

CISSP Official ISC² Bootcamp — Syllabus

Instructor: Omri Sagron, CISSP — ISC² Authorized Instructor

Format: Live Online — 10 Sessions × 4 Hours (40 Hours Total)

Accreditation: Aligned with ISC² CISSP CBK, 7th Edition

Course Description

This intensive bootcamp prepares learners for the **Certified Information Systems Security Professional (CISSP)** certification from ISC². The program explores all eight CISSP Common Body of Knowledge (CBK) domains, combining theoretical foundations with real-world scenarios and leadership-oriented decision making.

Students develop the competencies needed for governance, architecture, risk analysis, incident response, and secure systems engineering. The curriculum is designed to build both technical expertise and strategic thinking capabilities essential for senior-level cybersecurity professionals.

Through interactive sessions, case studies, and simulation exercises, participants gain practical experience applying CISSP concepts to complex organizational challenges. The bootcamp emphasizes critical thinking and the leadership perspective required to succeed on the exam and in executive security roles.



About ISC²

ISC² is the world's leading cybersecurity certification organization, dedicated to inspiring a safe and secure cyber world.

Global Reach

Over 600,000 members and candidates worldwide representing the largest community of certified cybersecurity professionals

Industry Recognition

Globally recognized certifications that set the standard for cybersecurity excellence and professional competence

Professional Standards

Rigorous ethical guidelines and continuing education requirements that maintain the highest professional standards

ISC² Certification Portfolio

Entry to Professional Level

- **CC** — Certified in Cybersecurity (entry-level foundation)
- **CISSP** — Certified Information Systems Security Professional
- **CCSP** — Certified Cloud Security Professional

Advanced & Specialized

- **CISSP-ISSAP** — Information Systems Security Architecture Professional
- **CISSP-ISSEP** — Information Systems Security Engineering Professional
- **CISSP-ISSMP** — Information Systems Security Management Professional
- **CSSLP** — Secure Software Lifecycle Professional
- **CGRC** — Governance, Risk & Compliance

Learn more at <https://www.isc2.org/> and explore all certifications at <https://www.isc2.org/Certifications>

Instructor Bio

Omri Sagron, CISSP


ISC² Authorized Instructor and senior cybersecurity leader with extensive experience in enterprise security architecture, risk management, and security operations. Omri brings real-world expertise from his role as former Chief Technology Officer of Cyber Risk Advisory at BDO Israel, where he led strategic security initiatives for multinational organizations.



His expertise spans governance frameworks, security architecture design, comprehensive risk assessments, SOC and incident response operations, and secure development practices. Omri combines deep technical knowledge with strategic business acumen, preparing students not just for certification but for leadership roles in cybersecurity.

As an ISC² Authorized Instructor, Omri delivers training that emphasizes practical application of CISSP concepts, critical thinking, and the leadership mindset required for senior security positions.

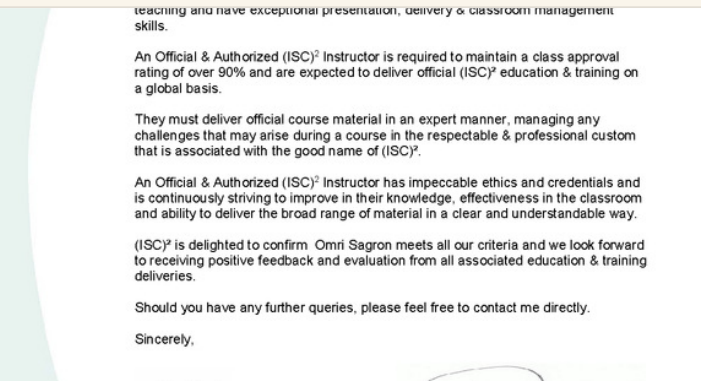
Connect: LinkedIn Profile: <https://www.linkedin.com/in/omri-sagron-cissp-24508331/>



☐ File upload

Official Instructor Certificate–Sagron copy.pdf

279.7 KB



☐ File upload

Authorized Instructor Letter – Sagron copy.pdf

95.2 KB

Course Learning Objectives

By the end of this comprehensive bootcamp, learners will achieve mastery across knowledge, skills, and professional competencies essential for CISSP certification and advanced security roles.

1

Knowledge Mastery

Develop comprehensive understanding of all CISSP CBK topics across eight domains, from foundational security principles to advanced implementation strategies.

