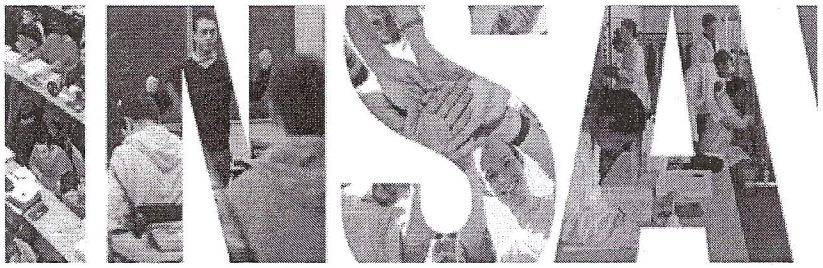
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE



# Partiel 4ème année filière STI.
# Module : Sécurité des systèmes d'information
# Promotion 2016

**Documents et calculette non autorisés**

**Le vendredi 16 janvier 2015.**

**Durée : 20 mn**

Connaissances générales sur la normalisation .

Soit l'offre de formation suivante, trouvée sur INTERNET :

## ISO 27005:2011 Risk Manager, certification

Ce stage d'une journée est un complément au séminaire "ISO 27005:2011 Risk Manager, préparation à la certification". Il a pour objectif de réviser les sujets présentés lors du séminaire et de préparer au passage de l'examen "Risk manager 27005:2011". Il se termine par l'examen proprement dit.

### » Contenu

- Préparation
- Corrections collectives
- Révision finale
- Durée et confidentialité de l'examen
- Les épreuves
- Points et résultats

### » Participants

RSSI ou correspondants Sécurité, architectes sécurité, directeurs ou responsables informatiques, ingénieurs, chefs de projets (MOE, MOA) devant intégrer des exigences de sécurité.

### » Pré-requis

Bonnes connaissances de la gestion de la sécurité des SI et des normes 27005. Avoir suivi le stage "ISO 27005:2011 Risk Manager, préparation à la certification" (réf. AIR). Expérience souhaitable.

### » Thématique

Formation ISO 27005

### » Certification

L'examen de certification est dirigé en partenariat avec l'organisme de certification LSTI (accrédité COFRAC). Il se déroule pendant la demi-journée de l'après-midi. Ce diplôme international officiel ISO vous apportera la plus grande crédibilité dans la conduite de vos projets d'analyse de risques.

1. **Le but de ce stage est une certification : qui ou quoi fait l'objet de certification ?**

2. **Dans la série de normes ISO 2700x, citez une autre norme pouvant faire l'objet d'une certification et indiquez l'élément pouvant être certifié.**

