

Řízení rizik podle ČSN/ISO/IEC 27005

Kód kurzu: GOC241

Dvoudenní kurz vysvětluje základní terminologii a principy identifikace a hodnocení aktiv, zranitelností a hrozeb pro informační bezpečnost a z nich vyplývajících rizik pro udržitelnost provozu (business continuity) podniků i organizací státní správy.

Předpokládané vstupní znalosti

Všeobecný přehled o možnostech informačních technologií a hrozbách pro informační bezpečnost

Osnova kurzu

Bezpečnostní požadavky obecně

Pojmy důvěrnost (confidentiality), integrita (integrity), dostupnost (availability)

Složitější pojmy jako non-repudation, privacy, safety, authenticity, reputation

Pojmy kontinuita provozu (business continuity) a obnova po havárii (disaster recovery)

Vztah informační bezpečnosti k BCP a DR

Pojmy aktivum (asset), hodnocení aktiv (valuation), zranitelnost (vulnerability), hrozba (threat), riziko (risk)

Role pracovníků jako například vlastník aktiva, vlastník rizika

Hodnocení rizik obecně

Vztah hrozba - riziko

Řízení aktiv

Metodiky hodnocení rizik podle ISO 27005

Příklady zranitelností v informačních technologiích

Příklady hrozeb v informačních technologiích

Příklady budování analýzy rizik nad hrozbami informačním technologiím

GOPAS Praha

Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno

Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava

Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk



Copyright © 2020 GOPAS, a.s.,
All rights reserved