Cloud Controls Matrix — Identity, Data, Monitoring, Network & Governance (Azure)

Scope: Mapping of ISM/Cloud Controls Matrix controls to Azure services, recommended implementation steps, and evidence artifacts for audits. Focus areas: **Identity**, **Data**, **Monitoring**, **Network**, **Governance**. Use this as a working spreadsheet to populate into your System Security Plan (SSP).

Legend

- **Control** — short ID used by your CCM/SSP (customizable)
- **Requirement** — what the ISM/PSPF control requires
- **Azure Service(s)** — recommended Azure services/features to satisfy the requirement
- **Implementation Steps (high-level)** — steps to implement in Azure
- **Evidence / Artifacts** — what to collect for audit evidence
- **Policy / Automation** — Azure Policy initiatives, automation or scripts to enforce
- **Priority** — High / Medium / Low (risk-based)

Identity Controls

(same as before — ID-01 to ID-05, MFA, PIM, RBAC, logging, etc.)

Data Controls

(same as before — DATA-01 to DATA-06, classification, encryption, DLP, backup, etc.)

Monitoring & Logging Controls

(same as before — MON-01 to MON-05, centralised logging, Sentinel, incident response, forensic retention, drift detection, etc.)

Network Controls

Control	Requirement	Azure Service(s)	Implementation Steps (high-level)	Evidence / Artifacts	Policy / Automation	Priority
NET-01: Network Segmentation	Segregate workloads into separate network zones with least privilege connectivity	Azure Virtual Network, Subnets, NSGs, Azure Firewall	- Design VNet with app, db, mgmt subnets\n- Apply NSG rules for least-privilege communication\n- Enforce UDRs through Firewall for outbound	NSG rule exports, topology diagrams, firewall policy exports	Azure Policy: audit public IPs on NICs; automation: deploy NSGs automatically to new subnets	High
NET-02: Secure Remote Administration	Ensure remote access to workloads is controlled and logged	Azure Bastion, Just-in-Time VM Access, Azure AD PIM	- Deploy Bastion for secure remote RDP/SSH\n- Configure JIT VM access with Defender for Cloud\n- Require PIM for administrator roles	Bastion session logs, JIT activation logs, PIM records	Azure Policy: audit public RDP/SSH; automation: block NSG rules with *:3389/*:22 inbound	High
NET-03: Boundary Protection	Protect ingress/egress with firewalls and gateways	Azure Firewall, Application Gateway (WAF), Front Door	- Deploy Firewall at hub\n- Configure outbound deny rules and FQDN filters\n- Enable WAF for web applications	Firewall rule exports, WAF policy logs, blocked traffic reports	Policy: enforce WAF for App Service; automation: alert on firewall policy changes	High
NET-04: Private Connectivity	Prevent sensitive workloads from exposing public endpoints	Private Link, Service Endpoints, VPN/ExpressRoute	- Configure Private Endpoints for Storage/SQL\n- Remove public IP from sensitive resources\n- Establish ExpressRoute for hybrid connectivity	Resource configs, endpoint settings, network diagrams	Azure Policy: deny public endpoints; automation: remediate to Private Endpoint	High

Control	Requirement	Azure Service(s)	Implementation Steps (high-level)	Evidence / Artifacts	Policy / Automation	Priority
NET-05: DDoS & Network Resilience	Protect workloads against volumetric and protocol attacks	Azure DDoS Protection Standard, Load Balancers, Traffic Manager	- Enable DDoS Protection Plan on VNets\n- Deploy Azure Load Balancer/Traffic Manager for HA\n- Test failover scenarios	DDoS protection plan config, DDoS mitigation reports, failover test reports	Policy: require DDoS plan on VNets; automation: monthly test failover drill	Medium

Governance Controls

Control	Requirement	Azure Service(s)	Implementation Steps (high-level)	Evidence / Artifacts	Policy / Automation	Priority
GOV-01: Security Governance Framework	Define security roles, responsibilities and policies	Management Groups, Azure Policy, RBAC	- Create management group hierarchy (Prod, Dev, Test) \n- Apply baseline Azure Policy initiatives\n- Document roles & responsibilities in SSP	Org chart, role assignment matrix, policy assignments export	Azure Policy initiatives assigned at mgmt group; automation: regular export of assignments	High
GOV-02: Policy Compliance & Reporting	Continuously assess compliance with ISM/PSPF	Azure Policy, Azure Blueprints, Defender for Cloud	- Assign policy initiatives for encryption, logging, networking\n- Monitor compliance in Azure Policy dashboard\n- Export reports monthly for audit	Azure Policy compliance reports, Blueprint assignments, secure score exports	Automation: scheduled compliance export to evidence repo	High

Control	Requirement	Azure Service(s)	Implementation Steps (high-level)	Evidence / Artifacts	Policy / Automation	Priority
GOV-03: Risk Management	Identify and manage risks of cloud workloads	Defender for Cloud (secure score), Risk Register (external), Security Center recommendations	- Monitor secure score trends\n- Record risks not mitigated in risk register\n- Track remediation of high severity issues	Secure score export, risk register entries, remediation tickets	Automation: export secure score daily; policy: flag subscriptions < threshold score	Medium
GOV-04: Change Management & Configuration Control	Manage configuration drift and approvals for changes	Azure DevOps Pipelines, Azure Policy, Change Tracking	- Require IaC (Terraform/ Bicep) for deployments\n- Enforce approval gates in pipelines\n- Enable Change Tracking on resources	Pipeline logs, PR approvals, change tracking logs	Automation: CI/CD pipelines enforce change approvals; Policy: drift alerts to SOC	High
GOV-05: Logging of Administrative Actions	Track privileged actions for accountability	Azure Activity Logs, Log Analytics, Sentinel	- Enable Activity Log export to Log Analytics\n- Create Sentinel alerts for sensitive operations (role assignment, policy changes)	Activity log queries, Sentinel incidents	Policy: audit Activity Log export enabled; automation: daily review report	High
GOV-06: Training & Awareness Evidence	Ensure technical staff trained on ISM/PSPF and Azure security	LMS records (external), linked Azure training paths	- Track Azure certifications & security training\n- Maintain awareness campaigns	Training records, certificates	N/A	Medium

How to use this document

1. Integrate these rows into your Cloud Controls Matrix spreadsheet.\n2. Align each with ISM/PSPF control numbers and internal policy references.\n3. Collect listed evidence and link into an evidence repository.\n4. Apply Azure Policy and automation scripts to enforce compliance systematically.

Appendix — Useful Azure Governance Tools

- **Azure Blueprints**: package policy, RBAC, ARM templates into reusable landing zones.
- **Management Groups**: apply governance at scale across subscriptions.
- **Defender for Cloud Secure Score**: quantify compliance posture.
- **Service Trust Portal**: download compliance reports for physical & platform controls.

This extended Cloud Controls Matrix now covers Identity, Data, Monitoring, Network, and Governance.