Auditing Microsoft 365 and Azure Cloud Security

This is a one-day course for auditors and security teams responsible for security and compliance of their Microsoft 365 and Azure Active Directory (AzureAD) environments. This course will provide students with knowledge and practical skills to audit Microsoft 365 tenants, and to improve security of Microsoft 365 configuration and monitoring capabilities. This course is designed with real world scenarios in mind to provide **practical**, effective approaches for asking and answering compliance questions, auditing Microsoft 365 before and after solution adoption; **practitioner approach to continuous audit,** monitoring, and creating additional security and compliance visibility. At the end of the course student will be able to effectively audit Microsoft 365 configuration and organization compliance, understand and improve security of the environment, and implement basic continuous audit and monitoring of the organization Microsoft 365 tenant.

Audience profile: This course is intended for IT professional, managers, system administrators, cybersecurity teams and auditors responsible for managing, securing and auditing Microsoft 365 environments (tenants).

At course completion students will be able to:

- Answer questions and describe how Microsoft 365 complies with various regulatory frameworks and data protection standards
- Assure proper basic Microsoft 365 configuration before solution adoption and email migration
- Audit Microsoft 365 configuration after adoption (email migration) using graphical user interface (GUI) – Azure Active Directory (AzureAD), Security & Compliance center, Cloud App Security, Microsoft 365 Admin center, Exchange, SharePoint, Teams, Intune.
- Audit specific Microsoft 365 elements that require use of PowerShell
- Understand and use Security & Compliance Center for continuous audit / monitoring
- Understand Windows Defender Security ATP Center role and capabilities in protecting the organization
- Understand how Azure security tools can enhance organization security and compliance, by integrating data from multiple computing platforms and environments. Audit and configure Azure security tools for Microsoft 365 and some other computing platforms.
- Understand how Microsoft 365 cybersecurity strategy works and protects users, devices and data when implemented correctly.

Students will receive PDF copies of entire course, including screenshots, talking points (PowerPoint with notes) and verbiage associated with the training, auditing PowerShell scripts, Excel templates and resources.

Students should be able to run hands-on labs:

- Using own PCs (Win 10 Pro recommended) (with PowerShell Exchange Online module installed)
- Using own Microsoft 365 tenant.

Instructor / author: Robert Brzezinski MBA, CISA, CHPS, CISM

Workshop format:

1. Slide deck used for demonstrating audit approaches and M365 interface associated with specific phases
    a. PDF version and additional materials provided to attendees – download from SharePoint or OD4B, will need attendees email address
2. Microsoft demo environment used for navigating through M365 and Azure modules and demonstrating functionality and security capabilities
3. PowerShell Exchange Online used for demonstrating some PowerShell commands used in audit.

Attendees hands-on participation will require:

1. Laptop – Windows 10 Pro recommended
2. M365 or O365 existing tenant
    a. Participant will need Global Admin privileges to see or interact with all functionalities
    b. Install PowerShell Exchange Online module for trying some PowerShell commands
3. O365 tenant can be a trial subscription obtained from https://www.microsoft.com/en-us/microsoft-365/business/compare-more-office-365-for-business-plans
    a. Choose O365 E3 or E5 trial (Enterprise subscriptions)
    b. !!! Trial subscriptions last 30 days – coordinate timing of your trial subscription !!!
    c. Add a few fictious users to your tenant before workshop
4. Azure subscription (Not a must have), (Pay-as-you-go recommended) is required to interact with Azure security tools.
    a. Steps below assure that your Azure subscription will be associated with your O365/M365 tenant AzureAD
    b. From O365/M365 Admin center -> navigate to Azure Active Directory
    c. Replace address https://aad.portal.azure.com with https://portal.azure.com/
    d. Type subscriptions in Search box at the top -> navigate to Subscriptions -> Add Subscription
    e. Select Free trial if available or Pay-as-you-go -> you will need to provide credit card number in both scenarios
        i. Cost consumed will be minimal if any -> unless participant starts creating additional resources e.g. VMs, storage etc.
        ii. Azure Pay-as-you-go Subscription can be canceled at any time – delete resources before canceling to avoid any charges