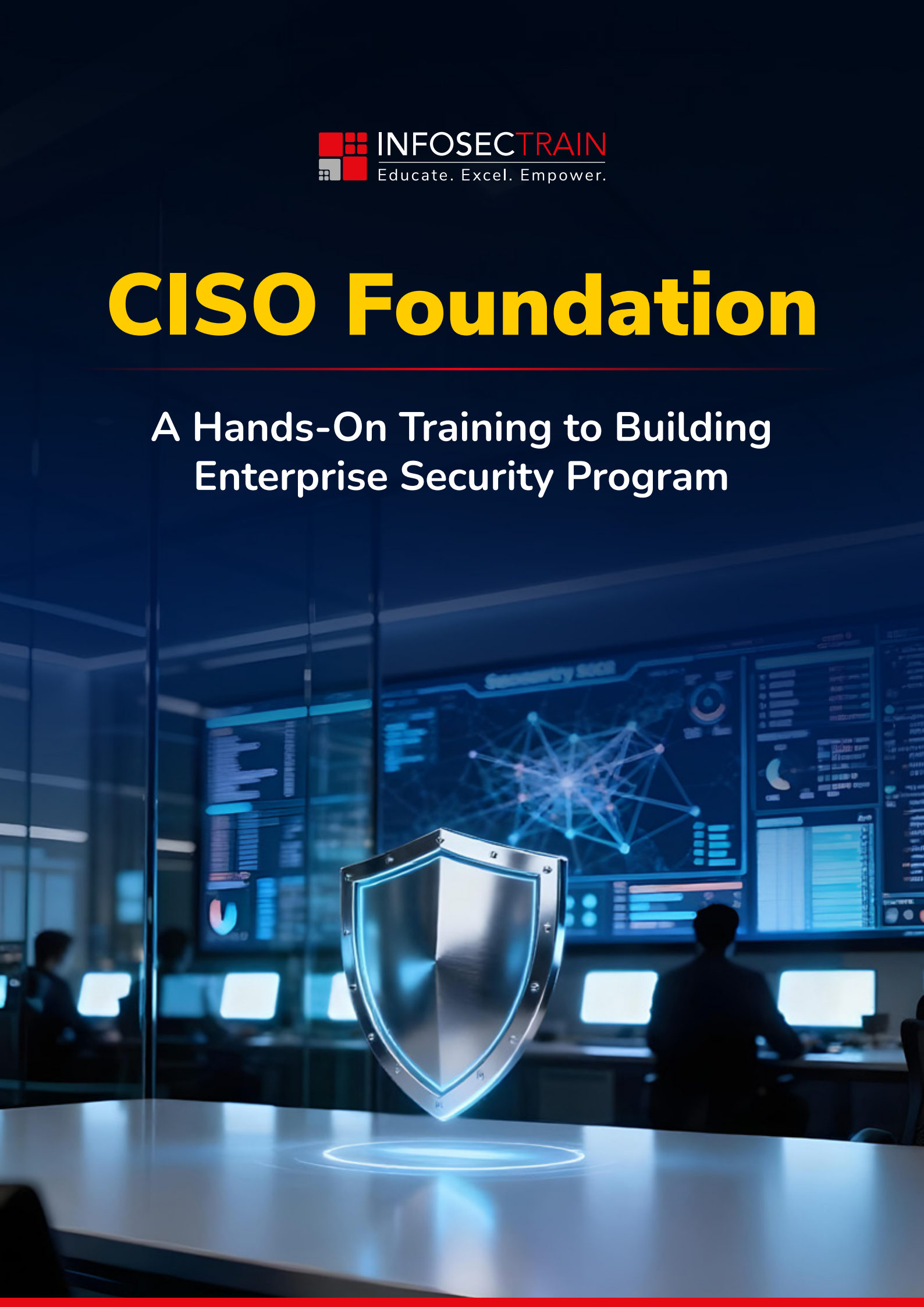
INFOSECTRAIN
Educate. Excel. Empower.

CISO Foundation

A Hands-On Training to Building Enterprise Security Program



INFOSECTRAIN

Course Highlights

32-Hour LIVE
Instructor-Led Training
(Workshop)

Hands-On
Learning

Practical
Implementation

Policy
Development

Highly Interactive
& Dynamic
Sessions

Certified Expert
with **24+ Years**
of Experience

Dedicated
Telegram Support
Group

Access to **Recorded**
Sessions

Career Guidance &
Mentorship

INFOSECTRAIN

About Course

The **Enterprise Information Security Program** takes participants through the full lifecycle of building and sustaining an enterprise information security program, from business alignment and risk assessment to governance, audit, and continuous improvement. Through real-world examples and case-driven exercises, participants learn how to assess current security posture, identify compliance gaps, and design scalable policies that align with global standards such as ISO/IEC 27001:2022 and NIST CSF 2.0. Whether you're developing a new security roadmap or refining an existing one, this program provides the tools, methodologies, and leadership mindset to build resilient, compliant, and adaptive enterprise security frameworks.

Course Objectives

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

- Develop and implement an enterprise information security program aligned with organizational goals and regulatory requirements.
- Conduct enterprise-wide risk assessments and design robust mitigation and monitoring frameworks.
- Establish and maintain governance structures such as ISO/IEC 27001 and NIST CSF.
- Create and update information security policies, procedures, and standards tailored to business and compliance needs.
- Define and track security performance metrics for continuous improvement and reporting to leadership.
- Strengthen stakeholder engagement and executive communication for effective security decision-making.
- Drive organizational readiness and audit preparedness through documented processes and governance reviews.
- Promote a culture of cybersecurity awareness, accountability, and continuous improvement across all business units.

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** is recommended.
- 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

Our Expert Instructor

RAHUL

24+ Years of Experience

Principal Consultant – GRC

CMGR | MCMI | MIET | MBCS

CITP | CISSP | CIPM | CISM

Rahul is a seasoned GRC and cybersecurity consultant with over 24 years of experience in information security, data privacy, and business continuity. He holds prestigious designations as a Chartered Manager (CMI, UK) and Chartered IT Professional (BCS, UK). Rahul has successfully implemented, operated, and audited global governance frameworks and ISO standards across complex hybrid organizations. With experience as a vCISO, vDPO, and global head of information security, he specializes in aligning process and technology controls with business goals, driving compliance, and managing secure enterprise transformations.

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.

INFOSECTRAIN

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 information security controls.

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.

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on