Certifications PECB

Référentiels de compétences et de certification

Identifiants	Intitulés
3717	Certification PECB – Analyse forensique
3675	Certification PECB - Protection des données personnelles
3209	Certification PECB - Fondamentaux de la continuité d'activité
3202	Certification PECB - Audit du système de management de la continuité d'activité (SMCA)
3198	Certification PECB - Mise en œuvre du système de management de la continuité d'activité (SMCA)
3211	Certification PECB - Sécurité de l'information
3204	Certification PECB - Fondamentaux du management de la sécurité de l'information
3203	Certification PECB - Audit du système de management de la sécurité de l'information
3177	Certification PECB - Mise en œuvre du système de management de la sécurité de l'information
1804	Certification PECB – Fondamentaux de la sécurité des applications
1802	Certification PECB - Audit de la sécurité des applications
1803	Certification PECB - Mise en œuvre de la sécurité des applications
3212	Certification PECB - Management du risque
3716	Certification PECB - Conception et mise en œuvre des tests d'intrusion

PECB
25 Place de la Madeleine
75008 PARIS

Contact : Eric LACHAPELLE
Directeur général
eric.lachapelle@pecb.com
09 70 46 33 90

Juillet 2018

Analyse forensique Certification PECB Lead Forensics Examiner		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Analyser le système d'information d'une organisation publique ou privée en vue de collecter les traces d'une attaque informatique (virus, intrusion, etc.).	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - Une note méthodologique d'analyse d'incident. - Le recensement des traces de l'attaque informatique et des dommages causés. - La caractérisation des preuves numériques en vue d'une action en justice. - Un rapport d'investigation. L'évaluation est individuelle.	• Précision dans la caractérisation de l'incident • Qualité de la méthodologie utilisée pour l'analyser
Exploiter les traces d'une attaque informatique afin de reconstituer le parcours de l'attaquant, d'identifier les informations exfiltrées et de comprendre les vulnérabilités exploitées.		• Logique de la reconstitution du parcours de l'attaquant • Exhaustivité dans l'identification des informations exfiltrées • Précision dans l'explicitation des vulnérabilités
Appliquer des techniques et protocoles d'investigations numériques respectant les procédures légales, en vue de produire des preuves numériques dans le cadre d'une action en justice.		• Maîtrise des protocoles d'investigation • Maîtrise des procédures légales • Qualité des preuves numériques produites
Planifier et exécuter un plan de réponse à un incident de type cyber-attaque, afin d'assurer la protection des preuves numériques.		• Cohérence du plan proposé en réponse à l'incident • Robustesse de la protection des preuves
Rédiger le rapport enregistrant les étapes d'une investigation numérique, afin de garantir que les preuves sont issues de manière irrévocable d'une information numérique.		• Conformité du rapport d'investigation aux normes et référentiels en vigueur en matière de cyber sécurité • Clarté de sa rédaction • Précision des réponses aux questions du jury

Protection des données personnelles Certification PECB Délégué à la protection des données		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Réaliser une analyse d'impact relative à la protection des données collectées par une entreprise, une collectivité ou une association, en vue de concevoir les mesures de protection appropriées.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - Une analyse d'impact sur la vie privée réalisée sur les données collectées par une organisation. - Une note de conseil destinée à l'organisation en vue d l'application du RGPD par celle-ci. - L'identification des indicateurs de qualité en matière de protection des données. - La structure du registre des activités et des traitements des données sensibles. L'évaluation est individuelle.	• Qualité et exhaustivité du repérage des données sensibles • Précision de l'analyse d'impact sur la vie privée
Décrire l'objectif, le contenu et la corrélation entre le RGPD et les autres lois en matière de protection des données en vue d'aider une entreprise, une collectivité ou une association à se mettre en conformité avec la réglementation.		• Clarté de la note de conseil rédigée à l'intention de l'organisation concernée • Maîtrise des attendus du RGPD et les lois en vigueur en matière de protection des données personnelles
Animer une équipe de personnes relais au sein de l'organisation, afin d'assurer la mise en place des bonnes pratiques et règlements du RGPD.		• Cohérence de la note de conseil en matière de répartition des tâches au sein de l'organisation • Capacité du dispositif à mobiliser les collaborateurs et acteurs externes
Identifier les indicateurs de qualité et de progression en matière de protection des données personnelles par une organisation, afin d'améliorer le dispositif mis en place par celle-ci dans le cadre du RGPD.		• Pertinences des indicateurs au regard de l'organisation mise en place pour la protection des données • Conformité avec les attendus du RGPD
Tenir au sein de l'organisation un registre des activités et des traitements des données sensibles conforme au RGPD, destiné au contrôle de sa mise en œuvre et à la bonne gestion des relations avec les publics concernés.		• Efficacité opérationnelle du registre proposé • Conformité avec les attendus du RGPD et de la CNIL

