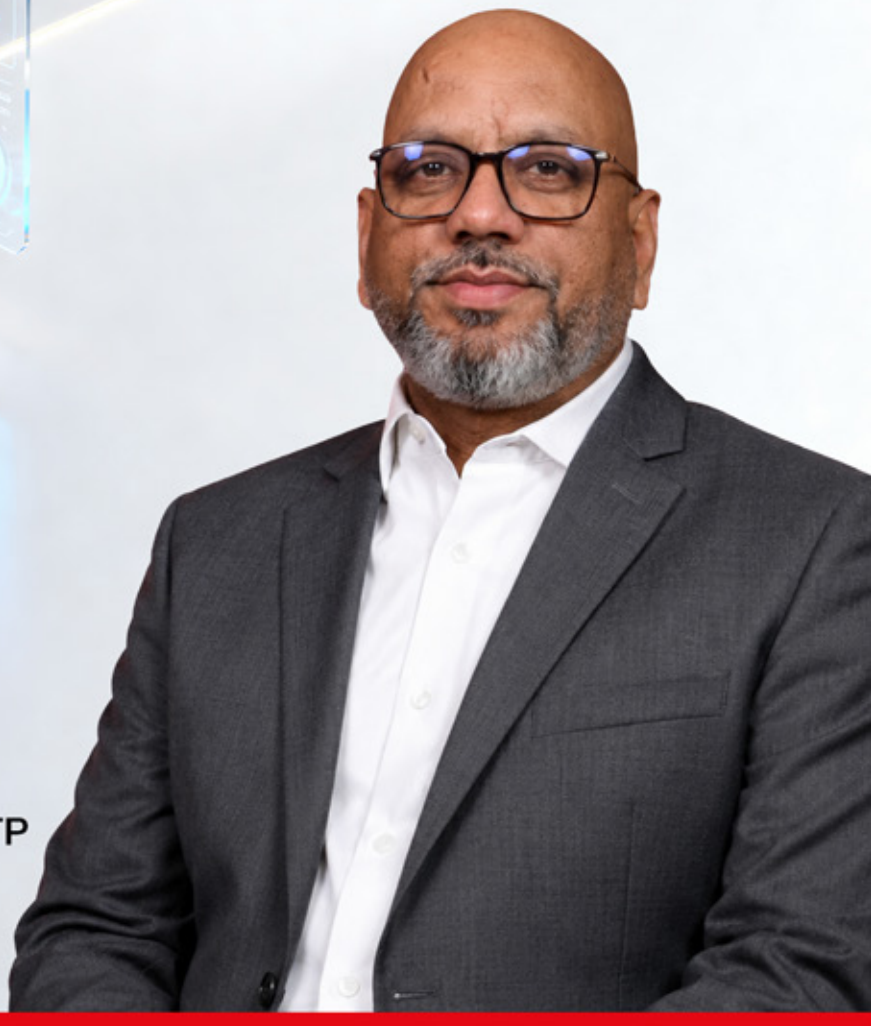
INFOSECTRAIN
Educate. Excel. Empower.

EXAM INCLUDED

PRACTICAL
CISO TRAINING
& READINESS PROGRAM



Instructor

RAHUL

25+ Years of Experience

vCISO | CISSP | CIPM | CISM | CITP
ISO 27701 | ISO 27001 | MIET
CMGR | MCMI | MIET | MBCS

INFOSECTRAIN

Course Highlights

- **32-Hour LIVE** Instructor-Led CISO Leadership Program
- **Hands-On** Learning with Case Studies & Scenarios
- Practical Risk Assessments & Internal Audit Plan
- Building KPI & Performance Framework
- Writing Information Security Strategy
- Policy & Process Development
- Building Compliance Program
- Connecting Management Expectations
- Learn from CISO Mentor with 25+ Years of Experience

INFOSECTRAIN

About Course

The Practical CISO Training & Readiness Program is a focused 32-hour leadership programme designed for experienced security professionals ready to think, operate and communicate like a Chief Information Security Officer.

Taught by a practising vCISO with 25+ years of GRC and governance experience, the course takes you through the complete CISO lifecycle. From business context mapping, enterprise risk assessment, policy and standards development, to security performance measurement and audit readiness, through real case studies and scenarios.

You won't just learn what a CISO does; you'll build the actual artifacts one needs: a requirement register, risk methodology, policy framework, KPI dashboard and continual improvement roadmap, all aligned to ISO/IEC 27001:2022 and NIST CSF 2.0.

