GRC Complete Course - Governance, Risk & Compliance Training

Welcome to the Governance and Compliance Complete Training

This course will help you in case you are preparing for many classes, including but not limited to

- ISC2 Certified Information System Security Professional (CISSP)

- ISC2 Certified in Governance, Risk and Compliance (CGRC)

- ISACA Certified Information System Auditor (CISA)

- ISACA Certified Information Security Manager (CISM)

In addition to that, this course represents a great reference to anyone working in GRC.

If you are preparing for CGRC Certification, this course will be an excellent aid for doing so; as per ISC2, the official CGRC outlines are

Domain 1: Information Security Risk Management Program

Domain 2: Scope of the Information System

Domain 3: Selection and Approval of Security and Privacy Controls

Domain 4: Implementation of Security and Privacy Controls

Domain 5: Assessment/Audit of Security and Privacy Controls

Domain 6: Authorization/Approval of Information System

Domain 7: Continuous Monitoring

During this course, you will get introduced to all of the above concepts in great details, however we suggest that in addition to following this course be familiar with the following resources "remember that our course is also aligned with the below"

Who this course is for:

- IT and Security Professionals: Individuals working in information technology and cybersecurity roles who want to strengthen their understanding of governance and compliance.
- Risk Management Professionals: Professionals involved in risk management who aim to integrate risk management seamlessly into governance practices.
- Compliance Officers: Compliance officers and specialists looking to deepen their expertise in compliance frameworks and governance policies.
- CAP Certification Aspirants: Individuals preparing for the Certified Authorization Professional (CAP) certification to validate their skills in security authorization processes.
- Governance Professionals: Those responsible for governance practices within an organization seeking a comprehensive understanding of foundational governance principles.
- Policy and Procedure Developers: Professionals involved in developing governance policies and documenting procedures for compliance.
- Training and Communication Specialists: Individuals responsible for communication, training, and employee awareness in the context of governance, risk, and compliance.
- Incident Response Teams: Professionals involved in incident response planning and management who want to enhance their skills in handling security incidents.
- Professionals in Emerging Technologies: Individuals working with emerging technologies, particularly cloud computing, and remote work environments, who want to address governance and risk considerations.
- Continuous Learners in GRC: Professionals who recognize the importance of continuous learning and staying updated on emerging trends in governance, risk, and compliance.
- Course is designed to cater to a broad audience, from those new to the field to experienced professionals seeking to deepen their expertise. The content covers a range of topics to provide a well-rounded understanding of contemporary GRC practices and prepares individuals for the challenges and opportunities in this dynamic domain.

Course requirements

To enrol in this course, you should have a basic understanding of information security concepts and practices. There are no other prerequisites for this course.

Course Duration

25 Hours

Course Overview:

1. Introduction to Information Security GRC:
   - Overview of information security governance, risk management, and compliance.
   - Importance of GRC in ensuring organizational security.
2. Information Security Governance:
   - Roles and responsibilities of key stakeholders in information security.
   - Development and implementation of information security policies, procedures, and standards.
   - Information security frameworks and best practices (e.g., ISO 27001, NIST Cybersecurity Framework).
3. Risk Management:
   - Risk assessment methodologies and techniques.
   - Identification and classification of information security risks.
   - Risk mitigation strategies and controls.
   - Risk monitoring and reporting.
4. Compliance Management:
   - Regulatory and legal requirements related to information security (e.g., GDPR, HIPAA, PCI DSS).
   - Compliance frameworks and controls.
   - Compliance audits and assessments.
   - Incident response and breach management.
5. Security Metrics and Reporting:
   - Key performance indicators (KPIs) for measuring information security effectiveness.
   - Security metrics and reporting frameworks.
   - Dashboards and visualizations for presenting security data to stakeholders.
6. Information Security Policies and Procedures:
   - Development and implementation of information security policies.
   - Creation of security awareness and training programs.
   - Incident response planning and procedures.
7. Vendor Risk Management:
   - They are assessing and managing risks associated with third-party vendors.
   - Contractual and legal considerations for vendor security.
   - Ongoing monitoring and evaluation of vendor security controls.
8. Security Auditing and Assurance:
   - Internal and external audits of information security controls.
   - Compliance with auditing standards and frameworks.
   - Assurance and attestation processes.
9. Emerging Trends and Technologies:
   - Current trends and challenges in information security GRC.
   - Emerging technologies impacting GRC practices (e.g., cloud computing, IoT, artificial intelligence).
   - Privacy and data protection considerations.