**Landing Zone ARM Template Deployment**

**What will be deployed?**

By default, all recommendations are enabled and you must explicitly disable them if you don't want it to be deployed and configured.

* A scalable Management Group hierarchy aligned to core platform capabilities, allowing you to operationalize at scale using centrally managed Azure RBAC and Azure Policy where platform and workloads have clear separation.
* Azure Policies that will enable autonomy for the platform and the landing zones.
* An Azure subscription dedicated for **management**, which enables core platform capabilities at scale using Azure Policy such as:
  + A Log Analytics workspace and an Automation account
  + Azure Security Center monitoring
  + Azure Security Center (Standard or Free tier)
  + Azure Sentinel
  + Diagnostics settings for Activity Logs, VMs, and PaaS resources sent to Log Analytics
* An Azure subscription dedicated for **connectivity**, which deploys core Azure networking resources such as:
  + A hub virtual network
  + Azure Firewall (optional - deployment across Availability Zones)
  + ExpressRoute Gateway (optional - deployment across Availability Zones)
  + VPN Gateway (optional - deployment across Availability Zones)
  + Azure Private DNS Zones for Private Link (optional)
  + Azure DDoS Network Protection (optional)
* (Optionally) An Azure subscription dedicated for **identity** in case you requires to have Active Directory Domain Controllers in a dedicated subscription.
  + A virtual network will be deployed and will be connected to the hub VNet via VNet peering.
* Landing Zone Management Group for **corp** connected applications that require connectivity to on-premises, to other landing zones or to the internet via shared services provided in the hub virtual network.
  + This is where you will create your subscriptions that will host your corp-connected workloads.
* Landing Zone Management Group for **online** applications that will be internet-facing, where a virtual network is optional and hybrid connectivity is not required.
  + This is where you will create your Subscriptions that will host your online workloads.
* Landing zone subscriptions for Azure native, internet-facing **online** applications and resources.
* Landing zone subscriptions for **corp** connected applications and resources, including a virtual network that will be connected to the hub via VNet peering.
* Azure Policies for online and corp-connected landing zones, which include:
  + Enforce VM monitoring (Windows & Linux)
  + Enforce VMSS monitoring (Windows & Linux)
  + Enforce Azure Arc VM monitoring (Windows & Linux)
  + Enforce VM backup (Windows & Linux)
  + Enforce secure access (HTTPS) to storage accounts
  + Enforce auditing for Azure SQL
  + Enforce encryption for Azure SQL
  + Prevent IP forwarding
  + Prevent inbound RDP from internet
  + Ensure subnets are associated with NSG
  + Associate private endpoints with Azure Private DNS Zones for Azure PaaS services.