When Recognition Matters

CERTIFIED ISO/IEC 27034

LEAD APPLICATION SECURITY IMPLEMENTER

MAÎTRISER LA MISE EN ŒUVRE DES PROCESSUS, DES ACTIVITÉS ET DES TECHNIQUES DE SÉCURITÉ DE LA SÉCURITÉ DES APPLICATIONS (SA) À TRAVERS L'ORGANISATION, CONFORMÉMENT À LA NORME INTERNATIONALE ISO/IEC 27034 – SÉCURITÉ DES APPLICATIONS

RÉSUMÉ

Ce cours intensif de cinq jours permet aux participants de comprendre les principes spécifiques et les concepts proposés par la norme ISO/IEC 27034 pour la sécurité des applications et comprendre de quelle façon ils peuvent être mis en œuvre étape par étape, pour aider les organisations à développer, acquérir, mettre en œuvre et utiliser des applications fiables, en fonction du contexte spécifique de l'entreprise, avec des coûts acceptables. Plus précisément, le cadre de la norme ISO/IEC 27034 propose des composants et des processus afin de fournir des preuves vérifiables qu'une application a atteint et maintenu un niveau ciblé de confiance tel que défini par l'organisation. La responsabilité de l'ISO/IEC 27034 Lead Implementer est d'assister les organisations dans la mise en œuvre des éléments du cadre 27034 et les guider dans l'intégration des contrôles de la sécurité des applications (CSA) de manière parfaite à travers tout le cycle de vie de leurs applications. La sécurité des applications s'applique au logiciel d'une application et à d'autres composants et à ses facteurs de contribution qui ont un impact sur sa sécurité, tel que le contexte technologique, le contexte règlementaire, le contexte de son entreprise, ses spécifications, la sensibilité de ses données et les processus et les acteurs soutenant son cycle de vie entier. Ce cadre peut s'appliquer également à tous les types et les tailles des organisations (par exemple les entreprises commerciales, les agences gouvernementales, les organisations à but non lucratif qui utilisent les applications, mais aussi aux vendeurs de petite, de moyenne et de grande taille qui développent des logiciels, des applications et des services) exposées à des risques associés aux applications.

JOUR 1

Aperçu de la Sécurité des applications et des concepts, définis par la norme ISO/IEC 27034

- Introduction à la norme ISO/IEC 27034 et sa vision globale
- Principes fondamentaux de la sécurité de l'information
- Aperçu général, concepts, principes, définitions, domaine d'application, composants, processus et acteurs impliqués dans la SA
- Concepts implicites intégrés
- Présentation de la série 27034 :
  - ISO/IEC 27034-1 : Aperçu général & concepts
  - ISO/IEC 27034-2 : La sécurité des applications dans une organisation
  - ISO/IEC 27034-3 : La sécurité des applications dans un projet
  - ISO/IEC 27034-4 : Validation, vérification et certification de la SA
  - ISO/IEC 27034-5 : Exigences de la structure de la SA
  - ISO/IEC 27034-5-1 : Schémas XML
  - ISO/IEC 27034-6 : Exemples et études de cas

JOUR 2

Mise en œuvre de la Sécurité des applications selon l'ISO/IEC 27034

- La sécurité dans un projet des applications
  - Le processus de gestion de la sécurité des applications
  - Fourniture et opération d'une application
  - Maintien du niveau actuel de confiance au niveau ciblé de confiance
  - Développement de la validation de la SA

JOUR 3

Mise en œuvre de la SA conformément à la norme ISO/IEC 27034 (suite)

- La SA au niveau organisationnel
  - Objectifs de la SA pour une organisation
  - Le Organization Normative Framework (ONF) (cadre normatif de l'organisation)
  - Le comité ONF
  - le processus de gestion de l'ONF
  - Intégration des éléments ISO/IEC 20034 au sein des processus existants de l'organisation
  - conception, validation, mise en œuvre, vérification, opération et évolution des contrôles de la sécurité des applications
  - Les bibliothèques des CSA
  - La mesure de la traçabilité de la SA
  - Rédaction d'un processus de certification

Lignes directrices de sécurité pour les organisations et les applications spécifiques