- Master governance, compliance, and regulatory frameworks
- Understand security architecture and engineering principles
- Apply identity and access management controls
- Comprehend cryptography, network security, and risk frameworks
- Explain operational security and incident management

2

Practical Skills

Build hands-on capabilities to analyze, design, and implement enterprise security solutions using CISSP reasoning and best practices.

- Analyze complex cybersecurity scenarios using critical thinking
- Design comprehensive enterprise security architectures
- Evaluate vulnerabilities and propose effective mitigations
- Lead incident response operations and security programs
- Conduct risk assessments and develop treatment strategies

3

Professional Competencies

Cultivate the leadership mindset, ethical foundation, and exam readiness required for CISSP certification and senior security roles.

- Apply the ISC² Code of Ethics in real-world scenarios
- Demonstrate readiness for the CISSP CAT examination
- Build a personalized post-course study plan
- Develop leadership and strategic thinking capabilities
- Communicate security concepts to executive stakeholders

Target Audience

This bootcamp is designed for cybersecurity professionals seeking to validate their expertise and advance to senior-level positions through CISSP certification.



Security Engineers & Analysts

Technical professionals implementing security controls, conducting assessments, and protecting organizational assets who want to expand their strategic perspective and leadership capabilities.



SOC & Incident Response Professionals

Security operations center analysts, incident responders, and threat hunters who manage security events, investigate breaches, and coordinate organizational response efforts.



CISSP Certification Candidates

Experienced professionals preparing for the CISSP examination who need comprehensive review, exam strategy guidance, and confidence-building through structured preparation.



IT Leaders & Managers

Managers, directors, and aspiring CISOs responsible for security strategy, team leadership, and aligning security initiatives with business objectives across the enterprise.



GRC Specialists

Governance, risk, and compliance professionals who develop policies, manage frameworks, conduct audits, and ensure regulatory compliance across security programs.



Security Architects

Professionals designing security solutions, defining technical standards, and creating enterprise architecture frameworks who want to formalize their expertise with industry-recognized certification.

Prerequisites

Recommended Background

While not strictly required to attend the bootcamp, the following experience and knowledge will enhance your learning outcomes and exam preparation:

- **Professional Experience:** 3–5 years in IT or information security roles
- **Technical Foundation:** Familiarity with networks, operating systems, and security fundamentals
- **Risk Concepts:** Understanding of basic risk management principles
- **Language Proficiency:** Strong English reading and communication skills

These prerequisites ensure you can fully engage with advanced concepts and participate meaningfully in discussions and exercises.



ISC² Certification Requirements

To earn CISSP certification, ISC² requires:

- **Experience:** Minimum 5 years of cumulative, paid work experience in two or more of the eight CISSP domains
- **Education Waiver:** Four-year college degree or additional credential can satisfy one year of experience
- **Exam:** Pass the CISSP examination
- **Endorsement:** Endorsement by an ISC² certified professional
- **Ethics:** Agree to the ISC² Code of Ethics

Alternative: Associate of ISC² designation available with less than 5 years experience.

Course Structure

10 Sessions × 4 Hours

The bootcamp delivers 40 hours of intensive instruction over 10 comprehensive sessions, each carefully designed to build knowledge progressively while maintaining engagement and maximizing retention.

10

Live Sessions

Interactive online sessions
with real-time instruction
and discussion

40

Total Hours

Comprehensive coverage
of all eight CISSP domains

8

CBK Domains

Complete alignment with
ISC² Common Body of
Knowledge

100+

Practice Questions

Exam-style questions
throughout the course

Learning Methodology

Each session combines multiple teaching approaches to accommodate different learning styles and reinforce critical concepts. Expect interactive lectures, case study analysis, group discussions, hands-on exercises, and practice questions that simulate the actual CISSP examination format.

The curriculum follows a logical progression, starting with foundational governance and risk concepts, moving through technical domains like architecture and network security, and culminating in operational and development security. The final session provides comprehensive exam preparation and readiness assessment.

Session 1 — ISC² & Exam Orientation

Duration: 4 Hours

The opening session establishes the foundation for your CISSP journey, introducing you to ISC² as an organization, the certification landscape, and the specific requirements and structure of the CISSP examination.

Session Topics

- **ISC² Organization:** History, mission, and the global cybersecurity community
- **Certification Portfolio:** Overview of ISC² credentials and career pathways
- **CISSP Exam Deep Dive:** CAT format, question types, scoring methodology, and exam rules
- **Certification Process:** Requirements, endorsement, and maintaining certification
- **VitalSource Platform:** Navigating your official textbook and study resources
- **CISSP Mindset:** How to think like a security leader and manager
- **Diagnostic Assessment:** Sample test to identify knowledge gaps
- **Study Planning:** Creating your personalized preparation roadmap



Understanding the CAT Format

The CISSP uses Computer Adaptive Testing (CAT), which adjusts question difficulty based on your responses. This session demystifies the format and helps you understand how to approach adaptive testing strategically.

By the end of this session, you'll have clarity on the certification journey ahead, understand what makes CISSP questions unique, and begin developing the critical thinking skills needed to succeed.

Session 2 — Domain 1: Security & Risk Management

Duration: 4 Hours

Domain 1 establishes the foundational principles of information security and organizational risk management. This domain represents the strategic and managerial perspective that distinguishes CISSP from purely technical certifications.

01

Security Fundamentals

Confidentiality, Integrity, Availability (CIA) triad and core security principles

02

Governance & Policy

Policies, standards, procedures, and guidelines that guide organizational security

03

Risk Management

Qualitative and quantitative risk analysis methodologies and frameworks

04

Legal & Regulatory

Privacy laws, compliance requirements, and regulatory frameworks worldwide

05

Ethics & Professional Conduct

ISC² Code of Ethics, due care, due diligence, and professional responsibility

06

Business Continuity

BCP fundamentals and organizational resilience concepts

Key Learning Outcomes

Understand how security aligns with business objectives and supports organizational mission. Learn to balance security requirements with operational needs, budget constraints, and stakeholder expectations.

Master risk assessment methodologies including qualitative approaches (risk matrices, expert judgment) and quantitative techniques (ALE, SLE, ARO calculations).

Navigate the complex landscape of legal and regulatory requirements, including GDPR, HIPAA, SOX, PCI DSS, and other compliance frameworks relevant to global organizations.

Develop an understanding of third-party risk management, vendor assessment, and supply chain security considerations essential for modern enterprises.

Session 3 — Domain 2: Asset Security

Duration: 4 Hours

Domain 2 focuses on protecting organizational assets throughout their lifecycle, from creation through disposal. This domain emphasizes data classification, handling, and the responsibilities of asset owners and custodians.

Classification
Labeling and categorizing information assets based on sensitivity and criticality

Destruction
Secure disposal, sanitization, and data remanence prevention



Storage

Secure storage mechanisms and access controls for data at rest

Use & Sharing

Controlled access and secure transmission of information assets

Retention

Archival policies and compliance with retention requirements

Core Concepts

Information Classification

Learn to develop and implement classification schemes appropriate for government, military, commercial, and private sector organizations. Understand sensitivity labels like Top Secret, Secret, Confidential, Unclassified or Confidential, Private, Sensitive, Public.

Ownership & Stewardship

Distinguish between data owners (who determine classification), data custodians (who implement controls), and data processors (who handle information on behalf of others).

Data Lifecycle Management

Master techniques for protecting data at every stage, including encryption at rest and in transit, secure backup and recovery, and proper decommissioning procedures.

Privacy & Compliance

Address privacy requirements including data minimization, purpose limitation, consent management, and cross-border data transfer restrictions under various regulatory regimes.

Data Sanitization Methods

Understand the spectrum of sanitization techniques: clearing (logical deletion), purging (overwriting or degaussing), and physical destruction. Learn when each method is appropriate based on media type and classification level.

Session 4 — Domain 3: Security Architecture & Engineering

Duration: 4 Hours

Domain 3 covers the design and implementation of secure systems, from foundational security models to modern cloud and IoT architectures. This technical domain requires understanding how security principles translate into practical system design.



Secure Design Principles

Defense in depth, least privilege, separation of duties, fail-secure, and other foundational design concepts



Security Models

Bell-LaPadula (confidentiality), Biba (integrity), Clark-Wilson, Chinese Wall, and other formal models



Evaluation Frameworks

Common Criteria (ISO 15408), FIPS 140-2/3, and security evaluation assurance levels



System Security

Hardware security (TPM, HSM), firmware protection, and operating system hardening techniques



Cloud & Virtualization

IaaS/PaaS/SaaS security, hypervisor protection, container security, and cloud-specific threats



Cryptography Fundamentals

Symmetric vs. asymmetric encryption, hashing, digital signatures, PKI, and cryptographic protocols

Emerging Technologies

Explore security considerations for Internet of Things (IoT) devices, Operational Technology (OT) and Industrial Control Systems (ICS), embedded systems, and convergence of IT and OT environments. Understand the unique challenges these technologies present, including limited computing resources, long operational lifecycles, and safety-critical requirements.

