



Information Security Management Professional (ISMP) based on IEC/ISO 27001 + examen

Cursusduur: 3 Dagen Cursuscode: ISMP-EXIN

Beschrijving:

Informatiebeveiliging wordt steeds belangrijker. De globalisering van de economie leidt tot een toenemende uitwisseling van informatie tussen organisaties (medewerkers, klanten en leveranciers), een toenemend gebruik van netwerken, zoals het interne bedrijfsnetwerk, de koppeling met netwerken van andere bedrijven en Internet. Bovendien zijn de activiteiten van veel bedrijven nu afhankelijk van ICT, waarbij informatie een kostbaar bedrijfsmiddel is geworden. Informatiebeveiliging is essentieel om de goede werking en de continuïteit van de organisatie te waarborgen: informatie moet betrouwbaar zijn.

Doelgroep:

De doelgroep voor de ISMP zijn beginnende professionals welke de ISF hebben afgerond. Deze module is bestemd voor iedereen die vanuit zijn/haar functie is betrokken bij onder andere de implementatie, evaluatie van en rapportage over informatiebeveiliging, zoals de Information Security Manager en de Information Security Officer of de Lijnmanager en de Project Manager.

Doelstelling:

■ 1 Perspectieven op informatiebeveiliging

- 1.1 De cursist begrijpt het zakelijke belang van informatiebeveiliging en kan
 - verschillende soorten informatie op basis van hun zakelijke waarde onderscheiden.
 - de eigenschappen van een managementsysteem voor informatiebeveiliging uitleggen.
- 1.2 De cursist kent het perspectief van de klant ten aanzien van informatiebeheer, en kan
 - het belang van informatiebeheer bij uitbesteding uitleggen.
 - een leverancier op basis van garanties aanbevelen.
- 1.3 De cursist kent de verantwoordelijkheden van de leverancier ten aanzien van veiligheids garanties, en kan
 - beveiligingsaspecten in servicemanagementprocessen onderscheiden.
 - nalevingsactiviteiten ondersteunen.

■ 2 Risicobeheer

- 2.1 De cursist kent de principes van risicobeheer, en kan
 - principes voor het analyseren van risico's uitleggen.
 - risico's voor geclassificeerde bedrijfsmiddelen identificeren.
 - risico's voor geclassificeerde bedrijfsmiddelen berekenen.
- 2.2 De cursist weet hoe risico's beheerd worden en kan
 - maatregelen op basis van Vertrouwelijkheid, Integriteit en Beschikbaarheid (Confidentiality, Integrity and Availability (CIA)

- 2.3 De cursist weet hoe om te gaan met risico's, en kan
 - risicostrategieën onderscheiden.
 - business cases voor maatregelen opstellen.
 - over risicoanalyses rapporteren.

■ 3 Maatregelen voor informatiebeveiliging

- 3.1 De cursist heeft kennis van organisatorische maatregelen en kan
 - beleid en procedures voor informatiebeveiliging schrijven.
 - incidentafhandeling bij informatiebeveiliging implementeren.
 - een bewustzijns campagne binnen de organisatie uitvoeren.
 - rollen en verantwoordelijkheden voor informatiebeveiliging implementeren.
- 3.2 De cursist heeft kennis van technische maatregelen, en kan
 - het doel van beveiligingsarchitecturen uitleggen.
 - het doel van beveiligingsdiensten uitleggen.
 - het belang van beveiligingselementen in de IT-infrastructuur uitleggen.
- 3.3 De cursist heeft kennis van fysieke, werknemer-gerelateerde en continuïteitsmaatregelen, en kan
 - maatregelen voor fysieke toegang aanbevelen.
 - beveiligingsmaatregelen in de levenscyclus van dienstverbanden aanbevelen.
 - de ontwikkeling en het testen van een bedrijfscontinuïteitsplan

indelen.

ondersteunen.

- maatregelen op basis van de fasen van de incidentcyclus kiezen.
- relevante richtlijnen voor het toepassen van maatregelen kiezen.

Vereiste kennis en vaardigheden:

ISF-EXIN, Information Security Foundation based on IEC/ISO 27001

Examens en certificering

■

Cursusinhoud:

De deelnemer verkrijgt kennis over opstellen van het ICT-beleid, het inrichten van de security managementorganisatie, hoe verantwoording is geregeld voor implementatie van (informatie)beveiligingsmaatregelen uit het informatiebeveiligingsplan. Verder wordt ingegaan op kwaliteit en kwaliteitssystemen.

- Context van de organisatie
- Informatiebeveiligingsbeleid
- Organisatie van Informatiebeveiliging
- Personeel en Informatiebeveiliging
- Asset Management
- Toegangscontrole
- Cryptografie
- Fysieke en Omgevingsbeveiliging
- Beveiliging Bedrijfsvoering (Operations Security)
- Communicatiebeveiliging
- Aanschaf, Ontwikkeling en Onderhoud van een systeem
- Leveranciersrelaties
- Incidentmanagement
- Bedrijfscontinuïteitsbeheer
- Compliance

Practical Assignments

Sample Exam

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein