Certified Information Systems Security Professional (CISSP®)

Certification Training

CISSP®

TRUSTED

decabyte

Certified Information Systems Security Professional (CISSP®) Training **Overview**

The CISSP (Certified Information Systems Security Professional) certification is a globally recognized credential for cybersecurity professionals, validating their expertise in designing, implementing, and managing cybersecurity programs. This comprehensive training is designed to equip learners with in-depth knowledge of security principles, risk management, cryptography, network security, and more. By the end of this course, participants will be well-prepared to take the CISSP certification exam and advance their careers in cybersecurity.

Who Should Enroll?

⭐
Security Analysts
Professionals responsible for designing

⭐
Cybersecurity Consultants
Experts providing security assessments & compliance.

⭐
Penetration Testers
Professionals identifying security vulnerabilities.

⭐
IT Auditors
Those responsible for compliance with security.

How this Program Works Differently with Highlighted **Key Solutions** ?

Live Instructor-Led Sessions
Interactive classes with expert trainers.

Dedicated Q&A Sessions
Get your doubts cleared in live sessions.

Hands-on Labs
Gain practical experience through real-time projects.

Exam-Oriented Training
Covers the Exam objectives in detail.

Lifetime Access
Recorded Sessions. Revisit concepts anytime, anywhere.

Study Materials & Resources
Access to e-books, practice questions, and video tutorials.

Certification Prep
Industry-Recognized skills that top employers demand.

Career Pathways

With CISSP® certification, you can pursue roles such as:

- Security Analyst
- Cybersecurity Consultant
- Security Architect
- Chief Information Security Officer (CISO)
- Penetration Tester
- Risk and Compliance Manager

Additionally, **CISSP** serves as a foundation for advanced certifications like **CISM, CRISC, and CCISO.**
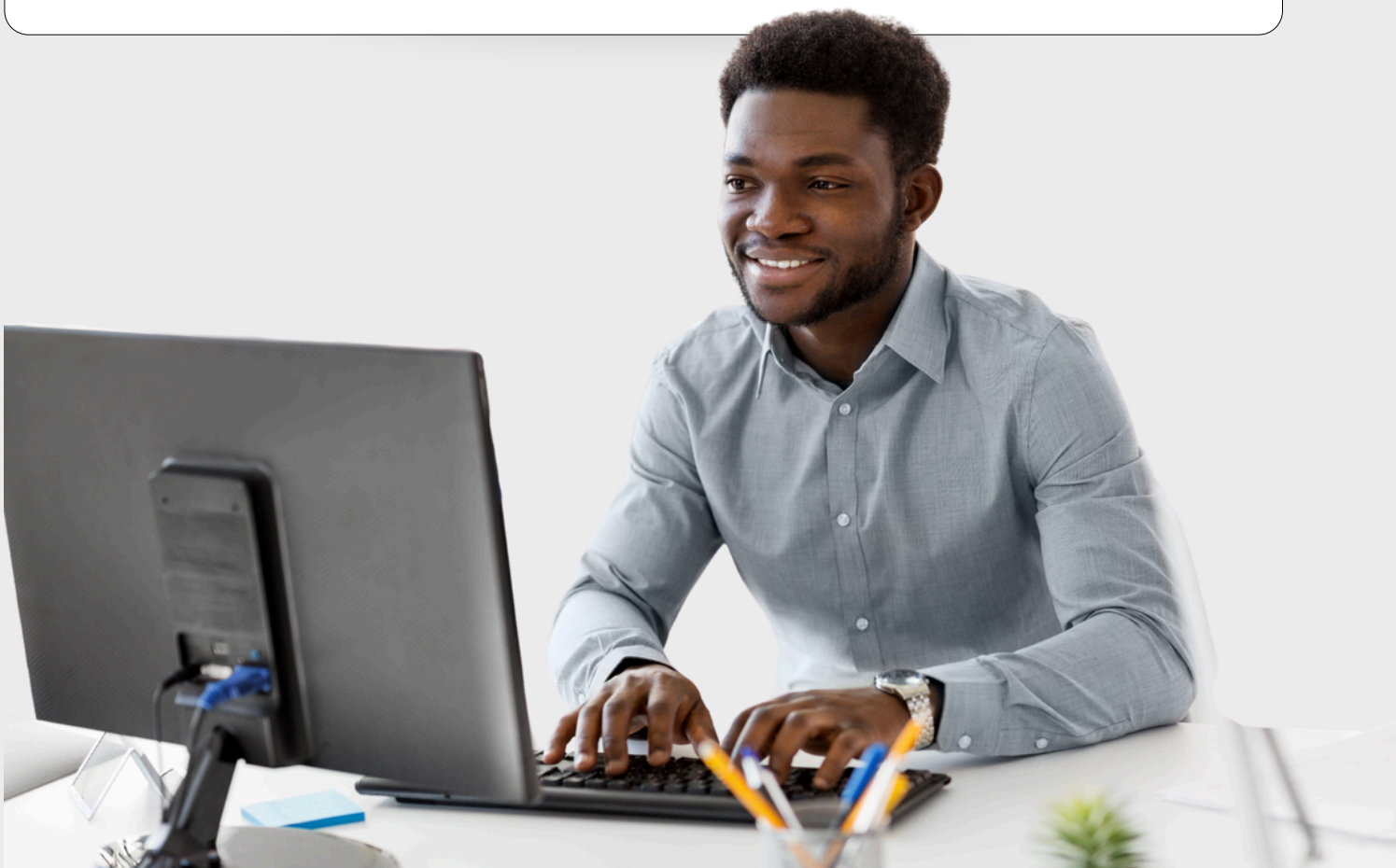
Power-Packed **Curriculum**

Module 01 : **Security and Risk Management**

- Security governance, risk management, and compliance.
- Legal, regulatory, and ethical considerations.
- Business continuity and disaster recovery planning.

Module 02 : **Asset Security**

- Data classification, ownership, and lifecycle management.
- Data protection techniques and encryption.
- Compliance with privacy regulations and secure data handling.

Module 03 : **Security Architecture and Engineering**

- Security models, frameworks, and system architecture.
- Cryptography principles and secure design concepts.
- Security controls for hardware, software, and cloud.

Module 04 : **Communication and Network Security**

- Network architecture, security protocols, and segmentation.
- Secure network components, VPNs, and wireless security.
- Threat mitigation strategies and network monitoring.

Power-Packed **Curriculum**

Module 05 : **Identity and Access Management (IAM)**

- Authentication, authorization, and identity management
- Role-based access control and Single Sign-On (SSO).
- Privileged access management and identity federation.

Module 06 : **Security Assessment and Testing**

- Security testing methodologies and evaluation techniques.
- Vulnerability assessments, penetration testing, and threat modeling.
- Security audits, compliance testing, and risk assessments.

Module 07 : **Security Operations**

- Incident detection, response, and digital forensics.
- Security monitoring, logging, and SIEM implementation.
- Disaster recovery, business continuity, and crisis management.

Module 08 : **Software Development Security**

- Secure coding practices and secure software development lifecycle (SDLC).
- Application security vulnerabilities and threat mitigation.
- DevSecOps principles and security testing in software development.

How **Schedule** and **Commitments** will work?

Course Duration
8 Weeks

Live Classes
3 Sessions per Week (2 Hours per Session)

Recordings Available
Yes, lifetime access

Practice Assignments
Weekly hands-on tasks

Doubt-Solving Sessions
Dedicated Q&A sessions

Support You'll Receive:

24/7 Learner Support

Doubt-Solving Forums

Mock Exams & Interview Prep

Community Access

Why Choose CISSP® Training with Decabyte?

Industry Experts as Trainers : Learn from certified professionals.

Practical Learning Approach : Hands-on labs and real-world case studies.

Flexible Learning : Live & self-paced options for all learning styles.

Exam-Focused Preparation : Tailored course material to maximize your success.

Career Support & Guidance : Resume building, interview prep, and job placement assistance.

Upon **Completing** the Program, You'll **Receive**:

CISSP®

- Decabyte Certified Information Systems Security Professional Certificate
- Portfolio-ready projects and access to career advancement resources

CERTIFICATE
OF COMPLETION

This certificate is proudly presented to

Adam Reeds

For successfully completing the training on August 20, 2024, congratulations on your achievement!

