**Quizz #1 :**

Quelle est la meilleure personne pour accepter un risque de sécurité de l’information jugé modéré :

* Le RSSI qui a conduit l’analyse des risques
* Le responsable du Service Informatique
* La Direction Générale
* L’audit interne
* Le responsable de la gestion des risques pour l’entreprise

Sensibiliser les employés est une mesure qui constitue un contrôle avant tout :

* Préventif
* Détectif
* Correctif

Quelle est la 1ère étape d’une analyse des risques au niveau du S.I. :

* Comprendre les menaces et le niveau de vulnérabilité envers chacune
* Identifier les actifs à protéger
* Evaluer les risques résiduels
* Déterminer les besoin de sécurité (C, I, D)

Collecter les évènements de sécurité sur les équipements réseau et serveurs permet d’assurer un contrôle :

* Préventif
* Détectif
* Correctif

Disposer d’un plan de secours informatique à jour et aligné sur l’analyse des risques constitue un contrôle :

* Préventif
* Détectif
* Correctif

Pour quelle raison principale une entreprise (par exemple société active dans le commerce électronique) a-t-elle intérêt à s’assurer que ses sous –traitants & partenaires ont en place un système de gestion de la sécurité fonctionnel :

* Pour assurer la conformité réglementaire
* Pour réduire le risque qu’une cyber attaque au niveau d’un sous-traitant puisse compromettre sa propre sécurité
* Pour s’assurer que le sous-traitant aligne sa politique de sécurité sur celle de l’entreprise

Dans l’entreprise A, les données du service X sont accessibles en lecture seule aux employés du service Y. Ce contrôle d’accès permet d’assurer pour les données leur:

* Confidentialité
* Intégrité
* Disponibilité

Parmi les données suivantes, lesquelles ne sont a priori pas confidentielles :

* Procédure de demande d’accès aux applications métier sensibles
* Rapports de l’audit interne après publication
* Résultats comptables avant leur publication
* Logs des proxy web d’entreprise contenant l’historique des accès à l’Internet des employés

Une menace constitue un risque inhérent qui plane sur l’entreprise et ne peut pas être réduit :

* Vrai
* Faux

Une vulnérabilité représente l’exposition à une menace suite à une faiblesse particulière dans l’environnement de contrôle :

* Vrai
* Faux

Un entreprise anticipe un plan social qui impactera toute l’entreprise et entrainera un gel des salaires pour tout le personnel. La Direction anticipe également que cela pourra provoquer le départ de plusieurs employés expérimentés au sein du Service Informatique. En réponse à ces inquiétudes, la direction du groupe est prête à faire appel à des intérimaires en CDI pendant le temps qu’il faudra pour assurer la continuité en cas de départ de personnes expérimentées au sein du service informatique. Quelle est la meilleure recommandation que pourrait faire le RSSI pour limiter l’impact de ces départs potentiels sur le fonctionnement du S.I.?

* Augmenter les bonus des employés clé du service informatique pour s’assurer de leur fidélité.
* S’assurer que des procédures détaillées et à jour existent pour détailler les tâches des employés du service informatique
* Vérifier qu’une grande partie des tâches opérationnelles de gestion du S.I. est automatisée via des outils de contrôle (par ex. surveillance et alertes automatiquement remontées en cas d’anomalies)
* Suggérer de renoncer au plan social vu les risques qu’il perçoit.

Laquelle des techniques suivantes pour évaluer un contrôle donnera le plus d’assurance :

* Entretiens avec le responsable informatique et avec la personne de son équipe qui connait le mieux le contrôle
* Revue des procédures à jour qui détaillent le fonctionnement du contrôle
* (Si contrôle automatisé) Un test d’observation avec un employé pour vérifier que le contrôle automatisé est en place
* (Si contrôle manuel) Sélection d’un échantillon représentatif et revue de chaque cas pour confirmer que le contrôle a bien été appliqué au bon moment et par la bonne personne

**Quizz #2 :**

Quelle est la personne la plus indiquée pour confirmer la classification d’un document en terme de confidentialité :

* Le RSSI
* Le DSI
* Le propriétaire de l’information
* La Direction Générale
* Un utilisateur qui traite cette information quotidiennement
* L’Audit interne

