

**Microsoft Cybersecurity Architect (SC-100)**

**Course Number:** MOC-SC-100
**Duration:** 4 days

**Overview**

This Microsoft Cybersecurity Architect training, MS official course SC-100, teaches students how to design and evaluate cybersecurity strategies in Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps), and data and applications. Students also learn how to design and architect solutions using zero trust principles and how to specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS). This course prepares students for the [SC-100 exam](https://docs.microsoft.com/en-us/learn/certifications/exams/SC-100) for which every attendee receives a voucher.

**Prerequisites**

* Advanced experience and knowledge in identity and access, platform protection, security operations, securing data, and securing applications.
* Experience with hybrid and cloud implementations.
* Although not required to attend, students are strongly encouraged to have taken and passed another associate-level certification in the security, compliance, and identity portfolio (such as [AZ-500](file:////training/microsoft-azure-security-technologies), [SC-200](file:////training/sc-200-microsoft-security-operations-analyst), or [SC-300](file:////training/sc-300-microsoft-identity-and-access-administrator)) before attending this class.

**Materials**

All Microsoft training students receive Microsoft official courseware.

For all Microsoft Official Courses taught in their entirety that have a corresponding certification exam, an exam voucher is included for each participant.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computer for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will be fine.

**Objectives**

* Design and evaluate cybersecurity strategies in Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps)
* Design and architect solutions using zero-trust principles
* Specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS)

**Outline**

* Build an overall security strategy and architecture
* Design a security operations strategy
* Design an identity security strategy
* Evaluate a regulatory compliance strategy
* Evaluate security posture and recommend technical strategies to manage risk
* Understand architecture best practices and how they are changing with the Cloud
* Design a strategy for securing server and client endpoints
* Design a strategy for securing PaaS, IaaS, and SaaS services
* Specify security requirements for applications
* Design a strategy for securing data
* Recommend security best practices using Microsoft Cybersecurity Reference Architectures (MCRA) and Microsoft Cloud Security Benchmarks
* Recommend a secure methodology using the Cloud Adoption Framework (CAF)
* Recommend a ransomware strategy by using Microsoft Security Best Practices