This session bridges theoretical security models with practical implementation challenges, preparing you to design architectures that are both secure and operationally feasible.

Session 5 — Domain 4: Communication & Network Security

Duration: 4 Hours

Domain 4 addresses network architecture, transmission methods, and security controls for protecting data in motion. Understanding network security is essential for designing secure communications and defending against network-based attacks.



Network Fundamentals

OSI model, TCP/IP stack, protocols, and network topologies



Network Threats

Attacks, vulnerabilities, and exploitation techniques



Security Controls

Firewalls, IDS/IPS, segmentation, and defensive architecture



Secure Protocols

TLS, IPsec, SSH, and encrypted communications

Detailed Coverage

Network Defense Architecture

- **Firewalls:** Packet filtering, stateful inspection, application-layer, and next-generation firewalls
- **IDS/IPS:** Signature-based vs. anomaly-based detection, deployment models, and tuning
- **Network Segmentation:** VLANs, DMZs, zero trust architecture, and microsegmentation
- **Network Access Control:** 802.1X, NAC solutions, and endpoint compliance enforcement

Wireless & Remote Access

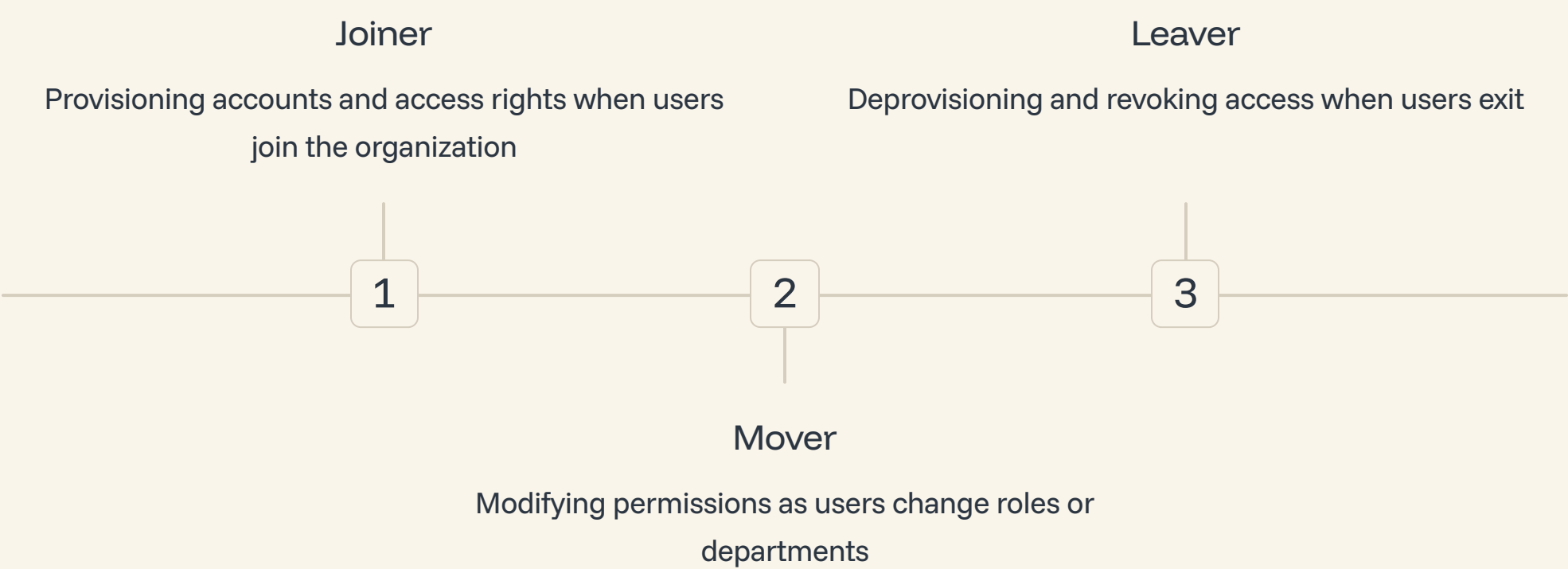
- **Wireless Security:** WPA2/WPA3, EAP methods, rogue AP detection, and WIPS
- **VPN Technologies:** Site-to-site and remote access VPNs, IPsec vs. SSL/TLS VPN
- **Tunneling Protocols:** GRE, L2TP, SSH tunneling, and secure transport mechanisms
- **Remote Access Security:** Authentication, authorization, and monitoring of remote connections

Master common network attacks including man-in-the-middle, session hijacking, DNS poisoning, ARP spoofing, DDoS, and packet sniffing. Understand both the attack vectors and the defensive countermeasures required to mitigate these threats in enterprise environments.

Session 6 — Domain 5: Identity & Access Management

Duration: 4 Hours

Domain 5 focuses on controlling who can access resources and what actions they can perform. Effective IAM is fundamental to implementing least privilege, separation of duties, and need-to-know principles across the organization.



IAM Core Components

<h3>Authentication</h3> <p>Verifying identity through something you know (passwords), something you have (tokens), or something you are (biometrics). Multi-factor authentication (MFA) combines multiple factors for stronger assurance.</p> <ul style="list-style-type: none">• Password policies and management• Biometric authentication methods• Hardware and software tokens• Adaptive authentication and risk-based access	<h3>Authorization</h3> <p>Determining what authenticated users can access and do. Authorization models include Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC).</p> <ul style="list-style-type: none">• RBAC role design and management• ABAC policy definition• MAC security labels and clearances• DAC ownership and permissions	<h3>Accountability</h3> <p>Logging and auditing user activities to ensure traceability and enable forensic investigation. Accountability requires robust audit trails and regular review of access patterns.</p> <ul style="list-style-type: none">• Audit logging and SIEM integration• Access review and recertification• Session monitoring and recording• Privileged activity auditing
--	---	---

Federation & Modern IAM

Single Sign-On (SSO): Enable users to authenticate once and access multiple systems. Learn about SAML, OAuth 2.0, OpenID Connect (OIDC), and federation architectures that support SSO across organizational boundaries.

Privileged Access Management (PAM): Special controls for administrative and high-risk accounts, including credential vaulting, session management, just-in-time access, and privileged session monitoring.

Identity Governance: Automated lifecycle management, access certification campaigns, separation of duties enforcement, and analytics to detect inappropriate access patterns or privilege creep.

Zero Trust Principles: Never trust, always verify. Continuous authentication, least privilege access, microsegmentation, and assuming breach as the foundation of modern identity security.

Session 7 — Domain 6: Security Assessment & Testing

Duration: 4 Hours

Domain 6 covers methods for evaluating security posture, identifying vulnerabilities, and validating that controls function as intended. Regular assessment and testing are essential for maintaining effective security programs.



Security Audits

Comprehensive evaluations of security controls, policies, and procedures against established standards and frameworks. Audits provide assurance to stakeholders and identify gaps requiring remediation.



Application Security Testing

SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), IAST (Interactive), and SCA (Software Composition Analysis) for identifying code vulnerabilities.



Penetration Testing

Authorized simulated attacks to identify exploitable vulnerabilities. Learn the pentesting lifecycle: planning, reconnaissance, scanning, exploitation, reporting, and remediation verification.



Vulnerability Scanning

Automated tools to identify known vulnerabilities in systems, networks, and applications. Understand scanning methodologies, false positive management, and prioritization of remediation efforts.

Testing Methodologies

Types of Testing

- **White Box:** Full knowledge of systems and architecture
- **Black Box:** No prior knowledge, simulating external attacker
- **Gray Box:** Partial knowledge, simulating insider threat

Each approach provides different perspectives and reveals unique vulnerabilities. Comprehensive programs incorporate multiple testing types.

Business Continuity Testing

- **Tabletop Exercises:** Discussion-based scenario walkthrough
- **Functional Tests:** Testing specific systems or processes
- **Full Interruption:** Complete failover to disaster recovery site

Regular BCP/DR testing validates recovery capabilities and identifies gaps before actual disasters occur.

Metrics & Monitoring

Establish Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to measure security program effectiveness. Learn to implement continuous monitoring through logging, SIEM platforms, and security analytics. Develop dashboards and reports that communicate security posture to technical teams and executive stakeholders.

