

## KOENIG SOLUTIONS • COURSE OUTLINE

# Microsoft 365 Administration, Security, Compliance, and AI Copilot Mastery

Comprehensive Course Outline

**42**

MODULES

**167**

TOPICS

**88**

HANDS-ON ACTIVITIES

## COURSE OVERVIEW

This comprehensive course equips IT professionals, administrators, and power users with the skills to configure, secure, manage, and optimize Microsoft 365 environments while unlocking the potential of AI-powered productivity with Microsoft 365 Copilot. Master tenant configuration, user and group management, custom domains, client connectivity, administrative delegation, and service health monitoring. Dive deep into security, compliance, identity synchronization, Microsoft Defender, and Microsoft Purview capabilities. Explore the latest AI-driven tools within Microsoft 365 Copilot to create impactful presentations, draft documents, analyze data, manage meetings, and streamline communications across PowerPoint, Word, Excel, Outlook, and Teams.

## WHO THIS COURSE IS FOR

**Microsoft 365 Administrators**

**IT Professionals**

**Security Administrators**

**Compliance Officers**

**Power Users**

**Identity Administrators**

## PREREQUISITES

- Fundamental knowledge of Microsoft 365 services and subscription models.
- Basic understanding of cloud concepts, including SaaS, identity, and security principles.
- Experience with Microsoft 365 admin center and basic PowerShell commands is beneficial.
- Familiarity with productivity tools like Word, Excel, PowerPoint, Outlook, and Teams.

## What You Will Learn

- Configure tenant settings, user identities, groups and custom domains
- Manage administrative roles, delegation and client connectivity
- Monitor tenant health, service incidents and app deployment
- Apply Microsoft 365 Copilot across PowerPoint, Word, Excel and Outlook
- Assess security posture using Microsoft Secure Score and Defender XDR
- Implement identity protection with Entra ID Protection and PIM
- Configure Purview compliance tools including DLP and retention
- Implement sensitivity labels and classify sensitive data

## COURSE SYLLABUS

## 42 Modules, 167 Topics

01

8 Labs

### Configure Your Microsoft 365 Experience

## TOPICS

Microsoft 365 subscription and tenant · Set up your organizational profile · Manage your services and add-ins · Finalize your tenant

02

### Manage Users, Licenses, and Mail Contacts in Microsoft 365

## TOPICS

Understanding user identities · Creating and managing user accounts · Managing user licenses · Recovering deleted user accounts · Create and manage guest users · Create and manage mail contacts

03

4 Labs

### Manage Groups in Microsoft 365

## TOPICS

- Creating and managing groups
- Creating dynamic groups using Azure rule builder
- Creating a Microsoft 365 group naming policy
- Creating groups in Exchange Online and SharePoint Online

**04****2 Labs**

## Add a Custom Domain in Microsoft 365

### TOPICS

- Plan a custom domain for your Microsoft 365 deployment
- Plan the DNS zones for a custom domain
- Plan the DNS record requirements for a custom domain
- Create a custom domain in Microsoft 365

**05**

## Configure Client Connectivity to Microsoft 365

### TOPICS

- Understand how automatic client configuration works
- Understand which DNS records are required for automatic client configuration
- Configure Outlook clients
- Troubleshoot client connectivity

**06****4 Labs**

## Configure Administrative Roles in Microsoft 365

### TOPICS

- Microsoft 365 permission model
- Microsoft 365 admin roles and best practices
- Assign admin roles to users in Microsoft 365
- Delegate admin roles to partners
- Manage permissions using administrative units in Microsoft Entra ID
- Elevate privileges

**07****4 Labs**

## Manage Tenant Health and Services in Microsoft 365

### TOPICS

- Monitor the health of your Microsoft 365 services

### MONITOR TENANT HEALTH USING:

- Microsoft 365 Adoption Score
- Microsoft 365 usage analytics
- Develop an incident response plan
- Request assistance from Microsoft

**08****4 Labs**

## Deploy Microsoft 365 Apps for Enterprise

### TOPICS

- Validate app readiness using the Readiness Toolkit
- Microsoft 365 Apps for enterprise deployment options
- Manage cloud apps and app updates using the Microsoft 365 Apps admin center
- Control how often their users get new features by specifying the update channel

