

# Manuel du candidat

ISO/IEC 27005 RISK MANAGER

## Table des matières

---

<b>SECTION I : Introduction</b> .....	<b>3</b>
À propos de PECB .....	3
Valeur de la certification PECB .....	4
Code de déontologie de PECB .....	5
<b>SECTION II : PROCESSUS DE CERTIFICATION ET PRÉPARATION, RÈGLES ET POLITIQUES RELATIFS À L'EXAMEN DE PECB</b> .....	<b>7</b>
Décidez de la certification qui vous convient .....	7
Préparer et programmer l'examen .....	7
Domaines de compétence.....	7
Faire l'examen .....	16
Transmission des résultats d'examen.....	19
Politique de reprise d'examen .....	19
Sécurité de l'examen.....	19
Demande de certification .....	20
Renouveler la certification.....	20
<b>SECTION III : EXIGENCES DE LA CERTIFICATION</b> .....	<b>21</b>
ISO/IEC 27005 Risk Manager .....	21
<b>SECTION IV : POLITIQUES ET RÈGLEMENTS RELATIFS À LA CERTIFICATION</b> .....	<b>22</b>
Expérience professionnelle .....	22
Évaluation des demandes de certification .....	22
Refus de la demande de certification .....	22
Suspension de la certification .....	22
Révocation de la certification.....	23
Mise à niveau des titres de compétences .....	23
Déclassement des titres de compétences .....	23
Autres statuts.....	23
<b>SECTION V : POLITIQUES GÉNÉRALES DE PECB</b> .....	<b>24</b>

## SECTION I : Introduction

---

### À propos de PECB

PECB est un organisme de certification qui propose des services d'éducation<sup>1</sup> et de certification de personnes selon la norme ISO/IEC 17024, dans un large éventail de disciplines.

Nous aidons les professionnels à démontrer engagement et compétence en leur fournissant des services d'évaluation et de certification de qualité conformément aux exigences de normes reconnues mondialement. Notre mission est de fournir des services qui inspirent la confiance et l'amélioration continue, qui démontrent une reconnaissance et bénéficient à toute la société.

### Les principaux objectifs de PECB sont les suivants :

1. Établir les exigences minimales nécessaires à la certification des professionnels
2. Examiner et vérifier les qualifications des candidats pour s'assurer qu'ils sont éligibles à la certification
3. Développer et maintenir des évaluations de certification fiables
4. Délivrer des certifications aux candidats qualifiés, maintenir à jour et publier un registre des titulaires de certifications en cours de validité.
5. Établir des exigences pour le renouvellement périodique de la certification et assurer la conformité à ces exigences
6. S'assurer que les candidats respectent les normes éthiques dans leur pratique professionnelle
7. Représenter ses membres, le cas échéant, dans les questions d'intérêt commun
8. Promouvoir les avantages de la certification aux employeurs, aux fonctionnaires, aux praticiens des domaines connexes et au grand public

---

<sup>1</sup> Éducation fait référence aux formations développées par PECB, et offertes dans le monde entier par les Partenaires PECB.

## Valeur de la certification PECB

### Pourquoi choisir PECB en tant qu'organisme de certification ?

#### Reconnaissance mondiale

Nos certifications sont reconnues à l'échelle internationale et accréditées par l'IAS (International Accreditation Service), signataire du Multilateral Recognition Arrangement (MLA) de l'IAF qui assure la reconnaissance mutuelle de la certification accréditée entre les signataires du MLA et l'acceptation de la certification accréditée dans de nombreux marchés. Par conséquent, les professionnels qui obtiennent un titre de certification de PECB bénéficieront de la reconnaissance de PECB sur les marchés nationaux et internationaux.

#### Personnel compétent

L'équipe centrale de PECB est composée de personnes compétentes qui possèdent une expérience pertinente des différents domaines.

Tous nos employés détiennent des titres professionnels et sont constamment formés pour fournir des services plus que satisfaisants à nos clients.

#### Conformité aux normes

Nos certifications sont une démonstration de la conformité à la norme ISO/IEC 17024. Elles garantissent que les exigences de la norme ont été remplies et validées avec la cohérence, le professionnalisme et l'impartialité adéquats.

#### Service client

Nous sommes une entreprise centrée sur le client et nous traitons tous nos clients avec estime, importance, professionnalisme et équité. PECB dispose d'une équipe d'experts qui se consacrent au soutien des demandes, problèmes, préoccupations, besoins et opinions des clients. Nous faisons de notre mieux pour maintenir un temps de réponse maximum de 24 heures sans compromettre la qualité du service.

## Code de déontologie de PECB

### Les professionnels de PECB sont tenus de :

1. Se comporter de manière professionnelle, avec honnêteté, exactitude, équité, responsabilité et indépendance
2. Agir en tout temps uniquement dans le meilleur intérêt de leur employeur, de leurs clients, du public et de la profession, en respectant les normes professionnelles et les techniques applicables tout en offrant des services professionnels
3. Maintenir leurs compétences dans leurs domaines respectifs et s'efforcer d'améliorer constamment leurs capacités professionnelles
4. Ne proposer que des services professionnels pour lesquels ils sont qualifiés et informer correctement les clients de la nature des services proposés, y compris de toute préoccupation ou risque pertinent
5. Informer chaque employeur ou client de tout intérêt commercial ou affiliation qui pourrait influencer leur jugement ou nuire à leur équité
6. Traiter de manière confidentielle et privée les informations obtenues dans le cadre des relations professionnelles et commerciales de tout employeur ou client, actuel ou ancien
7. Se conformer à toutes les lois et réglementations des juridictions dans lesquelles les activités professionnelles sont exercées
8. Respecter la propriété intellectuelle et la contribution d'autrui
9. Ne pas communiquer, intentionnellement ou non, des informations fausses ou falsifiées qui pourraient compromettre l'intégrité du processus d'évaluation d'un candidat à un titre professionnel
10. Ne pas agir d'une manière qui pourrait compromettre la réputation de PECB ou de ses programmes de certification
11. Coopérer pleinement à l'enquête menée à la suite d'une prétendue violation du présent Code de déontologie

La version complète du Code de déontologie de PECB peut être téléchargée [ici](#).

## Présentation de certification « ISO/IEC 27005 Risk Manager »

L'ISO/CEI 27005 est une norme internationale qui donne des lignes directrices pour la gestion des risques liés à la sécurité de l'information et soutient les concepts généraux de la sécurité de l'information spécifiés dans la norme ISO/CEI 27001. Les processus de gestion des risques liés à la sécurité de l'information permettent aux organismes d'identifier, d'analyser et de traiter les risques liés à l'utilisation des technologies de l'information.

Le cyberspace devenant de plus en plus dangereux, la protection contre les menaces à la sécurité de l'information est devenue essentielle pour la plupart des organismes. La gestion des risques est un élément de base de la sécurité de l'information. C'est pourquoi, l'une des compétences les plus demandées sur le marché est la capacité à établir et à mettre en œuvre une approche systématique de la gestion des risques liés à la sécurité de l'information.

La certification « ISO/IEC 27005 Risk Manager » est une certification professionnelle destinée aux professionnels de la sécurité de l'information qui visent à attester de leur aptitude à gérer efficacement les risques liés à la sécurité de l'information. Une certification reconnue au niveau international apporte une grande valeur ajoutée à votre carrière et vous aidera à atteindre vos objectifs professionnels.

Il est important de préciser que les certifications de PECB ne sont pas une licence ou une simple adhésion. Il s'agit d'une reconnaissance par les pairs qu'une personne a démontré sa maîtrise et sa compréhension d'un ensemble de compétences. Les certifications PECB sont accordées aux candidats qui peuvent fournir la preuve de leur expérience et qui ont réussi un examen normalisé dans le domaine de la certification.

Ce document décrit le système de certification PECB ISO/IEC 27005 Risk Manager, conformément à la norme ISO/IEC 17024:2012. Il contient également des informations sur le processus par lequel les candidats peuvent obtenir et renouveler leur certification. Il est très important que vous lisiez toutes les informations contenues dans ce manuel avant de remplir et de soumettre votre candidature. Si vous avez des questions après la lecture de ce document, veuillez contacter le bureau international de PECB à [certification.team@pecb.com](mailto:certification.team@pecb.com)

## SECTION II : PROCESSUS DE CERTIFICATION ET PRÉPARATION, RÈGLES ET POLITIQUES RELATIFS À L'EXAMEN DE PECB

---

### Décidez de la certification qui vous convient

Toutes les certifications PECB sont assorties d'exigences spécifiques en matière de formation et d'expérience professionnelle. Pour déterminer le titre de compétence qui vous convient, vérifiez les critères d'admissibilité des diverses certifications et vos besoins professionnels.

### Préparer et programmer l'examen

Les candidats sont responsables de leur propre étude et de leur préparation aux examens de certification. Aucun ensemble spécifique de cours ou de programmes d'études n'est requis dans le cadre du processus de certification. Toutefois, la participation à une session de formation peut augmenter de manière significative les chances de réussite à l'examen PECB.

Pour programmer un examen de certification PECB, les candidats ont deux options :

1. Contacter l'un de nos partenaires qui proposent des sessions de formation et d'examen. Les candidats trouveront un Partenaire de formations dans une région donnée sur la page [Liste des partenaires](#). Le calendrier des sessions de formation PECB est également disponible sous l'onglet [Calendrier des formations](#).
2. Passer un examen PECB à distance de chez eux ou de n'importe quel endroit qu'ils préfèrent grâce à l'application PECB Exams, qui est accessible ici : [Sessions d'examens](#).

Pour en savoir plus sur les examens, les domaines de compétences et les énoncés de connaissances, veuillez vous référer à la *section III* du présent document.

### Frais de demande d'examen et de certification

PECB propose aussi les examens directement, où un candidat peut se présenter à l'examen sans assister à la formation. Les prix sont les suivants :

- Examen Lead : 1 000 \$
- Examen Manager : 700 \$
- Examens Foundation et Transition : 500 \$

Les frais de demande de certification sont de 500 \$ US.

Pour tous les candidats qui ont suivi la formation et passé l'examen auprès d'un partenaire PECB, le coût de la session de formation comprend les frais associés à l'examen (examen et première reprise) et à la demande de certification, ainsi que la première année de frais annuels de maintenance (FAM).

### Domaines de compétence

L'objectif de l'examen de certification « PECB Certified ISO/IEC 27005 Risk Manager » est de s'assurer que le candidat a acquis les compétences et les aptitudes nécessaires pour établir, mettre en œuvre et gérer un programme de gestion des risques liés à la sécurité de l'information.

La certification ISO/IEC 27005 Risk Manager est destinée aux profils suivants :

- Responsables ou consultants impliqués dans la sécurité de l'information dans un organisme
- Personnes responsables de la gestion des risques liés à la sécurité de l'information

- Membres des équipes de sécurité de l'information, professionnels de l'informatique et responsables de la protection de la vie privée
- Personnes responsables du maintien de la conformité aux exigences de sécurité de l'information de la norme/IEC 27001 au sein d'un organisme
- Gestionnaires de projet, consultants ou conseillers experts cherchant à maîtriser la gestion des risques liés à la sécurité de l'information

L'examen couvre les domaines de compétences suivants :

- **Domaine 1** : Principes et concepts fondamentaux d'un système de gestion des risques liés à la sécurité de l'information
- **Domaine 2** : Mise en œuvre d'un programme de gestion des risques en sécurité de l'information
- **Domaine 3** : Cadre de gestion des risques en sécurité de l'information et des processus selon la norme ISO/IEC 27005
- **Domaine 4** : Autres méthodes d'appréciation des risques liés à la sécurité de l'information

