# Course Outline of Certified in Governance, Risk Management & Compliance (CGRC™)

Module 1 : Cyber Security Fundamentals

- Introduction to Information Security
- Network Fundamentals
- Windows Fundamentals
- Linux Fundamentals

Module 2 : IT Risk Management, Governance and Compliance

- Briefing on Definition of Risk and Risk in context of Information Technology
- IT Risk Management cycle
- Understanding concepts & techniques
- IT Risk Assessment
- IT Risk Mitigation
- Risk Assessment
- Risk Management
- Risk Management framework
- Methodologies & guidelines

Module 3 : Information Security Management System

- Introduction
- Need of ISMS
- Structure of standards
- ISO 27001:2013 domains
- ISO 27001:2013 objective controls & Controls

Module 4 : Payment Card Industry Data Security Standard

- Introduction of PCI SSC
- Introduction of PCI-DSS & requirements
- Introduction of PA-DSS & requirements
- Introduction of PTS
- SAQ (Self-Assessment Questionnaire)
- QSA (Qualified Security Assessor)

## Module 5 : ISO 22301 (Business Continuity Management)

- Introduction
- BCP (Business Continuity Planning)
- DRP (Disaster Recovery Planning)
- Identification of Threats and Risk Control
- RTO & RPO
- Disaster Recovery Training
- MTPOD - Maximum Tolerable Period of Disruption
- Documentation

## Module 6 : HIPAA (Health Insurance Portability and Accountability Act)

- Introduction to HIPAA
- Applicability of HIPAA
- Health information usage flow
- PHI
- HIPAA rules
- HIPAA Requirements

## Module 7 : IT Act

- Introduction
- Short Title, Extent & Applicability
- Definitions
- Offences
- Case Studies

## Module 8 : ITIL (Information Technology Infrastructure library)

- Introduction to ITIL
- ITIL implementation
  - Process, Change, Patch management
  - Incident management
  - Demand Management
- Functions definitions and allocation
  - Service Desk Function
  - Technical Management Function
  - Application Management Function

## Module 9 : GDPR (General Data Protection Regulation)

- Introduction
- Subject-matter and objectives
- Definitions
- Principles
- Rights of data subject
- Controller and processor
- Transfer of personal data to third countries or international organizations
- Violations & penalties

## Module 10 : Network Security

- Introduction
- Subject-matter and objectives
- Definitions
- Principles
- Rights of data subject
- Controller and processor
- Transfer of personal data to third countries or international organizations
- Violations & penalties

## Module 11 : Operating System Security and Database Security

- Operating System Security
  - Windows Hardening
  - Linux Hardening
  - Web Server Hardening
- Database Security
  - Database Fundamentals
  - SQL
  - MySQL & MySQL Security
  - Oracle Database Security
  - MongoDB & MongoDB Security
  - Database Security Testing Tools
  - Database Security Best Practices

## Module 12 : Web Application Security

- Introduction to web application architecture
- OWASP Top 10 2017
- Automated tools
- Attacking the issue
- Countermeasures
- ESAPI Security
- Threat Modelling
- Source Code Analysis
- Report Writing

## Module 13 : Sarbanes Oxley Act

- Introduction to Sarbanes Oxley Act
- Title, Extent & applicability of Act
- Implementation of various Provisions & SOX Requirements
- Penalties for Non-Compliance
- SOX Audit

- Case studies & exercises