Network Security – Part 1

1. Control of IT
   - Control of computing assets
   - Management of software update mechanisms
   - Monitoring of IT assets for performance, capacity, and availability
   - Systems lifecycle management
   - Policy enforcement for configurations

2. Perimeter Security
   - Network traffic access rules
   - Security Services for inbound/outbound traffic

3. Public Facing IT Assets
   - Application and service hardening
   - Security of communication protocols for connecting to services
   - Network segmentation for public facing assets

4. Access Control
   - Determination of who should have access to what
   - Permissions and privileges
   - Account Control

5. Internal Security
   - Hardening of internal assets
   - Use of secure network protocols
   - Network segmentation for internal services