**Final Project**

**Overview of the Big Automobile Company**

You are working for a large, multinational automobile company. The company manufactures and sells trucks, sedans, SUVs, and electric cars. Its headquarters in Kentucky and Detroit. Its manufacturing facilities are located in Georgia, Vietnam, and China.

**Network environment**

The company has many Windows servers in an active directory environment. Active directory has multiple domains and users in the active directory can request access to SQL Server services available in the domains. To manage its certificate, the company uses Symantec as a certificate authority.

**Database server environment**

The database for online transaction processing is located at the headquarters. The databases in the headquarters deal with manufacturing, sales, marketing, accounting and finance, and supplier data. Branch offices have replicas of the main databases and these databases can be read for reporting and querying purposes. The company manages the databases with high availability and disaster recovery solutions to prepare for security incidents. However, according to the last auditing report, the current high availability solutions are not robust enough considering the growth of its business.

**Current situation**

Recently, the company experienced ransomware attacks and some databases were locked out for a few weeks. To investigate this incident, you organized a team of DBAs and conducted an auditing. You are attempting to revise the companywide database security policy. While doing this, you need to consider the laws and regulations including the Sarbanes-Oxley act and PCI-DSS.

Before you create a new security policy, identify the following elements.

1. Role players (i.e., stakeholders)

Local:

cyberarena

Philliphuff7

Groups:



2. Critical information assets

Microsoft Kernel Power

3. Threats

critical Microsoft Corpartaion Services are Stopped

Unknown Services are running in the background

OS Updates Never Installed,

Connected to an UnKnown Network

4. Vulnerabilities

Local Server has Remote Desktop enabled

Product Id Not Activated

IP Address is on DHCP

Remote Desktop is enabled

on a Public Network

UnEncrptyed DNS Server

Website are allowed to Knowthe Physical location of the server

No Connection Security Rules for Remote access

Not notified if Apps make account changes.