### Role Based Access Control (RBAC)

RBAC defines what an end user or administrator can do. In relation to system administration, RBAC provides various roles each of which can only perform certain tasks. For example, help desk staff may be able to only view certain resources, whereas system administrators could view, create, and delete those resources.

When deploying the RBAC model in Azure, there are two scopes where access can be granted. The use of the scopes can be used separately or together depending on the services activated. The scopes include:

* Tenant Scope - Roles within the Tenant Scope allow access to perform tasks at the Tenant and Office 365 administration level. By default, there are 51 built-in RBAC roles that can be assigned at this level to ensure least privilege access is implemented.
* Subscription Scope – Roles within the Subscription Scope allow access to perform tasks within a subscription. Subscription roles do not have permissions at the Tenant Scope level.

Privileged Identity Management (PIM) can be leveraged to enhance the Azure RBAC model. PIM is an implementation of Just-in-time (JIT) access. JIT access ensures that an administrative account only has privileges when required to complete a function. JIT aligns to the principal of Zero Standing Privilege.

Each PIM role assignment can have the following attributes:

* Activation Duration - the Activation Duration attribute specifies the duration to allow the access request, the maximum is 72 hours.
* Approver – the Approver attribute specifies the person or people who can approve role activation requests.
* Notification – the Notification attribute specifies that a pending request is awaiting approval via email.
* Incident Request Ticket – the Incident Request Ticket attribute specifies that the approver add an incident ticket number to the approval request.
* Multi-factor Authentication – the Multi-factor Authentication attribute specifies whether MFA is required for activation.

RBAC Design Decisions for all agencies and implementation types.

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Azure AD Role Based Management | Least Privilege, using PIM | PIM will be utilised to provide Just-in-Time role-based management to ensure elevated access is only provided when required. |
| PIM Roles | Authentication AdministratorAzure Information Protection AdministratorGlobal AdministratorExchange Service AdministratorHelpdesk AdministratorIntune Service AdministratorOffice Apps AdministratorPower BI Service AdministratorPower Platform AdministratorPrivileged Role AdministratorSecurity AdministratorSecurity OperatorSharePoint Service AdministratorTeams Communications AdministratorTeams Communications Support EngineerTeams Communications Support SpecialistTeams Service AdministratorUser Account Administrator | The configured PIM roles align to the services utilised within the solution. |
| PIM approval | Automatic approval for all roles except for Global Administrator | Approval will only be required for Global Administrators. |
| Activation duration | 8 hours | The activation duration will be one workday to ensure that administrative actions are not impeded. |