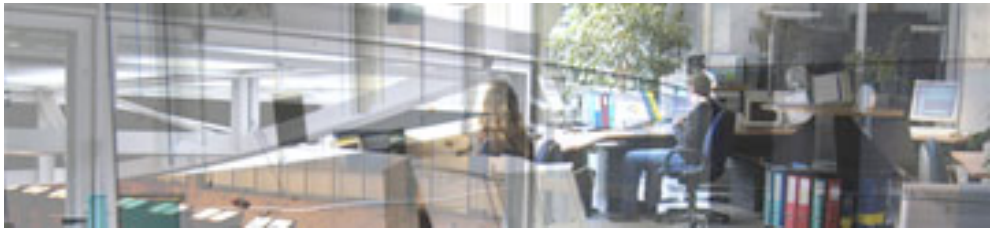
CCSIE
Centre de Compétence pour la Sécurité de l'Information des Entreprises
h e g



SMB-RISC

Risk Management, Information Security, and Compliance for SMB's

> Reduce information risk

> Improve information security

> Assure compliance

> Provide measurable results

> Scaled for small and medium businesses

The Business Information Security Competency Center (CCSIE) at the Geneva School of Business Administration (HEG) provides training programs at HEG in Geneva, Switzerland and throughout Europe using academic and private partnerships.

NOUVEL

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

The Problem

Many businesses and organizations are aware they have inadequate information security. Most are attempting to address the issue, but there are many obstacles to success. Often, the biggest obstacle is not knowing how to systematically address information security in a way that makes sense for the organization. As a result, many organizations spend money on information security, but at the end of the year have difficulty showing how they have improved security and reduced information risk.

The Solution

The Continuous Process Improvement–Risk, Information Security, and Compliance (CPI-RISC) methodology is a pragmatic, standards-based, business-oriented approach to information security. CPI-RISC was developed to help organizations create sustainable information security programs and demonstrate measurable improvement over time.

CPI-RISC uses a continuous process improvement cycle, adapted for information security. The three steps are:

CPI·RISC 1 Assess 2 Implement 3 Verify

The methodology is based on well-known industry standards from ISO, SANS Institute, and the Software Engineering Institute.*

CPI-RISC can help organizations assess their IT- and information-related risks, create a 3-5 strategic year plan for implementing information security, and verify compliance to assure the organizations stakeholders that risks are being managed.

Duration

3 days

Materials

The course is a combination of lecture and practice exercises. The course materials include templates, so students can immediately apply the methodology after completing the course.

Target audience

The SMB-RISC course is targeted at Finance, IT, or General Managers at SMB's.

* The International Organization for Standardization (ISO) 27001 Information Security Management System (ISMS), ISO 27005 Information Security Risk Management, SANS Institute 20 Critical Security Controls, and the Software Engineering Institute (SEI) Capability Maturity Model (CMM).

Day 1 • Assessing Information Risk

The first step is to **Assess Risk**. Risks are assessed in the context of the business environment, organized by business function, and prioritized based upon their impact to critical business processes. This step delivers a risk treatment proposal for management approval.

Tasks

1.1 Analyze the business environment by performing a mini-BIA (Business Impact Analysis).

1.2 Prioritize and organize IT- and information-related risks, using an information risk framework.

1.3 Assess risk using an information risk survey.

1.4 Report results as a risk treatment proposal.

Day 2 • Implementing Information Security

The second step, **Implement Information Security**, takes the risks identified in the first step, and addresses them using an ISO 27001-like Information Security Management System (ISMS). This step delivers strategic and tactical implementation plans, as well as an implementation progress report for management review.

Tasks

2.1 Analyze the risk environment and create a risk treatment plan.

2.2 Plan the ISMS by preparing a multi-year strategic implementation plan.

2.3 Develop the Information Security Policy.

2.4 Implement the ISMS by preparing a 1-year tactical implementation plan and selecting targeted controls.

2.5 Assess implementation progress.

2.6 Report implementation progress.

SMB-RISC • Risk Management, Information Security, and Compliance for SMB's

Day 3 • Verifying Compliance

The third step, **Verify Compliance**, provides assurance to the organization that the information security program is effectively managing IT- and information-related risk. Compliance is verified using an assessment that can be self-performed or performed by an auditor. This step delivers a compliance report for management review.

Tasks

3.1 Analyze the compliance environment by performing a compliance gap analysis.

3.2 Prepare the compliance checklist and plan the assessment fieldwork.

3.3 Verify compliance using a compliance checklist.

3.4 Report compliance.

Price

1,800 CHF

Registration

Online registration is available at: http://www.hesge.ch/heg/ccsie/

Course dates

Information about the dates and locations for upcoming courses can be found online at: http://www.hesge.ch/heg/ccsie/CCSIE_agenda.html

Additional information

Additional information about the SMB-RISC course and the CPI-RISC methodology can be found online at: http://www.hesge.ch/heg/ccsie/

Contact: Rolf Hauri, Director
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

© 2010 NOUVEL Strategies Sàrl, 2010-08 v2