

Date : 14/12/2021 Session : 2021/2022

Diplôme / filière / niveau : 12 Technologie  
de l'Internet

UE : SSI - Partie EBios

Épreuve :

Note : (de 0 à 20)

Appréciation du correcteur :

Signature du/des correcteur(s) :

### Partie EBios

- 4) Cette décision s'appelle les objectifs de sécurité.
- Éviter le risque (refuser) = enlever le bien support où le risque est
  - Réduire le risque = renforcer la protection du bien support susceptible d'être attaqué
  - Prendre le risque (maintenir) = ne rien faire
  - Transférer le risque (partager) = transférer à un organisme tiers.

5) L'acceptation des risques est possible en l'état car on passe pour certains risques à de niveau inacceptable à des niveaux acceptables.

On valide cette décision avec la direction de l'entreprise.  
Si il y a non-acceptation, une itération sera nécessaire.



### Question n°1 (4 points)

Pour la liste des libellés ci-dessous :

- Veuillez dire s'il s'agit d'une menace ou d'une vulnérabilité
- Veuillez donner des vulnérabilités associées s'il s'agit d'une menace.
- Veuillez donner des menaces associées s'il s'agit d'une vulnérabilité.

Vulnérabilité ou Menace ?	V ou M	Catégorie de bien support concerné	Indiquez une liste de vulnérabilités exploitables par la menace ou des menaces capables d'exploiter la vulnérabilité
Données non effacées des serveurs du prestataire et rendues accessibles	N	SYS: RSX	Non surveillance des serveurs
Espionnage	N	ORG: PER	Faible surveillance du matériel.
Transfert du mot de passe en clair	V	SYS: RSX	Espionnage du mot de passe par une personne tierce.
Politique de mot de passe faible	V	SYS: RSX	Usurpation du mot de passe.
Faible loyauté	N	ORG: PER	Deception professionnelle d'un employé.
Action d'un aimant sur un disque dur	N	SYS: NAT	Non surveillance du matériel.
Datacenter mal protégé contre les catastrophes naturelles	V	SYS: NAT	Déviolation du matériel intentionnelle.
Sujet à la dissipation	V	ORG: PER	Vol de documents.



### Question n°2 (2 points)

Veuillez rappeler quelles sont les sept composantes d'un risque et retrouvez ces sept composantes dans le risque rédigé suivant :

#### Risque

Les administrateurs du site de vente en ligne de l'entreprise commettent une erreur de configuration due à un manque de formation. Ceci entraîne une indisponibilité du site qui est aggravée par un manque d'organisation dans le processus de sauvegarde / restauration. L'impact est une perte financière de 10 000 € à chaque heure d'indisponibilité.

Vous pouvez présenter les résultats sous la forme d'un tableau de ce type :

<b>Composante 1</b> source de risque	Administrateurs du site.
<b>Composante 2</b> Cause / mode opératoire	Manque de formation.
<b>Composante 3</b> vulnérabilité	Manque de sauvegarde / restauration.
<b>Composante 4</b> Bien support	Site de vente en ligne.
<b>Composante 5</b> Bien essentiel / valeur métier	Configuration du site.
<b>Composante 6</b> Besoin de sécurité	Disponibilité
<b>Composante 7</b> Impact.	Perte financière



### Question n°3 – 8 points

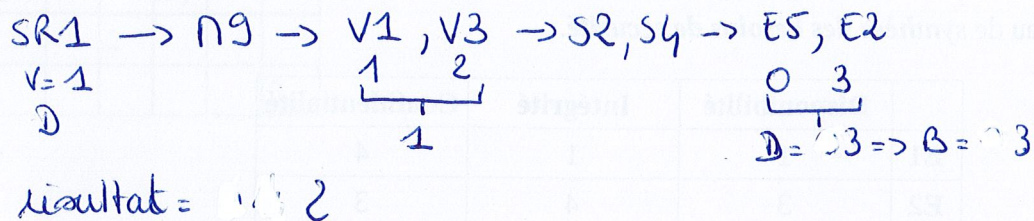
Dans cette question, les libellés des objets manipulés ne sont pas utiles à la réalisation de l'exercice. Votre travail consiste ici, à l'aide des tableaux fournis, à identifier et estimer les risques.

Voici quatre scénarios de menace identifiés avec leur vraisemblance :

En utilisant les tableaux précédents, veuillez identifier et estimer les risques.

