Azure Sandbox Profiles

	Highly Managed (Shared)	Lightly Managed (Shared)	Isolated (Dedicated per Project)
Main scenario(s)	From a developer's perspective, things are **mostly managed <u>for</u> them**. Designed mostly to provide self-service capabilities including virtual machine provisioning, and curated solutions that are managed on behalf of developers. Typical self-service tooling include: • Azure DevTest Labs • Azure Managed Apps • Custom using Power App Management on behalf of developers = High Ability for developers to customise = Low Network access to Prod = Yes (limited, managed)	From a developer's perspective, this is the **middle ground** where management is a **responsibly shared** between developers and Central IT Teams. Designed mostly to provide a more flexible, managed sandbox environment compared to the 'Highly Managed' scenario. Typical tooling include: • ARM/Bicep/Terraform template libraries • Portal/CLI/PowerShell access Management on behalf of developers = Medium Ability for developers to customise = Medium Network access to Prod = By exception	From a developer's perspective, things are **mostly managed <u>by</u> them**. Designed mostly to provide dedicated, isolated sandbox environments which provide a higher degree of customisation and self-management. Typical tooling include: • ARM/Bicep/Terraform template libraries • Portal/CLI/PowerShell access Management on behalf of developers = Low/None Ability for developers to customise = High Network access to Prod = No (isolated)
Target audience	Intended for individual developers and/or development teams that require relatively simple and quick stand-up time, and would prefer someone else to cover most of the management overhead on their behalf. Good for: • Minimal management overhead for developers • Pre-crafted / curated content Not so good for: • Developers that require more control and flexibility Considerations: • It can take some time to build up a catalog of services and reusable IaC templates	Intended for individual developers and/or development teams that require relatively simple and quick stand-up time but require a little more flexibility than that provided by the 'Highly Managed' sandbox. Good for: • Developing and testing new solutions where IaC templates don't currently exist • More complex pre-crafted / curated content Not so good for: • Larger teams with very complex workloads that require a higher degree of flexibility and autonomy	Intended for large, complex workloads/solutions run by project teams who require more flexibility and a dedicated environment that they have more control over. Good for: • Product teams that require the most amount of autonomy • When needing to work outside of the typically highly restrictive Prod environment No so good for: • Workloads that require integration into Prod systems and data Considerations: • Workloads that require integration into Prod systems and data may be better suited to the 'Lightly Managed' sandbox model
Controls	• Azure Policy (Managed on behalf of developers) • Self-Service build-in (Managed by tool admins)	• Service Principals life cycle (Managed on behalf of developers – Azure AD Access Review) • Azure Policy (Managed on behalf of developers)	• Prod tenant: Service Principals life cycle managed on behalf of developers – Azure AD Access Review)

		• Self-Service build-in (Managed by tool admins)	• Non-Prod tenant: Service Principals life cycle management is the responsibly of the individual subscription owners/project teams – Azure AD Access Review) • Management Group level: Azure Policy (Managed on behalf of developers) • Subscription level: Azure Policy (Responsibly of the individual subscription owners)
AAD Tenant	• Existing Prod tenant	• Existing Prod tenant	• Existing Prod tenant -or- separate tenant
Subscription type	• EA or Enterprise DevTest (*for Visual Studio subscribers*)	• EA or Enterprise DevTest (*for Visual Studio subscribers*)	• EA or Enterprise DevTest (*for Visual Studio subscribers*)
Subscription instance(s)	• Single	• Single	• Multiple (per app/project team) Consideration: • Azure Blueprints may be used to provide the high-level Policy, RBAC and resources to quickly provision subsequent subscriptions.
Life cycle	• Short to medium term use	• Medium to long term use	• Long term use
Subscription Quota	• Managed on behalf of developers • Shared	• Managed on behalf of developers • Shared	• Responsibly of the individual subscription owner(s) • Per subscription
Owner / Management	• Management Group - Central IT team • Subscription - Central IT team • Foundation shared services - Central IT team • Self-service capabilities - Central IT team • DevTest Labs ○ Lab provisioning - Central IT team ○ Lab administration - Central IT team or Lab Admin ○ Lab resources - Lab Users • Managed Apps ○ App publisher - Central IT team or App Publisher ○ App consumer - AAD User or Group ○ App administration - Central IT team or App Consumer • Power App (Custom)	• Management Group - Central IT team • Subscription - Central IT team • Foundation shared services - Central IT team • Provisioned resources - Central IT team and/or developers	• Management Group - Central IT team • Subscription - Individual project teams • Foundation shared services - Individual project teams • Provisioned resources - Individual project teams
Resource Groups	• Resource Groups are managed on behalf of developers either by Central IT teams and/or Self-Service tooling.	• Resource Groups are managed on behalf of developers by Central IT teams.	• Resource Groups are the responsibly of the individual subscription owners/project teams.

Virtual Machine Images	• Controlled/curated by self-service tooling • Azure Compute Gallery (Managed on behalf of developers) • Azure Marketplace Private Collections (Managed on behalf of developers)	• Azure Compute Gallery (Managed on behalf of developers) • Azure Marketplace Private Collections (Managed on behalf of developers)	• Azure Compute Gallery (Shared or dedicated) • Azure Marketplace Private Collections • Azure Marketplace
Virtual Machine Management	Active Directory Domain Services: • Can be Prod Domain joined Patch Management: • Managed on behalf of developers by Central IT teams.	Active Directory Domain Services: • Can be Prod Domain joined *(Exception based)* Patch Management: • Managed on behalf of developers by Central IT teams.	Active Directory Domain Services: • Should not be Prod Domain joined • Can join own dedicated Domian Patch Management: • The responsibly of the individual subscription owners/project teams.
Networking	Networking peered with Prod: (Default) • Networking is managed on behalf of developers either by the central IT team and/or self-service tooling. Isolated network: • Networking is managed on behalf of developers either by the central IT team and/or self-service tooling. NSG (Network Security Groups) can either be enforced using Azure Policy and/or configured using the self-service tooling.	Networking peered with Prod: *(Exception based)* • Networking is managed on behalf of developers either by the central IT team and/or self-service tooling Isolated network: (Default) • Networking is managed by developers. NSG (Network Security Groups) can either be enforced using Azure Policy and/or configured using the self-service tooling.	Networking peered with Prod: • Should not be allowed. Isolated network: (Default) • Networking is the responsibly of the individual subscription owners/project teams. NSG (Network Security Groups) are the responsibly of the individual subscription owners/project teams.