Cybersecurity: GRC Frameworks and Certifications

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

- CISOs, compliance officers
- IT managers
- Auditors
- Executives involved in cybersecurity governance

Training objectives

- Understand the role of GRC in cybersecurity
- Explore the major frameworks (ISO 27001, SOC 2, NIST, Law 25)
- Learn how to design and implement a GRC program
- Prepare for an audit or certification

Summary

This training gives a clear understanding of governance, risk management and compliance (GRC) as applied to cybersecurity. It explores international standards, certification programs and the role of the RCMP in organizational resilience.

Course outline

Module 1: Introduction to Cybersecurity GRC

- Definition and Fundamental Concepts
- GRC as a Strategic Compass
- Stakeholders and Responsibilities

Module 2: Standards and Frameworks

- ISO/IEC 27001 and the basis of an ISMS
- SOC 2 Trust Criteria

- NIST Cybersecurity Framework and AI Risk Framework
- Bill 25 and GDPR Overview

Module 3: Building a GRC Program

- Risk Assessment Methodologies
- Policy Development and Control Choices
- Monitoring, Audit and Continuous Improvement

Module 4: Certifications and Audit Preparation

- ISO and SOC 2 Certification Process
- Preparation of Documentation and Evidence
- Case Study: Setting Up a GRC in an SME

Approach and methodology

- Progressive presentation of the concepts of governance, risk management and compliance in cybersecurity
- Explanation of the main reference frameworks and standards (ISO 27001, SOC 2, NIST, Law 25) based on concrete examples
- Contextualization of organizational resilience, audit and certification issues
- Case studies to illustrate the implementation of a GRC program, particularly in an SME
- Exchanges and support from the trainer to facilitate the application of the concepts to the reality of the participants

Prerequisites

- General knowledge of cybersecurity

Recommendations

- Interest in governance, risk management and compliance
- Be involved in security, audit, compliance or IT management issues
-

Have a general understanding of how an organization operates and its regulatory obligations

- Experience in security, auditing, compliance or risk management (asset)