<ul style="list-style-type: none"> <li>• <b>Domaine 1 : Principes et concepts fondamentaux d'un système de gestion des risques liés à la sécurité de l'information</b></li> <li>• <b>Objectif principal</b> : S'assurer que le candidat comprend et est capable d'interpréter les principes fondamentaux et les concepts de la gestion des risques de la sécurité de l'information</li> </ul>	
<p style="text-align: center;"><b>Compétences</b></p> <ol style="list-style-type: none"> <li>1. Comprendre, interpréter et analyser les exigences de la norme ISO/IEC 27005</li> <li>2. Comprendre la relation entre la norme ISO/IEC 27005 et d'autres cadres de gestion des risques</li> <li>3. Décrire l'objectif de la gestion des risques et les avantages de la norme ISO/IEC 27005</li> <li>4. Comprendre et expliquer les concepts de la sécurité de l'information</li> <li>5. Comprendre les principes de la sécurité de l'information à savoir les concepts de confidentialité, d'intégrité et de disponibilité des informations</li> <li>6. Comprendre et interpréter la définition du risque</li> <li>7. Comprendre les concepts et principes fondamentaux de la gestion des risques</li> <li>8. Comprendre les vulnérabilités et les menaces en matière de sécurité de l'information</li> <li>9. Décrire et expliquer les concepts d'événement, d'opportunité, de conséquence et de vraisemblance</li> </ol>	<p style="text-align: center;"><b>Énoncés de connaissances</b></p> <ol style="list-style-type: none"> <li>1. Connaissance des principaux concepts et de la terminologie de la norme ISO/IEC 27005</li> <li>2. Connaissance des principales normes de la famille ISO/IEC 27000</li> <li>3. Connaissance des normes et des cadres internationaux et sectoriels en matière de sécurité de l'information et de gestion des risques</li> <li>4. Connaissance des risques liés à la sécurité de l'information, tels que définis par la norme ISO/IEC 27005</li> <li>5. Connaissance de la définition de la notion de vulnérabilité</li> <li>6. Connaissance des différences entre les concepts de risques et d'opportunités</li> <li>7. Connaissance de la définition de la notion de menace</li> <li>8. Connaissance des notions de confidentialité, de l'intégrité et de la disponibilité des informations</li> <li>9. Connaissance du type et de la fonction des mesures de contrôle de la sécurité</li> <li>10. Connaissance des principes de gestion des risques</li> </ol>



<p>10. Comprendre la classification des contrôles de sécurité par type et par fonction</p> <p>11. Comprendre le rôle du propriétaire du risque</p>	<p>11. Connaissance des rôles et responsabilités du propriétaire du risque</p> <p>12. Connaissance des avantages de la gestion des risques</p>
----------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------

## Domaine 2 : Mise en œuvre d'un programme de gestion des risques en sécurité de l'information

**Objectif principal :** S'assurer que le candidat comprend et est capable d'initier la mise en œuvre d'un programme de gestion des risques basé sur la norme ISO/IEC 27005.

Compétences	Énoncés de connaissances
<ol style="list-style-type: none"> <li>1. Comprendre l'intégration du cycle PDCA (Plan, Do, Check, Act) dans le programme de gestion des risques liés à la sécurité de l'information</li> <li>2. Comprendre et expliquer les principales étapes nécessaires à l'établissement et à la mise en œuvre d'un programme de gestion des risques liés à la sécurité de l'information</li> <li>3. Identifier les rôles et responsabilités des principales parties prenantes pendant et après la mise en œuvre et le fonctionnement d'un programme de gestion des risques liés à la sécurité de l'information</li> <li>4. Comprendre le concept d'appréciation du risque</li> <li>5. Comprendre l'importance d'une politique de gestion des risques</li> <li>6. Identifier les ressources nécessaires à la mise en œuvre d'un programme de gestion des risques</li> <li>7. Analyser et comprendre le contexte interne et externe d'un organisme</li> <li>8. Comprendre les processus et activités clés d'un organisme</li> <li>9. Comprendre et fixer des objectifs pour le programme de gestion des risques</li> <li>10. Établir et maintenir des critères de risque en matière de sécurité de l'information, y compris des critères d'acceptation des risques et des critères d'appréciation des risques en matière de sécurité de l'information</li> <li>11. Définir et justifier le domaine d'application du processus de gestion des risques liés à</li> </ol>	<ol style="list-style-type: none"> <li>1. Connaissance du processus de gestion des risques</li> <li>2. Connaissance de la manière dont la direction générale peut faire preuve de leadership et d'engagement en matière de gestion des risques</li> <li>3. Connaissance des rôles et responsabilités d'un risk manager (gestionnaire de risques) en ce qui concerne le programme de gestion des risques</li> <li>4. Connaissance des rôles et responsabilités des principales parties prenantes dans la mise en œuvre d'un programme de gestion des risques</li> <li>5. Connaissance de ce qui constitue typiquement le contexte interne et externe d'une organisation</li> <li>6. Connaissance de l'importance de comprendre les processus et activités clés d'un organisme en matière de gestion des risques</li> <li>7. Connaissance des objectifs de l'appréciation des risques et de la manière d'obtenir des résultats spécifiques</li> <li>8. Connaissance de la manière dont sont établis les critères d'acceptation des risques et les critères d'appréciation des risques en matière de sécurité de l'information</li> <li>9. Connaissance des cycles de gestion des risques liés à la sécurité de l'information</li> <li>10. Connaissance de l'applicabilité de l'analyse quantitative et qualitative dans la détermination des critères d'acceptation du risque</li> <li>11. Connaissance des ressources nécessaires à la gestion des risques liés à la sécurité de l'information</li> <li>12. Connaissance du domaine d'application et des limites de la gestion des risques liés à la sécurité de l'information</li> </ol>

<p>la sécurité de l'information et de l'adapter aux objectifs de l'organisme</p> <p>12. Définir une méthode appropriée de gestion des risques liés à la sécurité de l'information</p>	<p>13. Connaissance des approches et des méthodologies utilisées pour l'évaluation des risques liés à la sécurité de l'information</p> <p>14. Connaissance des principales étapes de la planification des activités d'évaluation des risques</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Domaine 3 : Cadre de gestion des risques en sécurité de l'information et des processus selon la norme ISO/IEC 27005

**Objectif principal :** S'assurer que le candidat est capable d'identifier, d'analyser, d'évaluer, de traiter, de communiquer, d'enregistrer et de surveiller en permanence les risques liés à la sécurité de l'information sur la base de la norme ISO/IEC 27005.

