






E-HOOYIA

Governance, Management,
and Compliance

Presented by:
Hooyia

 +237 691435485
+237 697907096

 e-hooyia.com

 Bafoussam, Cameroon

contact@e-hooyia.com

Module 3: Governance, Management, and Compliance (GRC)	2
Course Overview	2
Targeted Audience.....	2
Module Objectives	3
Course Structure	3

Module 3: Governance, Management, and Compliance (GRC)

Course Overview

This module elevates the focus of cybersecurity from purely technical operations to the strategic, regulatory, and organizational dimensions of security. It provides participants with a comprehensive understanding of how to manage an organization's cybersecurity risk, align security policies with business goals, and ensure compliance with complex regulatory frameworks. The inclusion of this discipline in the program demonstrates a deep understanding that the most significant cybersecurity challenges today are often non-technical, requiring strong leadership and strategic foresight. The curriculum is designed to train future leaders who can communicate security value to management and navigate the complexities of corporate governance.

Targeted Audience

This training is ideal for professionals aiming for leadership and advisory roles. It is particularly suited for aspiring Chief Information Security Officers (CISOs), GRC Consultants, Risk Managers, and Security Auditors.¹

Module Objectives

Upon successful completion of this module, participants will be able to:

- Navigate and apply major normative and regulatory frameworks, including ISO 27001, GDPR, NIST, and PCI-DSS.¹
- Implement effective risk management methods and treatment plans, such as EBIOS and OCTAVE, to evaluate and mitigate security risks.¹
- Define and supervise a comprehensive security policy framework and lead security teams.¹
- Conduct and manage security audits, from methodology to reporting and communicating findings to senior leadership.¹
- Provide strategic cybersecurity consulting and support to businesses, aligning security with their overarching objectives.¹

Course Structure

The module is structured to provide a clear progression from foundational GRC concepts to practical application and strategic management.

- **Week 1: Security Governance & Regulatory Frameworks**
 - Introduction to the strategic role of cybersecurity in an organization.
 - In-depth overview of the ISO 27001 standard and the NIST Cybersecurity Framework.
 - Understanding the key requirements of GDPR and PCI-DSS compliance.
- **Week 2: Risk Management & Policy Development**
 - Methodologies for risk identification and assessment.
 - Developing effective risk mitigation and treatment strategies.
 - Creating a robust security policy framework and acceptable use policies.¹
- **Week 3: Auditing, Compliance & Strategic Leadership**
 - The role of the CISO and how to communicate security value to the business.
 - Auditing methodologies and preparing for compliance assessments.
 - Case studies on how to build and maintain a culture of security within an organization.