Course Objectives

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

- Build and lead an enterprise information security program aligned to business strategy
- Conduct enterprise-wide risk assessments and design structured mitigation frameworks
- Develop and maintain security policies, standards and procedures from scratch
- Establish governance structures aligned to ISO/IEC 27001:2022 and NIST CSF 2.0
- Define KPIs and security metrics that demonstrate program value to executive leadership
- Communicate risk, priorities and security decisions confidently to C-suite and board
- Drive audit readiness through documented governance reviews and internal audit schedules
- Identify, assign and track corrective actions tied to audit findings and incidents
- Build a cybersecurity culture of accountability and awareness across all business units
- Walk away with real CISO-grade artifacts you can deploy in your organisation immediately

INFOSECTRAIN

Target Audience

This program is ideal for professionals responsible for building, managing, or governing enterprise-wide information security programs, including:

Management & Governance Roles

- IT Director / IT Manager
- Information Security Manager
- Risk & Compliance Manager
- Business Continuity / Resilience Manager
- Data Protection Officer (DPO)
- IT Governance, Risk, and Compliance (GRC) Specialist
- Internal / IT Auditor

Technical & Implementation Roles

- Security Systems Engineer
- Security Architect
- Network Architect
- Cloud Security Engineer
- Enterprise Security Consultant
- IS / IT Consultant
- Security Operations (SOC) Lead
- Security Analyst / Senior Analyst

Emerging & Advisory Roles

- Cybersecurity Program Manager
- Security Policy / Framework Specialist
- Audit & Assurance Professional
- Privacy & Data Governance Consultant
- IT Strategy and Transformation Leader

Pre-requisites

This program is designed for experienced IT and security professionals aiming to advance into enterprise-level information security leadership roles.

Participants should ideally have:

- **3–5 years of cumulative experience** in information security, risk management, IT governance, or related domains.
- A **foundational understanding of security concepts, frameworks, and compliance standards** such as ISO/IEC 27001, NIST CSF, and NIST SP 800-53.
- Prior exposure to **security operations or audit** will be an advantage.
- While formal certifications like **CISSP, CISM, or ISO/IEC 27001 LI/LA** are not mandatory, familiarity with their principles will significantly enhance learning outcomes.

INFOSECTRAIN

Exam Details

Certification Body	InfosecTrain
Exam Format	Multiple-choice Questions and Scenario-based Questions
Number of Questions	40 Questions
Exam Duration	60 Minutes
Exam Language	English
Passing Score	70%
Testing Mode	Online

INFOSECTRAIN

Our Industry Expert Instructor

RAHUL

25+ Years of Experience

vCISO | CISSP | CIPM | CISM
ISO 27701 | CMGR | MCMI | MIET
MBCS | CITP | ISO 27001

- Rahul brings over 25+ years of global experience in information security, data privacy, and business continuity management across diverse industries.
- Currently works as a principal consultant, delivering GRC implementations, managed services (vCISO/vDPO), and audit assessments based on global standards.
- Successfully built and operated integrated GRC programs across 40+ global sites in hybrid product and services organizations.
- Former global head and regional lead for InfoSec, data privacy, and BCM in top-tier digital transformation and software service firms.
- Expert in implementing and managing frameworks like ISO/IEC 27001, 27701, 27018, 22301, 31000; NIST CSF, SP 800-53; PCI-DSS; SOC 2; HIPAA; GDPR; PDPPL.
- Played a key role in establishing enterprise-wide application security frameworks tailored to hybrid environments.
- Led successful security integrations during complex mergers involving both product- and service-based organizations.

INFOSECTRAIN

Course Content

Domain 1 : Business Understanding and Stakeholder Engagement

Case Study

Define the context of the organization and a comprehensive list of information security requirements

- Conduct a thorough review of the organization's business model, strategic objectives, and operational landscape.
- Identify and document client-specific information security and compliance requirements.
- Assess all applicable legal, regulatory, and contractual obligations related to information security.
- Engage with executive leadership to understand corporate vision, mission, and long-term strategic priorities.
- Collaborate with IT and application management teams to review current technology strategies, infrastructure, and planned initiatives.
- Meet with business unit leaders to capture their specific goals, operational challenges, and security expectations.
- Coordinate with support function leaders such as HR, Finance, Facilities, and Procurement to understand their processes, operational challenges, and control needs.

Domain 2 : Current State Assessment and Risk Management

Case Study

Develop a risk assessment methodology and conduct the risk assessment of your organization or the given case study.

- Schedule walkthrough sessions and review meetings across business and support functions to assess existing security practices, tools, and controls.
- Perform a comprehensive enterprise-wide risk assessment to identify threats, vulnerabilities, and potential impacts.
- Present the risk assessment findings to executive leadership, ensuring clear visibility into critical risks and resource implications.
- Collaborate with respective process owners and managers to develop, assign, and implement risk treatment and mitigation plans.

Domain 3 : Develop Policies, Processes, and Plans

Case Study

Develop information security policies aligned with business objectives and addressing identified risks.