**09**

## Analyze Your Microsoft 365 Workplace Data Using Microsoft Viva Insights

### TOPICS

- The analytical features of Microsoft Viva Insights
- Personal insights
- Team insights
- Organization insights
- Advanced insights

**10**

## Introduction to Microsoft 365 Copilot

### TOPICS

What is Microsoft 365 Copilot? · How Microsoft 365 Copilot Works · Core Components of Microsoft 365 Copilot · Microsoft's Commitment to Responsible AI

**11**

## Build Effective Presentations with AI (Copilot in PowerPoint)

### TOPICS

- Introduction to Copilot in Microsoft PowerPoint
- Craft Engaging Slides Using Copilot
- Refine and Enhance Presentations
- Build a Presentation from Start to Finish

12

## Draft Impactful Documents with AI (Copilot in Word)

### TOPICS

Craft Content with Copilot in Microsoft Word · Elevate Your Content in Word · Draft, Improve, and Share Documents

13

## Make Your Meetings More Productive with AI (Copilot in Teams)

### TOPICS

- Grow Collaboration with Copilot in Teams Chats
- Amplify Collaboration with Copilot in Teams Meetings
- Manage Collaboration from Start to Finish

14

## Uncover New Data Insights with AI (Copilot in Excel)

### TOPICS

- Simplify Data Summary, Analysis, and Visual Insights
- Customize Data Integration and Visualization with Copilot in Excel
- Boost Productivity with Data-Driven Decisions

15

## Improve Your Email Workflows with AI (Copilot in Outlook)

### TOPICS

- Draft Engaging Emails with Copilot in Outlook
- Simplify Meeting Administration with Copilot in Outlook
- Supercharge Collaboration with Outlook

16

Exercise

## Unlock Productivity and Creativity with AI-Powered Chat

### TOPICS

- Understand Microsoft 365 Copilot Chat
- Optimize Workflow with Work-Grounded Data
- Maximize Productivity with Web-Grounded Copilot Chat

17

## Examine Threat Vectors and Data Breaches

### TOPICS

Compromise user accounts through email · Gain control over resources · Compromise data

18

## Explore the Zero Trust Security Model

### TOPICS

- Effectively adapts to the complexity of the modern environment
- Embraces the mobile workforce
- Protects people, devices, apps, and data wherever they are located

19

## Explore Security Solutions in Microsoft Defender XDR

### TOPICS

Microsoft Defender for Office 365 · Microsoft Defender for Identity · Microsoft Defender for Endpoint · Microsoft 365 Threat Intelligence · Microsoft Defender for Cloud App Security

20

## Examine Microsoft Secure Score

### TOPICS

- Benefits of using Microsoft Secure Score
- Assessing your organization's security posture with Microsoft Secure Score
- Improving your secure score
- Tracking your Microsoft Secure Score history and meeting your goals

21

16 Labs

## Examine Privileged Identity Management

### TOPICS

Configure PIM for use in your organization · Audit PIM roles · Privileged Access Management

22

## Examine Microsoft Entra ID Protection

### TOPICS

- Most security breaches take place when attackers gain access to an environment by stealing a user's identity
- Microsoft Entra ID uses adaptive machine learning algorithms and heuristics to detect anomalies and suspicious incidents that indicate potentially compromised identities
- Using this data, Microsoft Entra ID Protection generates reports and alerts that enable organizations to evaluate the detected issues and take appropriate mitigation or remediation actions

24

## Examine Email Protection in Microsoft 365

### TOPICS

- EOP technologies that block spam, bulk email, and malware before mail arrives in users' mailboxes
- EOP protection against phishing, spoofing, and outbound spam filtering

25

## Enhance Your Email Protection Using Microsoft Defender for Office 365

### TOPICS

- Climb the security ladder from EOP to Microsoft Defender for Office 365
- Expand EOP using Safe Attachments and Safe Links
- Manage spoofed intelligence
- Outbound spam filtering policies
- Unblock users from sending email

