Mastering Compliance and Security in Microsoft 365 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

- **Microsoft 365 genelinde Microsoft Purview uyumluluk ve güvenlik kontrollerini uygulayın.**
- **Microsoft 365 ortamlarında veri koruma, güvenlik ve uyumluluk süreçlerinden sorumlu profesyoneller için tasarlanmıştır.**
- **Uygulamalı laboratuvar çalışmaları için her katılımcıya gerçek bir Microsoft 365 tenant ortamı sağlanır.**

Microsoft 365'te Uyumluluk ve Güvenlik Uzmanlığı, Microsoft 365 ortamlarında güvenlik, veri koruma ve uyumluluk gereksinimlerini Microsoft Purview çözümleriyle yönetmeye odaklanan, uygulamalı laboratuvarlarla desteklenen kapsamlı bir **5 günlük eğitimdir**.

Eğitim boyunca katılımcılar Microsoft Purview'un Microsoft 365 için sunduğu uyumluluk ve güvenlik özelliklerini hem kavramsal hem de uygulamalı olarak ele alır. Program; Microsoft 365 Business, E3 ve E5 dahil olmak üzere farklı Microsoft 365 aboneliklerinde kullanılabilen ilgili özellik ve çözümleri kapsar.

Eğitim, Microsoft Information Protection yaklaşımının temel aşamalarını destekleyecek şekilde yapılandırılmıştır:

- Verilerinizi tanıma
- Verilerinizi koruma
- Veri kaybını önleme
- Verilerinizi yönetme ve yönetişim altına alma

Program kapsamında Microsoft Purview Portal, veri sınıflandırma, Content Search, eDiscovery, veri saklama, SharePoint güvenliği ve harici paylaşım, Microsoft 365 Groups ve Teams yönetişimi, Sensitivity Labels, Microsoft Defender for Cloud Apps, Insider Risk Management, Data Loss Prevention (DLP), denetim ve uyumluluk araçları gibi konular ayrıntılı biçimde ele alınır.

Uygulamalı Laboratuvarlar

Katılımcılara isteğe bağlı laboratuvar çalışmalarını gerçekleştirebilmeleri için**30 gün süreyle kullanılabilen ticari bir Microsoft 365 tenant ortamı** sağlanır.

Laboratuvarlarda öncelikle Microsoft 365 ortamı örnek verilerle hazırlanır. Katılımcılar daha sonra eğitim sırasında öğrendikleri Microsoft Purview ve Microsoft 365 güvenlik/uyumluluk çözümlerini bu ortam üzerinde uygular.

Laboratuvarlar isteğe bağlıdır ve katılımcıların ihtiyaçlarına göre belirli çalışmaları seçebilecekleri şekilde hazırlanmıştır.

Not: Microsoft Purview servislerinin çalışma ve işleme süreleri nedeniyle bazı laboratuvar sonuçlarının oluşması birkaç saat veya daha uzun sürebilir. Bu nedenle tüm çalışmalar eğitim süresi içerisinde tamamlanamayabilir. Katılımcıların Microsoft 365 tenant ortamına 30 gün boyunca erişebilmesi, kalan uygulamaları eğitim sonrasında tamamlamalarına imkân verir.

Mastering Compliance and Security in Microsoft 365 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Prerequisites

Katılımcıların Microsoft 365'in temel teknolojileri hakkında genel bilgi sahibi olmaları ve Microsoft Purview'un güvenlik, veri koruma ve uyumluluk açısından sağlayabileceği iş faydalarına ilgi duymaları önerilir.

Çok Faktörlü Kimlik Doğrulama (MFA)

Eğitim sırasında **Multi-Factor Authentication (MFA)** kullanılması gerekebilir. Bu nedenle katılımcıların eğitim öncesinde Microsoft Authenticator veya uyumlu başka bir kimlik doğrulama uygulamasını mobil cihazlarına yüklemeleri önerilir.

Microsoft'un MFA gereksinimleri ve ilgili güvenlik politikaları eğitim öncesinde kontrol edilmelidir.

Eğitmen, program boyunca temel özellikleri ve uygulamaları canlı olarak gösterecektir. Katılımcılar ayrıca kendilerine sağlanan 30 günlük Microsoft 365 tenant ortamında isteğe bağlı laboratuvar çalışmalarını gerçekleştirebilir.

Who Should Attend

Bu eğitim özellikle aşağıdaki katılımcılar için uygundur:

- Microsoft 365 IT profesyonelleri,
- Microsoft 365 yöneticileri,
- Veri koruma ve bilgi güvenliği ekipleri,
- Uyumluluk ve yönetişim süreçlerinden sorumlu profesyoneller,
- Microsoft Purview çözümlerini kurumlarında uygulamak isteyen teknik uzmanlar,
- Microsoft 365 ortamlarında güvenlik ve uyumluluğun nasıl uygulanacağını öğrenmek isteyen ilgili paydaşlar.

