Partie 1

01) Développer l'acronyme DICP :

02) Sélectionner le(s) critère(s) de qualification d'un risque :

a. Dérogation
b. Impact
c. Montan
d. Probabilité
e. Recommandation
f. Vulnérabilité

03) Développer l'acronyme IAM :

04) Sélectionner les termes relatifs à l'IAM :

a. Authentification forte
b. CNI
c. KPI
d. Fédération d'identité
e. OTP
f. SSO

05) Définition de provisioning :

a. Ajouter des droits validés une application
b. Valider des droits théoriques pour un utilisateur
c. Mettre de l'argent en réserve pour s'assurer contre les risques sécurité

06) Quel modèle de gestion des habilitations apporte le plus de gains en entreprise ?

a. Le modèle MAC
b. Le modèle DAC
c. Le modèle RBAC

07) Laquelle de ces propositions n'est pas en lien avec l'IAM :

a. L'utilisation d'un identifiant pour l'ensemble des applications d'une entreprise (SSO) permet d'accroître la productivité de ces employés
b. Afin de protéger ses données confidentielles, il faut utiliser un chiffrement fort
c. Pour s'assurer de l'identité d'un individu, il faut utiliser des moyens d'authentification

08) Lequel de ces points est un facteur clé d'échec :

a. Le sponsor projet n'est pas dans la DSI
b. Les intervenants RH, achats, métiers, DSI sont tous impliqués dans le projet
c. L'organisation métier sera revue pour s'intégrer à la solution technique retenue

09) Laquelle de ces affirmations est vraie :

a. Avec un IAM efficient, ma secrétaire envoie plus vite ses mails
b. Avec un IAM efficient, mes applications fonctionnent mieux
c. Avec un IAM efficient, les validations de droits vont plus vite

10) Quels sont les principaux enjeux d'un projet IAM ?

a. La performance métier
b. Les besoins en sécurité et en contrôles
c. Les deux

11) Quels sont les 4 pans de l'IAM ?

12) Sélectionner la définition d'une vulnérabilité :
a. Faiblesse d'un système
b. Perte business due à la réalisation avec succès de l'attaque
c. Élément agissant sur la faiblesse

13) Laquelle de ces affirmations n'est pas une brique de l'IAM
a. SSL
b. Authentification forte
c. Profilage

14) Afin de s'assurer de la cohérence des droits accordés, on réalise :
a. Des revues d'habilitations
b. Des tableaux de bord
c. Un processus métier

15) Quel est le processus d'habilitations :
a. Demande – Validation hiérarchique – Validation métier – Réalisation
b. Demande – Validation métier – Validation hiérarchique – Réalisation
c. Réalisation – Validation hiérarchique – Validation métier – Demande
d. Réalisation – Validation métier – Validation hiérarchique – Demande

Partie 2

01) Sélectionner le processus mis en avant par ISO 27001 :

a. Check Plan Act Do
b. Check Plan Act Do
c. Do Check Act Plan
d. Do Check Plan Act
e. Plan Act Check Do
f. Plan Do Check Act

02) Quelle norme ISO définit le SMSI :

a. 9001
b. 9002
c. 14001
d. 14002
e. 27001
f. 27002

03) Développer l'acronyme SMSI :

04) Sélectionner le(s) grand(s) principe(s) du SMSI :

a. Amélioration continue
b. Application des recommandations
c. Approche processus
d. Engagement du management
e. Pilotage par les risques
f. Réalisation d'audits

05) Sélectionner ce qui s'applique à ISO 27002 :

a. Annexe de l'ISO 27001
b. Code de bonnes pratiques en matière de sécurité de l'information
c. Exigences pour les organismes procédant à l'audit et à la certification des SMSI
d. Guide d'implémentation du SMSI
e. Lignes directrices pour l'audit des SMSI
f. Programme de mesure de la sécurité de l'information

06) Les normes ISO sont définies par :

a. Le gouvernement
b. Les entreprises
c. Un organisme international

07) À quelle(s) fin(s) peut-on utiliser ISO 27001 :

a. Pour s'aligner sur les grands principes de sécurité
b. Pour obtenir une certification dans le domaine de la sécurité de l'information
c. Pour augmenter les bénéfices de l'entreprise

08) Qu'apportent les référentiels :

a. Un langage commun
b. Une méthodologie reconnue
c. Une réponse unique à toutes les problématiques de sécurité

09) À quel(s) type(s) d'organisme peut-on appliquer ISO 27001 :

a. Une agence gouvernementale
b. Une association
c. Une entreprise
d. Une université

10) Dans le cadre de l'ISO 27001, la roue de Deming représente :

a. Le principe d'amélioration continue
b. Un pilotage par les risques
c. Les lignes directrices d'un audit