Fondamentaux de la continuité d'activité Certification PECB ISO 22301 Foundation		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Analyser l'impact métier d'une interruption d'activité de l'entreprise en vue de déterminer les seuils financiers, légaux, techniques et humains au-delà desquels sa pérennité serait compromise.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - Une analyse de l'impact métier d'une rupture d'activité. - Le recensement des moyens nécessaires aux activités critiques. - L'identification des menaces sur le personnel et les installations. - Une proposition de PCA assortie des procédures de test et de maintenance. L'évaluation est individuelle.	• Précision de l'analyse d'impact • Précision et justification des seuils identifiés
Recenser et chiffrer les moyens nécessaires au redémarrage des activités « critiques » en cas d'indisponibilité du site, des installations ou du personnel, afin de prévenir les conséquences d'une interruption d'activité de l'entreprise.		• Exhaustivité du repérage des moyens nécessaires aux activités critiques • Qualité des justifications apportées et du chiffrage des coûts associés
Caractériser les menaces identifiées sur l'informatique, les locaux et les hommes afin de concevoir des mesures d'atténuation appropriées.		• Exhaustivité de la liste des menaces identifiées • Cohérence des parades et mesures d'atténuation proposées
Elaborer un plan global de continuité de l'activité (PCA) conforme à la norme ISO 22301, en vue d'impliquer l'ensemble des personnels de l'entreprise dans la prévention des menaces et des ruptures d'activité.		• Cohérence du PCA au regard de l'analyse des menaces • Conformité à la norme ISO 22301
Tester un PCA par un ensemble d'exercices impliquant les acteurs internes et externes à l'entreprise, afin de valider les procédures et parades aux menaces prévues par celui-ci.		• Efficacité du programme de test au regard des objectifs du PCA • Niveau d'implication des acteurs internes et externes à l'entreprise
Créer des procédures de mise à jour et des outils de reporting, afin d'assurer la maintenance du PCA et l'amélioration continue de la gestion des crises.		• Compatibilité des procédures et outils de reporting avec la gestion des crises

Audit du système de management de la continuité d'activité (SMCA) Certification PECB ISO 22301 Lead Auditor		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Décrire les éléments et le fonctionnement d'un système de management de la continuité d'activité (SMCA) à l'intention des responsables de l'entreprise, en vue de les impliquer dans l'élaboration d'un programme d'audit de celui-ci.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore trois documents remis au jury et soutenus oralement : - Le schéma d'un programme d'audit du SMCA adapté au cas étudié. - Un dispositif d'encadrement de l'équipe d'auditeurs. - Un schéma du rapport d'audit incluant des propositions d'activités de suivi du système. L'évaluation est individuelle.	• Maîtrise des éléments et du fonctionnement d'un système de management de la continuité d'activité • Aptitude à les exposer clairement
Préparer et planifier un audit du SMCA conformément à la norme ISO 22301, afin d'assurer la fiabilité des résultats de celui-ci.		• Cohérence du programme d'audit proposé • Conformité de celui-ci à la norme ISO 22301
Diriger un audit SMCA conformément à la norme ISO 19011, afin d'assurer un encadrement de l'équipe d'auditeurs adapté aux objectifs.		• Cohérence du dispositif d'encadrement de l'équipe d'auditeurs • Conformité de celui-ci à la norme ISO 19011
Clôturer un audit du SMCA, en vue d'assurer un suivi conforme à la norme ISO 22301.		• Pertinence des activités de suivi proposées • Conformité à la norme ISO 22301
Rédiger un rapport d'audit du SMCA, en vue de conseiller une entreprise sur les meilleures pratiques en matière de continuité d'activité.		• Qualité de rédaction du rapport • Pertinence des propositions et cohérence de leurs justifications • Efficacité en termes de prise de décisions et de gestion des crises

