accès aux codes sources et configurations  
   d) Effectue un audit financier

**Réponse : b**

1. Une analyse de vulnérabilité a pour objectif de :  
   a) Identifier les failles de sécurité d’un système informatique  
   b) Modifier les codes sources d’un logiciel  
   c) Accélérer le traitement des données  
   d) Remplacer les anciens équipements informatiques

**Réponse : a**

1. La mise en place d’un plan de reprise d’activité (PRA) permet de :  
   a) Gérer les sauvegardes des données  
   b) Automatiser l’audit des systèmes informatiques  
   c) Assurer la continuité des opérations après un incident informatique  
   d) Bloquer tous les accès réseau en cas d’attaque

**Réponse : c**

## **Chapitre 3 : Gouvernance et Cadres de Référence en Audit Informatique**

1. ITIL est un référentiel qui concerne :  
   a) La gestion des services informatiques (IT Service Management)  
   b) Le développement de logiciels sécurisés  
   c) La réglementation des données personnelles  
   d) La gestion des bases de données

**Réponse : a**

1. Un DPO (Data Protection Officer) est responsable de :  
   a) La suppression automatique des fichiers obsolètes  
   b) L’installation des serveurs et des routeurs  
   c) La protection des données personnelles au sein d’une entreprise  
   d) L’audit financier des entreprises

**Réponse : c**

1. La norme PCI DSS est obligatoire pour :  
   a) Les réseaux sociaux  
   b) Les fournisseurs d’accès Internet  
   c) Les entreprises traitant des paiements par carte bancaire  
   d) Les hôpitaux

**Réponse : c**

1. Une politique de gestion des accès doit :  
   a) Supprimer les mots de passe pour simplifier l’accès  
   b) Permettre à tous les employés d’accéder à toutes les données  
   c) Désactiver tous les pare-feu  
   d) Restreindre les autorisations aux utilisateurs selon leurs besoins

**Réponse : d**

1. Un audit SOX (Sarbanes-Oxley) est obligatoire pour :  
   a) Toutes les entreprises du monde  
   b) Les entreprises cotées en bourse aux États-Unis  
   c) Les écoles et universités  
   d) Les entreprises de e-commerce uniquement

**Réponse : b**

1. Le principe de séparation des tâches (SoD - Segregation of Duties) permet de :  
   a) Réduire les risques de fraude et d’abus en répartissant les responsabilités  
   b) Supprimer les audits financiers  
   c) Bloquer les accès administratifs pour tous les utilisateurs  
   d) Accélérer le travail des employés en fusionnant les rôles

**Réponse : a**

1. Un audit de gouvernance IT vise à :  
   a) Vérifier que les processus IT sont alignés avec la stratégie d’entreprise  
   b) Identifier les failles de sécurité réseau  
   c) Remplacer les systèmes informatiques obsolètes  
   d) Effectuer des tests de charge sur les serveurs

**Réponse : a**

1. Un contrôleur des systèmes d’information (CISA - Certified Information Systems Auditor) est un professionnel qui :  
   a) Conçoit des jeux vidéo  
   b) Crée des bases de données relationnelles  
   c) Développe des applications mobiles  
   d) Effectue des audits IT selon des standards internationaux

**Réponse : d**

1. Le cadre réglementaire HIPAA concerne la protection des :  
   a) Licences de logiciels open source  
   b) Comptes bancaires des entreprises  
   c) Données médicales et de santé aux États-Unis  
   d) Fichiers multimédias des utilisateurs

**Réponse : c**

1. L’objectif du NIST Cybersecurity Framework est de :  
   a) Développer des logiciels antivirus  
   b) Supprimer tous les audits informatiques  
   c) Augmenter la vitesse des réseaux  
   d) Offrir un guide pour gérer et réduire les risques de cybersécurité

**Réponse : d**