Compétences	Énoncés de connaissances
<ol style="list-style-type: none"> <li>1. Comprendre les processus d'identification, d'analyse et d'évaluation des risques en matière de sécurité de l'information</li> <li>2. Déterminer l'approche d'identification des risques et à comprendre et interpréter les techniques de collecte d'informations</li> <li>3. Identifier les biens, les menaces, les mesures de sécurité existantes, les vulnérabilités, les conséquences potentielles et les responsables des risques.</li> <li>4. Comprendre et à interpréter les méthodes d'analyse des risques</li> <li>5. Comprendre et à évaluer les conséquences</li> <li>6. Déterminer les niveaux de risque sur la base des critères d'évaluation des risques</li> <li>7. Classer les risques par ordre de priorité</li> <li>8. Comprendre le processus de traitement des risques et les options de traitement des risques sur la base de la norme ISO/IEC 27005</li> <li>9. Sélectionner les contrôles appropriés pour réduire, conserver, éviter ou partager les risques</li> <li>10. Comprendre et expliquer les critères d'acceptation des risques en matière de sécurité de l'information</li> <li>11. Comprendre la gestion du risque résiduel</li> <li>12. Comprendre et interpréter le concept de communication et de concertation sur les risques</li> <li>13. Comprendre et interpréter les principes d'une communication efficace</li> <li>14. Comprendre et établir une communication interne et externe</li> </ol>	<ol style="list-style-type: none"> <li>1. Connaissance des processus d'appréciation des risques en matière de sécurité de l'information, y compris l'identification, l'analyse et l'évaluation des risques</li> <li>2. Connaissance des méthodes d'identification des risques pour la sécurité de l'information</li> <li>3. Connaissance des techniques de collecte d'informations</li> <li>4. Connaissance de la définition des notions de bien et d'identification des biens essentiels et des biens support</li> <li>5. Connaissance de l'identification et de la classification des vulnérabilités, des menaces et des mesures de sécurité existantes</li> <li>6. Connaissance de l'identification des conséquences potentielles qui peuvent affecter la disponibilité, la confidentialité, l'intégrité et la sécurité des données</li> <li>7. Connaissance des techniques d'analyse des risques</li> <li>8. Connaissance de la manière de déterminer les conséquences et la vraisemblance et de déterminer le niveau de risque</li> <li>9. Connaissance de l'évaluation des niveaux de risque sur la base des critères d'évaluation des risques</li> <li>10. Connaissance de la manière de classer des risques par ordre de priorité</li> <li>11. Connaissance des processus et options de traitement des risques, y compris la modification des risques, la prise de risque, la prévention des risques et le partage des risques.</li> <li>12. Connaissance de la formulation et de l'approbation d'un plan de traitement des risques</li> </ol>

<ol style="list-style-type: none"><li>15. Comprendre les objectifs et les activités de communication</li><li>16. Comprendre les approches et les outils de communication</li><li>17. Documenter les processus de gestion des risques liés à la sécurité de l'information</li><li>18. Enregistrer et communiquer les résultats de l'évaluation et du traitement des risques</li><li>19. Contrôler et revoir l'efficacité d'un programme de gestion des risques liés à la sécurité de l'information</li><li>20. Comprendre le concept d'amélioration continue et ses avantages en matière de gestion des risques</li><li>21. Conseiller un organisme sur la manière d'améliorer en permanence l'efficacité et l'efficience d'un programme de gestion des risques liés à la sécurité de l'information</li></ol>	<ol style="list-style-type: none"><li>13. Connaissance de la méthode d'évaluation et d'acceptation des risques résiduels</li><li>14. Connaissance du processus de communication sur les risques liés à la sécurité de l'information</li><li>15. Connaissance des principes d'une stratégie de communication efficace</li><li>16. Connaissance de la manière dont la communication interne et externe doit être établie</li><li>17. Connaissance des approches et des outils de communication</li><li>18. Connaissance des informations documentées et de l'importance de l'enregistrement des risques</li><li>19. Connaissance de la documentation des résultats de la gestion des risques</li><li>20. Connaissance des principaux concepts liés à l'amélioration continue</li><li>21. Connaissance des processus qui doivent faire l'objet d'une surveillance et d'une revue continues</li></ol>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Domaine 4 : Autres méthodes d'appréciation des risques liés à la sécurité de l'information

**Objectif principal :** S'assurer que le candidat peut utiliser les méthodologies et les cadres d'appréciation des risques, tels que OCTAVE, MEHARI, EBIOS, NIST, EMR, et CRAMM.

Compétences	Énoncés de connaissances
<ol style="list-style-type: none"> <li>1. Comprendre et interpréter les méthodologies OCTAVE : OCTAVE, OCTAVE-S, OCTAVE Allegro, et OCTAVE FORTE.</li> <li>2. Mener une appréciation des risques liés à la sécurité de l'information selon la méthodologie OCTAVE Allegro</li> <li>3. Analyser et gérer les risques selon la méthode MEHARI</li> <li>4. Comprendre et utiliser la méthode EBIOS pour l'appréciation des risques</li> <li>5. Identifier les publications du NIST relatives à la gestion des risques</li> <li>6. Comprendre et interpréter le RMF du NIST et l'utiliser pour gérer les risques liés à la sécurité de l'information</li> <li>7. Comprendre et interpréter la méthodologie CRAMM pour la gestion des risques</li> <li>8. Comprendre et expliquer comment la méthode EMR (Évaluation harmonisée des menaces et des risques) peut être utilisée pour l'évaluation des risques</li> </ol>	<ol style="list-style-type: none"> <li>1. Connaissance des trois phases de la méthode OCTAVE</li> <li>2. Connaissance des phases de la méthode OCTAVE-S pour l'appréciation des risques</li> <li>3. Connaissance de la manière dont les phases d'OCTAVE-Allegro peuvent être utilisées pour mener une appréciation des risques liés à la sécurité de l'information</li> <li>4. Connaissance des étapes de la méthode OCTAVE FORTE pour la gestion des risques</li> <li>5. Connaissance des trois phases principales de MEHARI pour la gestion des risques</li> <li>6. Connaissance de la manière dont les risques liés à la sécurité de l'information peuvent être identifiés, estimés, évalués et traités à l'aide de la méthodologie MEHARI</li> <li>7. Connaissance de la méthodologie d'appréciation des risques EBIOS et de ses cinq ateliers et modules</li> <li>8. Connaissance des publications du NIST sur la gestion des risques</li> <li>9. Connaissance des sept étapes du cadre de gestion des risques du NIST</li> <li>10. Connaissance de la méthodologie et de l'outil d'analyse et de gestion des risques CRAMM</li> <li>11. Connaissance des cinq phases de la méthodologie EMR (Évaluation harmonisée des menaces et des risques)</li> </ol>

