

MGT414: SANS Training Program for CISSP® Certification



GISP
Information Security
Professional
giac.org/gisp

6 Day Program | 52 CPEs | Laptop Not Needed

You Will Be Able To

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

What You Will Receive

- Electronic courseware for each of the eight domains
- 320 questions to test knowledge and preparation for each domain
- MP3 audio files of the complete course lectures

“This course really pulls a lot together for me and it has been hugely valuable. I know parts of this are going to impact my approach to my work from the first day back.”

— Merewyn Boak, Apple

Need training for the CISSP® exam?

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the Certified Information Systems Security Professional (CISSP®) exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

After completing the course, students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:

The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

Course Authors' Statement

“The CISSP® certification has been around for nearly 25 years. The exam is designed to test your understanding of the Common Body of Knowledge, which may be thought of as the universal language of information security professionals. It is often said to be a mile wide and two inches deep. The CISSP® exam covers a lot of theoretical information that is critical for a security professional to understand. However, this material can be dry, and since most students do not see the direct applicability to their jobs, they find it boring. The goal of this course is to bring the eight domains of knowledge of the CISSP® to life. The practical workings of this information can be discovered by explaining important topics with stories, examples, and case studies. We challenge you to attend the SANS CISSP® training course and find the exciting aspect of the eight domains of knowledge!”

—Eric Conrad and Seth Misener

Section Descriptions

SECTION 1: Introduction; Security and Risk Management

In this first section, MGT414 introduces the specific requirements needed to obtain CISSP® certification. The 2021 exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, will be discussed using real-world scenarios to illustrate the critical points.

TOPICS: Introductory Material; Overview of the Eight Domains; Domain 1: Security and Risk Management

SECTION 3: Security Engineering – Part 2; Communication and Network Security

This section continues the discussion of the Security Engineering domain, including a deep dive into cryptography. The focus is on real-world implementation of core cryptographic concepts, including the three types of cryptography: symmetric, asymmetric, and hashing. Quantum cryptography and fault injection attacks (newly added in the 2021 exam) will be discussed, as well as salts and rainbow tables. We will round out Domain 3 with a look at physical security before turning to Domain 4, Communication and Network Security. The discussion will cover a range of protocols and technologies, from the Open Systems Interconnection (OSI) model to storage area networks. New topics for the 2021 exam will be discussed, including micro-segmentation, Virtual eXtensible Local Area Network (VXLAN), Software-Defined Wide Area Network (SD-WAN), and Li-Fi.

TOPICS: Domain 3: Security Engineering (Part 2); Domain 4: Communication and Network Security

SECTION 5: Security Assessment and Testing; Security Operations

This course section covers Domain 6 (Security Assessment) and Domain 7 (Security Operations). Security Assessment covers types of security tests, testing strategies, and security processes. Security Operations covers investigatory issues, including eDiscovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as cloud, and we'll wrap up the section with a deep dive into disaster recovery.

TOPICS: Domain 6: Security Assessment; Domain 7: Security Operations

SECTION 2: Asset Security and Security Engineering – Part 1

Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of the second course section, describes data classification programs, including those used by governments, the military, and the private sector. We will also discuss ownership, covering owners ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods to purge data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2021 exam such as Data Loss Prevention (DLP), Cloud Access Security Brokers (CASB), microservices, containerization, serverless, High-Performance Computing (HPC) systems, and much more.

TOPICS: Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)

SECTION 4: Identity and Access Management

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on the identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The 2021 CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of credential management systems, federated identity, SSO, SAML, cloud identity, and third-party identity and authorization services like OpenID Connect (OIDC) and Open Authorization (OAuth)

TOPICS: Domain 5: Identity and Access Management

SECTION 6: Software Development Security

The final course section examines Domain 8 (Software Development Security), which describes the requirements for secure software. Security should be “baked in” as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the 2021 CISSP® exam update will be discussed, including DevOps. We will wrap up 414.6 by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

TOPICS: Domain 8: Software Development Security

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job



GIAC
Information Security
Professional
giac.org/gisp

GIAC Information Security Professional

The GIAC Information Security Professional (GISP) certification validates a practitioner's knowledge of the eight domains of cybersecurity knowledge as determined by (ISC)² that form a critical part of CISSP® exam. GISP certification holders will be able to demonstrate knowledge of asset security, communications and network security, identity and access management, security and risk management, security assessment and testing, security engineering, security operation, and software development security.

- Asset Security
- Communications and Network Security
- Identity and Access Management
- Security and Risk Management
- Security Assessment and Testing
- Security Engineering
- Security Operation
- Software Development Security

“Great discussions and examples that provide a clear understanding and relate material to examples.”

— Kelley O'Neil, Wells Fargo