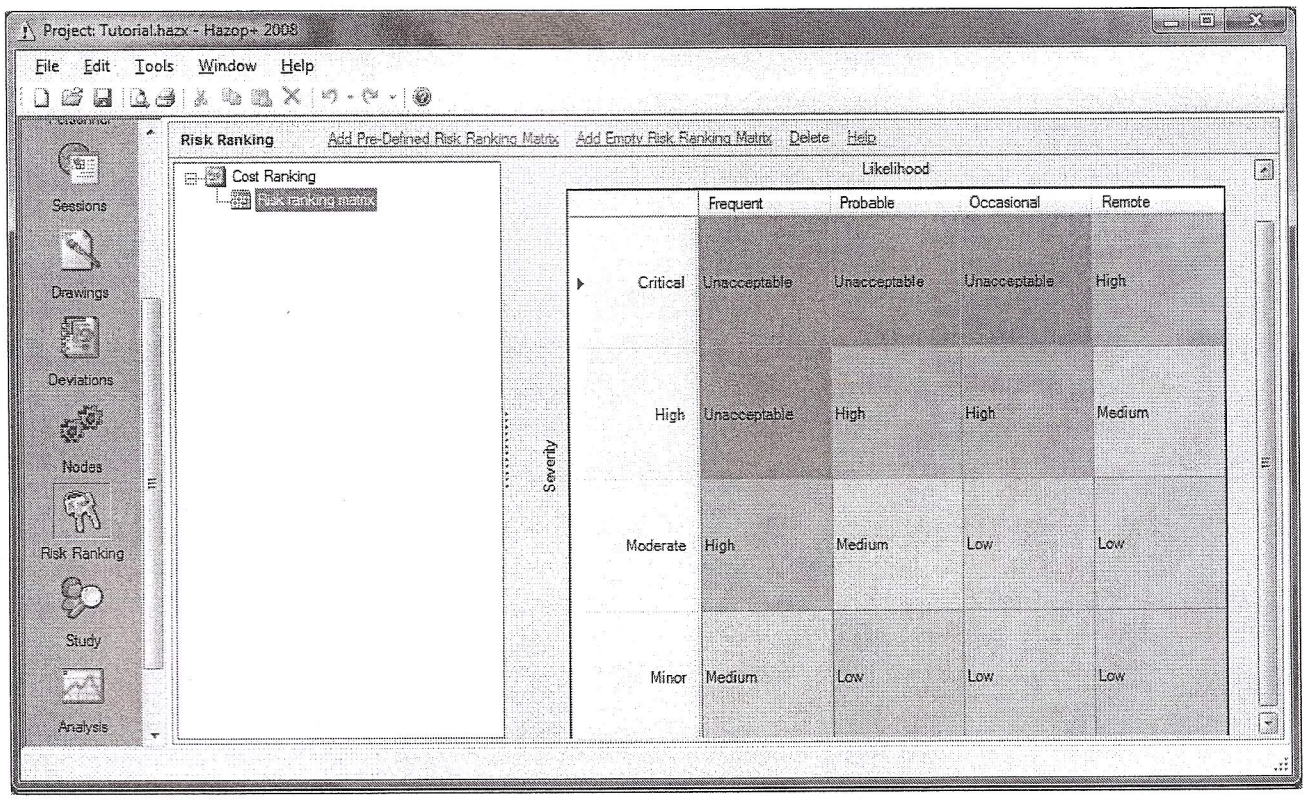
3. **Dans l'offre, on utilise, dans la partie « Participants », l'acronyme RSSI. Indiquez en quoi consiste le métier de RSSI.**

4. **On parle également de chefs de projets MOE et MOA, explicitez ces acronymes.**

Ebios (Expression des besoins et identification des objectifs de sécurité)

5. **Quels sont les modules qui composent la méthode EBIOS 2010 et quel est le but de chacun d'eux ?**

Soit la matrice, obtenue ci-dessous après une étude de risques avec la méthode HAZOP (non vue dans ce module).
La méthode HAZOP (HAZard and OPerability study) est une méthode d'analyse des risques industriels. Au départ, elle était surtout faite pour les industries chimiques mais elle a élargi son champ d'action.




6. **Dans quel « module » de la méthode « Ebios 2010 » rencontre-t-on une matrice similaire ?**

# Méthodologie d'analyse des systèmes d'information Partie ITIL

## Examen – Janvier 2015

*Veuillez répondre aux 20 questions suivantes.1 point par bonne réponse. 1 seule bonne réponse par question. Merci d'utiliser la grille de résultats en annexe pour vos réponses.*
*Documents de cours interdits.*

***1/ Parmi les caractéristiques suivantes, laquelle ou lesquelles sont des caractéristiques d'ITIL contribuant à sa réussite ?***

1. Il est neutre vis-à-vis des fournisseurs
2. Il n'est pas prescriptif
3. il s'agit des meilleures pratiques
4 C'est une norme

a) 3 seulement
b) 1, 2 et 3 seulement
c) Toutes les caractéristiques
d) 2, 3 et 4 seulement

