3. Vulnerability Identification Report

3.1 Assessment Scope

The network security assessment covered the following AWS VPC components and controls:

- VPC CIDR design, subnet tiering, and multi-AZ isolation
- Internet Gateway (IGW) exposure and routing controls
- Public, Application, and Data subnet segregation
- Security Group inbound and outbound rule enforcement
- NAT Gateway egress access and outbound traffic control
- Application Load Balancer (ALB) internet exposure
- EC2 instance network exposure and administrative access
- RDS network isolation and replication traffic protection
- Network logging, visibility, and alerting mechanisms

3.2 Core Network Vulnerabilities

Vulnerability	Risk	Business Impact
Flat trust between application and data subnets	High	Enables lateral movement to financial databases
Over-permissive Security Group inbound rules	High	Internet attackers gain access to internal tiers
Unrestricted outbound access via NAT Gateway	Medium	Enables data exfiltration and command-and-control
ALB exposing unnecessary ports or paths	High	Expands attack surface of web layer
Weak isolation between AZs	Medium	Increases blast radius during compromise
EC2 instances with public IPs	High	Direct exposure of compute workloads
Insufficient RDS subnet isolation	High	Unauthorized access to regulated financial data
Incomplete VPC flow logging	Medium	Delayed breach detection and investigation

3.3 Compliance Risk Analysis (FinTech Context)

Risk	Compliance Impact
Poor subnet tier segregation	Violates PCI DSS network segmentation requirements
Overexposed ALB and web layer	Breaches RBI perimeter security expectations
Weak Security Group controls	Fails ISO 27001 access restriction controls
Data subnet reachable from public tier	Expands PCI DSS scope unnecessarily
Missing network logs	Violates RBI audit trail and incident response mandates

3.4 Lateral Movement Attack Path

- Attacker compromises an internet-facing web EC2 via ALB
- Enumerates Security Groups and reachable subnets
- Moves laterally into application subnet
- Exploits overly trusted Security Group relationships
- Accesses RDS instances in data subnet
- Results in financial data theft or transaction manipulation

This demonstrates systemic risk caused by weak tier isolation.

3.5 Risk Scoring Model

Risk Rating	Category	Meaning
1	Very Low	Minimal security or business 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
Internet-exposed web tier	1	Primary attack vector to fintech workloads
Weak subnet segmentation	2	Enables rapid lateral movement to databases
Over-permissive Security Groups	3	Violates least-privilege and PCI DSS controls
Unrestricted NAT Gateway egress	4	Enables undetected data exfiltration
Insufficient network logging	5	Delays breach detection and regulatory reporting

3.7 Technical Exploitation Depth

- Internet scans discover ALB-exposed services
- Web tier compromise via vulnerable application
- Security Group trust abused for lateral movement
- Application tier compromise escalates privileges
- Database access achieved through internal routing
- Leads to fraud, ransomware, or financial data loss

This aligns with real-world cloud breach patterns.

3.8 Monitoring Gaps

Gap	Risk Impact
VPC Flow Logs disabled	East-west traffic invisible
ALB access logs missing	Web attack detection delayed
NAT Gateway traffic unmonitored	Data exfiltration unnoticed
RDS connection logs missing	Unauthorized access undetected
Logs not centralized	Ineffective incident response
Short log retention	Regulatory audit failures

3.9 Mitigation Strategy

Vulnerability	Mitigation
Weak subnet tier isolation	Enforce strict Public/App/Data separation
Over-permissive Security Groups	Apply least-privilege and periodic reviews
Public IPs on EC2	Remove public IPs; access via ALB only
Unrestricted outbound traffic	Restrict NAT egress destinations
ALB overexposure	Limit listeners and paths
RDS reachable from app tier broadly	Restrict DB access to required instances
Missing flow logs	Enable VPC Flow Logs
Logs not sent to SIEM	Centralize logging and alerting