Sur la base des compétences susmentionnées et de leur pertinence, 60 questions sont proposées dans l'examen, comme le résume le tableau ci-dessous :

		Niveau de compréhension (Cognitif/Taxonomique) requis			
		Nombre de questions/points par domaine de compétence	%/points de l'examen consacré à chaque domaine de compétence	Questions qui mesurent la compréhension, l'application et l'analyse	Questions qui mesurent la synthèse et l'évaluation
Domaines de compétence	Principes et concepts fondamentaux d'un système de gestion des risques liés à la sécurité de l'information	13	21.67	X	
	Mise en œuvre d'un programme de gestion des risques en sécurité de l'information	7	11.67	X	
	Cadre de gestion des risques en sécurité de l'information et des processus selon la norme ISO/IEC 27005	31	51.67		X
	Autres méthodes d'appréciation des risques liés à la sécurité de l'information	9	15	X	
Total des points		<b>60</b>	<b>100 %</b>		
Nombre de questions par niveau de compréhension				<b>29</b>	<b>31</b>
Pourcentage de l'examen consacré à chaque niveau de compréhension (cognitif/taxonomie)				<b>48.3 %</b>	<b>51.7 %</b>

La note de passage est établie à **70 %**.

Une fois l'examen réussi, les candidats pourront demander le titre de « PECB Certified ISO/IEC 27005 Risk Manager », en fonction de leur niveau d'expérience.

## Faire l'examen

### Informations générales sur l'examen

Les candidats sont tenus d'être présents au moins 30 minutes avant le début de l'examen. Les candidats qui arrivent en retard ne disposeront pas de temps supplémentaire pour compenser leur retard et pourraient se voir refuser l'accès à l'examen.

Les candidats doivent être en possession d'une carte d'identité valide (carte d'identité nationale, permis de conduire ou passeport) et la présenter au surveillant.

Si la demande en est faite le jour de l'examen, un délai supplémentaire peut être accordé aux candidats qui passent l'examen dans une langue autre que leur langue maternelle.

- 10 minutes supplémentaires pour les examens Foundation
- 20 minutes supplémentaires pour les examens Manager
- 30 minutes supplémentaires pour les examens Lead

### Format et type d'examen PECB

1. **Examen au format papier** : Les examens sont imprimés, où les candidats ne sont pas autorisés à utiliser autre chose que le papier d'examen et un stylo. L'utilisation d'appareils électroniques, tels qu'ordinateurs portables, tablettes ou téléphones, n'est pas autorisée. La session d'examen est supervisée par un surveillant agréé par PECB sur le lieu où le partenaire a organisé la formation.
2. **Examen en ligne** : Les examens sont fournis par voie électronique via l'application PECB Exams. L'utilisation d'appareils électroniques, tels que les tablettes et les téléphones portables, n'est pas autorisée. La session d'examen est supervisée à distance par un surveillant de PECB via l'application PECB Exams et une caméra externe/intégrée.

Pour des informations plus détaillées sur le format d'examen en ligne, veuillez vous référer au [PECB Online Exam Guide](#).

Les examens PECB sont disponibles en deux types :

1. Examen à développement
2. Examen à choix multiple

**Cet examen contient des questions à choix multiple** : Ce type d'examen a été choisi, car il s'est avéré efficace et efficient pour mesurer et évaluer les résultats d'apprentissage selon les domaines de compétence. L'examen à choix multiple peut être utilisé pour évaluer la compréhension d'un candidat sur de nombreux sujets, y compris des concepts simples ou complexes. En répondant à ces questions, les candidats devront appliquer divers principes, analyser des problèmes, évaluer des alternatives, combiner plusieurs concepts ou idées, etc. Les questions à choix multiple sont basées sur un scénario, ce qui signifie qu'elles sont élaborées sur la base d'un scénario que les candidats sont invités à lire et doivent fournir des réponses à une ou plusieurs questions liées à ce scénario. Cet examen à choix multiple est à livre ouvert, en raison de la caractéristique des questions qui dépendent du contexte. Vous trouverez ci-dessous un échantillon de questions d'examen.

L'examen étant « à livre ouvert », les candidats sont autorisés à utiliser les documents de référence suivants :

- Copie papier de la norme ISO/IEC 27005
- Support de formation du participant (accessible sur l'application PECB Exams ou imprimé)
- Notes personnelles prises pendant la session de formation (accessibles sur l'application PECB Exams ou papier)
- Dictionnaire au format papier



Toute tentative de copie, de collusion ou de tricherie pendant l'examen entraînera automatiquement un échec.

Les examens PECB sont disponibles en anglais et dans d'autres langues. Pour savoir si l'examen est disponible dans une langue particulière, veuillez contacter [examination.team@pecb.com](mailto:examination.team@pecb.com).

**Note :** PECB passera progressivement aux examens à choix multiples. Ils seront également à livre ouvert et comprendront des questions basées sur des scénarios qui permettront à PECB d'évaluer les connaissances, les capacités et les aptitudes des candidats à utiliser des informations dans de nouvelles situations (appliquer), à établir des liens entre des idées (analyser) et à justifier une position ou une décision (évaluer). Tous les examens à choix multiples de PECB comportent une question et trois alternatives, dont une seule est correcte.

Pour des informations spécifiques sur les types d'examens, les langues disponibles et d'autres détails, consultez la [Liste des examens PECB](#).

## Exemples de questions d'examen basées sur un scénario

*Techonics* est une entreprise technologique spécialisée dans les logiciels informatiques et l'électronique grand public. Elle procède régulièrement à des appréciations des risques afin de garantir la sécurité de l'information. Grâce à son processus de gestion des risques liés à la sécurité de l'information bien établi, *Techonics* est en mesure d'identifier les risques potentiels associés aux biens informationnels et de trouver des solutions. Son cadre de gestion des risques est basé sur les lignes directrices de la norme ISO/IEC 27005

Le dernier processus d'appréciation des risques en lien à la sécurité de l'information chez *Techonics* s'est déroulé le mois dernier. Elle a été menée par Lana, la risk manager (gestionnaire des risques) de *Techonics*, et ses résultats ont mis en évidence de nouveaux risques liés à la politique en matière de mots de passe. Selon le cadre de gestion des risques de *Techonics*, le processus d'appréciation des risques a commencé par une analyse approfondie de l'entreprise et de ses objectifs. Ensuite, les critères de base concernant la gestion des risques ont été définis.