***2/ Lesquels des énoncés suivants sur les indicateurs clés de performance (KPI) et les métriques sont CORRECTS ?***

1. Les métriques de services mesurent un service de bout en bout
2. Chaque KPI devrait être lié à un facteur critique de succès
3. Des métriques peuvent être utilisées afin d'identifier des opportunités d'amélioration
4. Les KPI peuvent être qualitatifs ou quantitatifs

a) 1 seulement
b) 2 et 3 seulement
c) 1, 2 et 4 seulement
d) Tous les énoncés

***3/ Une panne se produisant sur un système est détectée par un outil de surveillance.***
***Ce système soutient un service informatique en production. A quel moment devrait-on soumettre un incident ?***

a) Uniquement après que des utilisateurs aient remarqué la panne
b) Un incident ne devrait pas être soumis si les techniciens ont déjà constaté cette panne dans le passé et une solution de contournement existe
c) Uniquement si la panne provoque le non-respect d'un niveau de service
d) Immédiatement afin de limiter ou de prévenir un impact sur les utilisateurs

***4/ Lequel des énoncés suivants est CORRECT pour TOUT processus ?***

a) La définition des fonctions fait partie de sa conception
b) Il délivre des résultats à un client ou à une partie prenante
c) Il est effectué par un fournisseur de services externe pour soutenir un client
d) Il est une unité organisationnelle responsable de résultats spécifiques

***5/ Quel processus est en premier lieu responsable de l'assemblage, de la construction, des tests et du déploiement des services ?***

a) La gestion de la capacité
b) La gestion des déploiements et des mises en production

c) La gestion des actifs de services et des configurations
d) La gestion du catalogue des services

***6/ Parmi les énumérations suivantes des quatre étapes du Cycle de Deming, laquelle est CORRECTE?***

a) Planifier, Mesurer, Surveiller, Rapporter
b) Planifier, Faire, Vérifier, Agir
c) Planifier, Faire, Agir, Auditer
d) Planifier, Vérifier, Agir, Améliorer

***7/ Quels rôles sont définis dans le modèle RACI ?***

a) Responsable (Responsible), Imputable (Accountable), Consulté, Informé
b) Responsable (Responsible), Acteur, Consulté, Informé
c) Réaliste, Imputable (Accountable), Consulté, Informé
d) Responsable (Responsible), Imputable (Accountable), Corrigé, Informé

***8/ L'amélioration continue des services fournit des conseils sur lesquels des énoncés suivants ?***

1. Comment améliorer l'efficacité et l'efficience des processus
2. Comment améliorer des services
3. L'amélioration de toutes les étapes du cycle de vie des services

a) 1 et 2 seulement
b) 1 et 3 seulement
c) 2 et 3 seulement
d) Tous

***9/ Lequel des énoncés ci-dessous est un type d'accord de niveaux de service (SLA), tel que décrit dans ITIL?***

a) SLA orienté priorité
b) SLA orienté technologie
c) SLA orienté localisation
d) SLA orienté client

***10/ Lequel des énoncés suivants est la MEILLEURE définition d'un événement ?***

a) Une occurrence lors de laquelle un seuil de risque a été dépassé et qui engendre un incident
b) Un changement d'état qui est significatif pour la gestion d'un service informatique
c) Une défaillance système connue qui génère plusieurs rapports d'incidents
d) Une rencontre planifiée avec les clients et le personnel TI pour annoncer un nouveau service ou un programme d'amélioration

***11/ Dans quel but le modèle RACI est-il utilisé ?***

a) Documenter les rôles et responsabilités des parties prenantes dans un processus ou une activité
b) Définir les besoins pour un nouveau service ou un processus
c) Analyser l'impact business d'un incident
d) Créer un tableau de bord équilibré montrant le statut global de la gestion des services

***12/ Lequel des éléments suivants n'est PAS une phase du cycle de vie des services ?***

a) Exploitation des services
b) Conception des services
c) Réalisation des services
d) Stratégie des services

***13/ Quel est l'objet du processus d'exécution des requêtes ?***