CompTIA CASP+ (CAS-005) Certification Guide

Expert resource for advanced cybersecurity concepts and vulnerability assessment techniques, with mock exams and real-world scenarios

2nd Edition

Dr. Akashdeep Bhardwaj

www.bpbonline.com

Second Revised and Updated Edition 2025

First Edition 2022

Copyright © BPB Publications, India

ISBN: 978-93-65899-870

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true and correct to the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but the publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

To View Complete
BPB Publications Catalogue
Scan the QR Code:

www.bpbonline.com

Dedicated to

My beloved parents

Late Wg. Cdr. (Retd.) ***K C Bhardwaj*** *and* ***Usha Bhardwaj***

and

My wife ***Archana*** *and my daughter* ***Raavi***

About the Author

Dr. Akashdeep Bhardwaj is working as a professor at *UPES, Dehradun, India*. An eminent IT industry expert in cybersecurity, digital forensics and IT operations areas, he mentors graduate, masters and doctoral students. Additionally, as the Head of Cybersecurity (Center of Excellence), he leads several industry projects.

Dr. Akashdeep is a Post-Doctoral from Majmaah University, Saudi Arabia, and a PhD (doctoral) in computer science. He has over 150 international publications (including SCI, Scopus, WoS papers, Copyrights, Patents) and authored several books and chapters. He has also worked as a technology leader for several multinational organizations during his time in the IT industry. Dr. Akashdeep is certified in multiple technologies including compliance audits, cybersecurity, and industry certifications in Microsoft, Cisco, and VMware technologies.

Acknowledgement

There are a few people I want to thank for the continued and ongoing support they have given me during the writing of this book. First and foremost, I would like to thank my parents for continuously encouraging me to write the book. I could have never completed this book without their support.

My gratitude also goes to the team at BPB Publications for being supportive enough to provide me quite a long time to finish the first part of the book and also allow me to publish the book since the topics included are vast and it was impossible to explore different class of problems in a single book, especially by not making it too voluminous.

Preface

This book covers many different aspects of cybersecurity. Obtaining the CASP certification demonstrates proven capabilities in terms of knowledge and skills to design and maintain security services for complex, enterprise environments and large organizations to secure their valuable assets. This includes core, technical knowledge, and hands-on skills to design and implement and integrate security solutions across enterprise environments. This book will serve as a guide written to provide deep insights into the operations of IT security, risks, technical security integrations, and working of security operations at the enterprise level with real-world tasks and activities security professionals at the lead and specialist level tend to perform day-in and day-out on the security floor. This book provides added-value apart from enhancing the required technical skills in form of stories, tips, notes, and links for additional knowledge to prepare you for the certification.

Chapter 1: Introduction to CASP+ Exam- This chapter introduces the CASP exam certification is a popular security certification. There are several popular vendor-specific certifications in the IT industry but CASP is a unique, vendor-neutral certification. This certification is a stepping-stone to other specialized, vendor-specific certifications. CASP exam topics are generic and apply to several varied security technologies, irrespective of the vendors. This book has several examples associated with vendor tools, configurations, and technologies. For specific vendor products, training regarding that vendor hardware, device, or software can be found in training specific to that vendor.

Chapter 2: Bussiness and Industry Trends, Influences, and Risks- This chapter presents the business and industry, trends, influences and risks, as security and IT teams do not operate independently, the work and tasks are highly influenced by the organization's business objectives, which define the IT roadmap and decisions. However, factors outside the enterprise control, like constant attacks, technology changes, and upgrades, regulations, compliance add to the complexity of securing the organization's security ecosystem. This chapter includes the various security risks due to the influences and the global market trends affecting IT.

Chapter 3: Organization Security Policies and Documents- This chapter includes the organizational security and privacy, policies and procedures. Since IT security policy and governance procedures are implemented to secure organizational assets, this chapter presents the creation, implementation, and management of the security policy life cycle. Use of business contracts for service level agreements and project documents to support security is also covered.

Chapter 4: Risk Mitigation Strategies- This chapter presents the risk mitigation strategies and controls for security teams to ensure organizations have proper risk mitigation strategies and controls in place. Using risk management frameworks helps to identify and implement the appropriate controls. This chapter covers the steps involved in risk mitigation, which include Asset identification, CIA Triad, determination of threats, the likelihood of attacks, implementing countermeasures. Then conducting risk analysis to determine the security threshold level. This chapter also covers the best practices and scenarios to implement user authentication and authorization in organizations.

Chapter 5: Enterprise Risk Measurement and Metrics- This chapter covers the enterprise risk measurement and metrics for securing an organization and assigning the highest priority, yet the business and senior management need to be convinced to allocate budget and resources for ensuring top-notch security. Security heads need to justify implementing security controls or buying new security technologies. After the security controls have been implemented, this chapter presents the review and assessment of the effectiveness of the risk controls by gathering and analyzing the risk metrics. The results are further interpreted for future trends, existing security levels, and trends against industry standards and baselines.

Chapter 6: Components of Network Security- This chapter presents the components of network security for organizations that seek to implement secure architecture for its network and systems. The secure design needs to have an understanding of the organization services and delivery components like servers, networks to include in the secure design. To implement security features, IT teams need to account for users' ease of use, performance cost, and security standards and principles. This chapter presents the building blocks for implementing a secure architecture for enterprises and critical infrastructures, which includes physical, virtual, network and servers.

Chapter 7: Securing Networks, Hosts Systems, and Devices- This chapter includes securing host systems and devices even as securing an enterprise does not stop at network traffic monitoring, since cyberattacks are initiated to exploit servers and user systems (hosts). This chapter presents the various controls for protecting and securing servers and user systems. This includes the use of trusted OS, bootloader security, OS hardening, endpoint security, application-level vulnerabilities.

Chapter 8: Secure Storage Controls- This chapter presents the storage control security for organizations to implement network security controls and perform audits, as security assessments. If every component of the organization is not included, the assessment is incomplete and leaves the organization exposed. This chapter presents a defence-in-depth strategy that needs to be implemented which should include physical, virtual, cloud,

on-premise, and user devices connecting to the office network. This chapter presents the assessment tools for performing security assessments at all levels.

Chapter 9: Securing the Internet of Things- This chapter discusses the security of the Internet of Things, after securing operating system and hardening the security assessments should mandatorily assess the smart devices inside industrial plants, homes and organizations. The chapter explains the concept to include an industrial closed loop control system in which data is collected, combined with related data, sent to an intelligent station, processed, and acted upon to change the environment. IoT is an ideal domain for not only securing devices, but also for innovations in secure system design, secure building block technologies, and secure hardware and software development practise, all of which combine to make the Internet of Things into the Secure Internet of Things.

Chapter 10: Cloud and Virtualization Security- This chapter presents cloud and virtualization security to monitor and detect cloud security incidents, and investigate and respond to them, as organizations have in-house or outsourced security operations. The incident response is a well-defined document for normal operations about actions to perform during an attack or breach. This serves as a baseline for ensuring operational recovery and back to normal activities. This helps security analysts recognize security incidents or anomalies and a process to respond. Every organization gathers the attacks and response to create a baseline over some time and measures the security operational incident response and effectiveness.

Chapter 11: Application Security Controls- This chapter discusses the different application vulnerability controls as this chapter examines some of the cyberattacks that can be launched against application, as well as the vulnerabilities that apps running on various operating systems present. It also covers safe coding techniques. Finally, the devices and services utilised to secure apps are discussed in this chapter.

Chapter 12: Security Assessments- This chapter covers the different procedures and methodologies involved in security vulnerability assessments, penetration testing, internal and external audits and colour based-team exercises.

Chapter 13: Selecting Vulnerability Assessment Tools- The chapter presents the process for selecting vulnerability assessment tools, even as most people think in terms of the network when they consider security assessments, security assessments encompass much more than this. If only network security were considered, major vulnerabilities would be left exposed. It can be argued that without sufficient physical security, network security cannot be achieved. Moreover, when exercising a defence-in-depth strategy, security must be considered at the network, host, and physical levels. This chapter looks at the tools used to perform assessments at each of these levels.

Chapter 14: Securing Communication and Collaborative Solutions- The chapter discusses securing communication and collaborative solution since increasingly, workers and the organizations for which they work are relying on new methods of communicating and working together that introduce new security concerns. As a CASP professional, you need to be familiar with these new technologies, understand the security issues they raise, and implement controls that mitigate the security issues. This chapter describes these new methods and technologies, identifies issues, and suggests methods to secure these new workflow processes.

Chapter 15: Implementing Cryptographic Techniques- This chapter discusses cryptography since this is one of the most complicated fields of security expertise. Both at rest and in transit, cryptography is a vital component of data security. It's a science that comprises hiding data or altering it to make it unreadable. Message authorship, source verification, and delivery proof are all ensured via cryptography. cryptography is concerned with confidentiality, integrity, and authentication, but not with availability. The CIA triumvirate is a basic security paradigm that includes secrecy, integrity, and availability, with cryptography addressing two of the triad's main pillars. It aids in the identification and prevention of data manipulation, deletion, and modification. Cryptography also provides non-repudiation by demonstrating a message's origin. Each of these ideas is examined in further depth in this chapter.

Chapter 16: Identification, Authentication, and Authorization- This chapter discusses identification of persons and devices, as well as determining the actions that a person or device is permitted to undertake, are at the heart of access control models. While this paradigm has stayed consistent since network computing's conception, the methodologies for conducting this key set of activities have developed tremendously and continue to do so. While simple usernames and passwords have historically served as access control, in today's world, more complicated and secure approaches are fast developing. Not only are such primitive approaches no longer secure, but today's access credential systems value convenience above everything else. Single sign-on and federated access control are two techniques for making a system as user-friendly as possible. The newest authentication and authorization approaches and processes are discussed in this chapter.

Chapter 17: Security Incidents and Response- This chapter discusses security incident analysis that involve an organisation should first capture the usual actions and performance of a system before determining if an event has happened. This serves as a benchmark against which all other activities are measured. To effectively determine when an event has happened, security professionals should ensure that the baseline is captured during periods of high and low activity. Additionally, they should collect baselines over time to

ensure the best overall baseline is achieved. Following that, the company must design policies that detail how security personnel should respond to incidents.

Chapter 18: Integrating Hosts, Networks, Storage, and Applications- Organizations need to securely integrate hosts, storage, networks, and applications. It is the security practitioner's responsibility to ensure that appropriate security access controls are implemented and tested apart from several other steps. This chapter discusses integration of hosts, network, storage and applications.

Chapter 19: Security Activities across Technology Lifecycle- This chapter explores the security activities across the technology lifecycle when it comes to managing an enterprise's security, security practitioners must consider security throughout the whole technological life cycle. Security practitioners must ensure that the necessary security controls are installed as the company evolves as new devices and technologies are added, maintained, and removed. Understanding the systems and software development life cycles, adapting solutions to handle evolving risks, disruptive technologies, and security trends, and asset management are all part of providing security across the technology life cycle.

Chapter 20: CASP+ Skill Assessment Exam-I- This chapter presents the first part of the CASP+ skill assessment questions and answers.

Chapter 21: CASP+ Skill Assessment Exam-II- This chapter presents the second part of the CASP+ skill assessment questions and answers.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/9bc9ef

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/CompTIA-CASP-Plus-CAS-005-Certification-Guide-2nd-Edition.
In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Introduction to CASP+ Exam

Introduction

The **CompTIA Advanced Security Practitioner (CASP+)** certification is a popular security certification. There are several popular vendor-specific certifications in the IT industry, but CASP is a unique, vendor-neutral certification. This certification is a stepping-stone to other specialized, vendor-specific certifications. CASP exam topics are generic and apply to several varied security technologies, irrespective of the vendors. This book has multiple examples of vendor tools, configurations, and technologies. For specific vendor products, training regarding that vendor's hardware, device, or software can be found in training specific to that vendor.

Structure

In this chapter, we will cover the following topics:

- Intended audience
- Steps to exam preparation
- Exam objectives
- Exam topics description

Objectives

The objective of this book is to understand the topics and technologies covered by the CASP blueprint from CompTIA. This book will enhance your knowledge and help you master the goal of clearing the CASP exam. To help you understand the CASP certification objectives, the chapters provide the opening topics list, which defines all the topics covered in that chapter. It also provides key topic icons to indicate important figures, tables, or information. These icons are available throughout the chapters and are also summarized in a table format at the end. Memory tables help memorize the important information for the CASP topics. Key terms are listed at the end of each chapter; try to learn and understand the definitions of each term and check your understanding of that chapter.

This book will summarize external and business influences on security, compare organizational security policies and procedures, analyze and perform risk mitigations and controls, integrate network and OS architecture to comply with security requirements, and design and select appropriate security controls.

Intended audience

Readers of this book can vary from those attempting to attain specialist or lead roles in the IT security domain to those who want to sharpen their technical skills to apply for new project roles or even go for the certification as per the organization mandate that wants them to take the new CASP exam. Those seeking to acquire additional skills and certification beyond the CASP certification, say those planning for **Certified Information Systems Security Professional (CISSP)**, **Certified Information Security Manager (CISM)** certifications, and beyond will find this book useful.

The book is designed to offer an easy transition for future certifications for experienced security architects, security specialists, technical leads, and security application engineers, who seek to enhance their skills and expertise, along with work experience, to leverage their experience and grow in the security career.

To be successful in this certification, first, you will need to bring your work experience, with a recommendation of having around 10 years of hands-on, core technical security real-world experience. The expectation is to build and use your home lab of virtual machines and tools, which will provide you with an environment to make-break and test your security skills. This would include network security, operating systems, cloud, governance, risk, and tons of security tools. The practitioners will learn to analyze a real-world scenario involving cloud, virtualization, networks, servers, applications, and end-user systems to select and implement appropriate security controls and perform assessments and recovery procedures at the enterprise level.

Steps to exam preparation

The suggested strategy while preparing for the CASP exam is to read and understand the book chapters and take down notes of key topics and concepts on a notepad or a separate paper book. It is highly advised to download the latest CASP exam objective list from the CompTIA certification site at **http://certification.comptia.org/examobjectives.aspx**.

Practice exams have been included in this book and you are recommended to attempt the practice exams, find out areas where you lack confidence, and review the specific concepts. After you review those specific areas, re-attempt the practice exams a second time to rate yourself. As you attempt the exams, you will become familiar with the terms, questions, and keywords. After a few attempts, you will feel confident in your understanding and skills. Then, schedule the CompTIA CASP exam from a center near you. Refer to *Pearson* **Virtual University Enterprises (VUE)** or any information you need when planning to register for the exam at **www.pearsonvue.com/comptia**.

Following are the exam details:

- **Maximum questions**: 90
- **Type of questions**: **Multiple-choice questions (MCQ)** and performance-based
- **Test duration**: 165 minutes
- **Recommended experience**: The following are the recommendations:
    - Minimum of ten years of general hands-on IT experience, with at least five of those years being broad hands-on IT security experience.
    - Network+, Security+, CySA+, Cloud+, and PenTest+ or equivalent certifications.
- **Pass score**: Pass or Fail only

Exam objectives

Table 1.1 lists the domains measured by this examination and the extent to which they are being represented:

Domains	Percentage %
Security Architecture	29%
Security Operations	30%
Security Engineering and Cryptography	26%
Governance, Risk, and Compliance	15%
Total coverage	**100%**

Table 1.1: *Exam domains*

Exam topics description

The exam chapter descriptions are mentioned in the following section, which lists the chapter names along with the objectives, descriptions, and keyword topics for each chapter.