Lana a mené des entretiens avec le personnel clé. Elle a découvert que la plupart des employés de *Techonics* savaient que la politique en matière de mots de passe exigeait qu'ils modifient leurs mots de passe tous les trois mois. Cependant, la plupart d'entre eux ne respectaient pas cette règle, car le système ne l'obligeait pas.

Par ailleurs, elle a découvert que les employés avaient tendance à utiliser des mots de passe faibles, comme leur nom et leur prénom. Étant donné qu'il est plus facile de deviner les mots de passe faibles, la sécurité de *Techonics* pourrait s'en trouver sérieusement affectée. Lana a identifié plusieurs scénarios de risque concernant la situation identifiée, dont deux ont un niveau d'occurrence « élevé ».

Sam, le responsable de la sécurité de l'information, a proposé la mise en œuvre d'un gestionnaire de mots de passe multiplateforme dans le cloud. La plateforme pourrait être utilisée par tous les employés pour générer des mots de passe complexes et les stocker dans une base de données sécurisée. *Techonics* a accepté sa recommandation et a commencé à utiliser la plateforme afin de minimiser les risques liés aux mots de passe faibles. De plus, il a été décidé que Sam organiserait une formation à la sécurité de l'information afin de sensibiliser le personnel à l'importance de la protection par mot de passe.

Répondez aux questions suivantes en vous référant au scénario ci-dessus :

# PECB

1. **Techonics a utilisé la norme ISO/IEC 27005 comme ligne directrice pour établir son cadre de gestion des risques en matière de sécurité de l'information. Est-ce acceptable ?**
  - A. Non, la norme ISO/IEC 27005 spécifie les exigences à respecter pour assurer la sécurité de l'information par la mise en œuvre d'un SMSI.
  - B. Oui, la norme ISO/IEC 27005 s'applique à tout type de risque, indépendamment de leur nature ou de leurs conséquences.
  - C. **Oui, la norme ISO/IEC 27005 fournit des lignes directrices pour aider les organismes à réaliser des activités de gestion des risques liés à la sécurité de l'information.**
  
2. **Lana, la Risk Manager, a découvert que les employés de Techonics ne modifiaient pas leurs mots de passe, comme l'exige la politique en la matière. Qu'a identifié Lana ?**
  - A. **Une vulnérabilité**
  - B. Une menace
  - C. Un risque
  
3. **Quelle option de traitement des risques a été proposée pour traiter les risques identifiés concernant l'utilisation des mots de passe ?**
  - A. Refus du risque
  - B. **Modification du risque**
  - C. Prise de risque

## Transmission des résultats d'examen

Les résultats d'examens seront communiqués par e-mail.

- Le délai de communication commence à la date de l'examen et dure de deux à quatre semaines pour les examens à choix multiple sur papier.
- Pour les examens à choix multiples en ligne, les candidats reçoivent leurs résultats instantanément.

Les candidats qui réussissent l'examen pourront se porter candidats à l'un des titres de compétences du programme de certification correspondant.

En cas d'échec à l'examen, une liste des domaines dans lesquels le candidat a obtenu une note inférieure à la note de passage sera ajoutée à l'e-mail pour aider les candidats à mieux se préparer à une reprise.

## Politique de reprise d'examen

Il n'y a pas de limite au nombre de fois qu'un candidat peut reprendre un examen. Toutefois, il existe certains délais à respecter entre les reprises d'examen.

- Si le candidat échoue à l'examen à la 1<sup>re</sup> tentative, il doit attendre 15 jours à compter de la date de l'examen initial avant la tentative suivante (1<sup>re</sup> reprise).

**Note :** Les candidats qui ont suivi la formation auprès de l'un de nos partenaires et qui ont échoué à la première tentative d'examen peuvent se représenter gratuitement à l'examen dans un délai de 12 mois à compter de la date de réception du code promotionnel, car les frais payés pour la formation comprennent une première tentative d'examen et une reprise.) Sinon, des frais de reprise s'appliquent.

Aux candidats qui échouent à la reprise de l'examen, PECB recommande de suivre une formation afin d'être mieux préparé à l'examen.

Pour organiser une reprise d'examen, en fonction du format de l'examen, les candidats qui ont suivi une formation doivent suivre les étapes suivantes :

1. Examen en ligne : lors de l'organisation de la reprise de l'examen, utilisez le code coupon initial pour annuler les frais.
2. Examen sur papier : les candidats doivent contacter le partenaire/distributeur de PECB qui a organisé la session initiale pour organiser la reprise de l'examen (date, heure, lieu, coûts).

Les candidats qui n'ont pas suivi de formation avec un partenaire, mais qui se sont présentés à l'examen en ligne directement avec PECB, ne sont pas concernés par cette politique. La procédure pour organiser la reprise de l'examen est la même que pour l'examen initial.

## Sécurité de l'examen

Une composante importante de la certification professionnelle est le maintien de la sécurité et de la confidentialité de l'examen. PECB compte sur le comportement éthique des titulaires et des candidats à la certification pour maintenir la sécurité et la confidentialité des examens PECB. Toute divulgation d'informations sur le contenu des examens PECB constitue une violation directe du Code de déontologie de PECB. PECB prendra des mesures à l'encontre de toute personne qui enfreint les politiques et règlements, y compris l'interdiction permanente d'obtenir les certifications PECB et la révocation de toute certification antérieure. PECB intentera également une action en justice contre les personnes ou les organismes qui enfreignent ses droits d'auteur, ses droits de propriété et sa propriété intellectuelle.

## Reprogrammer l'examen

Pour tout changement concernant la date, l'heure, le lieu de l'examen ou d'autres détails, veuillez contacter [examination.team@pecb.com](mailto:examination.team@pecb.com).

