Guide de préparation

Édition 201804

Table de matières

1. Résumé

EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.FR)

Portée

EXIN Information Security Foundation basé sur la norme ISO/IEC 27001 est une certification de base. Elle valide des connaissances professionnelles sur :

- Information et sécurité : les concepts, la valeur de l'information et l'importance de la fiabilité
- Menaces et risques : les concepts de menace et de risque, et la relation entre les menaces et la fiabilité
- Approche et organisation : la politique de sécurité et la configuration de la sécurité de l'information incluant les composants de l'organisation de la sécurité et de la gestion des incidents (de sécurité)
- Mesures : l'importance des mesures de sécurité, notamment physiques, techniques et organisationnelles
  et
- Lois et réglementations : leur importance et leur impact

Sommaire

La sécurité de l'information est la protection de l'information contre une large gamme de menaces afin d'assurer la continuité des activités, de minimiser les risques auxquels elles sont soumises et de maximiser leur rentabilité et les opportunités qu'elles représentent.

La sécurité de l'information ne cesse de gagner en importance dans le monde des technologies de l'information. La mondialisation de l'économie entraîne un échange croissant d'informations entre les organisations (leurs employés, clients et fournisseurs) et une augmentation de l'utilisation des ordinateurs en réseau et des appareils informatiques.

La norme pour la gestion de la sécurité de l'information (ISO/IEC 27001) est une norme internationale largement appliquée et documentée. Elle fournit un cadre à l'organisation et à la gestion d'un programme de sécurité de l'information. La mise en œuvre d'un programme basé sur cette norme soutiendra grandement toute organisation soucieuse de satisfaire aux exigences de l'environnement complexe actuel dans lequel elle évolue. Il est important pour le développement personnel de chaque professionnel de la sécurité de l'information de bien comprendre cette norme.

Les modules EXIN sur la sécurité de l'information appliquent la définition suivante : la sécurité de l'information traite de la définition, la mise en œuvre, la maintenance, la conformité et l'évaluation d'un ensemble cohérent de mesures de contrôle, qui garantissent la disponibilité, l'intégrité et la confidentialité de la fourniture d'information (manuelle et automatisée).

Dans le module «EXIN Information Security Foundation basé sur la norme ISO/IEC 27001 », les concepts de base de la sécurité de l'information et leurs relations sont testés. Ce module a notamment pour vocation de sensibiliser au fait que l'information est vulnérable et que des mesures sont nécessaires pour la protéger.

Contexte

La Certification « EXIN Information Security Foundation basé sur la norme ISO/IEC 27001 » s'inscrit dans le cadre du programme de qualification « EXIN Sécurité de l'information ». Ce module est suivi par les Certifications « EXIN Information Security Management Professional basé sur la norme ISO/IEC 27001 » et « EXIN Information Security Management Expert basé sur la norme ISO/IEC 27001 ».

Groupe cible

L'examen correspondant au module « EXIN Information Security Foundation basé sur la norme ISO/IEC 27001 » s'adresse à tout membre de l'organisation chargé du traitement de l'information. Le module est également adapté aux entrepreneurs indépendants qui doivent disposer de connaissances élémentaires en matière de sécurité de l'information.
Ce module peut constituer un bon point de départ pour les nouveaux professionnels de la sécurité de l'information.

Exigences de la certification

- Réussite à l'examen EXIN Information Security Foundation based on ISO/IEC 27001.

Précisions sur l'examen

Type d'examen :	Questions à choix multiples
Nombre de questions :	40
Note minimale pour réussir :	65%
Accès à notes / manuel :	Non
Matériel / aides électronique autorisés :	Non
Durée de l'examen :	60 minutes

Les règles et règlements de l'EXIN en matière d'examens s'appliquent à cet examen.

Bloom level

Le certification EXIN Information Security Foundation based on ISO/IC 27001 teste les candidats aux niveaux 1 et 2 de la taxonomie révisée de Bloom :

- Niveau 1 : Souvenir - s'appuie sur le rappel de l'information. Les candidats doivent absorber des informations, se souvenir, reconnaître et se rappeler. Il s'agit du bloc de base de l'apprentissage, avant que les candidats puissent passer aux niveaux supérieurs.
- Niveau 2 : Compréhension – va une étape plus loin que le souvenir. À cette étape, le candidat montre qu'il comprend ce qui est présenté et qu'il peut identifier dans son propre environnement des applications de ce qu'il a appris.

