Microsoft 365 Certified: Enterprise Administrator Expert

Microsoft 365 Enterprise Administrators evaluate, plan, migrate, deploy, and manage Microsoft 365 services.

Job role: Administrator
Prerequisites: 1 of 6 certifications
Required exams: MS-100 MS-101

Courses

Course MS-100T00-A: Microsoft 365 Identity and Services

40hours + 8 extra exam prep
Instructor-led training / live-online training
Intermediate
Preparation for exam: MS-100

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 tenant and service management, Office 365 management, and Microsoft 365 identity management. In Microsoft 365 tenant and service management, you will examine all the key components that must be planned for when designing your Microsoft 365 tenant. Once this planning phase is complete, you will learn how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscription options, component services, user accounts and licenses, and security groups. Finally, you will learn how to manage your tenant, which includes the configuration of tenant roles and managing your tenant health and services.
With your Microsoft 365 tenant now firmly in place, you will examine the key components of Office 365 management. This begins with an overview of Office 365 product functionality, including Exchange Online, SharePoint Online, Microsoft Teams, Microsoft Power Platform, additional product resources, and device management. You will then transition to configuring Office 365, with a primary focus on configuring Office client connectivity. Finally, you will examine how to manage Microsoft 365 Apps for enterprise (formerly Office 365 ProPlus) deployments, from user-driven client installations to centralized deployments. You will wrap up this section by learning how to configure Office Telemetry and Microsoft Analytics.
The course concludes with an in-depth examination of Microsoft 365 identity synchronization, with a focus on Azure Active Directory Connect. You will learn how to plan for and implement Azure AD Connect, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multi-factor authentication and self-service password

management. This section wraps up with a comprehensive look at implementing application and external access. You will learn how to add and manage applications in Azure Active Directory, including how to configure multi-tenant applications. You will then examine how to configure Azure AD Application Proxy, including how to install and register a connector and how to publish an on-premises app for remote access. Finally, you will examine how to design and manage solutions for external access. This includes licensing guidance for Azure AD B2B collaboration, creating a collaborative user, and troubleshooting a B2B collaboration.

Audience profile
This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Skills gained
- Designing, configuring, and managing your Microsoft 365 tenant
- Office 365 product functionality
- Configuring Office 365
- Managing Office 365 ProPlus deployments
- Planning and implementing identity synchronization
- Implementing application and external access

Prerequisites
- Completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration.
- A proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- A proficient understanding of general IT practices.

Course outline

Module 1: Designing Your Microsoft 365 Tenant
After completing this module, students will be able to:
- Determine which Microsoft 365 subscription offering best suits your organization’s requirements
- Understand how to best use Microsoft 365 component services to meet your organizational needs
- Plan your Microsoft 365 subscription
- Identify the steps necessary to successfully migrate existing data to Microsoft 365
- Prepare your organization for Microsoft 365
- Estimate your network's bandwidth
- Test your existing network using the tools provided by Microsoft
- Describe the best practices for integrating to Microsoft 365

- Identify the different deployment strategies for implementing Microsoft 365 services
- Describe authentication behavior when connecting with or without modern authentication
- Explain multi-factor authentication in Microsoft 365 deployments
- Create a plan for directory synchronization and Azure AD Connect Pass-through authentication
- Describe the issues, benefits, and best practices when implementing ADFS
- Plan for Azure AD Seamless Single Sign-On
- Plan your Email migration to Office 365
- Plan your file storage and collaboration requirements
- Plan your Microsoft Teams environment
- Plan for user and group synchronization using Azure AD Connect
- Plan for hybrid Exchange, SharePoint, and Skype for Business environments
- Plan your deployment using the Deployment Planning Checklist
- Analyze your Active Directory and plan any necessary clean-up using the ID Fix tool
- Determine which migration strategy to use to move your mail, calendar, and contact information
- Describe the performance and network issues to consider when planning your migration strategy

Module 2: Configuring Your Microsoft 365 Tenant

After completing this module, students will be able to:

- Complete your company's organization profile
- Maintain minimum subscription requirements for your company
- Manage your services and add-ins
- Describe the user identities in Microsoft 365
- Create user accounts from both the Microsoft 365 admin center and in Windows PowerShell
- Manage user accounts and licenses
- Recover deleted user accounts
- Describe the various types of groups available in Microsoft 365
- Create and manage groups from Microsoft 365 admin center and using Windows PowerShell
- Implement your domain services
- Plan DNS for custom domains
- Identify DNS record requirements for custom domains
- Add a custom domain to Microsoft 365
- Describe how FastTrack for Microsoft 365 helps customers deploy Microsoft 365

- Request a partner to assist you with the FastTrack process

Module 3: Managing Your Microsoft 365 Tenant

After completing this module, students will be able to:

- Describe the key admin roles in Microsoft 365
- Identify the key responsibilities of the primary admin roles
- Configure tenant roles
- Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center
- Develop an incident response plan to deal with incidents in your Microsoft 365 services
- Request assistance from Microsoft to address technical, pre-sales, billing, and subscription support
- Describe how Microsoft 365 Apps for enterprise click-to-run technology works
- Describe the Microsoft 365 Apps for enterprise licensing and activation processes
- Plan which update branch might be applicable for your organization
- Plan which method to use for applying update branches to your users
- Identify typical obstacles that prevent successful Microsoft 365 Apps for enterprise installations
- Identify how to prevent users from installing Microsoft 365 Apps for enterprise
- Install and configure Microsoft 365 Apps for enterprise with the Office Deployment Tool
- Deploy Microsoft 365 Apps for enterprise using Group Policy
- Describe how to manage Microsoft 365 Apps for enterprise updates

Module 4: Office 365 Overview

After completing this module, students will be able to:

- Describe the most common recipient types are available in Exchange Online
- Manage anti-malware and anti-spam policies in Exchange Online
- Plan your organization's disaster recovery needs related to company and user emails
- Determine retention tags and policies that will help you manage your organization’s email lifecycle
- Describe migration and coexistence strategies and understand the differences between them
- Select the right mail migration strategy for your organization
- Determine when you want to change the DNS MX record for a domain in an Office 365 migration

- Describe the different ways to migrate mailboxes to Office 365 in a hybrid Exchange environment
- Determine the permission levels that your organization should use in SharePoint Online
- Describe the levels of encryption for data at rest and data in transit within SharePoint Online
- Describe the SharePoint Online options for maintaining and recovering content in an intranet
- Describe the different options that provide anti-malware protection in SharePoint Online
- Describe basic Teams functionality and the infrastructure that supports its goals
- Describe how Teams compares to the other collaboration apps in Office 365
- Manage user licenses in the Office 365 Admin Center and PowerShell to provide Teams access
- Describe the functionality provided by Guess access in Microsoft Teams
- Describe audio conferencing functionality that is available in Microsoft Teams
- Manage user settings for audio conferencing
- Implement phone systems in Microsoft Teams
- Identify the components that make up the Power Platform product family
- Describe the basic features of the Power Platform Admin center
- Describe what Power Apps are, including their business impact and primary components
- Describe how Power Apps connect to data sources
- Create a basic Power App
- Test and monitor a Power App
- Run a Power App
- Describe the Power Apps security structure
- Build and run a basic workflow using Power Automate
- Administer Power Automate
- Build and share a basic Power BI report and dashboard
- Administer Power BI
- Explain what Power Virtual Agents are and how they empower teams to easily create powerful bots
- Describe key features of Power Virtual Agents
- Describe how device management enables organizations to protect and secure their resources and data
- Describe how organizations use Microsoft Intune to secure proprietary data
- Manage security baselines to secure devices

- Use conditional access to manage devices and apps

Module 5: Configuring Microsoft 365 Clients

After completing this module, students will be able to:

- Identify the client packages supported by Microsoft 365
- Identify the mobile clients supported by Microsoft 365
- Identify the Microsoft 365 features that are available for each mobile client platform
- Compare Office Online, Microsoft 365 Apps for enterprise, and Office 2016 Professional Plus
- Work with Office Online apps
- Describe how Outlook utilizes Autodiscover to initially connect an Outlook client to Exchange Online
- Identify the DNS records needed for Outlook to locate the services in Office 365 using Autodiscover
- Describe the connectivity protocols that enable Outlook to connect to Office 365
- Describe how MFA increases security by adding an extra layer of user verification