## Demande de certification

Tous les candidats qui réussissent cet examen (ou un équivalent accepté par PECB) peuvent demander les titres de compétences de PECB pour lesquels ils ont été examinés. Des exigences spécifiques en matière d'éducation et d'expérience professionnelle doivent être remplies afin d'obtenir une certification PECB. Le candidat doit remplir le formulaire de demande de certification en ligne (accessible via son compte PECB), y compris les coordonnées des références qui seront contactées pour valider l'expérience professionnelle du candidat. Le candidat peut soumettre sa demande en plusieurs langues. Il peut choisir de payer en ligne ou d'être facturé. Pour de plus amples informations, veuillez contacter [certification.team@pecb.com](mailto:certification.team@pecb.com).

Le processus de demande de certification en ligne est très simple et ne prend que quelques minutes :

- [Inscrivez-vous](#).
- Vérifier vos e-mails pour activer le lien de confirmation.
- [Connectez-vous](#) pour demander la certification

Pour plus d'informations sur le processus de demande, suivez les instructions du manuel [Faire une demande de certification](#).

La demande est approuvée dès que le Service de certification valide que le candidat remplit toutes les exigences de certification relatives au titre concerné. Un e-mail sera envoyé à l'adresse électronique fournie au cours du processus de demande pour communiquer l'état de la demande. Si la demande est approuvée, le candidat pourra télécharger la certification à partir de son compte PECB.

PECB offre un soutien en anglais et en français.

## Renouveler la certification

Les certifications PECB sont valables pour une durée de trois ans. Pour les conserver, les candidats doivent démontrer chaque année qu'ils effectuent toujours les activités liées à la certification. Les professionnels certifiés par PECB doivent fournir chaque année des unités de formation professionnelle continue (FPC) et payer 100 \$ US de frais annuels de maintien (FAM) pour conserver leur certification. Pour de plus amples renseignements, veuillez consulter la page [Maintenance de la certification](#) sur le site Web de PECB.

## Fermeture d'un dossier

Si un candidat ne demande pas la certification dans les trois ans, son dossier sera fermé. Toutefois, même si la période de certification expire, le candidat a le droit de rouvrir son dossier. Cependant, PECB ne sera plus responsable de tout changement concernant les conditions, les normes, les politiques et le Manuel du candidat qui étaient applicables avant la fermeture du dossier. Un candidat qui demande la réouverture de son dossier doit le faire par écrit et payer les frais requis.

## SECTION III : EXIGENCES DE LA CERTIFICATION

### ISO/IEC 27005 Risk Manager

Les exigences pour les certifications PECB ISO/IEC 27005 Manager sont les suivantes :

Titre de compétence	Examen	Expérience professionnelle	Expérience en matière de gestion des risques	Autres exigences
<b>Certifié PECB ISO/IEC 27005 Provisional Risk Manager</b>	Examen de Certification PECB ISO/IEC 27005 Risk Manager ou équivalent	Aucune	Aucune	Signature du code d'éthique de PECB
<b>PECB Certified ISO/IEC 27005 Risk Manager</b>	Examen de Certification PECB ISO/IEC 27005 Risk Manager ou équivalent	Deux années : Un an d'expérience en gestion des risques liés à la sécurité de l'information	Activités de gestion des risques liés à la sécurité de l'information : total de 200 heures	Signature du code d'éthique de PECB

Pour être considérées comme valides, les activités de mise en œuvre doivent suivre les bonnes pratiques de mise en œuvre et de gestion et inclure les éléments suivants :

1. Définition d'une approche de gestion des risques
2. Détermination des objectifs et du domaine d'application de la gestion des risques
3. Réalisation d'une appréciation des risques
4. Élaboration d'un programme de gestion des risques
5. Définition des critères d'évaluation et d'acceptation des risques
6. Évaluation des options de traitement des risques
7. Surveillance et revue du programme de gestion des risques

## SECTION IV : POLITIQUES ET RÈGLEMENTS RELATIFS À LA CERTIFICATION

### Références professionnelles

Pour chaque demande de certification, deux références professionnelles sont requises. Les références professionnelles doivent provenir de personnes ayant travaillé avec le candidat dans un environnement professionnel et pouvant ainsi attester de son expérience de gestion de la sécurité de l'information, ainsi que de ses antécédents professionnels actuels et antérieurs. Les références professionnelles de personnes qui sont sous la supervision du candidat ou qui sont ses proches ne sont pas valables.

### Expérience professionnelle

Le candidat doit fournir des informations complètes et exactes concernant son expérience professionnelle, notamment le titre de chaque poste, les dates de début et de fin, la description des postes, etc. Il est conseillé au candidat de résumer ses missions précédentes et actuelles, en fournissant suffisamment de détails pour décrire la nature des responsabilités de chaque emploi. Des informations plus détaillées peuvent être incluses dans le CV.

### Expérience en matière de gestion des risques

Le registre des projets de gestion des risques du candidat sera vérifié afin de s'assurer qu'il dispose du nombre d'heures requis en matière de gestion des risques.

### Évaluation des demandes de certification

Le Service de certification évaluera chaque demande afin de valider l'éligibilité du candidat à la certification. Le candidat dont la demande est examinée en sera informé par écrit et disposera d'un délai raisonnable pour fournir tout document supplémentaire si nécessaire. Si un candidat ne répond pas dans le délai imparti ou ne fournit pas les documents requis dans le délai imparti, le service de certification validera la demande sur la base des informations initiales fournies, ce qui peut éventuellement conduire à la rétrogradation du candidat à un titre inférieur.

### Refus de la demande de certification

PECB peut refuser la demande de certification si le candidat :

- Falsifie la demande
- Enfreint les procédures d'examen
- Enfreint le code d'éthique de PECB
- Échoue à l'examen

Pour des informations plus détaillées, reportez-vous à la section **Plainte et appel**.

Le paiement de la demande de certification n'est pas remboursable.

### Suspension de la certification

PECB peut suspendre temporairement la certification si le candidat ne satisfait pas aux exigences de PECB. D'autres raisons peuvent justifier la suspension de la certification :

- PECB reçoit des plaintes excessives ou sérieuses de la part des parties intéressées (la suspension sera appliquée jusqu'à ce que l'enquête soit terminée).
- Les logos de PECB ou des organismes d'accréditation sont délibérément utilisés de manière abusive.
- Le candidat ne corrige pas l'usage abusif d'une marque de certification dans le délai déterminé par PECB.
- La personne certifiée a volontairement demandé une suspension.
- Toute autre condition jugée appropriée pour la suspension de la certification.