Mise en œuvre du système de management de la continuité d'activité (SMCA) Certification PECB ISO 22301 Lead Implementer		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Décrire les concepts principaux de la continuité d'activité à l'intention des responsables de l'entreprise, en vue de les impliquer dans la mise en œuvre d'un système de management de la continuité d'activité (SMCA) approprié.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - Le schéma d'un SMCA adapté au cas étudié. - Le schéma de planification de la mise en œuvre du SMCA. - Les indicateurs de performance du système. - Une série de propositions relatives à la continuité d'activité à l'intention des responsables de l'entreprise. L'évaluation est individuelle.	• Maîtrise des concepts principaux de la continuité d'activité • Aptitude à les exposer clairement
Elaborer un SMCA conforme à la norme ISO 22031, afin d'optimiser la prévention des menaces et des ruptures d'activité.		• Cohérence du SMCA proposé • Conformité à la norme ISO 22031
Planifier et coordonner la mise en œuvre du SMCA au sein de l'entreprise en tenant compte du nécessaire accompagnement des acteurs, en vue d'assurer son efficacité sur le long terme.		• Cohérence de la planification • Qualité du plan d'accompagnement
Evaluer et mesurer en continu la performance du SMCA au moyen d'indicateurs pertinents, en vue d'optimiser celui-ci grâce à une exacte identification des points d'amélioration.		• Pertinence des indicateurs retenus • Justification en termes d'amélioration continue
Conseiller une entreprise dans le contexte de la continuité d'activité, afin d'améliorer ses capacités d'analyse et de prise de décisions.		• Qualité et cohérence des propositions • Efficacité en termes de prise de décisions et de gestion des crises

Sécurité de l'information Certification PECB ISO 27005 Risk Manager		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Décrire les concepts et les processus fondamentaux de la gestion des risques en matière de sécurité de l'information à l'intention des responsables de l'entreprise, en vue de les impliquer dans la mise en œuvre d'un cadre de prévention.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - Le schéma d'un programme de gestion des risques adapté au cas étudié. - Le schéma de mise en place des processus de gestion des risques liés à la sécurité de l'information. - Les indicateurs de performance du système. - Une série de propositions relatives à la sécurité de l'information à l'intention des responsables de l'entreprise. L'évaluation est individuelle.	• Maîtrise des concepts et processus fondamentaux de la sécurité de l'information • Aptitude à les exposer clairement
Elaborer un programme de gestion des risques liés à la sécurité de l'information conforme à la norme ISO 27005, afin d'optimiser la prévention des menaces d'intrusions dans les systèmes et de destruction des données.		• Cohérence du programme de gestion des risques proposé • Conformité à la norme ISO 27005
Coordonner la mise en place des processus de sécurité de l'information en tenant compte du nécessaire accompagnement des acteurs, en vue d'assurer leur efficacité sur le long terme.		• Cohérence de la mise en œuvre des processus de gestion des risques avec les concepts de sécurité de l'information • Qualité du plan d'accompagnement
Evaluer et mesurer en continu la performance du programme de gestion des risques au moyen d'indicateurs pertinents, en vue d'optimiser celui-ci grâce à une exacte identification des points d'amélioration.		• Pertinence des indicateurs retenus • Justification en termes d'amélioration continue
Conseiller une entreprise sur les meilleures pratiques en matière de sécurité de l'information, afin de renforcer l'efficacité du programme de gestion des risques.		• Qualité et cohérence des propositions • Efficacité en termes de prise de décisions et de gestion des crises

Fondamentaux du management de la sécurité de l'information Certification PECB ISO/IEC 27001 Foundation		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Analyser le système d'information de l'entreprise, afin de repérer ses points de faiblesse au regard des menaces d'intrusion et de perte de données.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore cinq documents remis au jury et soutenus oralement : - L'analyse du système d'information. - Les principaux éléments du cahier des charges et le budget de sécurisation du système d'information. - Des propositions de parades appropriées. - Le schéma général de sécurité de l'information. - Le schéma d'un plan de formation des personnels. L'évaluation est individuelle.	• Précision de l'analyse • Exhaustivité du recensement des menaces
Etablir le cahier des charges de la sécurisation du système d'information conformément à la norme ISO/IEC 27001, afin de répondre aux impératifs de la protection de l'activité dans le cadre du budget disponible.		• Cohérence du cahier des charges avec les menaces identifiées • Précision du chiffrage • Conformité à la norme ISO/IEC 27001
Elaborer les parades adaptées aux menaces d'intrusion et de pertes de données conformément au cahier des charges et au budget imparti.		• Pertinence des parades proposées • Justification par l'analyse des coûts
Etablir le schéma général de sécurité de l'information à l'intention des responsables de l'entreprise, en vue de préparer un plan de communication vers l'ensemble du personnel.		• Clarté du schéma général de sécurité de l'information • Qualité du plan de communication
Concevoir un plan de formation des personnels aux bonnes pratiques en matière de sécurité de l'information, afin d'assurer leur implication à tous les niveaux de l'entreprise.		• Précision dans l'exposé des bonnes pratiques de sécurité de l'information • Cohérence du plan de formation

