SECURE AZURE SERVICES AND WORKLOADS WITH MICROSOFT DEFENDER FOR CLOUD REGULATORY COMPLIANCE CONTROLS (SC-5002)

Course Code: 834033

Learn Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls.

This learning path guides you in securing Azure services and workloads using Microsoft Cloud Security Benchmark controls in Microsoft Defender for Cloud via the Azure portal.

What You'll Learn

Students will learn to,

- Examine Defender for Cloud regulatory compliance standards
- Enable Defender for Cloud on your Azure subscription
- Filter network traffic with a network security group using the Azure portal
- Create a Log Analytics workspace
- Collect guest operating system monitoring data from Azure and hybrid virtual machines using Azure Monitor Agent
- Explore just-in-time virtual machine access
- Configure Azure Key Vault networking settings
- Connect an Azure SQL server using an Azure Private Endpoint using the Azure portal

Who Needs to Attend

- Security Engineer
- Azure Security Engineers

SECURE AZURE SERVICES AND WORKLOADS WITH MICROSOFT DEFENDER FOR CLOUD REGULATORY COMPLIANCE CONTROLS (SC-5002)

Course Code: 834033

CLASSROOM LIVE	$675 USD	1 Day

Classroom Live Outline

Module 1: Examine Defender for Cloud regulatory compliance standards

- Understand how to use Microsoft Defender for Cloud's compliance management dashboard.
- Identify and interpret key regulatory compliance standards applicable to your industry.
- Implement and manage compliance controls within Microsoft Defender for Cloud.
- Conduct regular compliance assessments and generate comprehensive compliance reports.

Module 2: Enable Defender for Cloud on your Azure subscription

- Learn how to connect your Azure subscriptions to Microsoft Defender for Cloud.
- Understand the benefits of integrating Azure subscriptions for enhanced security monitoring.
- Explore methods to manage and ensure compliance across connected Azure subscriptions.
- Gain skills to implement best practices for threat protection within your Azure environment.

Module 3: Filter network traffic with a network security group using the Azure portal

- Understand the purpose and benefits of using Azure NSG to filter network traffic.
- Learn how to create and configure NSGs to enforce access controls for Azure

resources.
- Gain insights into how NSGs can be used to allow or deny specific types of traffic based on source, destination, and port.
- Understand how to prioritize NSG rules and leverage Azure NSG flow logs for monitoring and troubleshooting.
- Recognize the role of NSGs in implementing network security best practices in Azure.

Module 4: Create a Log Analytics workspace

- Understand the importance of a centralized logging solution like Azure Log Analytics workspace for Microsoft Defender for Cloud.
- Learn how to create and configure a Log Analytics workspace in Azure.
- Gain insights into collecting and analyzing security data from Microsoft Defender for Cloud within the Log Analytics workspace.
- Understand how to create custom queries and alerts to proactively detect security threats and incidents.
- Recognize the benefits of integrating Log Analytics workspace with other Azure services and tools.

Module 5: Collect guest operating system monitoring data from Azure and hybrid virtual machines using Azure Monitor Agent

- Understand the importance of a centralized log collection and analysis solution in Microsoft Defender for Cloud.
- Learn how to configure and deploy the Log Analytics agent in Azure.
- Gain insights into creating and configuring a Log Analytics workspace for Defender for Cloud.
- Understand how to integrate the Log Analytics workspace with Defender for Cloud to collect and analyze security logs.
- Recognize the benefits of leveraging centralized log analytics for proactive security monitoring and threat detection.

Module 6: Explore just-in-time virtual machine access

- Understand the risks associated with open management ports on virtual machines.
- Learn how to implement JIT VM access using Microsoft Defender for Cloud.
- Explore how JIT VM access reduces attack surfaces in Azure and AWS environments.
- Gain skills to configure and manage temporary, controlled access to VMs for authorized users.

Module 7: Configure Azure Key Vault networking settings

- Understand the importance of configuring networking settings for Azure Key Vault in ensuring secure access and communication.
- Learn how to configure network access control for Azure Key Vault using virtual network service endpoints and private endpoints.
- Gain insights into configuring firewall rules and virtual network service endpoints to restrict access to Key Vault.

- Understand the process of configuring private endpoints to securely access Key Vault from virtual networks.
- Recognize the benefits of properly configuring networking settings for Azure Key Vault in enhancing overall security.

Module 8: Connect an Azure SQL server using an Azure Private Endpoint using the Azure portal

- Understand the importance of using Azure Private Endpoint to establish secure connections to Azure SQL Server.
- Learn how to configure and create an Azure Private Endpoint for Azure SQL Server in the Azure portal.
- Gain insights into the network architecture and components involved in setting up an Azure Private Endpoint.
- Understand how to validate and test the connection between the Azure Private Endpoint and Azure SQL Server.
- Recognize the benefits of using Azure Private Endpoint for securing database connections and isolating network traffic.