- Etudes de cas
  - Exemples de mise en œuvre 27034 pour les petites et les grandes organisations
  - De quelle façon la norme 27034 aide la résolution des exigences réglementaires conflictuelles pour une application
  - Elaboration des CSA
  - Acquisition des CSA

JOUR 4

Validation et certification de la SA

- L'objectif de l'audit interne de la SA
  - Réduire le coût d'un audit
  - Soyez sûr que les preuves requises sont prêtes
- Aperçu du processus de validation et de certification de la SA selon 27034
  - De quelle façon aider une organisation à obtenir la certification
  - De quelle façon aider un projet d'application à obtenir la certification

Protocoles et structure des données de CSA conformément à la norme ISO/IEC 27034

- Un langage formel gratuit pour la communication des CSA
- Schémas proposés XML de la norme ISO/IEC 27034
  - Structure des données, descriptions, représentation graphique
  - ISO/IEC 27034 SA revue finale

JOUR 5

Examen de certification

QUI EST CONCERNÉ ?

- Les gestionnaires des SI, les administrateurs, les gestionnaires de développement de logiciels et les propriétaires d'applications, qui souhaitent évaluer les coûts pour mettre en œuvre et maintenir la sécurité des applications contre les risques et la valeur que celle-ci représente pour l'organisme
- Les membres d'une équipe des approvisionnements ou des opérations, tels que les architectes, les analystes-programmeurs, les testeurs, les administrateurs de systèmes et le personnel technique, souhaitant intervenir dans la mise en œuvre de la sécurité applicative
- Les distributeurs et les fournisseurs souhaitant préparer et/ou répondre aux appels d'offres incluant les exigences de CSA et le niveau de confiance visé
- Les auditeurs désirant comprendre les processus de mise en œuvre de la sécurité d'une application selon la norme ISO/IEC 27034

OBJECTIFS DU COURS

- Comprendre la mise en œuvre de la Sécurité des applications selon l'ISO/IEC 27034
- Acquérir une compréhension globale des concepts, des approches, des standards, des méthodes et des techniques requises pour une gestion efficace de la Sécurité des applications
- Comprendre la relation entre les composants de la sécurité des applications y compris la gestion du risque, les contrôles et la conformité aux exigences des différentes parties prenantes d'une organisation
- Acquérir l'expertise nécessaire pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien de la sécurité des applications définies dans l'ISO/IEC 27034
- Acquérir l'expertise nécessaire pour gérer une équipe de mise en œuvre de l'ISO/IEC 27034
- Développer les connaissances et les compétences requises pour conseiller une organisation pour les meilleures pratiques du management de la sécurité des applications
- Améliorer la capacité d'analyse et de prise de décision dans le contexte de la sécurité des applications

EXAMEN

L'examen "PECB Certified ISO/IEC 27034 Lead Application Security Implementer" répond entièrement aux exigences du programme d'examen et de certification de PECB. L'examen couvre les domaines de compétence suivants :

1 **Domaine 1 : Principes fondamentaux et concepts de la sécurité des applications**

Objectif principal : S'assurer que le candidat ISO/IEC 27034 AS Lead Implementer est en mesure de comprendre, interpréter et illustrer les concepts principaux de la sécurité des applications liés à la mise en oeuvre de la SA dans une organisation et la mise en œuvre de la SA dans un projet d'application de la norme ISO/IEC 27034, incluant le domaine d'application de la SA, de quelle façon la SA est alignée à la norme ISO/IEC 27001, ses avantages et ses limites

2 **Domaine 2 : Les meilleures pratiques et les contrôles de la sécurité des applications**

Objectif principal : S'assurer que le candidat ISO/IEC 27034 AS Lead Implementer est en mesure de comprendre, interpréter et donner des conseils concernant la mise en œuvre et la gestion des meilleures pratiques des contrôles de la sécurité des applications pour soutenir les autres normes et des meilleures pratiques tel que ISO/IEC 27002, ISO/IEC 15288, Common Criteria, CMMI, PMI, ITIL, COBIT et OWASP

3 **Domaine 3 : Préparation d'un projet de la SA conforme à la norme ISO/IEC 27034**

