Azure Landing Zone Checklist (30-Point)

1. Root management group configured
2. Regional management groups created
3. Production & non-prod subscriptions separated
4. Subscription naming follows AZ-SUB-BU-REGION-ENV
5. AllowedLocations policy assigned
6. AllowedSKUs policy assigned
7. Tag inheritance policy applied
8. Diagnostic settings DeployIfNotExists policy applied
9. Azure AD tenant linked and MFA enforced
10. PIM configured for owner roles
11. Hub VNET deployed with /16 address space
12. Firewall subnet created (AzureFirewallSubnet)
13. Spoke VNETs peered to hub
14. ExpressRoute or VPN gateway deployed
15. DNS forwarders configured for on-prem resolution
16. Log Analytics workspace per region
17. Activity Log streaming enabled
18. Budgets set per subscription
19. Cost alerts routed to FinOps email
20. Storage account for Terraform state with Private Endpoint
21. Standardised resource locks on shared resources
22. Backup vault configured for VMs & SQL
23. RBAC least privilege custom role for DevOps pipelines
24. Automation Account for key rotation runbooks
25. Advisor recommendations workbook pinned
26. Grafana dashboards enabled in Azure Monitor
27. Security Center set to 'Enhanced' and no critical findings
28. Blueprint or IaC template stored in source control
29. CI/CD pipeline for landing zone has manual approval gate
30. Documentation wiki link added to README