

 - Powered

GRC Hands-on

(Governance Risk & Compliance)

Training



Course Highlights



40-Hour LIVE
Instructor-Led
Training



AI-Integrated
Case Studies &
Role-play



Hands-on Coverage:
ISO 27001, COSO,
GDPR Frameworks



Taught by Certified
GRC & Information
Security Experts



Capstone Project:
Develop a GRC
Plan



Identify & Assess AI
Risks in Modern Risk
Management



Career Guidance
and Mentorship



Extended Post
Training Support



Access to Recorded
Sessions

About Course

The GRC Hands-on Training from InfosecTrain offers a comprehensive exploration of Governance, Risk, and Compliance (GRC) within the realm of information security, including emerging considerations such as AI risks in modern risk management. This course encompasses both theoretical knowledge and practical exercises, covering essential topics like the CIA Triad, principles of information security, and the importance of GRC. Participants will delve into various governance frameworks such as COSO, develop and implement security policies, understand legal and regulatory compliance, and explore audit methodologies. The course also provides hands-on experience in setting up security controls, compliance frameworks and standards, risk management practices, and developing a GRC plan. Through interactive case studies and role-play exercises, learners gain real-world insights into governance structures, board dynamics, risk assessment, and mitigation strategies, preparing them for effective GRC integration in businesses.



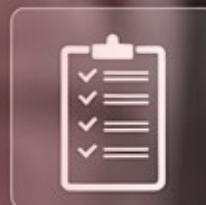
Course Objectives

Upon successful completion of the training, participants will be able to:

- ✓ Understand the basics of Governance, Risk, and Compliance (GRC), along with the principles of information security and the critical CIA Triad.
- ✓ Analyze and derive insights from interactive case studies and real-world incidents to apply GRC principles effectively.
- ✓ Gain expertise in key governance frameworks like COSO and learn to identify and assess organizational governance structures.
- ✓ Enhance knowledge of crucial laws and regulations, such as GDPR, essential for legal and regulatory compliance.
- ✓ Understand how to identify and assess AI risks as part of modern risk management practices.
- ✓ Understand and apply best practices in audit methodology, including the purpose and process of auditing.



GRC



Target Audience

This course is ideal for:

- ✓ IT Analysts
- ✓ System Administrators
- ✓ Network Engineers
- ✓ Business Analysts
- ✓ Project Managers
- ✓ Security Governance Consultant
- ✓ Compliance Analyst
- ✓ Risk Manager

Pre-Requisites

- ✓ Fundamental IT knowledge is required
- ✓ Prior experience in IT, security, or compliance roles can be beneficial, but is not mandatory



Course Content

Introduction to GRC

- ✓ Understanding GRC **(Theory)**
- ✓ Principles of Information Security **(Theory)**
- ✓ The CIA Triad: Confidentiality, Integrity, Availability **(Theory)**
- ✓ Importance of Governance, Risk, and Compliance (GRC) **(Theory)**
- ✓ Interactive Case Study Analysis **(Practical)**
- ✓ Governance Frameworks and Models **(Theory)**
- ✓ Overview of Various Governance Frameworks (e.g., COSO) **(Theory)**
- ✓ Practical Exercise: Identifying Governance Structures in Organizations **(Practical)**
- ✓ Board Dynamics and Decision-Making **(Theory)**
- ✓ Role-Play Exercise on Board Meetings and Decision-Making Processes **(Practical)**

Security Policies and Governance

- ✓ Developing and Implementing Security Policies **(Theory)**
- ✓ Key Components of Security Policies **(Theory)**
- ✓ Workshop: Creating a Security Policy **(Practical)**
- ✓ Governance Structures and Strategies **(Theory)**
- ✓ Roles and Responsibilities in Governance **(Theory)**
- ✓ Best Practices in Information Security Governance **(Practical)**
- ✓ Legal and Regulatory Compliance such as GDPR for high-risk AI systems **(Theory)**
- ✓ Understanding Key Laws and Regulations (e.g., GDPR) **(Theory)**

Audit

- ✓ Audit Methodology **(Practical)**
- ✓ Internal audit approach and methodology **(Practical)**
- ✓ Audit Definition and Real-Time Usage **(Practical)**
- ✓ Best Practices in the Audit Methodology **(Practical)**

Security Controls and Compliance Frameworks

- ✓ Implementing Security Controls **(Theory)**
- ✓ Types of Security Controls (Preventive, Detective, Corrective) **(Theory)**
- ✓ Types of Security Areas (Access Control, Change Management, BC/DR, Incident Management, Network Security, Communication Security, Encryption) **(Theory)**
- ✓ Compliance Frameworks and Standards **(Theory)**
- ✓ Walkthrough of ISO 27001 Framework Design and Implementation Aligning with a Real-Time Example **(Practical)**
- ✓ Workshop: Aligning Policies with Compliance Standards **(Practical)**
- ✓ Integration of Data Privacy Through Data Privacy Impact Assessment (DPIA) **(Practical)**
- ✓ Role of Technical Knowledge in GRC **(Theory)**
- ✓ Extent of Expertise Required in the GRC – Real-World Simulation **(Practical)**
- ✓ Workshop: Assessing System Controls Based on ISO 27001 **(Practical)**

Risk Management in Information Security

- ✓ Risk Assessment and Analysis **(Theory)**
- ✓ Risk Management (Including Top Frameworks to be Followed for Best Practices) **(Theory)**
- ✓ Techniques for Risk Identification and Evaluation including AI **(Theory)**
- ✓ Practical Exercise: Conducting a Risk Assessment including AI risks **(Practical)**
- ✓ Mitigation Strategies and Risk Treatment **(Theory)**
- ✓ Developing Risk Response Strategies **(Theory)**
- ✓ Case study: Risk Mitigation in Action **(Practical)**
- ✓ Tools and Techniques for Risk Management **(Theory)**
- ✓ Utilizing Software and Tools for Risk Management **(Theory)**

Integrating GRC

- ✓ GRC in Practice **(Theory)**
- ✓ Case Studies of GRC Integration in Businesses **(Practical)**
- ✓ Developing a GRC ecosystem **(Practical)**
- ✓ Final Project: Creating a Comprehensive GRC Plan for an Organization **(Practical)**
- ✓ Typical Interview Questions **(Practical)**
- ✓ Course Review and Q&A
- ✓ Review of Key Concepts and Questions



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on

