Certificate of Competence in Zero Trust (CCZT) Training

Duration: **2 Day**

BILGINC
IT Academy
info@bilginc.com
bilginc.com

This two-day instructor-led course provides a comprehensive introduction to Zero Trust concepts, principles, and architectures as defined by the Cloud Security Alliance (CSA). Participants will learn how to design, implement, and maintain Zero Trust strategies that align with modern enterprise and cloud environments.

Building on the foundational principle that no entity human or system can be implicitly trusted, this course enables learners to integrate Zero Trust into organisational planning, architecture, and technology deployment. Through a blend of theory, guided discussion, and applied examples, learners will develop the capability to reduce organisational risk and strengthen cyber resilience.

Prerequisites

There are no formal prerequisites for the CCZT.
It is recommended that participants have:

- A basic understanding of networking and network security
- Familiarity with cloud security principles or frameworks such as CCSKPLUS, or CCSP

Target audience

This course is designed for professionals involved in designing, implementing, or governing information security strategies, including:

- Security architects, analysts, and consultants
- Cloud and network engineers
- IT managers and system administrators
- Risk and compliance officers seeking to align Zero Trust with governance frameworks
- Technical decision-makers responsible for enterprise-wide security transformation

Certificate of Competence in Zero Trust (CCZT) Training

Duration: **2 Day**

BILGINC
IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this course, participants will be able to:

- Explain the concept of a Software-Defined Perimeter (SDP) and its relationship to Zero Trust
- Communicate the technology and business challenges that SDP and Zero Trust address
- Distinguish between key types of SDP deployment models
- Demonstrate understanding of the Zero Trust Maturity Model and its role in supporting organisational planning
- Identify the key steps and considerations involved in Zero Trust strategy development
- Map organisational data flows to identify protect and attack surfaces
- Apply recognised methods such as gap analysis, risk registers, and RACI diagrams in a Zero Trust planning process
- Design and plan Zero Trust policies aligned to business objectives
- Explain the preparatory and implementation activities required for Zero Trust Architecture (ZTA) adoption
- Leverage Zero Trust pillars and cross-cutting capabilities to build workflow documentation and audit-ready processes