- Review existing information security policies, standards, and procedures; update or develop new ones to ensure alignment with the organization's needs, recognized frameworks, and best practices.
- Develop a comprehensive information security plan to implement and operate enterprise information security program.

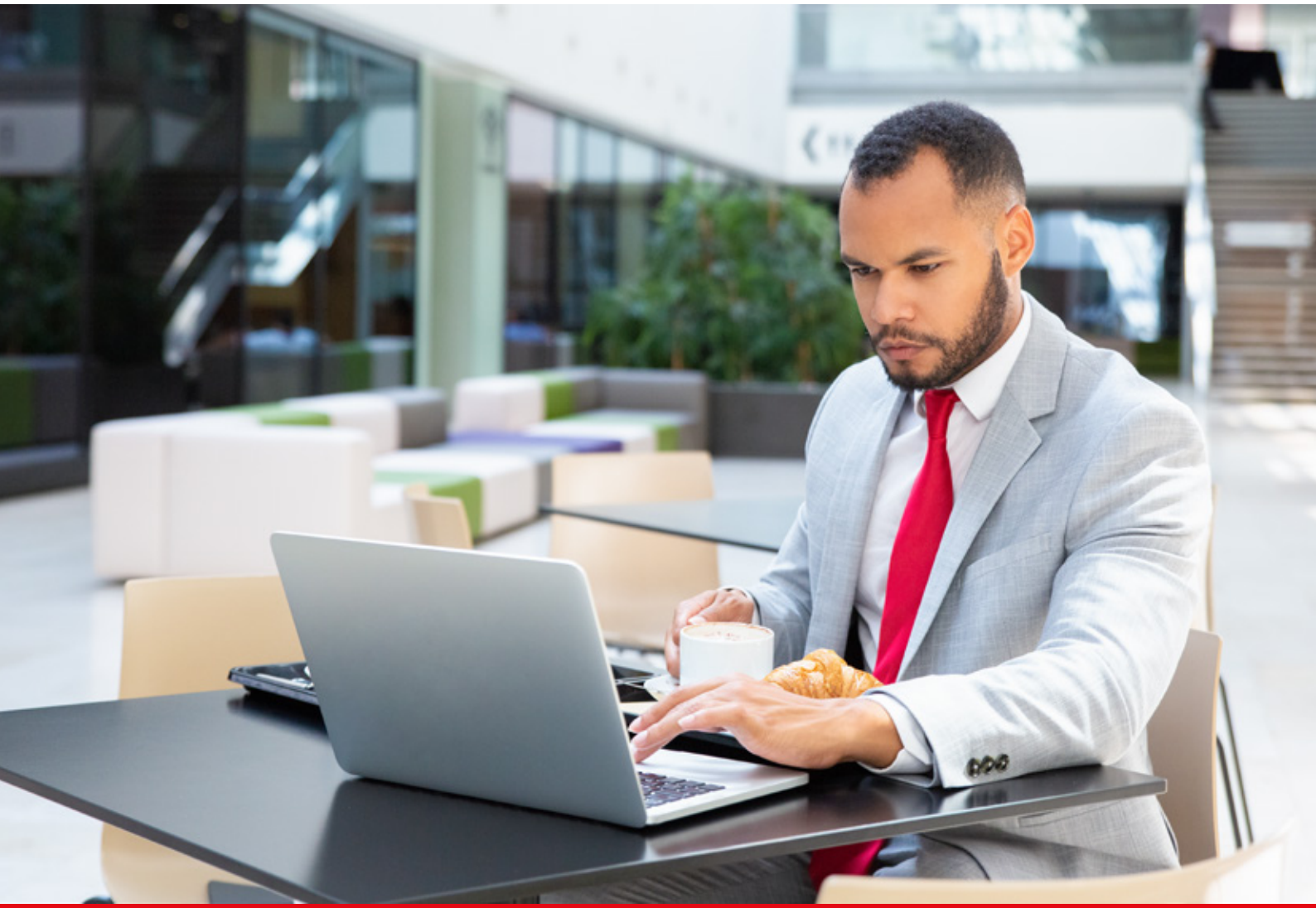
Domain 4 : Performance Evaluation, Monitoring, and Continuous Improvement

Case Study

Develop an information security performance evaluation framework to identify improvement areas for continual improvement.

- Identify data points and define measurable Key Performance Indicators (KPIs) to monitor program effectiveness and demonstrate continual improvement.
- Establish an internal audit and review schedule to verify compliance with policies and assess control effectiveness.
- Identify, document, and implement corrective actions and improvement initiatives based on audit findings, incidents, and evolving business needs to ensure continuous improvement.

INFOSECTRAIN
Educate. Excel. Empower.



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on