**Broad overview:**

Information Security is present in all environments:

* Corporate America to secure confidential data to give them a competitive edge
* Healthcare to ensure patient data is secure
* Retailers must ensure credit card data is secure during transmission
* Cloud computing presents issues of its own, which include shared resources, controls implemented outside of the organization, and possible network implementation differences

Regardless of industry or business sector, organizations must simultaneously maintain ongoing operations and secure the resources needed to operate. Modern organizations must maintain a security perimeter that thwarts attempts to identify and exploit vulnerabilities while supporting an ever increasingly mobile workforce. Additionally, some organizations are also held accountable under financial and federal regulations such as:

* SOX
* PCI DSS
* FIPS compliance
* FedRAMP
* CPNI – Customer Proprietary Network Information
* HIPAA

These organizations will use Risk Assessments to identify assets valuable to business continuity, create Policies and Procedures to guide employees and processes, and develop educational programs to ensure compliance with policy and secure technology use. In addition, the organization may choose to implement technical controls to supplement the security of information inside their corporate network as well as to ensure regulations are followed.

**Company Overview:**

Your group has been engaged by MotorHead Distributors Inc., located in the Midwest U.S.A. to perform an Information Security audit of the company’s network, policies, and procedures to ensure that compliance and regulatory guidelines are met. In addition, the company would like for you to do their yearly Risk Assessment, for auditing purposes, of their information assets. Here is a brief company overview.

* The company knows that IT is important and that it should supplement the mission of the company.
* The IT department budget allows for them to keep the business up and running but there are several systems in need of replacement. This is due to end of service life equipment and software in addition to application packages that need to be updated/decommissioned. However, some of these systems support mission critical operations and cannot suffer the downtime that would come with replacement.
* The company has dealt with security breaches in the past where customer data has been compromised and network services suffered as a result of these breaches.
* Policies for the company were reviewed during the last SOX audit for the company and were deemed as needing a revisit.
* There are no standard procedures for patching of server and network environments. In addition, antivirus software has been installed and configured but IT is lax on ensuring that updates are properly and timely done.
* One issue that continues to pop-up is understaffing in IT. They are able to keep the lights on but are frequently inundated with new requests.
* The company accepts credit card payments from their customers for orders placed online or via telephone or fax.
* The online site that takes these credit card payments uses SSL encryption and is hosted by a third-party vendor. The vendor has gone through the necessary audits to ensure compliance. The credit card numbers are never seen by employees at the company.
* The company offers their employees a full benefits package: medical/dental/vision, paid time off, company-owned gym, paid business travel, etc.
* Risk assessments for the IT assets are done when the asset is procured and installed. The IT department is responsible to work with the risk analysis group to classify and prioritize the network, server, and data assets of the company. Audits are performed yearly, to maintain compliance, but re-assessment of assets is not done regularly. In fact, internal risk assessments are usually overlooked.
* The Information Security area falls under the Chief Information Security Officer (CISO) who ultimately reports to the Chief Information Officer (CIO). The budget for Information Security comes from the IT budget.
* The company cannot tolerate prolonged downtimes to their information systems due to impact of revenue. Specifically, their high-priority systems are payroll, warehouse management, email, order entry, and financial systems. If any of these systems is down for longer than 3 hours, the CIO and CEO of the company are notified via Executive Dashboard.
* The company does have a remote access solution for employees to VPN into the network to do work after hours or work from home.
* Information Security is part of this company; however, they use standard methods for training employees and disseminating information regarding security posture and practices.