Microsoft recommendation

Based on your answers so far

Microsoft

Complete all 3 steps and click **Generate recommendation** (or **Finish**) to see suggested services, migration path, and a full onboarding playbook for the selected cloud.

Workload: OnPremMigrationPath: MigrationMigration scope: DC / estateArchitecture: legacy-vmData: analytics-lakeSensitivity: ps-l5Criticality: tier0Source: onprem-vmware7R: rehostIaC: ansible

Compute pattern

Lift & shift to **Azure VMs / VM Scale Sets**, or use **Azure VMware Solution (AVS)** if staying on VMware.

For on-prem VMware with minimal change, AVS + HCX gives low-friction relocation; otherwise migrate VMs to native Azure with Azure Migrate.

Data & storage

Use **Data Lake Storage Gen2** as the lake and **Synapse / Fabric** for lakehouse & analytics.

Use Data Factory / Synapse pipelines for ingestion, Microsoft Purview for governance/catalog, and Power BI for BI. For regulated workloads, prefer **Azure Government** or appropriately scoped commercial regions, with Key Vault / Managed HSM, private endpoints, and Microsoft Purview classification.

Integration & messaging

Use **Event Hubs** with **Stream Analytics** / Synapse.

Event Hubs for high-throughput event streams; Stream Analytics / Synapse for near-real-time processing.

Ops, resilience & governance

Treat this as **Tier 0 – mission critical** on Azure and design HA/DR accordingly. Use multi-zone deployments and consider active-active or active-passive across paired regions.

Use **Azure Monitor**, **Log Analytics**, and **Application Insights** for observability; **Microsoft Sentinel** for SIEM; **Defender for Cloud** and Azure Policy/Blueprints for security posture. For public sector IL workloads, deploy into **Azure Government** with ExpressRoute + VPN, Entra ID federation, and IL5/IL6-aligned logging to your central SIEM.

Migration & onboarding focus

Azure migration & onboarding focus.

Use **Azure Migrate** to discover and assess on-prem estates. For VMware-heavy environments and 'relocate/rehost' strategies, use **Azure VMware Solution (AVS)** with HCX. Provision landing zones with IaC (Terraform or Bicep/ARM) and enforce guardrails via Management Groups and Policy. Use **Ansible** for OS configuration, middleware setup, and application deployments on Azure VMs / AVS. For connectivity into CHEDC or central data centers, use **ExpressRoute + VPN**; send logs to your central SIEM per IL

guidance. Because this is a **migration** initiative, design waves, cutover rehearsals, and rollback plans around your chosen cutover strategy. Scope: *dc-estate*. Cutover strategy: *bluegreen*.

Sizing & environment footprint

This is a **high** traffic workload on **Azure** with a **Medium–large footprint, multi-AZ / multi-zone for HA**.

Data footprint: 20 TB+; very heavy streaming / ingest; very long / archival retention.

Hot storage for active data plus aggressive use of cool / archive tiers for retained data. Ensure encryption-at-rest, KMS/HSM key management and retention policies aligned to regulatory requirements.

Multi-region design with private connectivity and global entry points (front door / anycast / global load balancer).

Use this as the starting point for T-shirt sizing, cost estimation, and environment build-out in your landing zones.

Environment	Relative size	Notes
Dev	Large × 1	Scaled to ~100% of prod capacity.
Test	Large × 1	Scaled to ~100% of prod capacity.
Pre-prod / Stage	Large × 1	Scaled to ~100% of prod capacity.
Prod	Large	Primary live workload.
DR	Large × 1	Scaled to ~100% of prod capacity.

Implementation playbook · copy into Word

1. **Phase 1 – Intake & discovery.**
   Run a kickoff with business, security, and operations. Capture mission and business outcomes for this *migration initiative* for *OnPremMigration* focused on *data center / infrastructure estate migration*. Classify it as a public sector / IL workload, and document the current hosting situation (on-prem VMware estate), including dependencies, data flows, and any existing ATO / audit findings.
2. **Phase 2 – Requirements & readiness.**
   Define non-functional targets (SLOs/RTO/RPO for the chosen tier tier0), compliance scope (GLBA, PCI, SOX, NIST 800-53, FedRAMP / DoD SRG, FFIEC as applicable), data residency, and

identity/SSO requirements. Decide the primary migration or change approach (rehost (lift & shift)) per component and confirm which parts will be retained or retired.

3. **Phase 3 – Landing zone & architecture on Azure.**
   Design a secure landing zone: management hierarchy (accounts/subscriptions/projects/tenancies), network topology (hub–spoke or mesh), connectivity into CHEDC / enterprise core (ExpressRoute / Direct Connect / Interconnect / FastConnect + VPN), and baseline guardrails (policies, configuration rules, encryption standards). Produce a reference architecture for *OnPremMigration* (compute pattern, data services, integration and observability) using your cross-cloud service catalog and impact-level rules.

4. **Phase 4 – IaC, automation, and pipelines.**
   Implement the landing zone, guardrails, and core shared services using **ansible**. Stand up CI/CD pipelines (Azure DevOps / GitHub Actions / CodePipeline / Cloud Build / OCI DevOps) for both infrastructure and application code. Integrate secret management, image scanning, policy-as-code, and test gates into the pipelines so every change to OnPremMigration is repeatable and auditable.

5. **Phase 5 – Migration / change planning & wave design.**
   Group systems into migration waves (pilot → early adopters → bulk waves) according to dependency and risk. For VMware-heavy estates, plan which systems use native Azure services vs the cloud's VMware offering. Define cutover strategy per wave (blue/green, canary, phased, or big-bang), rollback plans, and detailed runbooks for both technical tasks and communications.

6. **Phase 6 – Security, RMF/ATO & controls.**
   Map controls to Azure services: identity, network segmentation, key management, logging, vulnerability management, and endpoint protection. For IL and financial workloads, inherit CSP controls where allowed and add overlays for gaps. Build your control implementation statements, diagrams, test plans, and evidence collection up front, so ATO / audit runs in parallel with build and migration rather than after the fact.

7. **Phase 7 – Implementation, rollout & cutover.**
   Provision target environments via IaC; harden baselines using Ansible or equivalent configuration management; execute data migrations (DB migration services, bulk object transfers, replication). Run rehearsals in lower environments, then execute production wave cutovers according to your chosen strategy, with practiced rollbacks. Validate stability, data integrity, and control effectiveness before decommissioning legacy environments.

8. **Phase 8 – Monitoring, FinOps & sustainment.**
   Turn on full observability (metrics, logs, traces) and wire them into your central SIEM/SOC. Implement tagging and cost allocation for FinOps reporting; set budgets and alerts by business service. Establish SRE/operations runbooks, on-call rotations, and continuous improvement loops. Every quarter, revisit architecture decisions, optimize cost/performance, and incorporate lessons learned into the next wave or initiative.

Use this playbook as the narrative section in your Word documents and CCoE artifacts. For each phase, attach the concrete evidence (diagrams, Terraform plans, Ansible playbooks, migration runbooks, control mappings, and sign-off sheets).

This is an end-to-end, multi-phase plan (intake → requirements → architecture → migration → security/ATO → cutover → monitoring → sustainment). It assumes you'll also track artifacts in your CCoE proposal and onboarding checklists.