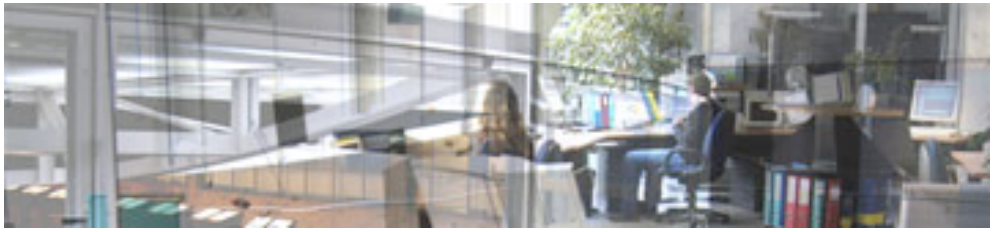
CCSIE
Centre de Compétence pour la Sécurité de l'Information des Entreprises
h e g



PME-RISC

Gérer les risques, la sécurité de l'information et la conformité dans les PME

> Réduire les risques liés au SI

> Améliorer la sécurité de l'information

> Assurer la conformité

> Fournir des résultats mesurables

> Adapter les standards au contexte des PME

Le CCSIE est un centre de compétence de la HEG Genève qui a pour vocation de fournir une offre de formation en matière de sécurité de l'information pour les entreprises, à la HEG de Genève et également en Suisse et en Europe au travers de partenaires accadémiques et privés.

NOUVEL

Hes·so
Haute Ecole Spécialisée de Suisse occidentale
University of Applied Sciences Western Switzerland

La problématique

Nombre d'entreprises sont conscientes de leurs lacunes en matière de sécurité de l'information. La volonté d'y remédier existe, mais bien souvent il est difficile de savoir par où commencer. Un des principaux obstacles à la mise en place d'un programme de sécurité adapté au contexte de l'entreprise est le manque d'alignement des objectifs de protection aux besoins de l'entreprise.

La solution

CPI-RISC ("Continuous Process Improvement–Risk, Information Security, and Compliance") est une approche orientée business, innovante et pragmatique. Cette méthodologie, basée sur les standards internationnaux reconnus de l'industrie*, et issue de l'expérience sur le terrain, aidera les entreprises à implémenter un programme de gestion de la sécurité de l'information aligné aux besoins de l'entreprise de manière durable.

CPI-RISC se base sur un processus d'amélioration continue adapté à la gestion de la sécurité de l'information. Les trois phases sont :

CPI·RISC 1 Evaluer 2 Mettre en oeuvre 3 Vérifier

CPI-RISC permet d'évaluer les risques liés au système d'information, de définir un plan de mise en oeuvre stratégique sur 3-5 ans et de vérifier la conformité des résultats par rapport aux objectifs fixés, afin de démontrer aux différentes parties prenantes que les risques sont correctement gérés.

Durée

3 jours

Contenu du cours

La formation est une combinaison de théorie et d'ateliers pratiques. Les supports de cours sont composés de modèles que les participants peuvent directement utiliser dans leur environnement respectif après la formation.

Public cible

Le cours PME-RISC est destiné aux cadres des départements finance, informatique ou directement à la direction des PME

* ISO 27001 Information Security Management System, ISO 27005 Information Risk Management, Les "20 Criticals Security Controls" du SANS Institute et les métriques du SEI Capability Maturity Model

Jour 1 • Evaluer les risques

La première phase permet d'**évaluer les risques**. Les risques sont évalués dans le contexte de l'entreprise. Ils sont organisés par fonction métier et priorisés selon leur impact sur les processus d'entreprise vitaux. Cette phase permet de proposer les options de traitement des risques, qui seront validées par la direction.

Activités

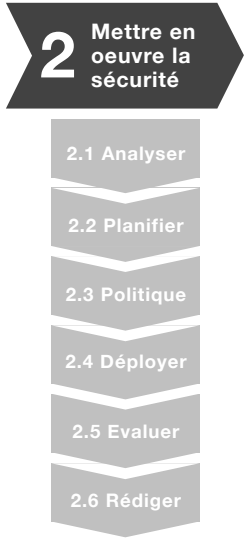
1.1 Analyser le contexte de l'entreprise en effectuant un mini-BIA (Analyse d'impact métier).

1.2 Prioriser et organiser les risques informationnels en utilisant un framework de risques établi.

1.3 Evaluer les risques à l'aide d'un questionnaire de risque.

1.4 Proposer les options de traitement des risques.

Jour 2 • Mettre en oeuvre la sécurité



La deuxième phase, **Mettre en oeuvre la sécurité**, permet de construire un système de management de la sécurité (SMSI) de type ISO 27001, à partir des risques identifiés. A l'issue de cette phase, le plan d'implémentation stratégique et le plan d'implémentation opérationnel sont rédigés. Durant la mise en oeuvre, une évaluation intermédiaire, permet de rédiger un rapport d'avancement pour la direction.

Activités

2.1 Analyser le contexte de risque établi et rédiger le plan de traitement des risques.

2.2 Planifier le SMSI à l'aide du plan d'implémentation stratégique pluriannuel.

2.3 Rédiger la politique de sécurité de l'information.

2.4 Mettre en oeuvre le SMSI à l'aide du plan d'implémentation opérationnel (annuel).

2.5 Evaluer l'implémentation.

2.6 Rédiger le rapport d'avancement.

PME-RISC • Gérer les risques, la sécurité de l'information et la conformité dans les PME

Jour 3 • Vérifier la conformité

La troisième phase, **Vérifier la conformité**, fournit l'assurance à l'entreprise que le programme mis en oeuvre gère de manière efficace les risques informationnels. La conformité est vérifiée par une évaluation conduite soit par un auditeur, soit par le chef de programme lui-même. A l'issue de cette phase, un rapport de conformité est rédigé pour la direction.

Activités

3.1 Analyser le contexte de conformité, à l'aide d'une analyse d'écart.

3.2 Préparer la checklist de conformité et planifier l'évaluation sur le terrain.

3.3 Vérifier la conformité à l'aide de la checklist.

3.4 Rédiger le rapport de conformité.

Prix

1,800 CHF

Inscriptions

Inscriptions: http://www.hesge.ch/heg/ccsie/

Dates des formations

Toutes les informations concernant les dates et les lieux des formations sont disponibles en ligne sur : http://www.hesge.ch/heg/ccsie/CCSIE_agenda.html

Informations supplémentaires

Toutes les informations concernant la formation PME-RISC et la méthodologie CPI-RISC sont disponibles en ligne sur : http://www.hesge.ch/heg/ccsie/

Contact : Rolf Hauri, Directeur
CCSIE
Haute Ecole de Gestion de Genève
7, route de Drize
1227 Carouge
E: ccsie@hesge.ch
T: +41 22 388 17 00

h e g
Haute école de gestion de Genève
Geneva School of Business Administration