AZURE PIM IMPLEMENTATION

Microsoft Entra Privileged Identity Management

vighnesh-notes
vighneshnaik.com
linkedin.com/in/vighneshnaik6

WHY PIM?

- Enforce least privilege by default
- Just-in-time (JIT) access when needed
- Reduce standing admin rights
- Require MFA and approvals
- Full audit trail and visibility

BEFORE: ALWAYS-ON ACCESS

Standing access always available

✗ Higher risk of misuse

AFTER: TIME-BOUND ACCESS

Activate just-in-time for limited duration

✓ Least privilege enforced

✓ Risk reduced & accountable access

IMPLEMENTATION ROADMAP

1. **ASSESS** — Evaluate current privileged access, roles, and risks
2. **PLAN** — Define scope, policies, approvals, and role strategy
3. **ONBOARD** — Enable PIM, connect Microsoft Entra ID
4. **ASSIGN** — Assign eligible roles to users or groups
5. **ACTIVATE** — Request, approve & activate access just in time
6. **REVIEW** — Monitor usage, review access & refine policies

WHAT PIM COVERS

MICROSOFT ENTRA ROLES
- Global Administrator
- Privileged Role Administrator
- User Administrator
- And other Entra roles

AZURE RESOURCE ROLES
- Subscription Owner
- Contributor
- Resource-specific roles
- Custom roles

PIM FOR GROUPS
- Make groups eligible for roles
- Activate groups when needed
- Centralize access management

SUCCESS OUTCOME

Secure, governed, and time-bound privileged access that reduces risk and improves security posture.

TIP

Start small, automate approvals, and review access regularly!

Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.

1. PLAN YOUR PIM FOUNDATION

Licensing, onboarding, prerequisites & scope


vighnesh-notes

vighneshnaik.com

linkedin.com/in/vighneshnaik6

PREREQUISITES

- Microsoft Entra ID P2 or Microsoft Entra ID Governance licensing
- Privileged Role Administrator / Global Administrator permissions
- Azure subscription Owner or User Access Administrator for resource roles
- MFA enabled & security baseline in place

WHAT TO DECIDE

- Pilot scope (subscriptions, resources, environments)
- In-scope roles to protect
- Approval model & approver groups
- Activation duration & maximum settings
- Emergency access (break-glass) accounts
- Communication plan & change awareness

ONBOARDING FLOW

1. **ASSESS TENANT** — Evaluate current state, roles, and existing access
2. **ENABLE PIM** — Enable PIM for Microsoft Entra ID & resources
3. **SELECT ROLE SCOPES** — Choose roles, resource scopes, and exclusions
4. **CONFIGURE SETTINGS** — Set approvals, duration, MFA, and notifications
5. **PILOT WITH A FEW ROLES** — Test with a small set of roles, learn & refine
6. **EXPAND ROLLOUT** — Scale to more roles & resources in phases

FOUNDATION CHECKLIST

BREAK-GLASS ACCOUNTS
- ✓ Dedicated accounts
- ✓ Excluded from PIM
- ✓ Stored securely
- ✓ Access tested

ROLE INVENTORY
- ✓ List all privileged roles
- ✓ Map to resources
- ✓ Identify owners

NAMED APPROVERS
- ✓ Define approver groups
- ✓ Ensure coverage
- ✓ Review regularly

NOTIFICATIONS & ALERTS
- ✓ Enable role activation alerts
- ✓ Review access reports

DOCUMENTATION
- ✓ Settings & decisions
- ✓ Runbooks & SOPs
- ✓ Change log
- ✓ Review cadence

SUCCESS OUTCOME

A well-planned PIM foundation that ensures least privilege, secure access, and audit readiness.

TIP

Start with high-impact roles first.

Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.

2. DISCOVER & CLASSIFY PRIVILEGED ACCESS

Inventory admins, roles, groups & risks


vighnesh-notes

vighneshnaik.com

linkedin.com/in/vighneshnaik6

WHAT TO INVENTORY

- Users with permanent admin access
- Microsoft Entra roles
- Azure resource roles
- Privileged groups
- Service principals
- Critical subscriptions / management groups

RISK SIGNALS

- Too many permanent admins
- No MFA
- Unused privileged assignments
- Orphaned accounts
- Excessive subscription owners
- Undocumented exceptions

CLASSIFICATION MODEL

PERMANENT ACTIVE ROLES

Always-on privileged access required for core operations. Minimize and tightly control.