Le département Marketing / Communication d’une entreprise soumise au secret des affaires souhaite préparer une campagne de communication auprès de clients. A des fins d'analyse statistique, une demande est soumise à l'accord du RSSI pour extraire les données suivantes de la base de données clients qui contient plus de 50.000 noms:

* Pays de résidence
* Année de naissance
* Langue principale
* Si la personne bénéficie d’une « Green Card » ou du statut de résident américain

Y a-t-il un risque de confidentialité ? Pourquoi ?  
**NON – pas de données directes, même agrégées.**

Parmi les points suivants, lequel représente un moyen pour suivre le niveau de service fourni par un sous-traitant auquel une entreprise délègue la gestion de son système d’information:

* S’assurer de l’existence d’un contrat de service indiquant les exigences de qualité de service attendues et prévoyant des pénalités en cas de non-respect
* Recevoir une fois par an un rapport ISAE 3402 de la part du sous-traitant qui certifie la mise en place de contrôles sur les services sous-traités
* **Une conférence téléphonique hebdomadaire dans laquelle le sous-traitant fait un compte rendu verbal des incidents relevés**
* S’assurer que le plan de continuité du sous-traitant est aligné avec le sien et le vérifier par des audits réguliers.

Dans un processus type de gestion des incidents, quelle est la personne la plus indiquée pour confirmer la clôture d’un incident :

* Le RSSI
* Le support de niveau 1 (« Service Desk ») qui enregistre les incidents et escalade tout incident non résolu dans les temps attendus
* Le support de niveau 2 qui réalise l’action corrective demandée et vérifie son bon fonctionnement
* **L’utilisateur qui a rapporté l’incident**

Afin de garantir que les accès aux répertoires partagés (dont certains contiennent des données sensibles) restent appropriés dans le temps, une entreprise a mis en place un processus de gestion des accès dans lequel les points suivants sont en place :

* Toute demande d’accès est validée par le responsable du demandeur
* Les accès sont ensuite attribués par les administrateurs Active Directory conformément à la demande (contrôle de 1er niveau)
* Le RSSI s’assure qu’un rapport de recertification est envoyé une fois par an aux responsables de chaque répertoire sensible pour revue (contrôle de 2ème niveau)

Y a-t-il un risque résiduel d’accès inappropriés ? Si oui, à quel niveau ?

**OUI – pas de revue de la recertification. Pas de validation par le responsable de l’information. Pas de validation par le RSSI que les niveaux d’accès sont appropriés.**

Lequel des tests suivants est le plus approprié pour vérifier que la gestion des accès fonctionne de manière effective pour réduire les risques d’accès non-autorisés?

* Observer les contrôles appliqués lors du traitement d’un exemple de demande d’accès standard
* S’assurer que le processus de gestion des accès est formellement documenté dans une procédure revue annuellement
* **Obtenir la liste des employés ayant quitté la société dans les 6 derniers mois et s’assurer que leurs accès au S.I. ont été révoqués**
* Vérifier que chaque accès demandé a bien été attribué par l’équipe en charge de la gestion des accès

Quel est une caractéristique de la norme ISO 27001 :

* **S’adresse à tous les types d’Organismes (toutes tailles, tous types d’activité) et sans obligation sur les méthodes**
* Elle fournit un guide de mise en place détaillé pour chaque contrôle
* C’est un document public
* Son objectif est d’assurer que toutes les mesures de sécurité attendues sont en place à l’instant T

Dans le cadre du processus de gestion des changements sur le S.I., lesquels des tests suivants font intervenir les utilisateurs du S.I. :

* Tests unitaires
* Tests d’intégration
* **Test d’acceptation (UAT)**

Dans le cadre du processus de gestion des changements sur le S.I., quelles sont les personnes les plus indiquées pour effectuer le déploiement de changements en environnement de Production :

* Le chef de projet chargé de la planification des changements
* **Les équipes d’exploitation des systèmes de Production**
* Le responsable du processus métier
* Les personnes en charge des tests finaux d’acceptation (UAT)

Quel risque type existe au niveau de la sécurité des environnements de pré-production (environnement de tests unitaires, de tests d’intégration, de tests UAT) :

* Les utilisateurs ont la possibilité de modifier les données copiées de la production lors des tests (risque d’intégrité)
* **Les données de production sont potentiellement confidentielles et exposées à des accès non-autorisés (risque de confidentialité)**
* Les environnements de pré-production ne sont pas intégrés au plan de secours (risque de continuité)
* Tous les risques ci-dessus

**Quizz #3 :**

La signature électronique assure la confidentialité d’un document :

* Vrai
* Faux

Préciser.