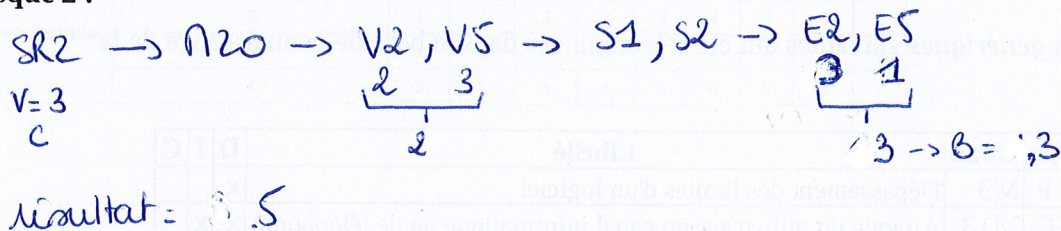
- Si les vulnérabilités V1 et V3 sont présentes, alors la source de risque SR1 pourra utiliser M9 (vraisemblance 1)

Risque 1 :



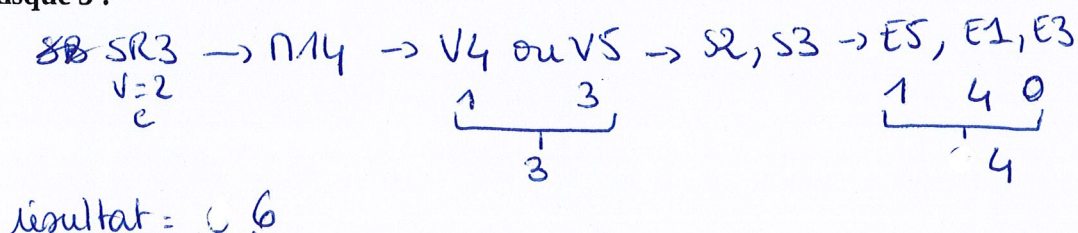
- Si les vulnérabilités V2 et V5 sont présentes, alors la source de risque SR2 pourra utiliser M20 (vraisemblance 3)

Risque 2 :



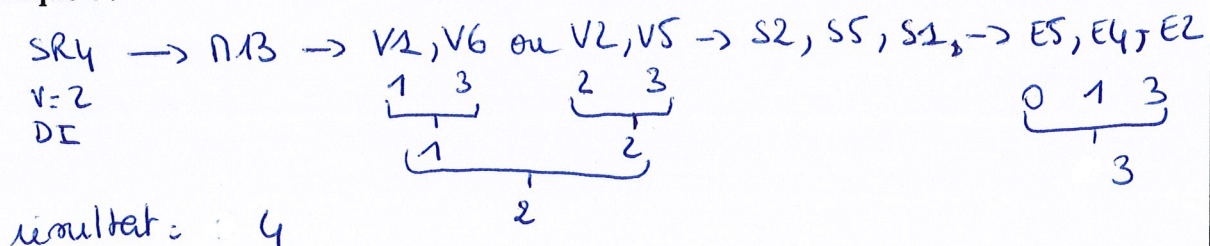
- Si les vulnérabilités V4 ou V5 sont présentes, alors la source de risque SR3 pourra utiliser la menace M14 (vraisemblance 2)

Risque 3 :



- Si les vulnérabilités (V1 et V6) ou (V2 et V5) sont présentes, alors la source de risque SR4 pourra utiliser la menace M13 (vraisemblance 2)

Risque 4 :





### Question n°4 (3 points)

Nous passons à la phase de traitement du risque.

Les 4 risques identifiés et estimés à la question 3 sont présentés au maître d'ouvrage par le maître d'œuvre de l'étude de sécurité. Notre maître d'ouvrage doit décider de la façon dont va être engagé le traitement de ce risque.

Comment s'appelle cette décision ?

Ce type de décision peut appartenir à quatre grandes catégories. Veuillez lister ces catégories et expliquer en quoi consiste chacune d'entre-elles.

### Question n°5 (3 points)

Pour les 4 risques, on décide de mettre en place 10 mesures de sécurité. Le tableau suivant donne la couverture des risques par les mesures. Chaque case du tableau représente une estimation de l'abaissement du risque si la mesure est mise en place. Les risques de valeur inférieur ou égal à 2 sont considérés comme acceptables.

Calculez le risque résiduel.

	Risque initial	Risque résiduel	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
R1	2	0,5		0,5	0,5				0,5			
R2	5	2	1	0,5	0,5		0,5					0,5
R3	6	1	1	0,5	0,5			1		1	1	
R4	4	2,5	0,5			0,5	0,5					

L'acceptation des risques est-elle possible en l'état ? Sinon que peut-on faire ? Avec qui validez-vous cette décision ?

— FIN —