Formation

Heures de contact

Le nombre minimal d'heures pour la formation est 14. Cela comprend les exercices de groupe, la préparation aux examens et de brèves pauses. Ce nombre d'heures n'inclut pas les devoirs, la logistique liée à la session de l'examen, la session de l'examen ni les pauses déjeuner.

Charge de travail estimée

60 heures, en fonction de connaissances existantes.

Organisme de formation

Vous trouverez une liste de sorganismes de formantion accrédités sur www.exin.com.

2. Conditions de l’examen

Les exigences relatives à l’examen sont indiquées dans les spécifications de l'examen. Le tableau suivant énumère les sujets du module (exigences relatives à l’examen) et les sous-thèmes (spécifications de l'examen).

Condition de l’examen	Spécification de l’examen	Pondération
1 Information et sécurité		**10%**
	1.1 Le concept d’information	2.5%
	1.2 Valeur de l’information	2.5%
	1.3 Critères de fiabilité	5%
2 Menaces et risques		**30%**
	2.1 Menaces et risques	15%
	2.2 Relations entre les menaces, les risques et la fiabilité de l’information	15%
3 Approche et organisation		**10%**
	3.1 Politique de sécurité et organisation de la sécurité	2.5%
	3.2 Composantes	2.5%
	3.3 Gestion des incidents	5%
4 Mesures		**40%**
	4.1 Importance des mesures	10%
	4.2 Mesures de sécurité physiques	10%
	4.3 Mesures techniques	10%
	4.4 Mesures organisationnelles	10%
5 Lois et réglementations		**10%**
	5.1 Lois et réglementations	10%
	Total	100%

Spécifications de l'examen

1 Information et sécurité

1.1 Le concept d'information

Le candidat peut…

1.1.1 expliquer la différence entre une donnée et une information.

1.1.2 décrire le support de stockage qui fait partie de l'infrastructure de base.

1.2 Valeur de l'information

Le candidat peut…

1.2.1 décrire la valeur des données/de l'information pour les organisations.

1.2.2 décrire comment la valeur des données/de l'information peut influencer les organisations.

1.2.3 expliquer comment les concepts de sécurité de l'information appliqués protègent la valeur des données/de l'information.

1.3 Critères de fiabilité

Le candidat peut…

1.3.1 nommer les critères de fiabilité de l'information.

1.3.2 décrire les critères de fiabilité de l'information.

2 Menaces et risques

2.1 Menace et risque

Le candidat peut…

2.1.1 expliquer les concepts de menace, de risque et d'analyse des risques.

2.1.2 expliquer la relation entre une menace et un risque.

2.1.3 décrire divers types de menaces.

2.1.4 décrire divers types de préjudices.

2.1.5 décrire diverses stratégies de gestion des risques.

2.2 Relations entre les menaces, les risques et la fiabilité de l'information

Le candidat peut…

2.2.1 reconnaître des exemples de divers types de menaces.

2.2.2 décrire les effets des divers types de menaces sur l'information et le traitement de l'information.

3 Approche et organisation

3.1 Politique de sécurité et organisation de la sécurité

Le candidat peut…

3.1.1 donner un aperçu des objectifs et du contenu d'une politique de sécurité.

3.1.2 donner un aperçu des objectifs et du contenu d'une organisation de la sécurité.

3.2 Composantes

Le candidat peut…

3.2.1 expliquer l'importance d'un code de conduite.

3.2.2 expliquer l'importance de la propriété.

3.2.3 nommer les rôles les plus importants dans l'organisation de la sécurité de l'information.

3.3 Gestion des incidents

Le candidat peut…

3.3.1 résumer la manière dont les incidents de sécurité sont signalés et indiquer les informations requises.
3.3.2 donner des exemples d'incidents de sécurité.
3.3.3 expliquer les conséquences de l'absence de signalement d'incidents de sécurité.
3.3.4 expliquer ce qu'implique le processus d'escalade des incidents (au niveau fonctionnel et hiérarchique).
3.3.5 décrire les effets du processus d'escalade des incidents au sein de l'organisation.
3.3.6 expliquer ce qu'est le cycle de vie d'un incident.

4 Mesures

4.1 Importance des mesures

Le candidat peut…

4.1.1 décrire diverses façons de structurer ou d'organiser des mesures de sécurité.
4.1.2 donner des exemples pour chaque type de mesure de sécurité.
4.1.3 expliquer la relation entre les risques et les mesures de sécurité.
4.1.4 expliquer l'objectif de la classification des informations.
4.1.5 décrire l'effet de la classification.