Outline

Modül 1 – Uyumluluk Standartları ve Microsoft Yaklaşımı

- Microsoft'un uyumluluk yaklaşımı
- Microsoft Shared Responsibility Model
- Microsoft Cybersecurity Reference Architecture (MCRA)
- Microsoft Purview'a giriş
- Microsoft Purview Portal ve PowerShell
- Purview lisanslama, roller ve izinler
- Entra ID yönetici rolleri
- Microsoft Purview rolleri
- Administrative Units
- Entra ID Privileged Identity Management (PIM)
- Purview rolleri için PIM

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Entra ID Access Reviews
- Microsoft 365 uyumluluk ortamındaki değişikliklerin yönetimi
- Uygulamalı PIM, kullanıcı ve grup çalışmaları

Modül 2 – Microsoft 365 Arama ve Veri Sınıflandırma Kavramları

- Microsoft Search
- SharePoint içeriklerinin eDiscovery açısından kullanımı
- SharePoint columns, search schema ve content types
- Purview Content Search ve eDiscovery özellikleri
- Microsoft Syntex
- Syntex classifiers ve extractors
- Sensitivity ve Retention Labels
- Microsoft Purview Data Classification
- Sensitive Information Types (SIT)
- Named Entities
- Custom Sensitive Information Types
- Exact Data Match (EDM)
- Trainable Classifiers
- Microsoft Purview Data Explorer
- SharePoint, Syntex ve Exact Data Matching laboratuvarları

Modül 3 – Microsoft 365 Content Search

- Content Search yapısı ve güvenliği
- eDiscovery Administrator ve Manager rolleri
- Güvenlik filtreleme
- Content Search limitleri
- Microsoft Teams içeriklerinde arama
- Targeted Collection Search
- KQL Editor ve Condition Card Builder
- Arama sonuçlarının önizlenmesi ve istatistikleri
- PowerShell üzerinden Content Search
- Arama sonuçlarının dışa aktarılması
- Unindexed Items
- eDiscovery sonuçlarında deduplication
- E-posta mesajlarını arama ve temizleme
- Çoklu Content Search işlemlerinin yönetimi
- Uygulamalı Content Search laboratuvarı

Modül 4 – Microsoft 365 eDiscovery

- Microsoft 365 eDiscovery görevleri ve vakaları
- eDiscovery güvenliği
- Compliance Boundaries
- eDiscovery Case oluşturma ve üyeleri yönetme
- İçeriklerin hold altında korunması
- Microsoft Teams eDiscovery
- Exchange Online Litigation Hold
- eDiscovery aramalarını oluşturma ve çalıştırma
- Sonuçların dışa aktarılması
- Vakaların kapatılması ve silinmesi

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Uygulamalı eDiscovery laboratuvarı

Modül 5 – Premium eDiscovery

- Standard ve Premium eDiscovery karşılaştırması
- Premium eDiscovery gereksinimleri ve lisanslama
- Roller ve izinler
- Premium eDiscovery workflow
- Attorney-client privilege
- Guest Users
- Tag Templates
- Data Custodians ve Non-Custodian Data Sources
- Collections ve Review Sets
- Microsoft Teams verilerinin işlenmesi
- Microsoft 365 dışındaki kaynaklardan veri yükleme
- Veri işleme ve hata giderme
- Review Set filtreleri, sorguları ve gruplama
- İçerik etiketleme
- Arama ve analitik özellikleri
- Case Data dışa aktarma

Modül 6 – Microsoft 365 Veri Saklama ve İmha Yönetimi

- Microsoft 365 Retention seçenekleri ve lisanslama
- Retention Policies
- Adaptive ve Static Retention Policies
- Adaptive Scopes
- Retention Policy Locations
- Teams retention gereksinimleri
- Preservation Lock
- Retention Labels
- Otomatik Retention Label uygulama yöntemleri
- Record Retention Labels
- Event-Driven Retention
- Disposition Reviews
- Regulatory Records
- Label Publishing ve Label Policies
- Retention izleme ve denetleme
- PowerShell ile Retention yönetimi
- Retention precedence
- Inactive Mailboxes
- Inactive Mailbox kurtarma ve geri yükleme yöntemleri
- Uygulamalı Retention Policies ve Retention Labels laboratuvarları

Modül 7 – SharePoint Güvenliği

- SharePoint izin modeli
- Team Sites ve Communication Sites
- Access Requests ve Sharing seçenekleri
- SharePoint Site Access
- Site, Document Library, List, Folder ve Item paylaşımı
- Advanced Permissions

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Permission Levels
- Explicit Permissions
- Permission Inheritance
- SharePoint Groups
- SharePoint Admin Center üzerinden izin yönetimi
- PowerShell ile SharePoint izinleri
- SharePoint güvenliği için iyi uygulamalar
- Restricted Access Control
- Block Download Policy
- Site Lifecycle Management
- SharePoint Antivirus
- OneDrive Sync Client
- Malware Detection Alerts
- Uygulamalı SharePoint Security laboratuvarı