26

Lab

## Manage Safe Attachments

### TOPICS

- Creating and modifying a Safe Attachments policy in the Microsoft Defender portal
- Creating a Safe Attachments policy by using Windows PowerShell
- Configuring a Safe Attachments policy
- Implementing a transport rule to bypass Safe Attachments scanning

**27****2 Labs**

## Manage Safe Links

### TOPICS

- Creating and modifying a Safe Links policy in the Microsoft Defender portal
- Creating a Safe Links policy by using Windows PowerShell
- Configuring a Safe Links policy to take certain actions
- Implementing a transport rule to disable the Safe Links functionality
- **Exercise 2:** Implement a Safe Links policy

**29****11 Labs**

## Explore Threat Intelligence in Microsoft Defender XDR

### TOPICS

Microsoft Intelligent Security Graph · How Microsoft Defender XDR uses alerts · Automated investigation and response · Threat hunting · Threat analytics and reports

**30**

## Implement App Protection by Using Microsoft Defender for Cloud Apps

### TOPICS

- Microsoft Defender for Cloud Apps features
- Deploying Microsoft Defender for Cloud Apps
- Controlling your Cloud Apps with policies
- Configuring Cloud Discovery in Microsoft Defender for Cloud Apps
- Troubleshooting Microsoft Defender for Cloud Apps

**31**

## Implement Endpoint Protection by Using Microsoft Defender for Endpoint

### TOPICS

Vulnerability management · Attack surface reduction · Next generation protection · Endpoint detection and response · Auto investigation and remediation

**32****12 Labs**

## Implement Threat Protection by Using Microsoft Defender for Office 365

### TOPICS

- Microsoft Defender for Office 365 protection stack
- Threat Explorer
- Threat Tracker widgets and views
- Attack simulation training

**34**

## Examine Data Governance Solutions in Microsoft Purview

### TOPICS

Data governance and compliance · Microsoft Purview Information Protection · Microsoft Purview Data Lifecycle Management · Microsoft Purview Insider Risk Management · Microsoft Purview eDiscovery solutions

**35**

## Explore Archiving and Records Management in Microsoft 365

### TOPICS

- Archive mailboxes in Microsoft 365
- Microsoft Purview Records Management
- Restore deleted data in Exchange and SharePoint

**36****7 Labs**

## Explore Retention in Microsoft 365

### TOPICS

- Retention policies and retention labels
- Principles of retention
- How organizations use Preservation Lock to restrict users

**37****3 Labs**

## Explore Microsoft Purview Message Encryption

### TOPICS

- Microsoft Purview Message Encryption
- Mail flow rules to encrypt email messages
- Organizational branding on encrypted email messages
- Microsoft Purview Advanced Message Encryption

**39**

## Explore Compliance in Microsoft 365

### TOPICS

- Planning for security and compliance in Microsoft 365 and Microsoft Purview
- Managing compliance requirements using Compliance Manager
- Analyzing the Microsoft Compliance Score

**40**

## Implement Microsoft Purview Insider Risk Management

### TOPICS

Insider risk management planning · Insider risk management policies · Insider risk management activities and alerts · Insider risk management cases

**41**

## Implement Microsoft Purview Information Barriers

### TOPICS

How to configure information barriers · Information barriers in Microsoft Teams · Information barriers in OneDrive · Information barriers in SharePoint Online

**42**

## Explore Microsoft Purview Data Loss Prevention

### TOPICS

DLP fundamentals in Exchange and SharePoint · Endpoint data loss prevention · DLP policies · DLP reporting tools

**43****5 Labs**

## Implement Microsoft Purview Data Loss Prevention

### TOPICS

- Create a DLP implementation plan
- Implement Microsoft Purview's default DLP policies
- Create a custom DLP policy
- Create policy tips for users when a DLP rule applies
- Configure email notifications for DLP policies

**45**

## Implement Data Classification of Sensitive Information

### TOPICS

Data classification in Microsoft 365 ·  
Trainable classifiers · Viewing sensitive data ·  
Document fingerprinting

**46**

## Explore Sensitivity Labels

### TOPICS

Insider risk management policies · Insider risk  
management activities and alerts · Insider risk  
management cases

