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 CISSP®

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

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.

“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

Available Training Formats

<table>
<thead>
<tr>
<th>Live Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live Events</td>
</tr>
<tr>
<td>sans.org/information-security-training/by-location/all</td>
</tr>
<tr>
<td>Summit Events</td>
</tr>
<tr>
<td>sans.org/cyber-security-summit</td>
</tr>
<tr>
<td>Private Training</td>
</tr>
<tr>
<td>sans.org/private-training</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Online Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnDemand</td>
</tr>
<tr>
<td>sans.org/ondemand</td>
</tr>
<tr>
<td>Simulcast</td>
</tr>
<tr>
<td>sans.org/simulcast</td>
</tr>
</tbody>
</table>
Section Descriptions

SECTION 1: Introduction; Security and Risk Management
In the first section of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The latest 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, is discussed using real-world scenarios to illustrate the critical points.

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

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 today’s course section, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2020 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

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

SECTION 3: Security Engineering – Part 2; Communication and Network Security
This course 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. Salts are discussed, as well as 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.

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

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 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 CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like Oauth and OpenID.

TOPICS: Domain 5: Identity and Access Management

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 the cloud, and we’ll wrap up day five with a deep dive into disaster recovery.

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

SECTION 6: Software Development Security
Domain 8 (Software Development Security) 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 CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

TOPICS: Domain 8: Software Development Security

Who Should Attend

• Security professionals and managers 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

“Great discussions and examples that provide a clear understanding and relate material to examples.”
— Kelley O’Neil, Wells Fargo

Course Preview
available at: sans.org/demo