Critical Assets:

- Customer Data AML Compliance (SSN, address, ect.)
- Physical Infrastructure (Data Centers and Buildings)
- Online Banking Website
- Other Customer Facing Websites
- Network Infrastructure
- IAM Protocol
- Bank Teller

Critical Asset	Threat	Vulnerabilities	Impact
Customer Data AML Compliance (SSN, address, ect.)	● Could get stolen ● Data loss, no backup ● Data could be changed	● No encryption ● Incorrect customer data ● Failure to report to authorities ● Access control, who gets to see what	● Reputational damage ● Financial damage ● Operational Disruption ● Getting very very very sued
Online Banking Website	● Website could be hacked ● Malware implanted ● WEbsite host goes down, website becomes unavailable	● Unpatched exploits ● Open ports (TELNET, HTML) ● No MFA ● No DDoS protection ● Nt sanitizing inputs	● Bank loses ● Increate in customer support calls ● INformation put on the darkweb
Network Infrastructure	● Legacy system and old protocols are exploited ● Physical failure, natural disaster ● Data interception		● Availability of all services ● Core cyber services potentially compromised impacting full operations ● Compliance breach

Resilience Program

- Principle of least Privilege - implementing AAA concept
- MFA everywhere
- Continjuous monitoring - monitor for weird activity
- Full data encryption
- Data input validation
- Redundancy and failover strategies
- IR Communication Plan