4.2 Mesures de sécurité physiques

Le candidat peut…

4.2.1 donner des exemples de mesures de sécurité physiques.
4.2.2 décrire les risques impliqués par des mesures de sécurité physiques insuffisantes.

4.3 Mesures techniques

Le candidat peut…

4.3.1 donner des exemples de mesures de sécurité techniques.
4.3.2 décrire les risques impliqués par des mesures de sécurité techniques insuffisantes.
4.3.3 comprendre les concepts de cryptographie, de signature numérique et de certificat.
4.3.4 nommer les trois étapes des opérations bancaires en ligne (PC, site Internet, paiement).
4.3.5 nommer divers types de logiciels malveillants.
4.3.6 décrire les mesures pouvant être utilisées contre les logiciels malveillants.

4.4 Mesures organisationnelles

Le candidat peut…

4.4.1 donner des exemples de mesures de sécurité organisationnelles.
4.4.2 décrire les dangers et les risques impliqués par des mesures de sécurité organisationnelles insuffisantes.
4.4.3 décrire les mesures de sécurité d'accès, telles que la séparation des tâches et l'utilisation de mots de passe.
4.4.4 décrire les principes de la gestion de l'accès.
4.4.5 décrire les concepts d'identification, d'authentification et d'autorisation.
4.4.6 expliquer l'importance d'une Gestion de la continuité des affaires correctement établie pour une organisation.
4.4.7 etablir clairement l'importance de la pratique d'exercices.

5 Lois et réglementations

5.1 Lois et réglementations

Le candidat peut…

- 5.1.1 expliquer pourquoi les lois et réglementations sont importantes pour la fiabilité de l'information.
- 5.1.2 donner des exemples de lois relatives à la sécurité de l'information.
- 5.1.3 donner des exemples de réglementations relatives à la sécurité de l'information.
- 5.1.4 indiquer d'éventuelles mesures susceptibles d'être prises pour satisfaire les exigences des lois et réglementations.

3. Liste des concepts de base

Pour les concepts dont l'abréviation et le nom complet sont inclus dans la liste, les deux peuvent être examinés séparément.

Veuillez noter que la connaissance de ces termes seule ne suffit pas pour l'examen ; le candidat doit comprendre le concept et être en mesure de fournir des exemples.

English	French
Access control	Contrôle d'accès
Asset	Actif
Audit	Audit / Vérification
Authentication	Authentification
Authenticity	Authenticité
Authorization	Autorisation
Availability	Disponibilité
Backup	Sauvegarde
Biometrics	Biométrie
Botnet	Réseau zombie
Business Assets	Actif d'entreprise
Business Continuity Management (BCM)	Gestion de la continuité des affaires (GCA)
Business Continuity Plan (BCP)	Plan de continuité des affaires (PCA)
Category	Catégorie
Certificate	Certificat
Change Management	Gestion du changement
Classification (grading)	Classification (classement)
Clear desk policy	Politique du bureau rangé
Code of conduct	Code de conduite
Code of practice for information security (ISO/IEC 27002)	Code de bonnes pratiques pour la gestion de la sécurité de l'information (ISO/IEC 27002)
Completeness	Exhaustivité
Compliance	Conformité
Computer criminality legislation	Lois sur la criminalité informatique
Confidentiality	Confidentialité
Continuity	Continuité
Controls	Contrôles
Copyright legislation	Lois sur les droits d'auteur
Corrective	Correctif(ve)
Correctness	Exactitude
Cryptography	Cryptographie
Cyber crime	Crime cybernétique / Cybercrime
Damage	Préjudice
Data	Donnée(s)
Detective	De détection
Digital signature	Signature numérique