ELIGIBLE JUST-IN-TIME ROLES

Activated only when needed via PIM for a limited duration. Preferred state.

TEMPORARY EXCEPTION ACCESS

Short-term, approved access for break-glass or special cases. Time-bound & tracked.

ROLE PRIORITIZATION

Focus on high-impact roles that can control your environment.

GLOBAL ADMINISTRATOR | PRIVILEGED ROLE ADMINISTRATOR | USER ADMINISTRATOR | SECURITY ADMINISTRATOR | SUBSCRIPTION OWNER | CONTRIBUTOR

HIGHEST IMPACT → LOWER IMPACT

TIP

Prioritize crown-jewel roles and shared admin paths. Reduce blast radius first.

Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.

4/7

3. Configure Role Settings & Assignments

Eligible vs active, activation rules & governance settings


vighnesh-notes
vighneshnaik.com
linkedin.com/in/vighneshnaik6

Assignment Types

Eligible Assignment

- User can activate the role when needed
- No immediate access
- Requires activation (just-in-time)
- Example: Global Administrator (Eligible)

Active Assignment

- User has immediate access to the role
- Standing access granted
- Higher risk if overused
- Example: Break-glass account (Active)

Role Settings

MFA on activation —
Require MFA when activating the role

Approval required —
Require approval before activation

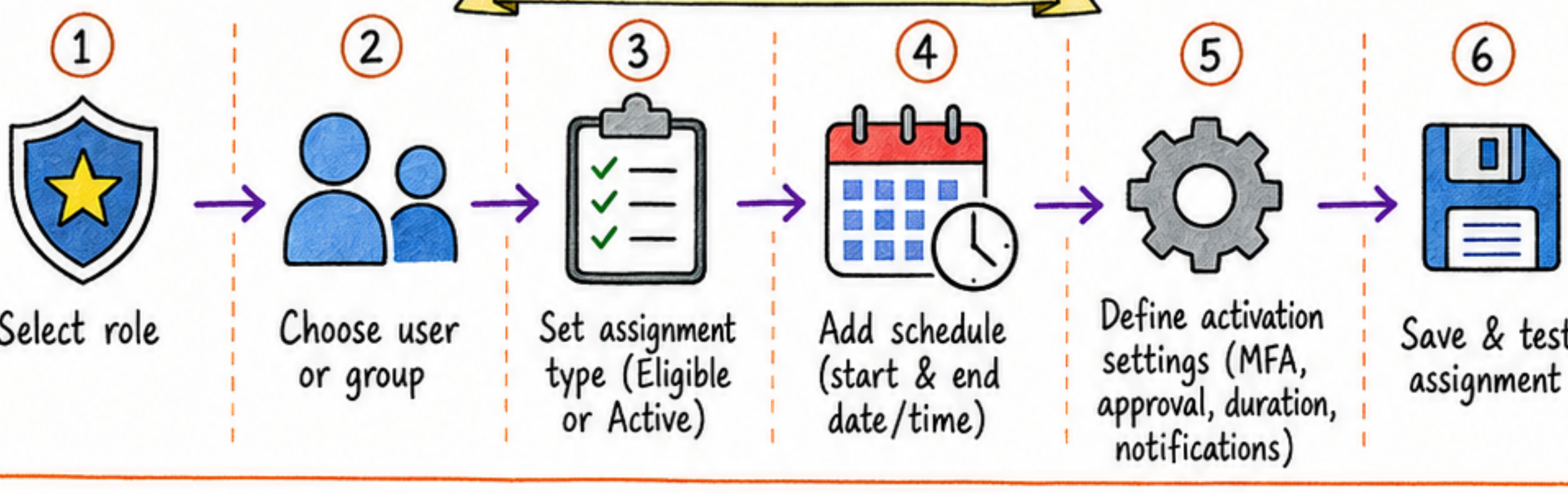
Justification required —
Require reason for activation

Ticket / Ticket system —
Link activation to ticket or change record

Maximum activation duration —
Set time-bound activation limits

Notifications —
Notify on activation, approval, & expiration

Configuration Flow



Best-Fit Examples

Global Administrator
Eligible assignment + approval + MFA for high security

Subscription Owner
Eligible assignment + time-bound activation

Break-glass account
Active assignment but tightly controlled & monitored

PIM for Groups
Centralized access for teams with least privilege

Tip

Keep standing access minimal. Use eligible + time-bound access with approval & MFA for maximum security.