Module 6: Capturing User-Driven Data

After completing this module, students will be able to:

- Identify the five components of the Office Telemetry Dashboard
- Describe the typical deployment requirements and issues that you might encounter when deployment Off
- Describe the types of data collected by the Office Telemetry Agent
- Install and configure Office Telemetry
- Describe how Workplace Analytics can help organizations
- Describe how organizations can use Workplace Analytics
- Configure Workplace Analytics
- Enroll devices in Workplace Analytics
- Assess readiness using Workplace Analytics

Module 7: Planning and Implementing Identity Synchronization

After completing this module, students will be able to:

- Describe the Microsoft 365 authentication options
- Explain directory synchronization
- Provide an overview of Azure AD Connect
- Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD
- Plan an Azure AD Connect implementation
- Plan for Azure AD Connect in a multi-forest scenario
- Configure Azure AD Connect Prerequisites

- Set up Azure AD Connect
- Describe Azure AD Connect Health
- Perform tasks to ensure users synchronize efficiently and successfully deploy Azure AD Connect
- Manage groups with directory synchronization
- Use Azure AD Connect Sync Security Groups to delegate control in Azure AD Connect to other users
- Troubleshoot directory synchronization using a variety of troubleshooting tasks and tools
- Describe the available password management features in Microsoft 365

Module 8: Implementing Application and External Access
After completing this module, students will be able to:

- Register an application or service within your Azure AD tenant
- Update an application within the Azure AD consent framework
- Modify the configuration of a single-tenant application to make it a multi-tenant application
- Remove an application's registration from your Azure AD tenant
- Describe the benefits of Azure AD Application Proxy and how it works
- Identify Azure AD application proxy prerequisites
- Install and register a connector and verify that it installed correctly
- Publish an on-premises app for remote access and test the published app to verify that it functions
- Manage External Access with Azure AD B2B collaboration.
- Explain the difference between Microsoft 365 external access and Azure AD B2B collaboration
- Explain the attributes of a collaborative User.
- Demonstrate Azure B2B Collaboration
- Manage external access and guest access using Microsoft Teams
- Manage customer lockbox requests

Course MS-101T00-A: Microsoft 365 Mobility and Security
40hours + 8 extra exam prep
Instructor-led training / live-online training
Intermediate
Preparation for exam: MS-101

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management. In Microsoft 365 security management, you will examine all the common types of threat vectors and data breaches facing organizations today, and you will

learn how Microsoft 365's security solutions address these security threats. You will be introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You will then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments, and Safe Links. Finally, you will be introduced to the various reports that monitor your security health. You will then transition from security services to threat intelligence; specifically, using the Security Dashboard and Advanced Threat Analytics to stay ahead of potential security breaches.

With your Microsoft 365 security components now firmly in place, you will examine the key components of Microsoft 365 compliance management. This begins with an overview of all key aspects of data governance, including data archiving and retention, Information Rights Management, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365 message encryption, and data loss prevention (DLP). You will then delve deeper into archiving and retention, paying particular attention to in-place records management in SharePoint, archiving and retention in Exchange, and Retention policies in the Security and Compliance Center.

Now that you understand the key aspects of data governance, you will examine how to implement them, including the building of ethical walls in Exchange Online, creating DLP policies from built-in templates, creating custom DLP policies, creating DLP policies to protect documents, and creating policy tips. You will then focus on managing data governance in Microsoft 365, including managing retention in email, troubleshooting retention policies and policy tips that fail, as well as troubleshooting sensitive data. You will then learn how to implement Azure Information Protection and Windows Information Protection. You will conclude this section by learning how to manage search and investigation, including searching for content in the Security and Compliance Center, auditing log investigations, and managing advanced eDiscovery.

