Privileged Identity Management (PIM) in Azure enables just-in-time (JIT) access with approval workflows and time-bound role assignments. To configure PIM for **Reader** and **Contributor** roles in your **Azure subscription**, follow this end-to-end process:

**Step 1: Enable PIM for Subscription Roles**

1. **Sign in** to the [Azure Portal](https://portal.azure.com) with a **Global Administrator** or **Privileged Role Administrator** account.
2. Navigate to **Azure AD** > **Privileged Identity Management**.
3. Under **Manage**, select **Azure resources**.
4. Click on **Discover resources** and select your **Azure subscription**.
5. Click **Manage PIM** to enable **Privileged Identity Management** for that subscription.

**Step 2: Assign Users to Eligible Roles in PIM**

1. Go to **Azure AD** > **PIM** > **Azure resources**.
2. Select the **subscription** where you want to assign roles.
3. Click **Roles** and search for **Reader** or **Contributor**.
4. Select the role and click **Add assignments**.
5. Set **Assignment Type**:
   * **Eligible** (User must activate access when needed)
   * **Active** (User has immediate access—less secure)
6. Choose the **user or group**.
7. Set **Assignment duration** (e.g., Permanent eligible or Expiring).
8. Click **Assign**.

**Step 3: Configure Just-In-Time (JIT) Access Requirements**

1. In **PIM**, go to **Azure resources** > Select **Subscription**.
2. Click on **Roles** > Select **Reader** or **Contributor**.
3. Click **Settings** and configure:
   * **Activation Time** (e.g., User must wait for 5 mins after requesting access).
   * **Approval Required** (Enable if you want an approver to approve access).
   * **Justification Required** (User must provide a reason when requesting).
   * **MFA Requirement** (Highly recommended for security).
4. Click **Update**.

**Step 4: Assign Approvers (Optional, if Approval is Enabled)**

1. Go to **PIM** > **Azure Resources**.
2. Select your **subscription** and go to **Roles**.
3. Click **Settings** for the **Contributor** or **Reader** role.
4. Under **Approval**:
   * **Enable Approval Workflow**.
   * Assign **Approvers** (e.g., Your team leads).
5. Click **Update**.

**Step 5: User Requests and Activates Role**

1. A user navigates to **Azure Portal** > **PIM** > **My roles**.
2. Under **Azure resources**, they find the **subscription** role (Reader/Contributor).
3. Click **Activate** > Provide **Justification**.
4. If **approval is enabled**, it will go to the approver.
5. Once approved, access is granted for the **configured time**.

**Step 6: Monitor PIM Activities**

1. Go to **Azure AD** > **PIM** > **Audit log**.
2. View:
   * **Who activated which role and when**.
   * **Who approved role activations**.
   * **Any failed activation attempts**.

**Step 7: Review and Remove Unused Assignments**

1. Periodically review **PIM Role Assignments**:
   * Go to **Azure AD** > **PIM** > **Azure Resources**.
   * Click **Review Access**.
   * Remove users who no longer need access.
   * Automate access review with **Access Reviews**.

**Summary**

✅ **Enable PIM for Subscription**  
✅ **Assign Eligible Roles** (Reader, Contributor)  
✅ **Configure Just-in-Time Access** (MFA, justification, approval)  
✅ **Set Approvers for Role Activation**  
✅ **Monitor Activation Logs & Conduct Reviews**