**47****4 Activities**

## Implement Sensitivity Labels

### TOPICS

Sensitivity label requirements · Developing a data classification framework · How to create and publish sensitivity  
labels · How to remove and delete sensitivity labels

# Practise What You Learn

| #  | MODULE                                                  | ACTIVITY                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 01 | Configure Your Microsoft 365 Experience                 | <b>LABS</b> <ul style="list-style-type: none"> <li>■ Initialize your Microsoft 365 tenant</li> <li>■ Obtain your Microsoft 365 credentials</li> <li>■ Set up the Adatum's organization profile</li> <li>■ Create a custom theme for Adatum's pilot project team</li> <li>■ Enable Information Rights Management for SharePoint Online</li> <li>■ Turn on Audit Logging to enable Alert policies</li> <li>■ Install Microsoft Graph PowerShell</li> <li>■ Run a PowerShell script to create and publish a sensitivity label</li> </ul> |
| 03 | Manage Groups in Microsoft 365                          | <b>LABS</b> <ul style="list-style-type: none"> <li>■ <b>Exercise 2:</b> Manage users and groups</li> <li>■ Create a user account for Adatum's Enterprise Administrator</li> <li>■ Create and manage groups</li> <li>■ Recover groups using PowerShell</li> </ul>                                                                                                                                                                                                                                                                      |
| 04 | Add a Custom Domain in Microsoft 365                    | <b>LABS</b> <ul style="list-style-type: none"> <li>■ <b>Exercise 3:</b> Add a custom domain</li> <li>■ Add a custom domain</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                 |
| 06 | Configure Administrative Roles in Microsoft 365         | <b>LABS</b> <ul style="list-style-type: none"> <li>■ Manage administration delegation</li> <li>■ Assign Delegated Administrators in the Microsoft 365 admin center</li> <li>■ Manage Delegated Administrators with Windows PowerShell</li> <li>■ Verify Delegated Administration</li> </ul>                                                                                                                                                                                                                                           |
| 07 | Manage Tenant Health and Services in Microsoft 365      | <b>LABS</b> <ul style="list-style-type: none"> <li>■ <b>Exercise 2:</b> Monitor and troubleshoot Microsoft 365</li> <li>■ Troubleshoot Mail Flow in Microsoft 365</li> <li>■ Monitor service health and analyze reports</li> <li>■ Submit a Help request to Microsoft Support</li> </ul>                                                                                                                                                                                                                                              |
| 08 | Deploy Microsoft 365 Apps for Enterprise                | <b>LABS</b> <ul style="list-style-type: none"> <li>■ Install Microsoft 365 Apps for enterprise</li> <li>■ Verify how licensing affects installing Microsoft 365 Apps for enterprise</li> <li>■ Verify how the global Office download setting affects installing Microsoft 365 Apps for enterprise</li> <li>■ Perform a User-Driven Installation of Microsoft 365 Apps for enterprise</li> </ul>                                                                                                                                       |
| 16 | Unlock Productivity and Creativity with AI-Powered Chat | <b>Exercise:</b> Ace Your Interview Using Copilot Chat                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| #  | MODULE                                                | ACTIVITY                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21 | Examine Privileged Identity Management                | <b>LABS</b> <ul style="list-style-type: none"> <li>■ <b>Exercise 1:</b> PIM Administrator approval</li> <li>■ Configure the Global Admin role to require approval</li> <li>■ Assign an eligible group to the Global Admin role</li> <li>■ Submit a request for the Global Admin role</li> <li>■ Approve the request for the Global Admin role</li> <li>■ PIM Self-approval</li> <li>■ Create an eligible group for the Helpdesk Admin role</li> <li>■ Configure the Helpdesk Admin role for self-approval</li> <li>■ Self-activate the Helpdesk Admin role</li> <li>■ Verify a PIM notification was issued</li> <li>■ PIM Teammate approval</li> <li>■ Create a group for the Intune Admin role</li> <li>■ Configure the Intune Admin role to require approval</li> <li>■ Submit a request for the Intune Admin role</li> <li>■ Approve the request for the Intune Admin role</li> <li>■ Verify a PIM notification was issued</li> </ul> |