Direct damage	Préjudice direct
Disaster	Sinistre
Disaster Recovery Plan (DRP)	Plan de reprise après sinistre
Encryption	Cryptage
Escalation • Functional escalation • Hierarchical escalation	Escalade • Escalade fonctionnelle • Escalade hiérarchique
Exclusivity	Exclusivité
Hacking	Piratage informatique
Hoax	Canular
Identification	Identification
Impact	Impact
Incident cycle	Cycle de vie d'un incident
Indirect damage	Préjudice indirect
Information	Information(s)
Information analysis	Analyse de l'information
Information architecture	Architecture de l'information
Information management	Gestion de l'information
Information security review	Examen de la sécurité de l'information
Information system	Système d'information
Infrastructure	Infrastructure
Integrity	Intégrité
Interference	Interférence
ISO/IEC 27001	ISO/IEC 27001
ISO/IEC 27002	ISO/IEC 27002
Key	Clé
Logical access management	Gestion d'accès logique
Maintenance door	Fenêtre de maintenance
Malware	Logiciel malveillant
Managing business assets	Gestion des actifs d'entreprise
Non-disclosure agreement	Accord de non-divulgation
Non-repudiation	Non-répudiation
Risk avoiding	Risque évité
Risk bearing	Risque encouru
Risk neutral	Risque neutre
Patch	Correctif
Personal data protection legislation	Lois sur la protection des données personnelles
Personal firewall	Pare-feu personnel
Phishing	Hameçonnage
Precision	Précision
Preventive	Préventif(ve)
Priority	Priorité
Privacy	Respect de la vie privée
Production factor	Facteur de production
Public Key Infrastructure (PKI)	Infrastructure à clés publiques (ICP)

Public records legislation	Lois sur les documents publics
Qualitative risk analysis	Analyse des risques qualitative
Quantitative risk analysis	Analyse des risques quantitative
Reductive	Réducteur(trice)
Redundancy	Redondance
Reliability of information	Fiabilité de l’information
Repressive	Répressif(ve)
Risk	Risque
Risk analysis	Analyse des risques
Risk assessment (Dependency & Vulnerability analysis)	Évaluation des risques (Analyse de dépendance et de vulnérabilité)
Risk management	Gestion des risques
Risk strategy	Stratégie de gestion des risques
Robustness	Robustesse
Rootkit	Rootkit
Secret authentication information	Information secrète d'authentification
Security event	Évènement de sécurité
Security in development	Sécurité au développement
Security incident	Incident de sécurité
Security measure	Mesure de sécurité
Security Organization	Organisation de la sécurité
Security Policy	Politique de sécurité
Security regulations for the government	Réglementations de sécurité pour le gouvernement
Segregation of duties	Séparation des tâches
Social engineering	Ingénierie sociale
Spam	Pourriel
Spyware	Logiciel espion
Stand-by arrangement	Disposition de remplacement
Storage medium	Support de données
System acceptance testing	Mise à l'essai pour l'acceptation du système
Threat	Menace
Timeliness	Rapidité d’exécution
Trojan	Programme troyen
Uninterruptible Power Supply (UPS)	Alimentation sans interruption (UPS)
Urgency	Urgence
User access provisioning	Mise en service des accès utilisateurs
Validation	Validation
Verification	Vérification
Virtual Private Network (VPN)	Réseau privé virtuel (RPV)
Virus	Virus
Vulnerability	Vulnérabilité
Worm	Ver

4. Bibliographie

Bibliographie

A. Hintzbergen, J., Hintzbergen, K., Smulders, A. et Baars, H.
Foundations of Information Security – Based on ISO 27001 and ISO 27002
Van Haren Publishing, 3ème édition, 2015
ISBN 978 94 018 0012 9
eBook 978 94 018 0541 4

Matrice de littérature

Condition de l'examen	Spécification de l'examen	Littérature
1 Information et sécurité		
	1.1 Le concept d'information	Chapitre 3
	1.2 Valeur de l'information	Chapitre 3 et 4
	1.3 Critères de fiabilité	Chapitre 3 et 4
2 Menaces et risques		
	2.1 Menaces et risques	Chapitre 3
	2.2 Relations entre les menaces, les risques et la fiabilité de l'information	Chapitre 3 et 11
3 Approche et organisation		
	3.1 Politique de sécurité et organisation de la sécurité	Chapitre 3, 5 et 6
	3.2 Composantes	Chapitre 6, 7, 8 et 13
	3.3 Gestion des incidents	Chapitre 3, 15 et 16
4 Mesures		
	4.1 Importance des mesures	Chapitre 3, 8 et 16
	4.2 Mesures de sécurité physiques	Chapitre 3 et 11
	4.3 Mesures techniques	Chapitre 6, 11 et 12
	4.4 Mesures organisationnelles	Chapitre 3, 6, 9, 17 et 18
5 Lois et réglementations		
	5.1 Lois et réglementations	Chapitre 18

Contacter EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER