

CCZT Knowledge Guide

The Certificate of Competence in
Zero Trust



CSA cloud
security
alliance®

CCZT™
Certificate of
Competence in Zero Trust

*Prepare for the industry's
first authoritative Zero Trust
training and certificate.*

Introduction to the CCZT

With rapid technological advances, new security vulnerabilities are constantly emerging. The Zero Trust model, which operates on the principle of 'never trust, always verify', is quickly rising as the most favored cybersecurity strategy to prevent breaches. Recognizing that organizations have varying security postures and may be challenged to find skilled staff critical to the development and implementation of a Zero Trust strategy, CSA created the [Certificate of Competence in Zero Trust](#) (CCZT).

The CCZT includes foundational Zero Trust best practices released by leading authoritative sources such as, CISA and NIST, innovative work around the [Software Defined Perimeter](#) (SDP) by CSA Research, and guidance from renowned Zero Trust experts such as John Kindervag, Founder of the Zero Trust philosophy. This integration of expertise uniquely positions CSA as the authoritative source to deliver the industry's first holistic benchmark for measuring Zero Trust knowledge.

The certificate provides an in-depth understanding of Zero Trust architecture, the drivers, benefits, and how to plan for adoption. Earning the CCZT is critical for security professionals seeking to advance their careers and for organizations who must maintain strong security postures. Earning the CCZT ensures professionals are equipped to implement the robust security measures required from taking a Zero Trust approach.

I'm extremely grateful to the Cloud Security Alliance for taking up the Zero Trust banner with the delivery of the CCZT, the world's first authentic, non-vendor-specific training and certificate that delivers the knowledge needed to understand the core concepts of Zero Trust. The sheer volume of passionate volunteers CSA has been able to bring together to collaborate on the development of Zero Trust tools and best practices is incredibly exciting.

John Kindervag
Creator of Zero Trust,
Chief Evangelist at Illumio

Who should earn the CCZT?

With Zero Trust established as the future of information security, a Zero Trust based approach will inevitably become a requirement for organizations and a required skill for security professionals. Here are just a few examples of those who should prepare for this inevitability with the CCZT:

- The C-Suite, managers, and decision makers to build a Zero Trust governance and risk posture
- Security engineers, architects, analysts, and administrators to protect devices and build/automate controls
- Compliance managers to identify the key components of their Zero Trust governance framework and how it supports an organization's risk and compliance programs
- Government agencies looking for training to meet federal mandates, enhance cybersecurity and ensure compliance with security directives



Download Authoritative Sources

CISA Zero Trust Maturity Model



Created by the Cybersecurity & Infrastructure Security Agency (CISA), the Zero Trust Maturity Model is a critical Zero Trust tool CCZT students should reference as they study for the exam. The maturity model provides guidance on the development of Zero Trust strategies and implementation plans as an organization moves to a more mature security posture. The maturity model, which includes five pillars and three cross-cutting capabilities, is based on the foundations of Zero Trust. Within each pillar, the maturity model provides specific examples of traditional, initial, advanced, and optimal Zero Trust architectures.

[Download Now →](#)

NIST Zero Trust Architecture (SP 800-207)



The US National Institute of Standards and Technology (NIST) [Zero Trust Architecture](#) (ZTA) document describes ZT for enterprise security architects. It is meant to aid understanding of ZTA and provide an enterprise implementation roadmap for zero trust security concepts. This includes information on how Cybersecurity managers and network administrators may also gain ZTA insight from IT. This document is not intended to be a single deployment plan for ZTA as enterprises will have unique business use cases and data assets to safeguard. Instead, it provides a starting point with a solid understanding of the organization's business and data will result in a strong approach to zero trust.

[Download Now →](#)

NSTAC Report: Zero Trust and Trusted Identity Management



The US President's National Security Telecommunications Advisory Committee (NSTAC) report focuses on Zero Trust and Trusted Identity Management. This report provides valuable guidance and recommendations for implementing Zero Trust and trusted identity management in systems. It helps organizations enhance their cybersecurity posture and protect critical infrastructure by adopting a Zero Trust approach. The report emphasizes the significance of strong identity management practices in ensuring secure access and authentication within a Zero Trust environment, which is crucial for safeguarding sensitive information and preventing unauthorized access.

[Download Now →](#)

Benefits of having your CCZT



Keep up with innovation

Demand for Zero Trust training is increasing. According to Gartner, 60% of organizations are expected to embrace Zero Trust by 2025.



Build a competent workforce and further individual development

The CCZT and Zero Trust Training (ZTT) builds a workforce that is proficient in implementing and managing Zero Trust models. This is crucial to keep up with evolving cybersecurity threats.



Ineffectiveness of traditional security

Traditional models are not effective against modern threats. Zero Trust assumes no user or device can be trusted. Earning the CCZT ensures professionals are equipped to implement the robust security measures required from taking a Zero Trust approach.

Additional Study Materials

CSA Research Publications

[CSA Research](#) is created by the industry for the industry and is both vendor-neutral and consensus driven. Our Zero Trust research publications are created by subject matter experts who volunteer for CSA's [Zero Trust working group](#) which focuses on developing Zero Trust principles to achieve consistency for cloud, hybrid and mobile endpoint environments.

To best prepare for the CCZT exam, we recommend reviewing the study guides attached in the [CCZT Prep-Kit](#), and reading the following publications from the Zero Trust working group. For additional industry leading resources, check out the [Zero Trust Resource Hub](#).

Communicating the Business Value of Zero Trust

Closing the gap between technical and non-technical or non-security audiences to improve communication of strategic business value that a Zero Trust approach can bring.

[Download Now →](#)



Zero Trust Guiding Principles

Providing a clear understanding of what Zero Trust security is and the guiding principles that any organization can leverage when planning, implementing and operating Zero Trust.

[Download Now →](#)



Zero Trust as a Security Philosophy

Taking a vendor and technology-neutral look at what Zero Trust means for an organization and providing recommendations to develop a strategy and the supporting architecture necessary to align IT to business goals and outcomes.

[Download Now →](#)



No Prerequisites Required

There are no prerequisites required for the CCZT, however it is helpful to have your [Certificate of Cloud Security Knowledge \(CCSK\)](#) or a basic understanding of security fundamentals. Completing the [CCZT Exam Bundle](#) is also highly recommended to prepare for the CCZT.

Topics and Domains

Topics

The following are the core topics covered throughout the exam. Some topics are covered in multiple domains.



Zero Trust Foundational Concepts

General concepts, definitions, goals, objectives and benefits of Zero Trust.



Zero Trust Architecture

Logical models, key components, workflows, and design of Zero Trust Architecture.



Software Defined Perimeter

The core tenets, underlying technologies, main architectural components, and technology and business benefits of SDP, a ZTA solution.



Zero Trust Planning

In-depth examination of the crucial facets of Zero Trust planning from initial considerations such as stakeholder identification and defining your protect surfaces, to organizational security policies and compliance.



Industry Best Practices

Developing best practices in Zero Trust by examining authoritative sources such as CISA's Zero Trust Maturity Model and NIST's Zero Trust Architecture (SP 800-207), among others.



Zero Trust Implementation

In-depth examination of the crucial facets of Zero Trust implementation, from creating project kick-off documents and disaster planning, to setting up the network environment, deploying agents to devices, and adding automation.

Domains

The following are the six domains that provide the structure of the CCZT exam. Domains may include reference to more than one topic area listed above.

1. Zero Trust and Zero Trust Architecture general concepts and definitions
2. Zero Trust goals, objectives, and benefits
3. Zero Trust Architecture logical model and key components
4. Software Defined Perimeter
5. Zero Trust Planning
6. Zero Trust Implementation

Choose How to Study

Option 1

Study on your own

Use the free CCZT Prep-Kit to facilitate your independent learning style. The kit includes this knowledge guide, study guides, an FAQ, overview presentation, and authoritative sources to help you prepare. Comprehensive CCZT Study Guides are included with the purchase of all CCZT exam tokens. To access the Study Guides, purchase your CCZT exam token then begin your self-paced study. Download the [CCZT Prep-Kit](#) and [purchase your exam token](#) to get started.