Audit du système de management de la sécurité de l'information Certification PECB ISO/IEC 27001 Lead Auditor		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Décrire les éléments et le fonctionnement d'un système de management de la sécurité de l'information à l'intention des responsables de l'entreprise, en vue de les impliquer dans l'élaboration d'un programme d'audit de celui-ci.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore trois documents remis au jury et soutenus oralement : - Le schéma d'un programme d'audit du système de management de la sécurité de l'information adapté au cas étudié. - Un dispositif d'encadrement de l'équipe d'auditeurs. - Un schéma du rapport d'audit incluant des propositions d'activités de suivi du système. L'évaluation est individuelle.	• Maîtrise des éléments et du fonctionnement d'un système de management de la sécurité de l'information • Aptitude à les exposer clairement
Préparer et planifier un audit du système de management de la sécurité de l'information conformément à la norme ISO/IEC 27001, afin d'assurer la fiabilité des résultats de celui-ci.		• Cohérence du programme d'audit proposé • Conformité de celui-ci à la norme ISO/IEC 27001
Diriger un audit du système de management de la sécurité de l'information conformément à la norme ISO 19011, afin d'assurer un encadrement de l'équipe d'auditeurs adapté aux objectifs.		• Cohérence du dispositif d'encadrement de l'équipe d'auditeurs • Conformité de celui-ci à la norme ISO 19011
Clôturer un audit du système de management de la sécurité de l'information, en vue d'assurer des activités de suivi conformes à la norme ISO/IEC 27001.		• Pertinence des activités de suivi proposées • Conformité de celles-ci à la norme ISO/IEC 27001
Rédiger un rapport d'audit du système de management de la sécurité de l'information, en vue de conseiller une entreprise sur les meilleures pratiques en matière de sécurité de l'information et de renforcer ainsi l'efficacité du système de management de la sécurité de l'information.		• Qualité de rédaction du rapport • Pertinence des propositions et cohérence de leurs justifications • Efficacité en termes de prise de décisions et de gestion des crises

Mise en œuvre du système de management de la sécurité de l'information Certification PECB ISO/IEC 27001 Lead Implementer		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Décrire les éléments et le fonctionnement d'un système de management de la sécurité de l'information à l'intention des responsables de l'entreprise, en vue de les impliquer dans la mise en œuvre de celui-ci.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - Le schéma d'un système de management de la sécurité de l'information adapté au cas étudié. - Le schéma de mise en place du système de management de la sécurité de l'information. - Les indicateurs de performance du système. - Une série de propositions relatives à la sécurité de l'information à l'intention des responsables de l'entreprise. L'évaluation est individuelle.	• Maîtrise des éléments et du fonctionnement d'un système de management de la sécurité de l'information • Aptitude à les exposer clairement
Elaborer un système de management de la sécurité de l'information conforme à la norme ISO/IEC 27001, afin d'optimiser la prévention des menaces d'intrusions dans le système d'information de l'entreprise.		• Cohérence du système de management de la sécurité de l'information proposé • Conformité à la norme ISO/IEC 27001
Coordonner la mise en place d'un système de management de la sécurité de l'information en tenant compte du nécessaire accompagnement des acteurs, en vue d'assurer son efficacité sur le long terme.		• Cohérence de la mise en place du système de management de la sécurité de l'information avec les concepts fondamentaux • Qualité du plan d'accompagnement
Evaluer et mesurer en continu la performance du système de management de la sécurité de l'information au moyen d'indicateurs pertinents, en vue d'optimiser celui-ci grâce à une exacte identification des points d'amélioration.		• Pertinence des indicateurs retenus • Justification en termes d'amélioration continue
Conseiller une entreprise sur les meilleures pratiques en matière de sécurité de l'information, afin de renforcer l'efficacité du système de management de la sécurité de l'information.		• Qualité et cohérence des propositions de conseil • Efficacité en termes de prise de décisions et de gestion des crises

