Microsoft

Governance, Risk, & Compliance

Clear Lines of Responsibility

Use this worksheet to designate the parties responsible for specific functions in Azure. Consistent procedures will avoid confusion that can lead to human and automation errors which increases an organization’s security risk.

**Most organizations map these closely to current on premises models.*

Network Security	*Typically existing network security team* Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.	
Network Management	*Typically existing network operations team* Enterprise-wide virtual network and subnet allocation	
Server Endpoint Security	*Typically IT operations, security, or jointly* Monitor and remediate server security (patching, configuration, endpoint security, etc.)	
Incident Monitoring and Response	*Typically security operations team* Investigate and remediate security incidents in SIEM or source console: • Azure Security Center • Azure AD Identity Protection	
Policy Management	*Typically GRC team + Architecture* Set Direction for use of Roles Based Access Control (RBAC), Azure Security Center, Administrator protection strategy, and Azure Policy to govern Azure resources	
Identity Security and Standards	*Typically Security Team + Identity Team Jointly* Set direction for Azure AD directories, PIM/PAM usage, MFA, password/synchronization configuration, Application Identity Standards	

Tip

Document and socialize this widely with all teams working on Azure