TRAINING SEMINAR

SETYM International Canada
85, SAINTE-CATHERINE WEST, 10TH FLOOR
MONTREAL, QUEBEC, CANADA H2X 3P4
+1 (514) 939-2200 | SETYM@SETYM.COM
setym.com

NEW

Cybersecurity: Prevention, Protection and Defence

The question is no longer whether a cyberattack will occur, but when. Cybersecurity is now a pillar of governance and a key factor in the success of projects. It is now imperative for any organisation to be able to anticipate threats in order to and not compromise its activities or even its survival.

In a context of accelerated digital transformation, organisations, critical infrastructure and donor-funded projects are prime targets. This seminar will provide you with the knowledge and skills you need to effectively analyse threats, assess risks and make informed decisions to strengthen the security and resilience of your activities. You will learn how to integrate cybersecurity into your management practices and mobilise your teams around a culture of sustained vigilance.

PRACTICAL OBJECTIVES

- **Understand** threats and their potential impact on your projects and your organisation.
- **Define** a strategic vision that integrates cybersecurity and accountability for decisions into governance.
- **Identify, assess and prioritise** cyber risk in your projects.
- **Develop** appropriate policies and response plans.
- **Strengthen** the culture of cybersecurity within your teams.

TARGET AUDIENCE:

- **Executives, project managers, programme managers and decision-makers who wish to integrate cybersecurity into their strategic decisions.**

DURATION: 2 weeks

SEMINAR TOPICS

- **Overview of Current Threats and Trends:** Identify the main cyber threats targeting organisations and their projects. Understand how cybercriminals operate and their potential impact on governance, operations and reputation.
- **Cybersecurity and Governance:** Clarify the strategic role of executives in preventing and managing cyber risks. Integrate cybersecurity into strategic planning and overall project management.
- **Cyber Risk Management:** Implement a process for identifying, assessing and prioritising risks. Determine preventive and corrective measures appropriate to the nature of the projects and assets being protected.
- **Compliance and Legal Obligations:** Familiarise yourself with the laws, regulations and international standards (GDPR, ISO 27001, NIST) that govern cybersecurity and data protection. Adapt organisational policies to ensure compliance.
- **Crisis Management and Business Continuity:** Develop and test an incident response plan. Strengthen cyber resilience by ensuring the continuity of critical activities in the event of an attack.
- **Project and Supply Chain Security:** Integrate cybersecurity requirements from the project design stage. Assess and secure relationships with suppliers, partners and subcontractors.