Fondamentaux de la sécurité des applications Certification PECB ISO 27034 Foundation		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Analyser le système d'information de l'entreprise et les procédures d'accès aux applications, afin de repérer les failles de sécurité représentant une menace pour l'activité.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore cinq documents remis au jury et soutenus oralement : - L'analyse du système d'information et des procédures d'accès aux applications. - Les principaux éléments du cahier des charges et le budget de sécurisation des applications - Des propositions de parades adaptées - Le schéma général de sécurité des applications - Le schéma d'un plan de formation des personnels L'évaluation est individuelle.	• Précision de l'analyse • Exactitude dans l'identification des failles de sécurité
Etablir le cahier des charges de la sécurité des applications, conformément à la norme ISO/IEC 27034, afin de répondre aux impératifs de la protection de l'activité dans le cadre du budget disponible.		• Cohérence du cahier des charges avec les menaces identifiées • Précision du chiffrage • Conformité à la norme ISO/IEC 27034
Elaborer les parades adaptées aux menaces sur le système applicatif, conformément au cahier des charges et au budget imparti, afin d'assurer la continuité de l'activité et le maintien du niveau de confiance.		• Pertinence des parades proposées • Justification par l'analyse des coûts
Etablir le schéma général de sécurité des applications à l'intention des responsables de l'entreprise, en vue de préparer un plan de communication vers l'ensemble du personnel.		• Clarté du schéma général • Qualité du plan de communication proposé
Concevoir un plan de formation des personnels aux bonnes pratiques en matière de sécurité des applications, afin d'assurer leur implication à tous les niveaux de l'entreprise.		• Précision dans l'exposé des bonnes pratiques de sécurité • Cohérence du plan de formation

Audit de la sécurité des applications Certification PECB ISO/IEC 27034 Lead Auditor		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Décrire les éléments et le fonctionnement d'un système de management de la sécurité des applications à l'intention des responsables de l'entreprise, en vue de les impliquer dans l'élaboration d'un programme d'audit de celui-ci.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore trois documents remis au jury et soutenus oralement : - Le schéma d'un programme d'audit de la sécurité des applications adapté au cas étudié. - Un dispositif d'encadrement de l'équipe d'auditeurs. - Un schéma du rapport d'audit et la formulation de conseils à l'entreprise en matière de sécurité des applications. L'évaluation est individuelle.	• Maîtrise des concepts, principes et bonnes pratiques de gestion de la sécurité applicative • Aptitude à les exposer clairement
Préparer et planifier un audit de la sécurité des applications, conformément à la norme ISO/IEC 27034, afin d'assurer la fiabilité des résultats de celui-ci.		• Cohérence du programme d'audit proposé • Conformité de celui-ci à la norme ISO/IEC 27034
Diriger un audit du système de management de la sécurité des applications, conformément à la norme ISO 19011, afin d'assurer un encadrement de l'équipe d'auditeurs adapté aux objectifs.		• Cohérence du dispositif d'encadrement de l'équipe d'auditeurs • Conformité de celui-ci à la norme ISO 19011
Clôturer un audit du système de management de la sécurité des applications, en vue d'assurer des activités de suivi conformes à la norme ISO/CEI 27034.		• Pertinence des activités de suivi proposées • Conformité à la norme ISO/IEC 27034
Rédiger un rapport d'audit de la sécurité des applications, en vue de conseiller une entreprise sur les meilleures pratiques de sécurité et de renforcer le niveau de confiance dans son système d'information.		• Qualité de rédaction du rapport • Pertinence des propositions et cohérence de leurs justifications • Efficacité en termes de prise de décisions et de gestion des crises

Mise en œuvre de la sécurité des applications Certification PECB ISO/IEC 27034 Lead Implementer		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Décrire les éléments et le fonctionnement d'un système de management de la sécurité des applications à l'intention des responsables de l'entreprise, en vue de les impliquer dans la mise en œuvre de celui-ci.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - Le schéma d'un système de management de la sécurité des applications adapté au cas étudié. - Les dispositifs de sécurité applicative à implémenter. - Les indicateurs de performance du système de sécurité applicative. - Une série de propositions relatives à la sécurité applicative à l'intention des responsables de l'entreprise. L'évaluation est individuelle.	• Maîtrise des concepts, principes et bonnes pratiques de gestion de la sécurité applicative • Aptitude à les exposer clairement
Elaborer les dispositifs de sécurité applicative adaptés au système d'information de l'entreprise, afin d'optimiser la prévention des menaces dans le cadre de la norme ISO/IEC 27034.		• Cohérence des dispositifs de sécurité applicative proposés • Conformité à la norme ISO/IEC 27034
Coordonner la mise en place d'un système de sécurité applicative en tenant compte du nécessaire accompagnement des acteurs, en vue d'assurer son efficacité sur le long terme.		• Cohérence de la mise en place du système de sécurité applicative avec les concepts fondamentaux • Qualité du plan d'accompagnement
Evaluer et mesurer en continu la performance des dispositifs de sécurité applicative au moyen d'indicateurs pertinents, en vue d'optimiser ceux-ci grâce à une exacte identification des points d'amélioration.		• Pertinence des indicateurs retenus • Justification en termes d'amélioration continue
Conseiller une entreprise sur les meilleures pratiques en matière de sécurité applicative, afin de renforcer son efficacité, ainsi que le niveau de confiance des utilisateurs dans le système d'information.		• Qualité et cohérence des propositions • Efficacité en termes de prise de décisions et de gestion des crises