The course concludes with an in-depth examination of Microsoft 365 device management. You will begin by planning for various aspects of device management, including preparing your Windows 10 devices for co-management. You will learn how to transition from Configuration Manager to Intune, and you will be introduced to the Microsoft Store for Business and Mobile Application Management. At this point, you will transition from planning to implementing device management; specifically, your Windows 10 deployment strategy. This includes learning how to implement Windows Autopilot, Windows Analytics, and Mobile Device Management (MDM). When examining MDM, you will learn how to deploy it, how to enroll devices to MDM, and how to manage device compliance.

Audience profile

This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Skills gained

- Microsoft 365 Security Metrics
- Microsoft 365 Security Services
- Microsoft 365 Threat Intelligence
- Data Governance in Microsoft 365
- Archiving and Retention in Office 365
- Data Governance in Microsoft 365 Intelligence
- Search and Investigations
- Device Management
- Windows 10 Deployment Strategies
- Mobile Device Management

Prerequisites

- Completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration.
- A proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- A proficient understanding of general IT practices.

Course outline

Module 1: Introduction to Microsoft 365 Security Metrics

After completing this module, students will be able to:

- Describe several techniques hackers use to compromise user accounts through email
- Describe techniques hackers use to gain control over resources
- Describe techniques hackers use to compromise data
- Describe the Zero Trust approach to security in Microsoft 365.
- Describe the components of Zero Trust security.
- Describe and five steps to implementing a Zero Trust model in your organization.
- Explain Zero Trust networking
- List the types of threats that can be avoided by using EOP and Office 365 ATP
- Describe how Microsoft 365 Threat Intelligence can be benefit your organization
- Monitor your organization through auditing and alerts
- Describe how ASM enhances visibility and control over your tenant through three core areas
- Describe the benefits of Secure Score and what kind of services can be analyzed
- Describe how to collect data using the Secure Score API
- Know where to identify actions that will increase your security by mitigating risks

- Explain how to determine the threats each action will mitigate and the impact it has on use
- Explain Privileged Identity Management (PIM) in Azure administration
- Configure PIM for use in your organization
- Audit PIM roles
- Explain Microsoft Identity Manager
- Explain Privileged Access Management in Microsoft 365
- Describe Azure Identity Protection and what kind of identities can be protected
- Understand how to enable Azure Identity Protection
- Know how to identify vulnerabilities and risk events
- Plan your investigation in protecting cloud-based identities
- Plan how to protect your Azure Active Directory environment from security breaches

Module 2: Managing Your Microsoft 365 Security Services

After completing this module, students will be able to:

- Describe the anti-malware pipeline as email is analyzed by Exchange Online Protection
- List several mechanisms used to filter spam and malware
- Describe additional solutions to protect against phishing and spoofing
- Describe the benefits of the Spoof Intelligence feature
- Describe how Safe Attachments is used to block zero-day malware in email attachments and documents
- Describe how Safe Links protect users from malicious URLs embedded in email and documents
- Create and modify a Safe Attachments policy in the Security & Compliance Center
- Create a Safe Attachments policy by using Windows PowerShell
- Configure a Safe Attachments policy to take certain actions
- Understand how a transport rule can be used to disable the Safe Attachments functionality
- Describe the end-user experience when an email attachment is scanned and found to be malicious
- Create and modify a Safe Links policy in the Security & Compliance Center
- Create a Safe Links policy by using Windows PowerShell
- Understand how a transport rule can be used to disable the Safe Links functionality
- Describe the end-user experience when Safe Links identifies a link to a malicious website or file
- Describe how reports provide visibility into how EOP and ATP is protecting your organization
- Understand where to access reports generated by EOP and ATP
- Understand how to access detailed information from reports generated by EOP and ATP

Module 3: Microsoft 365 Threat Intelligence

After completing this module, students will be able to:

- Understand how threat intelligence is powered by the Microsoft Intelligent Security Graph
- Describe how the threat dashboard can benefit C-level security officers
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant
- Describe how the Security Dashboard displays top risks, global trends, and protection quality
- Describe what Advanced Thread Analytics (ATA) is and what requirements are needed to deploy it
- Configure Advanced Threat Analytics
- Manage the ATA services
- Describe Cloud App Security
- Explain how to deploy Cloud App Security
- Control your Cloud Apps with Policies
- Troubleshoot Cloud App Security

