3. Vulnerability Identification Report

3.1 Assessment Scope

The network security assessment covered the following Azure components:

- VNet segmentation, peering configuration, route tables, and private endpoints
- NSG inbound/outbound rules and least-privilege enforcement
- Azure Firewall policies, DNAT rules, and threat intelligence mode
- Application Gateway WAF configuration, OWASP rule coverage, TLS enforcement
- VPN (S2S/P2S) encryption strength and tunnel scope restrictions
- Azure Bastion access governance and administrative exposure
- Public IP inventory and unnecessary internet-facing assets
- Network logging completeness, SIEM integration, and alerting coverage

3.2 Core Network Vulnerabilities

Vulnerability	Risk	Business Impact
Flat VNet without segmentation	High	Enables lateral movement to sensitive financial systems
Over-permissive NSG inbound rules	High	Direct internet exposure increases breach likelihood
Unrestricted outbound internet traffic	Medium	Enables data exfiltration and C2 communication
Misconfigured Azure Firewall DNAT	High	Exposes internal services to external attackers
WAF operating in detection mode only	Medium	Web attacks not actively blocked
Weak VPN encryption or shared keys	High	Secure partner connectivity can be compromised

VMs with public IPs attached	High	Expands attack surface and regulatory exposure
Incomplete network logging to SIEM	Medium	Delayed detection and incident response

3.3 Compliance Risk Analysis (FinTech Context)

Risk	Compliance Impact
Overexposed VNets enabling lateral movement	Violates PCI DSS segmentation and RBI defense-in-depth requirements
Over-permissive NSG rules on internet-facing subnets	Fails PCI DSS inbound access restriction controls
Misconfigured Azure Firewall or DNAT rules	Breaches ISO 27001 access control principles
WAF not enforcing prevention mode	Increases risk to PCI DSS scoped web systems
Incomplete logging and SIEM integration	Violates RBI incident detection and audit trail mandates

3.4 Lateral Movement Attack Path

1. Attacker compromises an internet-exposed Azure workload.
2. Harvests credentials, managed identity tokens, or stored secrets.
3. Enumerates VNets, subnets, NSGs, and reachable internal resources.
4. Moves laterally via permissive NSGs or VNet peering.
5. Accesses sensitive services through private endpoints or APIs.
6. Escalates impact to financial fraud or regulated data exfiltration.

This highlights how weak segmentation directly increases systemic risk.

3.5 Risk Scoring Model

Risk Rating	Category	Meaning
1	Very Low	Minimal business or security impact
2	Low	Limited operational impact
3	Medium	Noticeable security or compliance risk
4	High	Significant financial or regulatory exposure
5	Critical	Severe impact requiring immediate action

3.6 Critical Risks (Prioritized)

Risk Name	Priority	Justification
Overexposed internet-facing workloads	1	Direct attack path to regulated financial systems
Flat VNet enabling lateral movement	2	Rapid spread to payment processing workloads
Over-permissive NSG rules	3	Violates segmentation and least-privilege principles
Misconfigured Azure Firewall DNAT	4	Exposes internal services without inspection
Incomplete network logging and SIEM coverage	5	Delays detection and regulatory reporting

3.7 Technical Exploitation Depth

- Internet scans identify exposed Azure RDP/SSH endpoints
- Attackers brute-force or credential-stuff weak accounts
- Compromised access enables privilege escalation
- Lateral movement occurs via VNets and permissive NSGs
- Results in ransomware, fraud, or financial data theft

This demonstrates realistic attack progression aligned with Azure threat patterns.

3.8 Monitoring Gaps

Gap	Risk Impact
NSG Flow Logs disabled	Attack paths remain invisible
Firewall diagnostic logs not enabled	Malicious traffic bypasses detection
WAF logs not centrally collected	Web attacks unnoticed until damage
VPN tunnel logs not monitored	Compromised connectivity undetected
Logs not forwarded to SIEM	Delayed incident detection
Insufficient log retention	Regulatory audit and forensic failure

3.9 Mitigation Strategy

Vulnerability	Mitigation
Flat VNet architecture	Implement tiered subnet model and restrict east-west traffic
Over-permissive NSG rules	Enforce least-privilege and periodic rule audits
Internet-exposed management ports	Remove public access; use Bastion or VPN
Misconfigured Firewall rules	Centralize inspection and apply strict allowlists
WAF in detection mode	Enable prevention mode with updated OWASP rules
Weak VPN encryption	Enforce strong IKE/IPsec parameters and MFA
Public IPs on VMs	Remove public IPs; front with Firewall or WAF
Missing network logs	Enable flow, firewall, WAF logs; forward to SIEM