Option 2

Self-paced training online

If you need training flexible enough for your schedule and budget, self-paced online training may be a good fit. The CCZT is based on CSA's [CCZT Exam Bundle](#), an online course that delivers the fundamentals needed to understand the core concepts of Zero Trust covered in the exam. You can complete CCZT modules on-the-go, without any deadlines, at a pace that's right for you. Access the training on [CSA's Knowledge Center](#).



Option 3

Instructor-led training online

The online, [instructor-led training](#) is good for organizations with a tight travel budget or individuals who prefer a more personal instruction. You can learn remotely, while still being able to ask questions and interact with your instructor. Look for available [instructor-led online classes](#) or [contact CSA](#) support for information on custom in-person or online training options.



Exam Format

The CCZT is an open-book, online exam with **60 multiple-choice questions** covering six core areas of Zero Trust knowledge. Testers have two attempts to complete the exam in the allotted **120-minute timeframe** and achieve a minimum **passing score of 80%**.

Question Format

All questions are multiple choice or true or false.

Exam Difficulty

It may be open-book, but don't underestimate the difficulty of this exam. Questions are selected at random from the CCZT question pool, so having a solid understanding of each domain and the authoritative sources included in the recommended study materials is essential if you want to pass.

Domains	# of Questions
1 Zero Trust and Zero Trust Architecture general concepts and definitions	6
2 Zero Trust goals, objectives, and benefits	4
3 Zero Trust Architecture logical model and key components	3
4 Software Defined Perimeter	11
5 Zero Trust Planning	25
6 Zero Trust Implementation	11

Take the Exam



Register on the CSA Exams website

Simply [create an account](#) to register for the exam. Because the exam is online, you can take the test where and when you want after purchasing an exam token.

Purchase a CCZT exam token

Each [CCZT exam token](#) provides you with two test attempts. If you choose to [enroll in a training course](#), a complimentary exam token is included.

Take the exam

Make sure you have thoroughly studied the exam materials and reviewed your notes if you took a training course.

After Passing the Exam

CPE credits

Although there are currently no official CPE designations for any of CSA's training courses, we do issue a certificate of completion with a stated number of hours to complete the course for all courses we offer. You can then use this certificate of completion for CPE credit submission, but it will be determined if it qualifies for CPE credit by whomever receives your request. The online self-paced training automatically gives attendees **13 hours**.

Digital badge

A [CCZT digital badge](#) is issued upon successful completion of the exam. Leverage the CCZT digital badge on your social media channels and resume to showcase your knowledge and validate your expertise.



Share your Expertise

Forge industry connections on Circle

Connect with other CCZT holders or share your knowledge with students on [Circle](#), CSA's online community forum that provides a space for professionals, novices and visionaries to share information. Share tips learned from taking the training or exam, and gain insight from other industry leaders in Zero Trust to continue your learning journey.



Join a Research working group

After earning your Certificate of Competence in Zero Trust, start applying your knowledge by volunteering for CSA's [Zero Trust working group](#). Focused on developing Zero Trust standards to achieve consistency for cloud, hybrid and mobile endpoint environments, your successful completion of the CCZT provides you with the necessary skill and expertise to help us create best practices and guidance in Zero Trust. Whether you are looking to join as an observer or author a research report, we encourage you to join. Our working groups are comprised of a diverse network of industry practitioners and corporate members that continuously cycle through researching, analyzing, formulating and delivering arguably the most advanced research and tools available across the cloud security spectrum.



ZTAC Resource Hub

CSA's [Zero Trust Advancement Center](#) (ZTAC) aims to construct an impartial perspective of Zero Trust and what it means to organizational leaders looking to build a Zero Trust strategy. The [ZTAC Resource Hub](#) is a curated collection of the most important Zero Trust publications in the industry, displaying the most current and relevant Zero Trust content. Sharpen your Zero Trust knowledge and stay up to date with these resources, or submit your own industry leading content on Zero Trust to the Resource Hub for consideration.





**Knowledge
Center**

Online training based on CSA's vendor-neutral research

Level up your cloud computing knowledge with the variety of CSA online courses and certificates for beginners and pros alike.

knowledge.cloudsecurityalliance.org