Module 4: Introduction to Data Governance in Microsoft 365

After completing this module, students will be able to:

- Understand Data Governance in Microsoft 365
- Describe the difference between In-Place Archive and Records Management
- Explain how data is archived in Exchange
- Recognize the benefits of In Place Records Management in SharePoint
- Explain the difference between Message Records Management (MRM) in Exchange and Retention in SCC.
- Understand how MRM works in Exchange
- List the types of retention tags that can be applied to mailboxes
- Know the different Microsoft 365 Encryption Options
- Understand how IRM can be used in Exchange
- Configure IRM protection for Exchange mails
- Explain how IRM can be used in SharePoint
- Apply IRM protection to SharePoint documents
- Tell the differences between IRM protection and AIP classification
- Describe the use of S/MIME
- Explain what digital signatures are
- Apply a digital signature to a message
- Understand how message encryption works
- Perform encryption on a message
- Accomplish decryption of a message
- Understand the co-operation of signing and encryption simultaneously
- Tell what triple-wrapped messages are
- Describe when you can use Office 365 Message Encryption
- Explain how Office 365 Message Encryption works

- Describe Data Loss Prevention (DLP)
- Understand what sensitive information and search patterns are that DLP is using
- Know what a DLP policy is and what it contains
- Recognize how actions and conditions work together for DLP
- Express how actions contain functions to send emails on matches
- Show policy tips to the users if a DLP rule applies
- Use policy templates to implement DLP policies for commonly used information
- Explain document finger
- Understand how to use DLP to protect documents in Windows Server FCI

Module 5: Archiving and Retention in Microsoft 365

After completing this module, students will be able to:

- Understand the process of records management
- Create a file plan for your organization
- Describe two methods for converting active docs to records
- Describe the benefits of In-Place Records Management
- Configure of In-Place Records Management for your organization
- Enable and disable In-Place Archiving
- Create useful retention tags
- Create retention policies to group retention tags
- Assign retention policies to mailboxes
- Allocate permissions and scripts to export and import retention tags
- Export all retention policies and tags from an organization
- Import all retention policies and tags to an organization
- Explain how a retention policy works
- Create a retention policy
- Manage retention policy settings

Module 6: Implementing Data Governance in Microsoft 365 Intelligence

After completing this module, students will be able to:

- Describe the Microsoft 365 Compliance Center and how to access it
- Describe the purpose and function of Compliance score
- Explain the components of of how an organization's Compliance score is determined
- Explain how assessments are used to formulate compliance scores
- Explain how Microsoft 365 helps address Global Data Protection Regulation
- Describe insider risk management functionality in Microsoft 365
- Configure insider risk management policies
- Configure insider risk management policies
- Explain the communication compliance capabilities in Microsoft 365
- Describe what an ethical wall in Exchange is and how it works
- Explain how to create an ethical wall in Exchange

- Identify best practices for building and working with ethical walls in Exchange
- Understand the different built-in templates for a DLP policies
- Determine how to choose the correct locations for a DLP policy
- Configure the correct rules for protecting content
- Enable and review the DLP policy correctly
- Describe how to modify existing rules of DLP policies
- Explain how to add and modify custom conditions and action to a DLP rule
- Describe how to change user notifications and policy tips
- Configure the user override option to a DLP rule
- Explain how incident reports are sent by a DLP rule violation
- Describe how to work with managed properties for DLP policies
- Explain how SharePoint Online creates crawled properties from documents
- Describe how to create a managed property from a crawled property in SharePoint Online
- Explain how to create a DLP policy with rules that apply to managed properties via PowerShell
- Describe the user experience when a user creates an email or site containing sensitive information
- Explain the behavior in Office apps when a user enters sensitive information

Module 7: Managing Data Governance in Microsoft 365

After completing this module, students will be able to:

- Determine when and how to use retention tags in mailboxes
- Assign retention policy to an email folder
- Add optional retention policies to email messages and folders
- Remove a retention policy from an email message
- Explain how the retention age of elements is calculated
- Repair retention policies that do not run as expected
- Understand how to systematically troubleshoot when a retention policy appears to fail
- Perform policy tests in test mode with policy tips
- Describe how to monitor DLP policies through message tracking
- Describe the required planning steps to use AIP in your company
- Configure and customize labels
- Create policies to publish labels
- Plan a Deployment of the Azure Information Protection client
- Configure the advance AIP service settings for Rights Management Services (RMS) templates
- Implement automatic and recommended labeling
- Activate the Super User feature for administrative tasks
- Create your tenant key for encryption
- Deploy the AIP scanner for on-premises labeling

- Plan RMS connector deployment to connect on-premises servers
- Describe WIP and what it is used for
- Plan a deployment of WIP policies
- Implement WIP policies with Intune and SCCM
- Implement WIP policies in Windows desktop apps

Module 8: Managing Search and Investigations

After completing this module, students will be able to:

- Describe how to use content search
- Design your content search
- Configure search permission filtering
- Explain how to search for third-party data
- Describe when to use scripts for advanced searches
- Describe what the audit log is and the permissions that are necessary to search the Office 365 audit
- Configure Audit Policies
- Enter criteria for searching the audit log
- View, sort, and filter search results
- Export search results to a CSV file
- Search the unified audit log by using Windows PowerShell
- Describe Advanced eDiscovery
- Configure permissions for users in Advanced eDiscovery
- Create Cases in Advanced eDiscovery
- Search and prepare data for Advanced eDiscovery

Module 9: Planning for Device Management

After completing this module, students will be able to:

- Describe the benefits of Co-management
- Plan your organization's Co-management Strategy
- Describe the main features of Configuration Manager
- Describe how Azure Active Directory enables co-management
- Identify the prerequisites for using Co-management
- Configure Configuration Manager for Co-management
- Enroll Windows 10 Devices to Intune
- Modify your co-management settings
- Transfer workloads to Intune
- Monitor your co-management solution
- Check compliance for co-managed devices
- Describe the feature and benefits of the Microsoft Store for Business
- Configure the Microsoft Store for Business
- Manage settings for the Microsoft Store for Business

Module 10: Planning Your Windows 10 Deployment Strategy

After completing this module, students will be able to:

- Plan for Windows as a Service
- Plan a Modern Deployment

- Plan a Dynamic Deployment
- Plan a Traditional Deployment
- Describe Windows Autopilot requirements
- Configure Autopilot
- Create and Assign an Autopilot profile
- Deploy and validate Autopilot
- Describe Autopilot Self-deployments, White Glove deployments, and User-drive deployments
- Deploy BitLocker Encryption for Autopiloted Devices
- Understand Windows 10 Enterprise E3 in CSP
- Configure VDA for Subscription Activation
- Deploy Windows 10 Enterprise licenses
- Describe common fixes for Windows 10 upgrade errors
- Use SetupDiag
- Troubleshooting upgrade errors
- Describe Windows error reporting
- Understand the upgrade error codes and resolution procedure
- Describe Windows Analytics
- Describe Device Health
- Describe Update Compliance
- Determine Upgrade Readiness

Module 11: Implementing Mobile Device Management

After completing this module, students will be able to:

- Manage devices with MDM
- Compare MDM for Office 365 and Intune
- Understand policy settings for mobile devices
- Control Email and Document Access
- Activate Mobile Device Management Services
- Deploy Mobile Device Management
- Configure Domains for MDM
- Configure an APNs Certificate for iOS devices
- Manage Device Security Policies
- Define a Corporate Device Enrollment Policy
- Enroll devices to MDM
- Understand the Apple Device Enrollment Program
- Understand Enrollment Rules
- Configure a Device Enrollment Manager Role
- Describe Multi-factor Authentication considerations
- Plan for device compliance
- Configure conditional users and groups
- Create Conditional Access policies
- Monitor enrolled devices

For more information:

Hellenic American Education Center

Center for Life Long Learning

Technology Training

Tel. 2103680966, 2103680912

e-mail: it@haec.gr