3-IN-1 GRC
COURSE CURRICULUM

Welcome to the Cyber Savvy 3-in-1 GRC Course!
This comprehensive training bootcamp is designed to equip you with the knowledge and skills necessary to excel in Governance, Risk, and Compliance (GRC). Leveraging years of industry experience, our curriculum covers the critical aspects of GRC, providing you with a solid foundation and advanced insights into effective security operations.

GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE - DEMYSTIFIED

- Understanding GRC
- Importance of Governance, Risk Management and Compliance (GRC)
- Principles and benefits associated to Governance, Risk Management and Compliance
- GRC integrated approaches and their key enablers
- Overview of governance framework – COSO
- **Workshop: Real-Time GRC tool demo (Practical)**

GRC-USE-CASE-ISSUES MANAGEMENT

- Findings/Issues – Definition
- Roles and responsibilities of key stakeholders - Issues
- Issue structure and strategies
- Criticality, source and types of issues
- **Workshop: Industry used real-time issue use cases and examples (Practical)**
- Remediation Plan – Definition
- Roles and responsibilities of key stakeholders – Remediation Plans
- Types of Remediation Plans
- **Workshop: Industry used real-time remediation use cases and examples (Practical)**
- Exception Request and Exception Extension – Definition
- Roles and responsibilities of key stakeholders – Exception Requests
- **Workshop: Industry used real-time Exception Request use cases and examples (Practical)**
- **Swim line diagram for Issues, Remediation Plans and Exception Requests (Practical)**

GRC – USE CASE – POLICY MANAGEMENT

- Policy – Definition
- Importance of Policy Management
- Roles and responsibilities of key stakeholders – Policy Management
- Steps to handle an organization's Policy
- Key features of Policy Management
- Workshop: Developing and Implementing security policy (Practical)
- Workshop: Industry used real-time Policy use cases and examples (Practical)
- Swim line diagram of Policy Management (Practical)

GRC - USE CASE - CONTROL ASSURANCE

- Control Assurance – Key Definitions
- Understanding of Control Standards and its significance
- Workshop: Industry used real-time control standard example (Practical)
- Types of security controls (Preventive, Corrective, Detective)
- Understanding of Master Control and its significance
- **Workshop: Industry used real-time master control example (Practical)**
- Understanding of Control Procedure and its importance
- **Workshop: Industry used real-time control procedure example (Practical)**
- Relationship between Control Standard, Master Controls and Control Procedure
- Importance of Control Testing
- Understanding of Design Test Results (DTR), Operating Test Results (OTR), Control Self-Assessment (CSA)
- Control Effectiveness – Definition and Scale
- Roles and responsibilities of key stakeholders – Control Assurance

GRC - USE CASE - RISK MANAGEMENT

- Risk Assessment lifecycle and analysis
- Understanding and significance of – Enterprise, Operational and IT Risk Management
- Techniques for Risk identification and Risk evaluation matrix
- Exercise: Preparing a list of Key Risk Management activities (Practical)
- Developing a Risk Register with use case example (Practical)
- Risk Taxonomy – Risk Capacity, Tolwwerance, Appetite, Mitigation, Transfer
- **Workshop: Industry used real-time IT Risk Assessment example (Practical)**
- Exercise: Align Policy, Risk, Controls and Issues (Practical)

GRC - USE CASE - COMPLIANCE MANAGEMENT

- Compliance Frameworks and Standards
- Walkthrough of ISO 27001 Framework Design and Implementation Aligning with a Real-Time Example (Practical)
- Areas of Compliance (Financial, Regulatory, Ethical, Environmental, Health and Safety)
- Types of Compliance (Legal, Regulatory, Ethical and Internal)
- Roles and Responsibilities of Regulatory Compliance
- Pillars of Compliance
- **Workshop: Align GDPR checklist, articles and deliverables with organization (Practical)**

COURSE HIGHLIGHTS: - GRC ARCHER COURSE CONTENT

The course content is designed for various roles in the GRC domain, such as GRC business users and GRC administrators, making you an expert in RSA Archer implementations for GRC Solutions.

1. Introduction to RSA Archer GRC 6

- Basic GRC overview
- Basic RSA Archer overview
- working with content records, dashboards & workspaces

2. Building an Application

- Create an application from scratch
- Adding different types of fields
- Manipulate the layout and layout objects

3. Workflow Components

- Design and create a data-driven event or Actions
- Configure a calculated field
- Important functions and formulas overview
- Workflow

4. Access Control

- Create a user account
- Create a group
- Create a role
- Create a record permission field
- Make a field private
- Discuss best practices for configuring access control
- Troubleshoot common access control issues

5. Reporting and Dashboards

- Reporting basics
- Global searches
- Advanced searches
- Statistics searches

- Create an iView
- Create a Dashboard
- Configure a Workspace

6. Integration

- Data Import
- Import data into an application
- Import data into a leveled application
- Data Feed Manager
- Overview and basics

