Secure Azure Services and Workloads with Microsoft Defender for Cloud
SC 5002

Course Name	**Secure Azure Services and Workloads with Microsoft Defender for Cloud**
Course Code	**SC 5002**
Course Duration	2 Days
Course Structure	Instructor-Led
Course Overview	SC-5002: Secure Azure Services and Workloads with Microsoft Defender for Cloud equips delegates with the skills required to secure Azure services and workloads through the application of Microsoft Defender for Cloud and regulatory compliance controls. The course delivers comprehensive instruction on configuring network security, establishing monitoring through Log Analytics, implementing just-in-time virtual machine access, and securing connectivity using private endpoints. Through hands-on exercises, delegates will examine regulatory compliance standards, enable Defender for Cloud across Azure subscriptions, deploy network security groups, configure the Azure Monitor Agent, and apply Azure Key Vault networking controls. By the conclusion of the course, learners will be capable of applying a layered, defence-in-depth approach to securing Azure services and workloads.
Audience Profile	This course is designed for Azure administrators and security engineers responsible for the protection of Azure services and workloads. It is appropriate for IT professionals tasked with implementing security controls, monitoring threats, and ensuring regulatory compliance within an Azure cloud environment.
Course Prerequisites	There are no formal prerequisites; however, a working knowledge of Azure fundamentals, networking, and security concepts is recommended.
Course Outcome	Upon successful completion of this course, delegates will be equipped with the skills and knowledge required to: • Examine Defender for Cloud regulatory compliance standards • Enable Microsoft Defender for Cloud on an Azure subscription • Filter network traffic using network security groups • Collect monitoring data using Azure Monitor Agent • Implement just-in-time virtual machine access • Configure Azure Key Vault networking settings

	• Connect Azure SQL servers using Azure Private Endpoint
Assessment/Evaluation	This course prepares delegates for the Microsoft Applied Skills credential SC-5002: Secure Azure Services and Workloads with Microsoft Defender for Cloud Regulatory Compliance Controls. Successful completion of the associated assessment will result in attainment of the credential and a Certificate of Attendance issued by IT-IQ Botswana.

Course Details	
Topic	**Module 1: Examine Defender for Cloud Regulatory Compliance Standards** • Regulatory compliance standards overview • Microsoft cloud security benchmark • Improving regulatory compliance posture **Module 2: Enable Defender for Cloud on Your Azure Subscription** • Enabling Defender for Cloud plans • Configuring enhanced security features • Reviewing security recommendations **Module 3: Filter Network Traffic with Network Security Groups** • Creating and configuring network security groups • Inbound and outbound rule design • Applying NSGs to subnets and interfaces **Module 4: Collect Guest Monitoring Data with Azure Monitor Agent** • Deploying Azure Monitor Agent • Configuring data collection rules • Integrating with Defender for Cloud

	Module 5: Explore Just-in-Time Virtual Machine Access • Risks of open management ports • Enabling JIT VM access • Requesting and approving JIT access **Module 6: Configure Azure Key Vault Networking Settings** • Key Vault firewall and virtual networks • Service endpoints • Private endpoints for Key Vault **Module 7: Connect to Azure SQL Using Azure Private Endpoint** • Private Link concepts • Configuring private endpoints for Azure SQL • Validating and securing connectivity