Modül 8 – SharePoint Harici Paylaşım

- SharePoint External Sharing
- Authenticated External User Sharing
- Anonymous Access Links
- Tenant seviyesinde harici paylaşım yönetimi
- Entra ID B2B One-Time Passcodes
- Harici kullanıcıların önceden oluşturulması
- Gelişmiş External Sharing ayarları
- File ve Folder Links
- Site seviyesinde paylaşım seçenekleri
- Outlook Sharing Links
- PowerShell ile External Sharing
- Harici paylaşım uyarıları, Audit Logging ve Monitoring
- Uygulamalı External Sharing laboratuvarı

Modül 9 – Microsoft 365 Groups ve Teams

- Microsoft 365 Groups mimarisi
- Grup oluşturma, silme ve kurtarma
- Guest Access
- Microsoft 365 Admin Center ve Entra ID B2B kontrolleri
- Domain bazlı Guest Access
- PowerShell ile Microsoft 365 Groups yönetimi
- Grup oluşturmanın kontrol edilmesi
- Eski grupların bulunması ve arşivlenmesi
- Microsoft 365 Groups Governance
- Microsoft Teams Governance
- Teams rolleri ve izinları
- Teams kullanıcı erişimi
- External Access ve Guest Access
- Uygulamalı Microsoft 365 Groups laboratuvarı

Modül 10 – Sensitivity Labels

- Microsoft 365 Sensitivity Labels
- Dosya ve öğeler için etiketleme

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- PDF desteği
- Visual Marking, Watermarks, Headers ve Footers
- Encryption
- Double Key Encryption
- Co-Authoring
- Toplantılar için Sensitivity Labels
- Otomatik etiketleme
- Auto-Labelling Policies
- Microsoft Syntex ile etiket atama
- Microsoft Defender for Cloud Apps File Policies
- Teams, Microsoft 365 Groups ve SharePoint Sites için etiketleme
- Authentication Contexts
- Label Priority, Grouping ve Sublabels
- Label Policies
- Label Reports
- Data Access Governance Reports
- Sensitivity Label sorun giderme
- PowerShell ile Sensitivity Labels
- Uygulamalı Sensitivity Labels laboratuvarı

Modül 11 – Microsoft Defender for Cloud Apps

- Microsoft Defender for Cloud Apps'a genel bakış
- Lisanslama ve yönetici rolleri
- Network Requirements
- Automated Setup
- Uygulamaların bağlanması
- Cloud Discovery Dashboard
- Cloud App Catalog
- App Sanctioning
- Activity Log
- User Groups
- Scoped Deployment ve Privacy
- Investigations
- Files ve OAuth Apps
- App Governance
- Policies
- Session Policies
- Conditional Access App Control
- Policy Templates ve Alerts
- Uygulamalı Microsoft Defender for Cloud Apps laboratuvarı

Modül 12 – Insider Risk Yönetimi

- Insider Risk Management kavramları ve senaryoları
- Insider Risk Management süreci ve gereksinimleri
- Analytics ve Data Sharing
- Detection Groups ve Global Exclusions
- Intelligent Detections
- Policy Indicators ve Custom Indicators
- Priority Users ve Priority Physical Assets
- Privacy

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Policies, Alerts ve Cases
- Case Actions ve çözüm süreçleri
- Insider Risk Adaptive Protection
- Forensic Evidence
- Insider Risk Auditing
- Communication Compliance
- Communication Compliance Policies
- Investigation ve Resolution
- Information Barriers
- OneDrive, SharePoint ve Teams için Information Barriers
- Kullanıcı segmentlerinin yapılandırılması

Modül 13 – Microsoft 365 Data Loss Prevention (DLP)

- Microsoft 365 DLP temelleri
- DLP Policy bileşenleri
- DLP Policy oluşturma
- Custom DLP Policies
- Policy Locations ve Settings
- DLP Conditions ve Actions
- User Notifications ve Overrides
- Incident Reports
- Endpoint DLP
- Microsoft Edge üzerinde hassas veri aktivitelerinin kısıtlanması
- Device Restrictions
- File Activity Auditing ve Restrictions
- Restricted Apps Activities
- DLP Activity Explorer
- DLP Alerts
- Uygulamalı Data Loss Prevention laboratuvarı

Modül 14 – Denetim, Uyarılar, Raporlama ve Uyumluluk Araçları

- Microsoft 365 Auditing
- Audit Log Permissions
- Audit Log Search
- Sonuçların görüntülenmesi ve dışa aktarılması
- Audit Log Retention Policies
- Microsoft 365 Alerts
- Compliance Manager ve Compliance Score
- Automated Testing
- Microsoft Regulations and Assessments
- Microsoft Configuration Analyzer for Microsoft Purview (CAMP)
- Microsoft 365 Secure Score
- Compliance Score ve Secure Score için iyi uygulamalar
- Auditing, Alerts, Compliance Score ve Secure Score laboratuvarları