7. Packaging and Advanced Workflow Overview

- Packaging Overview
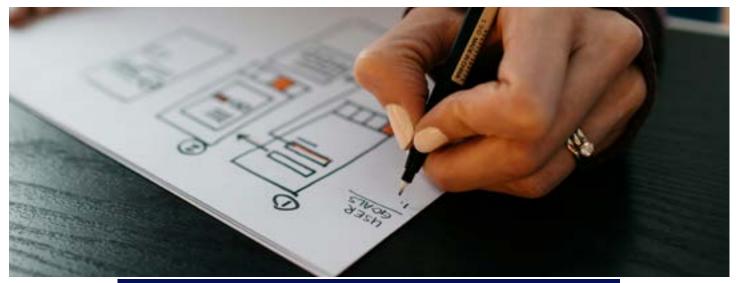- Advance Workflow Overview

8. Questionnaires

- Questionnaire basics
- Questionnaire exploration
- Creation of Questionnaire

9. Notifications (Overview and Basics)

- Subscription Notifications
- Scheduled Report Distributions
- On-Demand Notifications
- Admin Notifications
- Troubleshooting Notification

10. Certification Information & Resume Preparation

We offer advanced and scenario-based interview questions and answers along with RSA Archer resume samples. Take a free sample practice test before appearing in the certification to improve your chances of scoring high. Offer advanced and scenario-based interview questions. RSA Archer Resume Samples | Practice tests

COURSE HIGHLIGHTS: ISO 27001:2022 LEAD AUDITOR

ISO 27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

LEARNING OBJECTIVES

- Learn the fundamental concepts and principles of an information security management system (ISMS) based on ISO/IEC 27001:2022
- Understand the ISO/IEC 27001:2022 requirements for an ISMS from the viewpoint of an implementer
- Initiating and planning the Auditing of an ISMS based on ISO/IEC 27001:2022
- Able to provide Support to an organization in operating, maintaining, and continually improving an ISMS based on ISO/IEC 27001
- Prepare an organization to undergo a third-party certification audit

WHAT WILL THE CERTIFICATION ALLOW YOU TO DO?

Certificate is the conventional acknowledgment and evidence of information which conveys a significant weight when you are entering the work market, or when you need to progress in your vocation. Because of the mechanical progressions and the intricacy of cyberattacks, the interest for IT experts keeps on being popular. All things considered; the ISO/IEC 27001 affirmation has turned into the standard for best practice in data security. By taking a confirmation you grandstand a specific expertise level which will show added esteem not exclusively to your expert profession yet to your association also.

Course agenda

- About ISO
- Information Security Basic

- Risks
- About ISO 27000-1 & Related ISO Standards
- PDCA in Action
- Context of organization
- Leadership
- Planning
- Support
- Operations
- Performance Evaluation
- Improvement
- Introduction to controls
- A5. Organizational Controls (5.1 to 5.6)
- A5. Organizational Controls (5.7 to 5.12)
- A5. Organizational Controls (5.13 to 5.24)
- A5. Organizational Controls (5.25 to 5.37)
- A6. People Controls
- A7. Physical Controls
- A8. Technological Controls (8.1 to 8.12)
- A8. Technological Controls (8.13 to 8.24)
- A8. Technological Controls (8.25 to 8.34)
- Activity
- Fundamental Audit Concepts
- 7 Principles of Auditing (1 to 3)
- 7 Principles of Auditing (4 to 7)
- Activity
- Initiating the Audit
- Activity
- Stage 1 Audit
- Activity
- Stage 2 Audit
- Activity
- Audit Conclusions
- Beyond the Initial Audit
- Competencies and evaluation of auditors

WHY ATTEND THIS TRAINING?

Our training offers an unparalleled opportunity to master three critical areas in one powerhouse training:

1. **Comprehensive GRC Functional Course**
2. **In-Depth GRC Archer Course Content**
3. **ISO 27001:2022 Lead Auditor Certification**
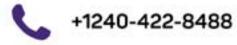
WHAT SETS THIS TRAINING APART?

Expert Instructors: Our trainers are seasoned professionals with extensive industry experience and a deep understanding of the latest trends and best practices.

Interactive Learning: Engage in dynamic sessions that combine theoretical knowledge with practical exercises, ensuring a well-rounded learning experience.

Career Advancement: Enhance your professional credentials and open doors to new career opportunities with recognized certifications.

Organizations are becoming increasingly concerned about managing and protecting their critical data as technology continues to advance. The most effective way to protect against threats and attacks is by properly implementing, auditing, and supervising data security controls and best practices. Data security is a fundamental expectation and requirement for clients, lawmakers, and other stakeholders. This unique combination of three training courses in one will equip you with the skills to navigate complex regulatory landscapes, leverage industry-leading GRC tools, and lead ISO audits with confidence.

support@cyberlyusa.com

+1240-422-8488

cyberlyusa.com

Join us in this transformative journey to become a GRC – RMF expert and safeguard your organization's future.