## Révocation de la certification

PECB peut révoquer (c'est-à-dire retirer) la certification si le candidat ne satisfait pas aux exigences de PECB. Le candidat n'est alors plus autorisé à se présenter comme un professionnel certifié par PECB. D'autres raisons de révocation de la certification peuvent être invoquées si le candidat :

- Enfreint le code d'éthique de PECB
- Fait une fausse déclaration et fournit de fausses informations sur la portée du certificat
- Enfreint toute autre règle de PECB

## Mise à niveau des titres de compétences

Les professionnels peuvent demander à passer à une certification supérieure dès qu'ils peuvent démontrer qu'ils remplissent les conditions requises.

Pour faire une demande de mise à niveau, les candidats doivent se connecter à leur compte PECB, visiter l'onglet **Mes certifications** et cliquer sur le lien **Mise à niveau**. Les frais de demande de mise à niveau sont de 100 \$ US.

## Déclassement des titres de compétences

Une certification PECB peut être déclassée à un titre inférieur pour les raisons suivantes :

- Les FAM n'ont pas été payés.
- Les heures de FPC n'ont pas été soumises.
- Un nombre insuffisant d'heures de FPC a été soumis.
- La preuve des heures de FPC n'a pas été soumise sur demande.

**Note :** Les professionnels certifiés par PECB qui détiennent des certifications Lead et qui ne fournissent pas de preuves des exigences de maintien de la certification verront leurs titres déclassés. D'autre part, les détenteurs de certifications Master qui ne soumettent pas les FPC et ne paient pas les FAM verront leurs certifications révoquées.

## Autres statuts

En plus d'être active, suspendue ou révoquée, une certification peut être retirée volontairement. Pour plus d'informations sur ces statuts et sur le statut de cessation permanente, ainsi que sur la manière de les appliquer, veuillez consulter la page [État de la certification](#).

## SECTION V : POLITIQUES GÉNÉRALES DE PECB

---

### Code de déontologie de PECB

L'adhésion au code d'éthique de PECB est un engagement volontaire. Il est important que les professionnels certifiés par PECB non seulement adhèrent aux principes de ce Code, mais aussi qu'ils encouragent et soutiennent les autres à faire de même. Plus d'informations sont disponibles [ici](#).

### Autres examens et certifications

PECB accepte les certifications et les examens d'autres organismes de certification accrédités et reconnus. PECB évaluera les demandes par le biais de son processus d'équivalence pour décider si la ou les certifications ou examens respectifs peuvent être acceptés comme équivalents à la certification PECB respective (par exemple, la certification ISO/IEC 27001 Lead Auditor).

### Non-discrimination et aménagements spéciaux

Toutes les candidatures seront évaluées objectivement, sans considération d'âge, de sexe, de race, de religion, de nationalité ou d'état civil du candidat.

Afin de garantir l'égalité des chances à toutes les personnes qualifiées, PECB fera des aménagements raisonnables pour les candidats, le cas échéant. Si un candidat a besoin d'aménagements spéciaux en raison d'un handicap ou d'une condition physique particulière, il devrait en informer le partenaire/distributeur afin que celui-ci puisse prendre les dispositions nécessaires. Toute information fournie par les candidats concernant leur handicap/besoin sera traitée de manière strictement confidentielle.

Cliquez [ici](#) pour télécharger le Formulaire de demande d'aménagements spéciaux pour les candidats présentant un handicap.

### Plainte et appel

Toute plainte doit être formulée au plus tard 30 jours après la réception de la décision de certification. PECB fournira une réponse écrite au candidat dans les 30 jours ouvrables suivant la réception de la plainte. Si la réponse de PECB n'est pas satisfaisante, le candidat a le droit de faire appel. Pour plus d'informations, consultez la Politique de plainte et d'appel de PECB [ici](#).

(1) Selon le Americans with Disabilities Act (ADA), le terme « aménagement raisonnable » peut inclure : (A) rendre les installations existantes utilisées par les employés facilement accessibles et utilisables par les individus souffrant d'invalidité ; et (B) la restructuration des tâches, les horaires de travail à temps partiel ou modifiés, la réaffectation à un poste vacant, l'acquisition ou la modification d'équipement ou d'appareils, l'adaptation ou la modification appropriée des examens, du matériel de formation ou des politiques, la fourniture de personnel qualifié.

(2) ADA Amendments Act of 2008 (P.L. 110-325) Sec. 12189. Examens et cours. [Section 309] : Toute personne qui propose des examens ou des cours liés à des demandes, des licences, des certifications ou des habilitations pour l'enseignement secondaire ou post-secondaire, à des fins professionnelles ou commerciales, doit proposer ces examens ou ces cours dans un lieu et d'une manière accessibles aux personnes handicapées ou proposer d'autres arrangements accessibles à ces personnes.



**Adresse :**

Siège social  
6683, rue Jean-Talon Est,  
bureau 336 Montréal  
H1S 0A5, QC,  
CANADA

**Tel./Fax.**

T: +1-844-426-7322  
F : +1-844-329-7322

**Centre d'aide de PECB**

Visitez notre [Centre d'aide](#) pour parcourir la Foire aux questions (FAQ), consulter les manuels d'utilisation du site Web et des applications de PECB, lire les documents relatifs aux processus de PECB ou nous contacter via le système de suivi en ligne du centre d'aide. Visitez le Centre d'aide ici : [www.pecb.com/help](http://www.pecb.com/help)

**E-mails**

Examen : [examination.team@pecb.com](mailto:examination.team@pecb.com)  
Certification : [certification.team@pecb.com](mailto:certification.team@pecb.com)  
Service client : [customer@pecb.com](mailto:customer@pecb.com)

Copyright © 2023 PECB. La reproduction ou le stockage sous quelque forme que ce soit et à quelque fin que ce soit n'est pas autorisé sans une autorisation écrite préalable de PECB.

[www.pecb.com](http://www.pecb.com)