Objectif principal : S'assurer que le candidat ISO/IEC 27034 AS Lead Implementer est en mesure de planifier et préparer de manière appropriée la mise en œuvre d'un projet organisationnel de la SA ou un projet d'application dans le contexte de la norme ISO/IEC 27034

4 **Domaine 4 : Mise en œuvre de la SA conforme à la norme ISO/IEC 27034**

Objectif principal : S'assurer que le candidat ISO/IEC 27034 AS Lead Implementer est en mesure de mettre en œuvre des processus et les contrôles de sécurité de la SA dans un projet organisationnel de la SA ou un projet d'application dans le contexte de la norme ISO/IEC 27034

5 **Domaine 5 : Evaluation de la performance, surveillance, et mesure du projet de la SA selon l'ISO/IEC 27034**

Objectif principal : S'assurer que le candidat ISO/IEC 27034 AS Lead Implementer est en mesure d'évaluer, surveiller et mesurer la performance d'un projet organisationnel de la SA ou d'un projet d'application dans le contexte des besoins de la SA de l'organisation selon la norme ISO/IEC 27034

6 **Domaine 6 : Amélioration continue du projet de la SA selon l'ISO/IEC 27034**

Objectif principal : S'assurer que le candidat ISO/IEC 27034 AS Lead Implementer est en mesure de donner des conseils pour l'amélioration continue du projet organisationnel de la SA ou du projet d'application dans le contexte de l'ISO/IEC 27034

7 **Domaine 7 : Préparation d'un projet d'application ou d'une organisation à l'audit de certification ISO/IEC 27034**

Objectif principal : S'assurer que le candidat ISO/IEC 27034 AS Lead Implementer est en mesure de préparer et assister une organisation pour la certification vis-à-vis de la norme ISO/IEC 27034. Ces certifications pourraient de faire au niveau organisationnel, ou pour des applications spécifiques.

- L'examen "PECB Certified ISO/IEC 27034 Lead Application Security Implementer" est disponible en plusieurs langues dont l'anglais, le français, l'espagnol et le portugais
- Durée : 3 heures
- Pour plus d'informations concernant l'examen, veuillez visiter : www.pecb.com

CERTIFICATION

- Après avoir réussi l'examen, les participants peuvent demander la qualification de Certified ISO/IEC 27034 Application Security Provisional Implementer, Certified ISO/IEC 27034 Application Security Implementer ou Certified ISO/IEC 27034 Application Security Lead Implementer, en fonction de leur niveau d'expérience
- Un certificat est délivré aux participants qui auront réussi l'examen et qui remplissent les exigences relatives au niveau de qualification choisi :

Certification	Examen	Expérience professionnelle	Expérience audit des TSTI	Expérience projet des TSTI	Autres exigences
PECB Certified ISO/IEC 27034 Provisional Application Security Implementer	PECB Certified ISO/IEC 27034 Lead Application Security Implementer Exam	Aucune	Aucune	Aucune	Signer le code d'éthique PECB
PECB Certified ISO/IEC 27034 Application Security Implementer	PECB Certified ISO/IEC 27034 Lead Application Security Implementer Exam	Deux années Dont un an d'expérience dans les techniques de la sécurité des TI	Aucune	Activités projet totalisant 200 heures	Signer le code d'éthique PECB
PECB Certified ISO/IEC Lead Application Security Implementer	PECB Certified ISO/IEC 27034 Lead Application Security Implementer Exam	Cinq années Dont deux ans d'expérience dans les techniques de la sécurité des TI	Aucune	Activités projet totalisant 300 heures	Signer le code d'éthique PECB

INFORMATIONS GÉNÉRALES

- Les frais de certification sont inclus dans le prix de l'examen
- Un manuel contenant plus de 450 pages d'information et d'exemples pratiques est fourni aux participants
- Un certificat de participation de 31 crédits CPD (Continuing Professional Development) est délivré aux participants
- En cas d'échec, les participants peuvent repasser l'examen gratuitement sous certaines conditions
- Les participants devraient avoir accès à une copie légale de la norme internationale ISO/IEC 27034 – Sécurité des applications – Partie 1 : Aperçu général et concepts, pour consultation en classe