|    |                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 26 | Manage Safe Attachments                               | <b>Labs:</b> Create a Safe Attachment policy and turn on Microsoft Defender for Office 365                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 27 | Manage Safe Links                                     | <b>LABS</b> <ul style="list-style-type: none"> <li>■ Create a Safe Links policy</li> <li>■ Validate the Safe Links policy</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|    |                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 29 | Explore Threat Intelligence in Microsoft Defender XDR | <b>LABS</b> <ul style="list-style-type: none"> <li>■ Prepare for Alert Policies</li> <li>■ Assign RBAC permissions for Alert notification testing</li> <li>■ Implement a Mailbox Permission Alert</li> <li>■ Create a Mailbox Permission Alert</li> <li>■ Test the Mailbox Permission Alert</li> <li>■ Implement a SharePoint Permission Alert</li> <li>■ Create a SharePoint Permission Alert</li> <li>■ Test the SharePoint Permission Alert</li> <li>■ Test the Default eDiscovery Alert</li> <li>■ Review the Default eDiscovery Alert</li> <li>■ Test the Default eDiscovery Alert</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
|    |                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| #  | MODULE                                                                        | ACTIVITY                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 32 | <b>Implement Threat Protection by Using Microsoft Defender for Office 365</b> | <b>LABS</b> <ul style="list-style-type: none"> <li>■ Conduct a Spear Phishing attack using Attack Simulation training</li> <li>■ Enable Multifactor Authentication for the Global Admin</li> <li>■ Configure and launch a Spear Phishing attack</li> <li>■ Conduct a Drive-by URL attack using Attack Simulation training</li> <li>■ Configure and launch a Drive-by URL attack</li> <li>■ Validate alert notifications and simulated attacks</li> <li>■ Validate the Mailbox Permission alert</li> <li>■ Validate the SharePoint Permission alert</li> <li>■ Validate the default eDiscovery alert</li> <li>■ Validate the simulated Spear Phishing attack</li> <li>■ Validate the simulated Drive-by URL attack</li> <li>■ Disable Multifactor Authentication for the Global Admin</li> </ul> |
| 36 | <b>Explore Retention in Microsoft 365</b>                                     | <b>LABS</b> <ul style="list-style-type: none"> <li>■ Exercise 1 - Initialize Compliance</li> <li>■ Create a security group for compliance testing</li> <li>■ Configure Mobile Device Management for compliance testing</li> <li>■ Exercise 2 - Configure In-Place Archiving and Retention Policies</li> <li>■ Activate In-Place Archiving for a new user's mailbox</li> <li>■ Create an email retention policy for test users</li> <li>■ Create an email retention policy for all users</li> </ul>                                                                                                                                                                                                                                                                                              |
| 37 | <b>Explore Microsoft Purview Message Encryption</b>                           | <b>LABS</b> <ul style="list-style-type: none"> <li>■ <b>Exercise 3:</b> Create message encryption rules</li> <li>■ Create a mail flow encryption rule using the Exchange admin center</li> <li>■ Create a mail flow encryption rule using Windows PowerShell</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 43 | <b>Implement Microsoft Purview Data Loss Prevention</b>                       | <b>LABS</b> <ul style="list-style-type: none"> <li>■ Manage DLP Policies</li> <li>■ Create a DLP policy with custom settings</li> <li>■ Test the DLP Policy</li> <li>■ Test the first DLP Policy rule</li> <li>■ Test the second DLP Policy rule</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 47 | <b>Implement Sensitivity Labels</b>                                           | <b>LABS: IMPLEMENT SENSITIVITY LABELS</b> <ul style="list-style-type: none"> <li>■ Install the Azure Information Protection Unified Labeling client</li> <li>■ Create a sensitivity label</li> <li>■ Assign your Sensitivity Label to a document</li> <li>■ Verify your Sensitivity Label policy</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

#### WHAT IS INCLUDED

## Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

#### ABOUT KOENIG

## Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

#### FLEXIBLE DELIVERY

## Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

## Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit [koenig-solutions.com](https://koenig-solutions.com)

✉ [info@koenig-solutions.com](mailto:info@koenig-solutions.com)