

AB 650- Administering Microsoft 365 and AI Services



Days: 3

Prerequisites: Before attending this course, students must have hands-on experience configuring and managing core Microsoft 365 workloads, knowledge of identity governance, user management, and access controls in Microsoft Entra ID, an understanding of Microsoft Defender XDR's extended detection and response security capabilities, and familiarity with running Microsoft Graph PowerShell commands and performing bulk management tasks.

Audience: This course is designed for users who configure, manage, secure, and govern Microsoft 365 tenants, workloads, and AI services, including Microsoft 365 Copilot, agents, and connected AI capabilities. You enable secure, compliant, and scalable productivity across the organization by governing data access, protecting information, and supporting collaboration between users and agents. You operate and continuously optimize Microsoft 365 and AI services at enterprise scale, helping to ensure reliable and effective outcomes in an AI-powered workplace.

Description: In this course, you will learn how to configure, manage, secure, and govern Microsoft 365 tenants, traditional workloads, and AI services like Microsoft 365 Copilot and AI agents. As a Microsoft 365 and AI services administrator, you collaborate with architects and administrators across workloads, infrastructure, identity, security, compliance, endpoints, and applications.

Course Objectives: Through this course, students will learn to:

- **Configure and Manage Tenants and Workloads**
 - **Tenant Setup:** Configure branding, custom themes, domains, and organizational settings.
 - **Licensing:** Manage user licenses, group-based licensing, and pay-as-you-go billing for standard and AI tools.
 - **Core Services:** Operate Exchange Online, SharePoint Online, OneDrive, and Microsoft Teams.
 - **Operations:** Monitor service health, network connectivity insights, and Microsoft 365 Backup.
- **Govern and Secure Microsoft 365**
 - **Identity & Access:** Manage Microsoft Entra ID, multifactor authentication (MFA), Conditional Access policies, and Privileged Identity Management (PIM).
 - **Threat Protection:** Use Microsoft Defender for Office 365 to investigate alerts and handle security policies.
 - **Compliance & Data:** Implement Microsoft Purview features like Data Loss Prevention (DLP), sensitivity labels, retention policies, and data security posture management (DSPM) for AI.
- **Manage and Secure AI Services**
 - **Copilot Administration:** Deploy Microsoft 365 Copilot, set up connectors, and manage tenant-level readiness.
 - **Agent Governance:** Administer Microsoft Agent 365, configure AI agent identities using Microsoft Entra Agent ID, and control access.
 - **Usage & Costs:** Monitor AI adoption rates, track service consumption, and audit operational costs.

OUTLINE:

LEARNING PATH: CONFIGURE AND MANAGE MICROSOFT 365 TENANTS AND WORKLOADS

- **Modules:**
 - Provision and brand a Microsoft 365 tenant
 - License Microsoft 365 and AI services at scale
 - Keep a Microsoft 365 tenant resilient and healthy
 - Configure Exchange Online and Microsoft Teams workloads

Baton Rouge | Lafayette | New Orleans

www.lantecctc.com

AB 650- Administering Microsoft 365 and AI Services

- Govern SharePoint and OneDrive for Microsoft 365 Copilot
- Exercises:
 - Delegate domain administration and add a custom domain
 - Configure organization branding
 - Configure organizational settings
 - Assign, verify, and troubleshoot Microsoft 365 Copilot licensing for Relecloud's marketing rollout
 - Configure pay-as-you-go billing for Relecloud's Copilot Studio pilot team
 - Configure Backup for Relecloud's critical workloads
 - Interpret Relecloud's Copilot adoption data
 - Configure Relecloud shared mailboxes and delegate access
 - Build a Copilot-ready team for Relecloud's account managers
 - Set up and audit a governed SharePoint site
 - Remediate the Finance site and choose the right control

LEARNING PATH: GOVERN AND SECURE MICROSOFT 365 TENANTS AND WORKLOADS

- Modules:
 - Provision and govern identities in Microsoft Entra
 - Implement authentication and access in Microsoft Entra
 - Secure email and collaboration with Microsoft Defender for Office 365
 - Protect information with Microsoft Purview information protection
 - Prevent data loss and govern the data lifecycle with Microsoft Purview
- Exercises:
 - Bulk-provision Relecloud's new-hire users with Microsoft Graph PowerShell
 - Scope Relecloud's regional HR admin with an administrative unit

- Scope authentication methods and enable SSPR for Relecloud's engineering team
- Build and verify a risk-based, device-compliant Conditional Access policy
- Configure and scope threat protection for Relecloud's finance team
- Investigate a threat and reduce human risk with attack simulation training
- Create a custom sensitive information type for Woodgrove's transaction pattern
- Configure and publish a sensitivity label policy, then verify priority resolution
- Create a DLP policy for Microsoft 365 Copilot
- Review a DLP alert in Microsoft Defender XDR
- Review a DSPM for AI data risk assessment

LEARNING PATH: MANAGE AND SECURE MICROSOFT 365 AI SERVICES

- Modules:
 - Assess readiness and roll out Microsoft 365 Copilot
 - Take action in external systems using connector and REST API agent tools in Microsoft Copilot Studio
 - Ground agents with enterprise knowledge using connectors and Azure AI Search in Microsoft Copilot Studio
 - Integrate agents with external systems via MCP in Microsoft Copilot Studio
- Exercises:
 - Run and interpret the Copilot readiness report
 - Remediate an oversharing risk before rollout
 - Stage a phased pilot rollout group