Session 8 — Domain 7: Security Operations

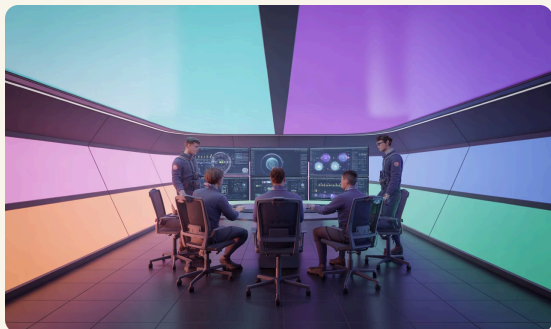
Duration: 4 Hours

Domain 7 addresses the day-to-day activities required to maintain security posture, respond to incidents, and support business operations. Operational security requires balancing protective measures with organizational productivity and user experience.



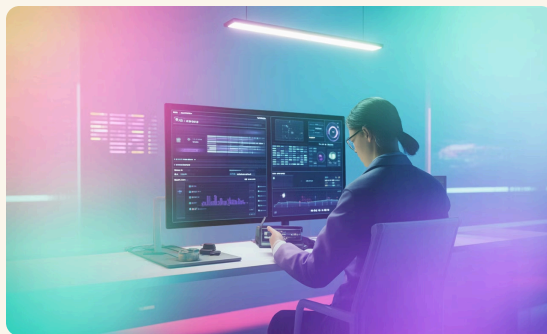
Incident Response

Structured approach to handling security events following the NIST SP 800-61 framework: Preparation, Detection & Analysis, Containment/Eradication/Recovery, and Post-Incident Activity.



Digital Forensics

Scientific collection, preservation, analysis, and presentation of digital evidence. Learn forensic principles including chain of custody, evidence integrity, proper acquisition techniques, and legal considerations.



Security Monitoring

SIEM operations, log management, correlation rules, threat intelligence integration, and security analytics. Effective monitoring requires proper log collection, normalization, and analysis to detect anomalies and threats.



Operational Security Topics

1 Change & Configuration Management

Controlling changes to systems, applications, and infrastructure through formal processes. Configuration management ensures systems remain in approved secure states and deviations are detected and corrected.

2 Malware Defense

Understanding malware types (viruses, worms, trojans, ransomware, rootkits), detection mechanisms (signature-based, heuristic, behavioral), and defensive strategies including endpoint protection and egress filtering.

3 Insider Threat Programs

Detecting and mitigating threats from trusted insiders. Learn indicators of insider risk, monitoring techniques that respect privacy, and response procedures for insider incidents.

4 Physical Security Integration

Physical access controls, environmental security, surveillance systems, and the intersection of physical and logical security in comprehensive protection programs.

Business Continuity Operations

Operational aspects of BCP and disaster recovery including emergency response procedures, crisis management, backup and restore operations, alternate site management, and coordination with business units during disruptions. Understand the operational cadence of testing, maintenance, and continuous improvement of continuity capabilities.

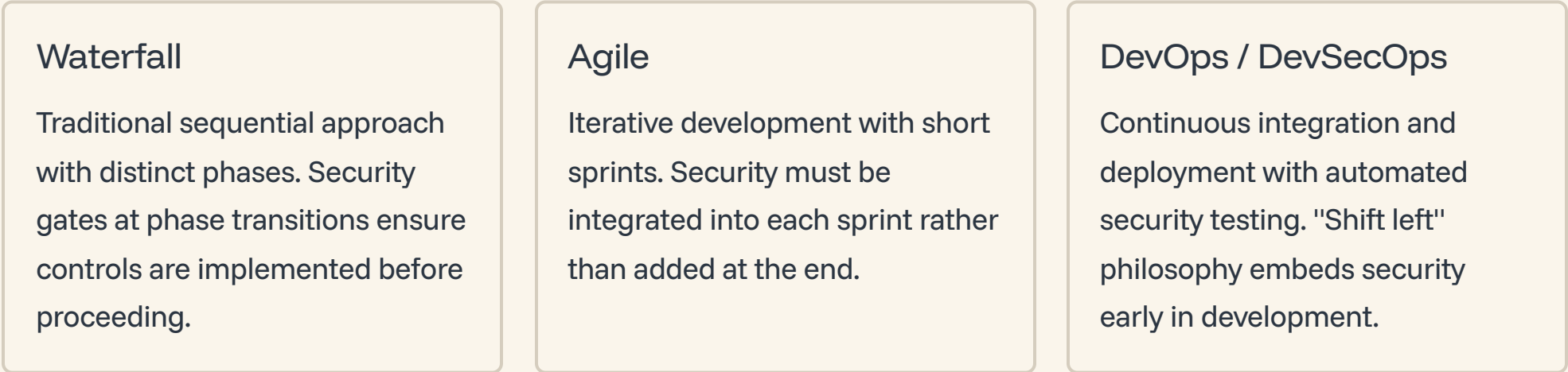
Session 9 — Domain 8: Software Development Security

Duration: 4 Hours

Domain 8 focuses on integrating security throughout the software development lifecycle. As organizations increasingly depend on custom applications, securing the development process is critical to preventing vulnerabilities from being introduced into production systems.



