SERIE DE TD N° 2

Exercice N°1 :

Partie 1 : Questions de cours :

1. SMSI désigne :
   - ***A.*** *Système de Management de la Sécurité Informatique.*
   - ***B.*** *Système de Management de la Sécurité de l'Information.*
   - ***C.*** *Système de Management des Système d'Information.*
2. Roue de Deming :
   - ***A.*** *Est une démarche de développement des systèmes d'information.*
   - ***B.*** *Est une démarche de gestion de projet.*
   - ***C.*** *Est une démarche de développement de la sécurité des systèmes d'information.*
   - ***D.*** *Améliore le pilotage de l'entreprise.*
   - ***E.*** *Est issue de la démarche qualité et de gestion de projet.*
   - ***F.*** *Est basée sur quatre étapes.*
   - ***G.*** *Est une approche d'amélioration continue.*
3. Termes : RSSI ; PDCA ; PSSI, DdA (SOA), RTP.
4. Grands problèmes souvent rencontrés lors du développement d'un SMSI ?
5. Intérêt de la classification des risques ?
6. Intérêt de la certification ISO du SMSI ?
7. Déroulement du processus de certification ISO ? par qui est effectuée la certification ?
8. Types d'actions menées suite à l'étape Check lors du développement du SMSI.
9. Selon les experts en sécurité :
   - *a. Les employés sont des menaces potentielles importantes.*
   - *b. La sécurité est aussi résistante que le maillon le plus fort d'une chaine.*
   - *c. La sécurité est un processus continu qui doit vivre tout au long de la vie de l'entreprise.*
   - *d. La sécurité dépend de la technologie beaucoup plus que les personnes.*
   - *e. La majorité du temps consacré pour la SI doit être accordé à la solution technique.*
10. Répartir les tâches suivantes sur les 4 étapes PDCA :
    - *a. Former et sensibiliser le personnel.*
    - *b. Réexaminer périodiquement l'adéquation du SMSI vis-à-vis son environnement.*
    - *c. Elaboration de la PSSI.*
    - *d. Définition du périmètre du SMSI.*

e. *Analyse des vulnérabilités.*
f. *Corriger les écarts soulevés et mener des actions préventives et amélioratrices.*
g. *Identification des menaces.*
h. *Calcul et estimation du gain ROSI.*
i. *Faire des audits internes vérifiant la conformité des mesures mises en place.*
j. *Identification, analyse et évaluation (gestion) des risques.*
k. *Acceptation des risques résiduels.*
l. *Recensement des mesures déjà mise en place avant le SMSI.*
m. *Contrôler le fonctionnement du processus.*
n. *Déploiement des mesures dans le DdA.*
o. *Achat, configuration et mise en place du matériel cité dans le DdA.*
p. *Générer et mettre en place des indicateurs de performances.*

11. La certification ISO du SMSI est une :
    a. *Obligation technique.*
    b. *Obligation légale.*
    c. *Exigence.*
    d. *Favori.*

12. Citer les documents dans lesquels sont inscrits les résultats des étapes suivantes :
    a. *Application des mesures choisies.*
    b. *Préparer une nouvelle itération de la phase Plan.*
    c. *Formation et sensibilisation du personnel.*
    d. *Méthodologie de gestion de risques.*
    e. *Evaluation et traitement des risques.*
    f. *Gestion de la documentation.*
    g. *Plan de réduction des risques.*
    h. *Identification des risques résiduels.*
    i. *Support et accord de la direction.*
    j. *Revue des risques acceptées et résiduels.*
    k. *Actions correctives et amélioratrices.*
    l. *Mesures de sécurité à appliquer.*
    m. *Affecter les ressources nécessaires.*

13. Les principales exigences que doit respecter la documentation du SMSI.

14. D'un point de vue strictement légal, les entreprises ont-elles une obligation de garantir leur sécurité informatique ?

15. On souhaite appliquer le principe PDCA sur le processus de certification du SMSI ; répartir les tâches sur les différentes étapes citées.

Partie 2 : Rechercher sur Internet :

1. Termes : ROI ; ROSI ; IAF ; ALGERAC, RNSI, KPI, SIEM.
2. La famille des Normes ISO 27000.
3. Organismes accrédités certification en Algérie.
4. Normes de certification.
5. Risque interne/externe.
6. Risque financier.
7. Risque juridique.
8. Risque politique.
9. Bug de l'an 2000 (*Y2K problem*)
10. Bug de l'an 2038 (*Y2038 problem*)

Exercice N° 2 :

En se basant sur les formules de calcul du ***ROI*** et du ***ROSI*** ci-dessous, évaluer la rentabilité des projets dans les deux exemples qui suivent :

$$ROI = \frac{Gains\ de\ l'investissement - Coût\ de\ l'investissement}{Coût\ de\ l'investissement} = \frac{Gain\ net}{Coût\ de\ l'investissement}$$
$$= \frac{Gains\ de\ l'investissement}{Coût\ de\ l'investissement} - 1$$

Pour le *ROSI* les gains sont calculés par :

$$Gains = Coût\ d'exposition\ au\ risque * \%\ de\ réduction\ du\ risque$$

Exemple1 :

Une société lance une nouvelle gamme de produit à commercialiser. Pour cela, elle prévoit procéder au lancement d'une phase projet sur 3 mois avec un coût d'investissement estimé à 250K€, puis une phase de mise sur le marché qui requiert un investissement de 50K€ sur 3 mois et finalement un investissement de 100K€ pour une production sur les 6 mois restants de l'année planifiée. Sur cette dernière phase des gains issus directement de la vente du nouveau produit sont estimés à 1M€. Quel est le **ROI** escompté **sur 1 an**.

Si on suppose que l'année suivante on a dépensé un montant proportionnel au coût de production des 6 mois précédents et dont la vente a rapporté 2M€, recalculer le ROI sur les 2 ans.

Exemple2 :

Une entreprise souhaite protéger les postes de travail par un antivirus en mettant en place une solution antivirale globale. On suppose que :

- *Le nombre de postes : 20 000*
- *Coût annuel de la solution antivirale (50€ par poste) : 1 000 000€*

Supposons que les virus sont classés en trois niveaux N1, N2 et N3 selon leurs impacts sur le business comme suit :

Niveau d'impact	Coût lié par virus
N1	10
N2	1000
N3	100000

Sur une année 50 000 virus ont été comptabilisés avec une répartition comme suit :

N de virus total	N de virus niveau 1	N de virus niveau 2	N de virus niveau 3
% :	90,00%	9,99%	0,01%
50000			
Coût d'exposition au risque associé			
R = % de réduction du risque	95%	75%	70%
Gains			

a. Calculer le ROSI ainsi.

Soit $R_0 = \frac{Coût\ de\ l'investissement}{Coût\ d'exposition\ au\ risque}$

b. Etudier la valeur de ROSI par rapport aux celles de R (% de réduction du risque) et R_0.