Chapter 1: Introduction to CASP+ Exam

This chapter introduces **CompTIA Advanced Security Practitioner (CASP+)** certification, describing CASP sponsoring bodies, goals, and the value of CASP as a career and business driver. The official objectives covered on the CASP exam and steps to become CASP are explained along with the information on the CompTIA certification exam policies. This book presents the topics with detailed subject contents, including key learnings and essential keywords at the end of each chapter.

The exam topics covered are as follows:

- CASP goals
- Target audience
- Steps to CASP
- Exam topic description

Chapter 2: Business and Industry Trends, Influences, and Risks

Security and IT teams do not operate independently. The work and tasks are highly influenced by the organization's business objectives, which define the IT roadmap and decisions. However, factors outside the enterprise's control, like constant attacks, technology changes and upgrades, regulations, and compliance, add to the complexity of securing the organization's security ecosystem. This chapter includes the various security technology and market trends, influences, and global risks affecting IT security.

The exam topics covered are as follows:

- Business and industry influences
- External and internal factors
- New and changing business models or strategies
- Risk management
- Dynamic business models
- New strategies
- Security concerns during integration
- External and internal influence
- De-Perimeterization

Chapter 3: Organization Security Policies and Documents

IT security policy and governance procedures are implemented to secure organizational assets. This chapter presents the creation, implementation, and management of the security policy life cycle. Use of business contracts for service level agreements and project documents to support security are also covered.

The exam topics covered are as follows:

- Organization security policies
- Enterprise security procedures
- Security process life cycle management
- Business documents for security management
- Legal support and compliance
- Research security requirements
- Privacy principles

Chapter 4: Risk Mitigation Strategies

Security teams ensure organizations have proper risk mitigation strategies and controls in place. Using risk management frameworks helps identify and implement the appropriate controls. This chapter covers the steps involved in risk mitigation, which include asset identification, **confidentiality, integrity, and availability (CIA)** triad, determination of threats, the likelihood of attacks, implementing countermeasures, and conducting a risk analysis to determine the security threshold level.

Following are the exam topics covered:

- Asset classification
- Threat identification
- Risk determination
- Countermeasures and controls
- CIA-impact decisions
- Aggregate score for security controls
- Worst case scenario
- Technical to business risk
- Risk controls
- Business continuity planning

Chapter 5: Enterprise Risk Measurement and Metrics

Securing an organization should be assigned the highest priority, yet the business and senior management need to be convinced to allocate budget and resources for ensuring top-notch security. Security heads need to justify implementing security controls or buying new security technologies. After the security controls have been implemented, this chapter presents the review and assessment of the effectiveness of the risk controls by gathering and analyzing the risk metrics. The results are further interpreted for future trends, existing security levels, and trends against industry standards and baselines.

Following are the exam topics covered:

- Effective security control review
- Create risk metrics
- **Key performance indicators (KPI), recovery time objective (RCO), total cost of ownership (TCO)**
- Compare security baselines
- Anticipate future needs
- Risk review of controls
- Analyze metrics
- Benchmarks
- Baselines
- Data analysis and interpretation
- Judgmental solutions

Chapter 6: Components of Network Security

Any organization seeks to implement secure architecture for its network infrastructure. The secure design needs to have an understanding of the organization's services and delivery components like servers, and networks to include in the secure design. To implement security features, IT teams need to account for users' ease of use, performance cost, and security standards and principles. This chapter presents the building blocks for implementing a secure architecture for enterprises and critical infrastructures, which include physical, virtual, and network devices.

Following are the exam topics covered:

- Physical and virtual network devices
- Application-aware technologies
- Secure and complex traffic flow