Quel est le niveau de confidentialité du hash cryptographique d’un document confidentiel:

* Public (peut être diffusé sur l’Internet sans conséquence)
* Interne (doit rester restreint aux employés de l’entreprise)
* Confidentiel (doit rester protégé de la même manière que les données)

Quel est le rôle d’une autorité de certification :

* Signer électroniquement les documents d’une entreprise
* Certifier que les communications entre une entreprise et ses clients sont chiffrées
* Sécuriser les clés privées d’une entreprise
* Agir en tant que tiers de confiance pour authentifier la clé publique d’une organisation

La signature électronique a une valeur légale en France :

* Oui si le document comporte une image de la signature manuscrite incrustée dans le document (PDF par exemple)
* Oui si la signature utilise un certificat qualifié
* Oui si la signature électronique est préalablement acceptée contractuellement par le destinataire
* Non, il vaut mieux utiliser une signature manuscrite pour éviter un risque juridique

Une entreprise doit-elle faire appel à une autorité de certification pour installer des certificats sur ses serveurs web internes ?

* Oui
* Non

Justifier.

Un certificat est-il forcément payant si l’on souhaite qu’il soit reconnu comme valide par un navigateur?

* Oui
* Non

Justifier

**NON (Let’s Encrypt + pas nécessaire sur réseau d’entreprise)**

Le protocole https utilise une cryptographie :

* Complètement symétrique
* Complètement asymétrique
* Hybride : une clé de session symétrique est échangée et chiffrée avec la clé privée du serveur
* **Hybride : une clé de session symétrique est échangée et chiffrée avec la clé publique du serveur**
* Hybride : une clé de session symétrique est échangée et chiffrée avec la clé privée du client

Est-ce que l’accès physique à un poste de travail (par exemple un ordinateur portable lors du passage en douane) permet à un attaquant d’accéder à des fichiers sensibles contenus sur le disque dur s’il le souhaite ?

* Non, sauf s’il obtient le mot de passe de l’utilisateur ou d’un compte administrateur
* **Oui, excepté si le disque dur est chiffré**
* Oui dans tous les cas, y compris si le disque dur est chiffré

Préciser : Live CD (permet aussi de modifier le mot de passe)

**(idem pour terminal mobile)**

Lors de la définition des droits d’accès sur le serveur SWIFT utilisé pour des virements bancaires, le RSSI vérifie qu’aucun utilisateur n’a en même temps des droits de saisie et d’auto-validation pour effectuer des paiements. Il s’assure également que le mot de passe du compte administrateur est bien divisé en deux parties séparées, connues d’une part par le responsable des opérations (1ère partie) et d’autre part par l’employé du département opérations qui connait le mieux le serveur SWIFT et se charge des modifications de droits d’accès lorsque nécessaire.

Y a-t-il un risque de ségrégation des tâches ?

* Oui
* Non

Justifier.

Cette situation crée-t-elle un autre risque de sécurité ?

Parmi les possibilités suivantes, laquelle correspond au hash du mot bonjour au format MD5 :

* Ym9uam91cg==
* **f02368945726d5fc2a14eb576f7276c0**
* 9498e39d292381f1216dad8c45a06a0a
* 1f71e0f4ac9b47cd93bf269e4017abaab9d3bd63
* f8ec9284e160c5afe456b48702e08a14095ab37bca36808e10a22f71
* c7e2d3a1a600319151a62b9abfcecfbeab4ca388375a1498dc6d7630c67e349140103c150815cd027447db5d117e7e04

**Quizz #4 :**

Une authentification forte se caractérise par:

* L’utilisation de mots de passe à forte complexité que les utilisateurs doivent changer régulièrement
* L’utilisation du protocole https et la vérification du certificat serveur par le navigateur web
* La combinaison d’un mot de passe et d’un PIN connus de l’utilisateur
* L’utilisation de plusieurs facteurs de type différent

Parmi les cas suivants, lesquels représentent une authentification forte :

* NIP + SMS
* Mot de passe + reconnaissance empreinte digitale
* Mot de passe + message vocal reçu par téléphone
* SMS + mot de passe à usage unique généré par une application sur le smartphone