CERTIFIED

Akash kumar
AKASH KUMAR
Founder of Decabyte

CISSP®

CERTIFICATE ID: FEB04001

⭐ **4.9 Average Rating**

💼 **3500+ Students Got Job**

🛡️ **4000+ Satisfied Learners**

🏅 **100+ Highly Qualified Trainers**

📞 **+91 98613 63118**

@ *support@decabyte.info*

Certification Exam Information

Name of the Certification	Certified Information Systems Security Professional (CISSP®)
Exam Code	CISSP
Certification Body	(ISC)²
Exam Duration	4 hours
No. of Questions	125–175 (Computer Adaptive Testing - CAT format)
Passing Score	700 out of 1000
Exam Delivery	Pearson VUE Testing Centers & Online Proctored Exam

Prerequisites to Enroll?

- Minimum 5 years of cumulative, paid work experience in at least two of the eight CISSP CBK domains (can be reduced to 4 years with a relevant degree or certification)
- Validity: 3 years (Continuing Professional Education (CPE) credits required for renewal)

What our **Students** say ?
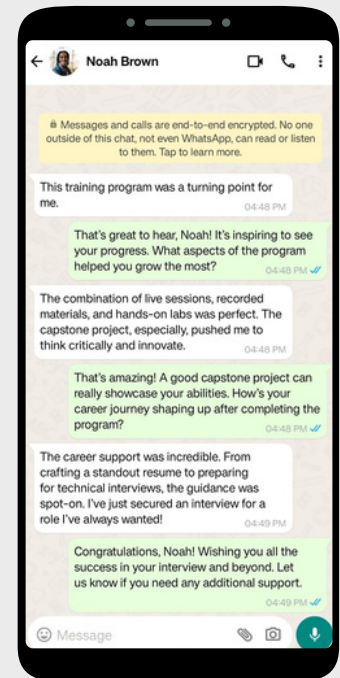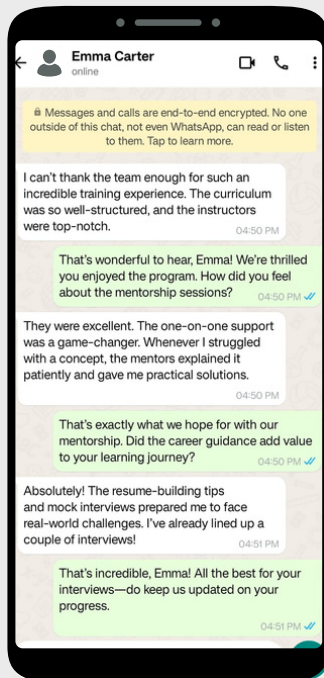
CISSP®
Frequently Asked Questions

? Who should take the CISSP training?

☑ This training is ideal for security professionals, IT managers, risk analysts, network administrators, and anyone pursuing a career in cybersecurity leadership.

? Do I need prior experience for CISSP?

☑ Yes, CISSP requires 5 years of cybersecurity experience, but a relevant certification (e.g., Security+) can waive 1 year.

? Is CISSP difficult to pass?

☑ CISSP is a challenging exam, but with structured training, hands-on labs, and study materials, you can pass it successfully.

? Will I get a certificate after completing the training?

☑ Yes! You will receive a completion certificate and guidance on the official CISSP exam.

? What is the format of the CISSP exam?

☑ The CISSP exam consists of 125–175 multiple-choice and advanced questions in a 4-hour adaptive test format.

? Does this course include hands-on labs?

☑ Yes, we provide practical exercises, case studies, and real-world security scenarios.

? What if I miss a class?

☑ You will have lifetime access to recorded sessions and study materials.

? What is the salary of a CISSP-certified professional?

☑ CISSP professionals earn between $90,000 - $150,000 annually, depending on experience and location.

? How can I enroll in the training?

☑ You can enroll by visiting our website or contacting our support team.

Social Media Handles :

@decabyteofficial

Decabyte

Ask Your Queries to Our Experts?

📞 +91 98613 63118
+91 62691 76510

@ support@decabyte.info