SECURE AZURE SERVICES AND WORKLOADS WITH MICROSOFT DEFENDER FOR CLOUD REGULATORY COMPLIANCE CONTROLS (SC-5002)

Course Code: 834033

VIRTUAL CLASSROOM LIVE	$675 USD	1 Day

Virtual Classroom Live Outline

Module 1: Examine Defender for Cloud regulatory compliance standards

- Understand how to use Microsoft Defender for Cloud's compliance management dashboard.
- Identify and interpret key regulatory compliance standards applicable to your industry.
- Implement and manage compliance controls within Microsoft Defender for Cloud.
- Conduct regular compliance assessments and generate comprehensive compliance reports.

Module 2: Enable Defender for Cloud on your Azure subscription

- Learn how to connect your Azure subscriptions to Microsoft Defender for Cloud.
- Understand the benefits of integrating Azure subscriptions for enhanced security monitoring.
- Explore methods to manage and ensure compliance across connected Azure subscriptions.
- Gain skills to implement best practices for threat protection within your Azure environment.

Module 3: Filter network traffic with a network security group using the Azure portal

- Understand the purpose and benefits of using Azure NSG to filter network traffic.
- Learn how to create and configure NSGs to enforce access controls for Azure

resources.
- Gain insights into how NSGs can be used to allow or deny specific types of traffic based on source, destination, and port.
- Understand how to prioritize NSG rules and leverage Azure NSG flow logs for monitoring and troubleshooting.
- Recognize the role of NSGs in implementing network security best practices in Azure.

Module 4: Create a Log Analytics workspace

- Understand the importance of a centralized logging solution like Azure Log Analytics workspace for Microsoft Defender for Cloud.
- Learn how to create and configure a Log Analytics workspace in Azure.
- Gain insights into collecting and analyzing security data from Microsoft Defender for Cloud within the Log Analytics workspace.
- Understand how to create custom queries and alerts to proactively detect security threats and incidents.
- Recognize the benefits of integrating Log Analytics workspace with other Azure services and tools.

Module 5: Collect guest operating system monitoring data from Azure and hybrid virtual machines using Azure Monitor Agent

- Understand the importance of a centralized log collection and analysis solution in Microsoft Defender for Cloud.
- Learn how to configure and deploy the Log Analytics agent in Azure.
- Gain insights into creating and configuring a Log Analytics workspace for Defender for Cloud.
- Understand how to integrate the Log Analytics workspace with Defender for Cloud to collect and analyze security logs.
- Recognize the benefits of leveraging centralized log analytics for proactive security monitoring and threat detection.

Module 6: Explore just-in-time virtual machine access

- Understand the risks associated with open management ports on virtual machines.
- Learn how to implement JIT VM access using Microsoft Defender for Cloud.
- Explore how JIT VM access reduces attack surfaces in Azure and AWS environments.
- Gain skills to configure and manage temporary, controlled access to VMs for authorized users.

Module 7: Configure Azure Key Vault networking settings

- Understand the importance of configuring networking settings for Azure Key Vault in ensuring secure access and communication.
- Learn how to configure network access control for Azure Key Vault using virtual network service endpoints and private endpoints.
- Gain insights into configuring firewall rules and virtual network service endpoints to restrict access to Key Vault.

- Understand the process of configuring private endpoints to securely access Key Vault from virtual networks.
- Recognize the benefits of properly configuring networking settings for Azure Key Vault in enhancing overall security.

Module 8: Connect an Azure SQL server using an Azure Private Endpoint using the Azure portal

- Understand the importance of using Azure Private Endpoint to establish secure connections to Azure SQL Server.
- Learn how to configure and create an Azure Private Endpoint for Azure SQL Server in the Azure portal.
- Gain insights into the network architecture and components involved in setting up an Azure Private Endpoint.
- Understand how to validate and test the connection between the Azure Private Endpoint and Azure SQL Server.
- Recognize the benefits of using Azure Private Endpoint for securing database connections and isolating network traffic.

Jun 20 - 20, 2025 | 9:00 AM - 5:00 PM EDT

Aug 8 - 8, 2025 | 9:00 AM - 5:00 PM EDT

Oct 6 - 6, 2025 | 9:00 AM - 5:00 PM EDT

SECURE AZURE SERVICES AND WORKLOADS WITH MICROSOFT DEFENDER FOR CLOUD REGULATORY COMPLIANCE CONTROLS (SC-5002)

Course Code: 834033

PRIVATE GROUP TRAINING	1 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/9/2025 12:39:17 AM