

EXHIBIT A

Shared Responsibility Matrix

BEMO Managed Azure Services

This Exhibit A is incorporated into and forms part of the Statement of Work (“SOW”) between BEMO Corporation (“BEMO”) and Customer for BEMO Managed Azure Services. It allocates responsibility across the Azure stack, from infrastructure (networking, storage, compute) up through applications and data. In the event of a conflict between this Exhibit and the main body of the SOW, the SOW controls.

The Azure environment is organized into eight layers:

- **Networking, Storage, Compute:** Managed by BEMO. BEMO has end-to-end responsibility for the underlying Azure infrastructure.
- **Operating System, Security, Governance:** Managed jointly by BEMO and Customer. BEMO configures, operates, and recommends; Customer approves changes that affect production and provides inputs (licensing, identity policy, business rules).
- **Applications:** Managed by Customer. BEMO provides infrastructure-level availability monitoring and vendor escalation support.
- **Data:** Managed by Customer. Customer owns data, backup/retention configuration, content integrity, and the compliance posture of business data usage.

Legend: ● in BEMO column = BEMO leads and executes | ● in Customer column = Customer leads and executes
| ● in Shared column = Joint execution (BEMO recommends and operates, Customer approves and provides inputs)

Layer	Component / Activity	BEMO	Customer	Shared
NETWORKING Managed by BEMO				
Networking	VPN	●		
Networking	Virtual Network	●		
Networking	Firewall	●		
STORAGE Managed by BEMO				
Storage	Managed Disks	●		
Storage	Storage Accounts	●		
Storage	File Shares	●		
COMPUTE Managed by BEMO				
Compute	Performance and Monitoring	●		
Compute	Scaling	●		

Layer	Component / Activity	BEMO	Customer	Shared
Compute	Sizing	●		
OPERATING SYSTEM Managed by BEMO & Customer				
Operating System	Update OS			●
Operating System	Update 3rd-party applications			●
Operating System	Lifecycle management			●
SECURITY Managed by BEMO & Customer				
Security	Defender for Cloud			●
Security	Backup and Disaster Recovery			●
Security	Vulnerabilities Management			●
GOVERNANCE Managed by BEMO & Customer				
Governance	Azure Policy			●
Governance	RBAC and Governance			●
Governance	Cost Optimization			●
APPLICATIONS Managed by Customer (BEMO infra-level support)				
Applications	Application availability monitoring (infra-level)	●		
Applications	Vendor escalation support	●		
Applications	User support		●	
Applications	Source code		●	
Applications	Integrations		●	
DATA Managed by Customer				
Data	Data platform availability		●	
Data	Backup and retention configuration		●	
Data	Data ownership		●	

Layer	Component / Activity	BEMO	Customer	Shared
Data	Content integrity		●	
Data	Compliance of business data usage		●	

Notes

- Networking, Storage, and Compute are managed entirely by BEMO under this SOW. Customer is not required to operate or maintain these layers.
- Operating System, Security, and Governance are shared. BEMO recommends, configures, and operates; Customer approves changes affecting production, maintains required Microsoft licensing, and provides identity/business inputs.
- Applications and Data remain owned and controlled by Customer. BEMO's responsibility is limited to infrastructure-level availability monitoring and vendor escalation support for application platforms.
- 24x7 Security Operations Center (SOC) monitoring is not included in this SOW; it is available with BEMO's Platinum Managed Security service under a separate SOW.
- Azure Virtual Desktop, if elected as an add-on, is delivered under the same layered model and is governed by an amendment to this SOW.
- Customer remains responsible for Microsoft Azure consumption charges, Microsoft licensing, and any third-party or Marketplace charges.