Microsoft
Azure Kubernetes Service

Responsibility Matrix

This document does not plan to give an exhaustive matrix because the product is continuously evolving, and each Kubernetes project is different. Take is as a starting point for your context

	Microsoft	Customer
SETUP		
Provision VMs	✓	
Select Network mode		✓
Install Kubernetes	✓	
Select public / private mode		✓
SECURITY		
Node hardening	✓	
Egress lockdown		✓
Protect API server (public cluster)		✓
Container hardening		✓
Configure Policies	✓	✓
OPERATION		
Keep a cluster up to date (=supported)		✓
Trigger version upgrade		✓
Perform Kubernetes components upgrade	✓	
Install security patch on Operating System	✓	
Reboot nodes to apply security patches [1]		✓
Patch container runtime [2]	✓	
Update AKS layer [2]	✓	
Scale pods (manual)		✓

Scale pods (HPA / VPA / KEDA)		✓
Scale nodes (manual)		✓
Scale nodes (cluster autoscaler)		✓

DISASTER RECOVERY		
Activate availability zones for VMs		✓
Auto repair nodes	✓	
Configure storage backup / restore		✓
Configure traffic management between clusters		✓

MONITORING		
Enable monitoring		✓
Capture metrics	✓	
Configure captured metrics (Prometheus)		✓
Configure capture metrics (host + containers)		✓

[1] Some patches require host reboot. Azure cannot decide when reboot them (could cause application disruption). Customer can either watch for reboot_required.txt file presence or use KURED.

[2] container runtime and AKS layer are only upgraded during Kubernetes upgrade (=a new node is created). To ensure to stay up to date in terms of runtime and AKS (security & bugs fixes), either you should upgrade the version of Kubernetes or you can use "node image upgrade"

For any remark / issue / question, do not hesitate to contact me on GitHub
https://github.com/lgmorand/aks-responsability-matrix

www.the-aks-checklist.com