Partie 3

01) Que signifie l'acronyme PCA ?
   a. Plan de Continuité d'Activité
   b. Poste de Commandement Avancé
   c. Prévention des Catastrophes et Accidents

02) Quel pourcentage d'entreprises ne disposant pas de PCA et ayant vécu un sinistre dépose le bilan les deux ans qui suivent ?
   a. 30%
   b. 50%
   c. 70%

03) Le PCA, une réponse nécessaire pour:
   a. Assurer la pérennité de l'entreprise et répondre aux exigences commerciales et contractuelles des clients
   b. Assurer des dividendes aux actionnaires
   c. Être en conformité avec les réglementations nationales

04) Donner les 4 familles de scénarios de sinistres à prévenir par un PCA : incendie

05) Une indisponibilité durable ou partielle du système d'information déclenche ?
   a. Un PCA
   b. Un PRA
   c. Un PRU

06) Une indisponibilité durable ou partielle d'un site hébergeant du personnel
   a. Une PCA
   b. Un PRA
   c. Un PRU

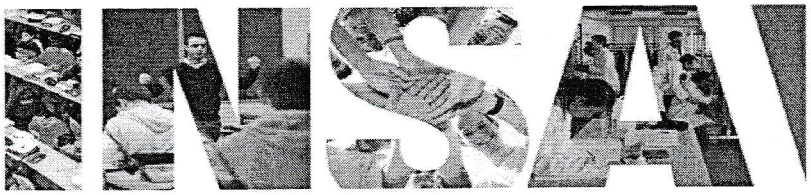
07) Quelles sont les 4 étapes de mise en place d'un PCA ?

08) Quels sont les responsables du PCA ?
   a. Direction
   b. Ensemble des collaborateurs
   c. Équipe PCA

09) Le PCA est une démarche qui couvre
   a. L'informatique
   b. Les deux
   c. Les métiers

10) Le Bilan d'Impact sur Activité (BIA) a pour but:
   a. D'identifier les activités critiques
   b. D'identifier les prestataires essentiels
   c. De réaliser une analyse des scénarios de sinistre

INSA | INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE



Partiel 4ème année, Département STI.

Module : Méthodologies d'analyse des systèmes d'information.

Les réponses seront sur une copie séparée du reste du partiel avec en haut à droite de la première page « Szpieg »

CONSIGNES :

Calculette non autorisée
Documents non autorisés
Téléphones mobiles éteints
Durée maximum conseillée: 20 mn

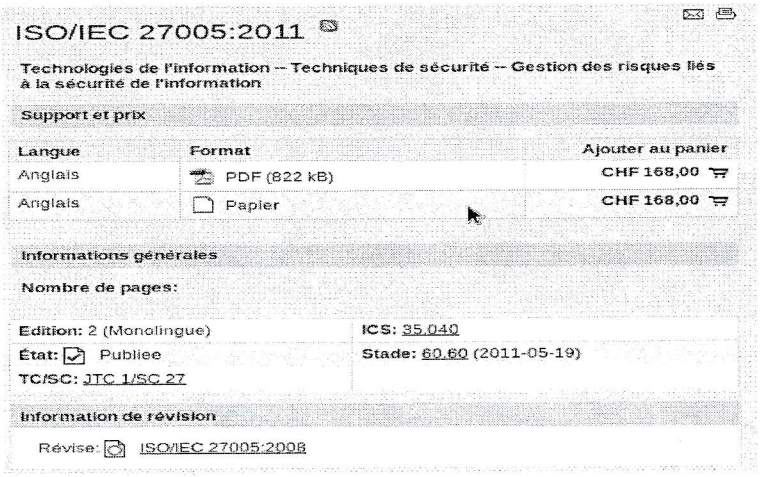
Le vendredi 15 janvier 2016

I) Les normes ISO et EBIOS

Les familles de normes internationales ISO 9000 (Qualité), ISO 14000(Management environnemental), ISO 27000 (Sécurité de l'information) offrent un « Dispositif de reconnaissance » :

1. **Que signifie cette expression « Dispositif de reconnaissance » ?**
2. **Quels sont les éléments fondamentaux qui composent ce dispositif ?**

Soit l'écran suivant obtenu sur le site « sagaweb » :



ISO/IEC 27005:2011

Technologies de l'information -- Techniques de sécurité -- Gestion des risques liés à la sécurité de l'information

Support et prix

Langue	Format	Ajouter au panier
Anglais	PDF (822 kB)	CHF 168,00
Anglais	Papier	CHF 168,00

Informations générales

Nombre de pages:

Edition: 2 (Monolingue) — ICS: 35.040
État: Publiee — Stade: 60.60 (2011-05-19)
TC/SC: JTC 1/SC 27