Management du risque Certification PECB ISO 31000 Risk Manager		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Piloter les démarches d'évaluation des risques encourus par une entreprise, conformément à la norme ISO 31000, afin d'établir un recensement exhaustif des menaces sur l'activité de celle-ci.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - Le schéma de pilotage de l'évaluation des risques. - Les dispositifs de prévention à mettre en place et leur chiffrage. - Un plan global de communication à l'intention des personnels. - Une série d'indicateurs de suivi du plan de prévention des risques. L'évaluation est individuelle.	• Maîtrise des concepts, approches, normes, méthodes et techniques nécessaires pour gérer efficacement le risque • Conformité à la norme ISO 31000
Elaborer les parades et dispositifs de prévention adaptés aux menaces, en vue d'évaluer le coût global d'un système de prévention des risques.		• Cohérence des dispositifs de prévention proposés • Conformité à la norme ISO 31000
Concevoir et mettre en place le plan de prévention des risques conforme à la norme ISO 31000 au sein de son entreprise, en prenant en compte l'ensemble des moyens humains, techniques et financiers disponibles.		• Cohérence de la mise en place du plan de prévention au regard des moyens disponibles • Qualité du plan d'accompagnement • Conformité à la norme ISO 31000
Communiquer à tous les niveaux de l'organisation afin d'assurer une bonne intégration du plan de prévention des risques au management de l'entreprise.		• Pertinence du plan de communication proposé au regard des principes d'organisation de l'entreprise
Evaluer l'efficacité du plan de prévention des risques à l'aide d'indicateurs soigneusement choisis pour répondre aux impératifs de la continuité d'activité au sein de l'entreprise et en direction de ses clients.		• Pertinence des indicateurs retenus • Justification au regard des impératifs stratégiques de l'entreprise

Conception et mise en œuvre des tests d'intrusion Certification PECB Lead Ethical Hacker		
Compétences évaluées	**Modalités d'évaluation**	**Critères d'évaluation**
Simuler l'attaque d'un système d'information d'entreprise par un utilisateur malintentionné ou un logiciel malveillant, afin de détecter les fragilités de celui-ci.	Evaluation par la mise en situation professionnelle sur une étude de cas réel. Le(la) postulante élabore quatre documents remis au jury et soutenus oralement : - La série des tests d'intrusion et leur justification. - Le rapport de test et l'échelonnage des risques. - Des propositions chiffrées des parades à mettre en place. - Des conseils à l'entreprise en matière de lutte contre le piratage. L'évaluation est individuelle.	• Maîtrise des processus d'attaque non destructive d'un système d'information • Précision dans l'identification des fragilités
Concevoir et mettre en œuvre une série de tests d'intrusion à même de situer le degré de risque représenté par chacune des fragilités identifiées.		• Cohérence de la batterie de tests avec la nature des fragilités • Pertinence de la hiérarchisation des risques
Rédiger un rapport de *pentest* présentant l'ensemble des vulnérabilités exploitables dans les configurations ou la programmation, en vue de la conception par les responsables d'un plan d'amélioration de la sécurité du système d'information cohérent avec l'échelle des risques.		• Clarté du rapport • Exhaustivité des vulnérabilités recensées
Identifier et chiffrer les parades adaptées aux menaces, afin de faciliter la prise de décision et la mise au point du plan de sécurité.		• Niveau d'adéquation des parades proposées • Cohérence du chiffrage
Conseiller une entreprise sur les bonnes pratiques en matière de détection et de lutte contre le piratage, afin de faciliter la mise en place des mesures et procédures adéquates.		• Qualité et précision des conseils à l'entreprise • Adaptation à la stratégie de celle-ci en matière de sécurité