Laquelle des fonctions suivantes n’est pas permise par le protocole SSH (Secure SHell) :

* Transfert de fichiers entre deux machines par un canal chiffré (SFTP)
* Administration de serveur à distance
* Tunnelling qui consiste à encapsuler les données d'un protocole réseau dans un autre
* Echanger des signatures électroniques entre client et serveur

Quel est le nom du client SSH le plus connu :

* Putty
* uTorrent
* PowerShell
* Dumpsec

Sécurité des mots de passe : laquelle des mesures suivantes permet de limiter au mieux l’impact d’une attaque « en ligne » contre un mot de passe :

* Exiger que l’utilisateur renouvelle son mot de passe fréquemment
* Bloquer le compte utilisateur après x tentatives de connexion
* Suspendre la possibilité de se connecter au serveur avec le compte de l’utilisateur pendant une durée de x heures
* Avertir l’utilisateur par e-mail qu’une personne a essayé de se connecter à son compte utilisateur

Sécurité des mots de passe : laquelle des mesures suivantes est la plus efficace pour limiter l’impact d’une attaque « hors ligne » contre un mot de passe (par exemple en cas de vol de la base des mots de passe sur le serveur par un administrateur malveillant ou suite à une cyber attaque):

* Demander par e-mail à tous les utilisateurs du service en ligne de renouveler leurs mots de passe
* Stocker les mots de passe des utilisateurs sous forme hachée avec un sel cryptographique
* Bloquer le compte utilisateur après 3 tentatives de connexion au lieu de 10
* Augmenter la complexité des mots de passe des utilisateurs pour que le cassage hors ligne soit plus compliqué en cas de vol.

Permissions sur un répertoire : parmi les points suivants, lequel ne constitue pas une bonne pratique pour la gestion des accès à un répertoire partagé contenant des données sensibles sur un serveur Windows

* Les accès sont attribués à des groupes d’utilisateurs plutôt que de manière nominative
* Une recertification des accès est réalisée par le propriétaire du répertoire sur base annuelle
* Les administrateurs du S .I. disposent d’une permission « Contrôle total »
* **Le Groupe « utilisateurs du Domaine » dispose d’un droit d’accès en lecture seule.**
* Certains comptes techniques disposent d’accès, toutefois ces comptes techniques sont soumis à l’accord du RSSI avant utilisation. Leur utilisation est enregistrée dans un log d’audit.

Gestion des correctifs de sécurité (« patchs »): laquelle des mesures suivantes présente un risque dans le processus de gestion des correctifs de sécurité sur les postes de travail et serveurs d’une entreprise utilisant de nombreux logiciels maison pour son activité :

* Tous les correctifs de sécurité sont appliqués automatiquement sur l’ensemble du parc informatique dès leur publication (utilisation d’un serveur WSUS)
* Les administrateurs du S.I. ne retiennent que les correctifs de sécurité qui s’appliquent au S.I. de l’organisation.
* Les utilisateurs nomades ne peuvent se connecter à distance au S.I. tant que leur machine n’est pas à jour.
* Les machines exposées à l’Internet reçoivent les patchs en priorité.
* Un rapport d’exception identifie les machines du parc qui ne sont pas à jour en terme de correctifs et est revu chaque semaine par les administrateurs système.

Quels sont les points d’attention principaux lors de la revue des utilisateurs sur un contrôleur de Domaine Windows :

* Revue des utilisateurs avec privilèges (ex : groupe Administrateurs du Domaine »)
* Revue des utilisateurs et recherche d’exceptions en terme d’authentification (ex : mot de passe qui n’expire pas, mot de passe ne devant pas être changé)
* Revue des stratégies de sécurité appliquées aux utilisateurs et vérification qu’elles sont appropriées (en ligne avec la politique de sécurité)
* Recherche d’anomalies ans la gestion des accès (ex : comptes utilisateurs non-utilisés, comptes utilisateurs d’employés ayant quitté la société mais toujours actifs)

Quelle est la personne la plus indiquée pour avoir le droit de modifier le paramétrage fonctionnel dans une application métier (ex : limite au-delà de laquelle une transaction est soumise à une approbation supplémentaire) :

* Le RSSI
* La Direction Générale
* Le responsable du processus métier
* Le responsable des Opérations
* Le responsable de la Conformité
* Un utilisateur autorisé à saisir les transactions