Information de révision

Révise: ISO/IEC 27005:2008

3. **Que signifie ISO/IEC.**
4. **Que représente l'écriture « JTC/SC 27 »**

II) CERT (*Computer Emergency Response Team*) s

1. **Définir ce qu'est un CERT et quels sont ses différents rôles ?**
2. **L'INSA-CVL bénéficie des services de deux CERT. Quels sont-ils ?**

Méthodologie d'analyse des systèmes d'information

Initiation ITILv3

Examen – Janvier 2016

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. Lequel des énoncés suivants sur les changements standards est INCORRECT ?
   a) Ils sont préautorisés par la gestion des changements
   b) Ils suivent une procédure ou une instruction de travail
   c) Leur risque est faible
   d) Ils doivent être mis en œuvre le plus tôt possible

2. Quelle phase du cycle de vie des services détermine quels services devraient être offerts, et à qui ?
   a) L'amélioration continue des services
   b) L'exploitation des services
   c) La conception des services
   d) La stratégie des services

3. Quels rôles sont définis dans le modèle RACI ?
   a) Réalisateur (Responsible), Imputable (Accountable), Consulté, Informé
   b) Réalisateur (Responsible), Atteignable, Consulté, Informé
   c) Réaliste, Imputable (Accountable), Consulté, Informé
   d) Réalisateur (Responsible), Imputable (Accountable), Corrigé, Informé

4. Parmi les énumérations suivantes des quatre étapes du Cycle de Deming, laquelle est CORRECTE ?
   a) Planifier, Mesurer, Surveiller, Rapporter
   b) Planifier, Vérifier, Réagir, Implémenter
   c) Planifier, Faire, Agir, Auditer
   d) Planifier, Faire, Vérifier, Agir

5. 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

6. 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

7. Qu'est-ce que le CAB (Change Advisory Board) dans ITIL ?
   a) Le Comité d'Implémentation des Changements
   b) Le Comité Consultatif des Changements
   c) Le Comité Stratégique des Changements
   d) Le Comité Opérationnel des Changements

8. Laquelle de ces caractéristiques de déploiement NE FIGURE PAS dans le processus de gestion des déploiements et des mises en production ?
   a) Push / Pull
   b) Big Bang / par étapes
   c) Automatique / Manuel
   d) Temporaire / Permanent

9. La valeur business d'un service est définie par :
   a) L'Utilité et la Capacité
   b) L'Utilité et la Disponibilité
   c) L'Utilité et la Garantie
   d) L'Utilité et la Continuité

10. Quels services NE SONT PAS indiqués dans le portefeuille de services ?
   a) Les services retirés
   b) Les services du catalogue de services
   c) Les services du pipeline
   d) Aucun. Tous les services sont dans le portefeuille de services.

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 énoncés suivants sur la création de valeur par les services est CORRECT ?
   a) La perception du client par rapport au service est un facteur important de la création de la valeur.
   b) La valeur d'un service ne peut être mesurée qu'en termes financiers
   c) L'obtention de résultats par le fournisseur de services est importante pour la valeur d'un service
   d) Les préférences du fournisseur de service façonnent la perception de la valeur d'un service

13. 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

14. Parmi les processus suivants, lequel ne fait pas partie de la phase de la Stratégie des services ?
   a) La gestion financière
   b) La gestion de la demande
   c) La gestion de la capacité
   d) La gestion du portefeuille de services

15. Le catalogue de services comporte 2 vues. Lesquelles ?

a) La vue client et la vue fournisseur
b) La vue client et la vue utilisateur
c) La vue client et la vue technique
d) La vue technique et la vue fournisseur

16. Que signifie le sigle ITIL ?

a) Information Technology Infrastructure Label
b) Infrastructures Technology Information Library
c) Information Technology Infrastructure Library
d) Information Technical Infrastructure Library

17. Quelles sont les 4 fonctions de la phase Exploitation des services

a) La gestion des applications, la gestion technique, le centre de services, la gestion des opérations IT
b) La gestion des évènements, la gestion des incidents, la gestion des problèmes, la gestion des accès
c) La gestion des applications, la gestion technique, la gestion des accès, la gestion des opérations IT
d) La gestion des applications, la gestion technique, le centre de services, la gestion des accès

18. Parmi les caractéristiques suivantes, laquelle ou lesquelles sont des caractéristiques d'un processus ITIL ?

1. C'est un ensemble structuré d'activités
2. Déclenché par un évènement spécifique
3. Pouvant être mesuré
4. Créé au moment à la Conception des services

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

19. Parmi les processus suivants, lequel n'appartient PAS à la phase d'exploitation des services ?

a) La gestion des Incidents
b) La gestion des Problèmes
c) La gestion des Changements
d) La gestion des Evènements

20. 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