Development Methodologies



Application Security

Secure Coding Principles

- Input validation and output encoding
- Parameterized queries to prevent injection
- Proper authentication and session management
- Cryptographic best practices
- Error handling that doesn't leak information
- Secure defaults and fail-safe mechanisms

Common Vulnerabilities

- OWASP Top 10 web application risks
- SQL injection and command injection
- Cross-site scripting (XSS) and CSRF
- Broken authentication and session management
- Security misconfigurations
- Insecure deserialization

API & Database Security

Secure API design including authentication, authorization, rate limiting, and input validation. Database security controls including encryption, access controls, monitoring, and protection against SQL injection. Learn about API security frameworks like OAuth 2.0 and API gateways for centralized security enforcement.

Explore software maturity models including OWASP SAMM (Software Assurance Maturity Model) and BSIMM (Building Security In Maturity Model) for assessing and improving organizational software security practices.

Session 10 — Final Exam Strategy

Duration: 4 Hours

The final session prepares you for exam day success through strategic test-taking techniques, comprehensive simulation, and personalized study planning. This session transforms your knowledge into exam performance.



CISSP Question Characteristics



The CISSP Mindset

CISSP questions test managerial judgment, not just technical knowledge. When faced with multiple "correct" answers, choose the response that reflects **best practices, organizational perspective, and risk management** rather than purely technical solutions. Think like a CISO, not a technician.

Common Question Traps

- All answers seem correct — choose the BEST answer
- Technical vs. managerial perspective confusion
- Assuming organizational context not stated in question
- Overthinking questions and adding assumptions
- Confusing similar concepts (authentication vs. authorization)

Elimination Strategies

- Remove obviously wrong answers first
- Eliminate answers that are too specific or absolute
- Identify answers that conflict with fundamental principles
- Look for the answer addressing root cause, not symptoms
- Choose comprehensive solutions over partial fixes

Next Steps After Bootcamp

Receive guidance on ISC² endorsement process, continuing professional education (CPE) requirements, and maintaining your CISSP certification. Understand the timeline from passing the exam through receiving your credential, and learn how to maximize the career value of your CISSP certification.

Assessments

The bootcamp employs a comprehensive assessment strategy that combines formative evaluation throughout the course with summative assessment at the conclusion. This multi-faceted approach ensures continuous learning while building confidence for the actual CISSP examination.



Formative Assessments

Continuous evaluation throughout the bootcamp to monitor progress, reinforce learning, and identify knowledge gaps early for timely intervention.

- **Weekly Domain Quizzes:** Short assessments after each domain to reinforce key concepts
- **Case Study Discussions:** Real-world scenarios requiring application of CISSP concepts
- **Breakout Activities:** Small group exercises and collaborative problem-solving
- **Diagnostic Assessments:** Initial testing to establish baseline and tailor instruction



Summative Assessments

Comprehensive evaluation at course conclusion measuring overall mastery and exam readiness, providing confidence for the actual CISSP examination.

- **Final Simulation Exam:** Comprehensive practice test simulating actual CISSP CAT format
- **Domain Proficiency Analysis:** Detailed breakdown of strengths and weaknesses by domain
- **Personalized Study Plan:** Custom post-course roadmap based on assessment results
- **Readiness Evaluation:** Determination of exam preparedness and recommended study duration

Assessment Philosophy

Assessments are designed not just to evaluate knowledge, but to prepare you for the unique format and reasoning required by CISSP questions. Each quiz and practice question exposes you to the managerial perspective, scenario-based reasoning, and "best answer" selection that characterizes the actual examination.

Feedback is provided immediately following assessments, with detailed explanations of correct and incorrect answers. This feedback loop accelerates learning and helps you understand not just what the right answer is, but why it's correct according to CISSP reasoning principles.

