Implement Privileged Identity Management

At the end of this episode, I will be able to:

1. Implement privileged identity management for Azure AD roles

Learner Objective: *Learn about Privileged Identity Management (PIM) in the context of Microsoft 365*

Description: In this episode, you will learn about PIM in the context of Microsoft 365. This feature enables you to manage, control, and monitor access to important resources in your organization.

- Privileged Identity Management (PIM) is a service in Azure Active Directory that enables management of important resources in the tenant
- Thanks to PIM, organizations can give users just-in-time privileged access to Azure AD and Azure AD resources
- Use of this feature requires an Azure AD Premium P2 license
- Some key features include:
    - Provide just-in-time privileged access to Azure AD and Azure resources
    - Assign time-bound access to resources using start and end dates
    - Require approval to activate privileged roles
    - Enforce multi-factor authentication to activate any role
    - Use justification to understand why users activate
    - Get notifications when privileged roles are activated
    - Conduct access reviews to ensure users still need roles
    - Download audit history for internal or external audit
    - Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments
- Once you set up Privileged Identity Management, you'll see Tasks, Manage, and Activity options in the left navigation menu.
- As an administrator, you'll choose between options such as managing Azure AD roles, managing Azure resource roles, or PIM for Groups.
- When you choose what you want to manage, you see the appropriate set of options for that option.

Additional Resources:

What is Azure AD Privileged Identity Management?
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure