



Microsoft Certified: Azure Security Engineer Associate

Candidates for the Azure Security Engineer Associate certification should have subject matter expertise in implementing Azure security controls that protect identity, access, data, applications, and networks in cloud and hybrid environments as part of an end-to-end infrastructure.

Responsibilities for an Azure security engineer include managing the security posture, identifying, and remediating vulnerabilities, performing threat modeling, implementing threat protection, and responding to security incident escalations.

Skills measured

- Manage identity and access
- Implement platform protection
- Manage security operations
- Secure data and applications

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives: AZ-500

Microsoft Azure Security Technologies

Manage identity and access	30-35%
Implement platform protection	15-20%
Manage security operations	25-30%
Secure data and applications	25-30%

Course Outline:

Chapter 1: Manage Identity and Access

Chapter 2: Implement Platform Protection

Chapter 3: Manage Security Operations

Chapter 4: Secure Data and Applications

Included

40 hours of instructor-led training sessions

Microsoft authorized textbook and class materials

Practice questions and exam study tips