Required Materials

1	<p>CISSP Official ISC² Textbook</p> <p>Format: VitalSource Digital Edition</p> <p>The official (ISC)² CISSP textbook, aligned with the CISSP Common Body of Knowledge (CBK), 7th Edition. This comprehensive resource covers all eight domains in depth and serves as the authoritative reference for exam preparation.</p> <ul style="list-style-type: none">• Accessible on multiple devices (computer, tablet, smartphone)• Searchable text for quick reference• Note-taking and highlighting capabilities• Aligned with latest exam content outline
2	<p>ISC² Online Portal Access</p> <p>Platform: ISC² Member/Candidate Portal</p> <p>Access to ISC² official resources including practice questions, study tools, candidate forums, and certification tracking. Portal access provides official practice questions written by ISC² that mirror actual exam format and difficulty.</p> <ul style="list-style-type: none">• Official practice question database• Study resources and reference materials• Candidate community and discussion forums• Certification status tracking
3	<p>Technical Requirements</p> <p>Platform: Zoom Video Conferencing</p> <p>Reliable high-speed internet connection and computer capable of running Zoom video conferencing software. Webcam and microphone required for full participation in interactive sessions.</p> <ul style="list-style-type: none">• Minimum 10 Mbps internet connection (25+ Mbps recommended)• Computer with webcam and microphone• Updated Zoom client software• Quiet environment for focused learning

Supplementary Resources

While not required, students often find value in additional study resources such as practice question databases, mobile study apps, and supplementary reference guides. Recommendations for supplementary materials will be provided during the first session based on your learning style and study preferences.



Academic Policies

Attendance Policy

Regular attendance is mandatory for successful completion of this intensive bootcamp. Each session builds upon previous content, and missing sessions creates gaps that are difficult to fill independently.

- **Attendance Required:** Participation in all 10 sessions expected
- **Punctuality:** Sessions begin promptly at scheduled times
- **Make-up Policy:** Recording access available for unavoidable absences
- **Completion Certificate:** Requires attendance at minimum 8 of 10 sessions

Participation Expectations

Active engagement enhances learning for all participants. The bootcamp format emphasizes discussion, case analysis, and collaborative problem-solving rather than passive lecture consumption.

- **Camera On:** Video participation encouraged to maintain engagement
- **Active Discussion:** Contribute to case studies and group exercises
- **Question Asking:** Clarification questions welcomed and encouraged
- **Respectful Environment:** Professional conduct in all interactions

Professional Ethics

ISC² Code of Ethics

All participants must acknowledge and agree to uphold the ISC² Code of Ethics. This code serves as the foundation for professional conduct in the information security field and is a requirement for CISSP certification.

Code of Ethics Canons:

1. Protect society, the common good, necessary public trust and confidence, and the infrastructure
2. Act honorably, honestly, justly, responsibly, and legally
3. Provide diligent and competent service to principals
4. Advance and protect the profession

Learn more: <https://www.isc2.org/Ethics>

Academic Integrity

This bootcamp emphasizes collaborative learning and knowledge sharing. However, all assessment work must represent your own understanding and reasoning. Practice exams and quizzes should be completed individually to accurately assess your exam readiness.

The skills and knowledge you develop in this bootcamp will serve you throughout your cybersecurity career. Shortcuts during learning ultimately limit your professional effectiveness and certification success.

Instructor Contact



Omri Sagron, CISSP

ISC² Authorized Instructor

I'm excited to guide you through your CISSP certification journey. My goal is not just to help you pass the exam, but to develop the strategic thinking and leadership mindset that distinguishes exceptional cybersecurity professionals.

Throughout this bootcamp, I'll share real-world experiences from enterprise security leadership, practical frameworks you can apply in your organizations, and the insights needed to think like a CISO.

Connect with me:

[LinkedIn: Omri Sagron](#)

<https://www.linkedin.com/in/omri-sagron-cissp-24508331/>

“

CISSP certification opens doors, but the journey of learning and professional development never ends. This bootcamp is your foundation — commit to continuous growth, ethical practice, and contributing to a safer cyber world.

”

Questions & Support

Don't hesitate to reach out with questions during the bootcamp or as you prepare for your exam. I'm here to support your success not just during our 10 sessions together, but throughout your certification journey.

I look forward to working with you and celebrating your CISSP achievement. Let's build your expertise, confidence, and readiness to join the elite community of CISSP-certified professionals.

Best of luck on your CISSP journey!