★ — Keep It Simple. Design for Scale. Secure by Design. Cost Optimized. — ★

4. ACTIVATION, APPROVALS & ACCESS REVIEWS

How just-in-time access works in practice

vighnesh-notes
vighneshnaik.com
linkedin.com/in/vighneshnaik6

1. USER ACTIVATION FLOW

1. Request role
2. Complete MFA
3. Add justification / ticket
4. Wait for approval if required
5. Activate
6. Use time-bound access

2. APPROVAL & NOTIFICATION MODEL

Approvers
Role-based approvers review and approve requests.

Requestor notifications
Stay informed at each stage of the request.

Activation alerts
Get notified when access is activated.

Activation duration
Access is granted for a defined, limited period.

Escalation path
Requests escalate if not acted on within SLA.

3. ACCESS REVIEWS

Review cadence
Define and follow a regular review schedule.

Reviewers
Business & IT owners review access assignments.

Remove stale access
Revoke access that is no longer needed or justified.

Review role-eligible users
Validate who is eligible for privileged roles.

Document exceptions
Capture justified exceptions with approvals.

4. PIM FOR GROUPS

- Enable eligible group membership
- Activate group-based privileged access
- Easier scaling for teams & projects
- Simplified governance & reviews

TIP

Review access regularly and remove stale privileges to reduce risk and improve security posture.

Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.

5. AUDIT, ALERTS & GOVERNANCE

Monitor privileged access and enforce continuous control

vighnesh-notes
vighneshnaik.com
linkedin.com/in/vighneshnaik6

AUDIT & HISTORY

- Activation records (who, what, when, why)
- Assignment history (eligible & active roles)
- Approvals & approver decisions
- Role changes & policy updates
- Who accessed what and when

IMPORTANT ALERTS

- Too many permanent admins
- Roles without MFA enforced
- No approvers configured
- Suspicious or unusual activations
- High-risk accounts active

OPERATING MODEL

1. **MONITOR** — Continuously monitor PIM activity, logs, and alerts
2. **INVESTIGATE** — Analyze alerts and investigate anomalies
3. **REVIEW** — Review access, decisions, and risk impact
4. **REMEDIATE** — Take corrective actions & enforce controls
5. **DOCUMENT** — Document findings, actions, and decisions
6. **IMPROVE** — Improve policies, automations, and controls

GOVERNANCE PRACTICES

- Quarterly access reviews
- Least privilege by design
- Separation of duties
- Emergency access governance
- Notification tuning
- Audit evidence retention

TIP | Tie PIM insights into your security operations and compliance reviews for continuous assurance.

Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.

PIM IMPLEMENTATION SUCCESS CHECKLIST

Best practices, rollout milestones & final review

vighnesh-notes

vighneshnaik.com

linkedin.com/in/vighneshnaik6

ROLLOUT CHECKLIST

- [x] Licensing validated & assigned
- [x] User onboarding completed
- [x] Critical roles inventoried
- [x] PIM settings configured
- [x] Approvers assigned
- [x] Notifications & alerts enabled
- [x] Emergency accounts documented

KEY PRINCIPLES

- Enforce least privilege
- Activate just-in-time access
- Maintain a strong approval path
- Require MFA for all activations
- Review access regularly
- Document & monitor exceptions

COMMON USE CASES

MICROSOFT ENTRA ROLES

- Global Administrator
- Privileged Role Administrator
- User Administrator
- Application Administrator
- Security Administrator

AZURE SUBSCRIPTION / RESOURCE ROLES

- Owner
- Contributor
- Reader
- Resource-specific roles
- Custom roles

PRIVILEGED GROUPS

- IT Admins
- Security Operators
- DevOps Engineers
- Break-glass Operators
- Application Support

SUCCESS OUTCOME

Reduced standing access, higher security posture, auditable privileged access, and scalable governance that grows with your organization.

GOVERN. ACTIVATE. REVIEW. IMPROVE.

Keep improving. Keep securing. Keep leading!

TIP

Iterate after the pilot. Refine policies, roles, and approvers!

Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.