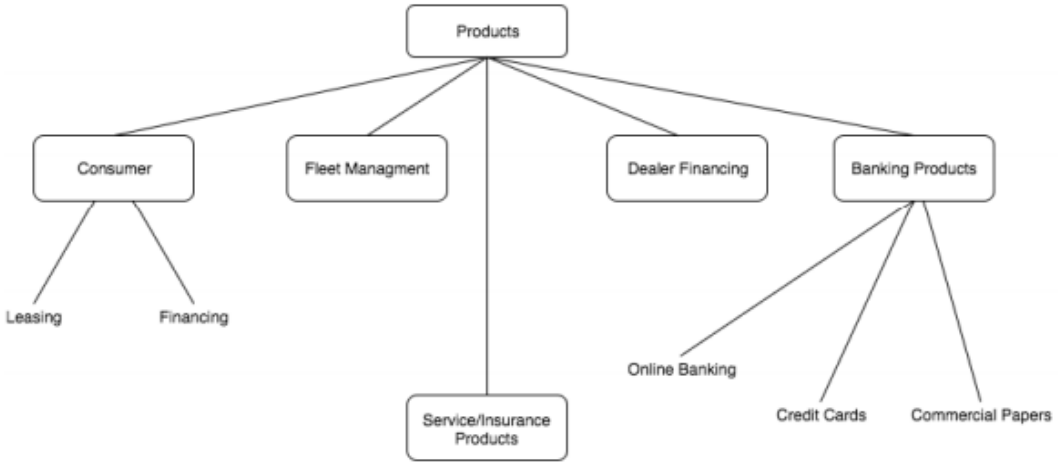
Information Security – Project Team Car Bank

1. Business Model:

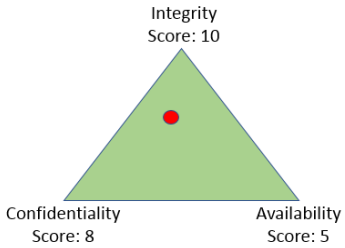
Provide a range of banking products to finance wholesale or retail purchases from the parent firm. In addition, providing traditional banking products helps the company maintain a high liquidity ratio. (liquidity ratio = current assets/current liabilities).



2. Importance of Information Technology:

- Information technology is crucial in fleet management. It allows companies to track their automobile fleet and analyse the data in order to improve the productivity, efficiency and to reduce the costs.
- Online banking relies heavily on information technology. A complex and secure server infrastructure has to be established so that guarantees the availability of the service as well as the security of user's data.
- Fleet management, financing, insurance, and other services have to have an appropriate IT infrastructure in place to cater to the customer's and bank's needs. Information technology is required to accomplish this task.

3. Main Security Targets for CIA:



1) **Integrity**:
Is the most important security target. First of all, without strong data integrity customer data would become unreliable. If it became unreliable then it would lose value as a top asset. Also, without strong data integrity the bank could end up charging a customer the wrong amount of money. This could then lead to a loss in profit. Finally, the trust of both the customers and the dealer could be lost if they became aware of the lack of data integrity. This would make it harder to attract new customers, and could lead to the dealer terminating the business relationship.

2) **Confidentiality**:
Without confidentiality, customer data could be accessed by unauthorized third parties. This would then lead to a top asset essentially being given away for free. Also, when customers sign up they expect a certain level of privacy when it comes to their data. This privacy would have been guaranteed to them as well. This guarantee being broken could lead to them wanting to leave the bank. It could also discourage potential customers.

3) **Availability**:
Is the least important security target. Availability is important for employees especially during work hours. If availability is lost, then profit would be diminished as well, due to a loss of productivity.

Customers also require access to their own data. This data could help them remember how much they have to pay and when they should pay it. The dealer should also have access to certain data. Customer availability is not as important as employee availability, because customers losing access for a day would not be significantly damaging productivity. This is the reason why availability as a whole is not as important as the other two security targets.

4. Overall Policy:

- ➢ Ensuring the confidentiality and security of our customers and partners information.
- ➢ Proper disposal of information and protection against unauthorised access.
- ➢ Protection against network threats by encryption of data and regularly monitoring the traffic on the network.
- ➢ Establishing responsibility and accountability for information security in the bank with appropriate level of awareness, knowledge, and skill to minimise the severity of incidents.
- ➢ Access Controls:
    - Controls to authenticate and permit access to authorised persons.
    - Controls to prevent employees from leaking data
    - Access restrictions to buildings, computer facilities and office equipment only to authorised individuals.

Topic Specific Policy:

- ➢ Access Control
- ➢ Information Classification
- ➢ Communications Security
- ➢ Information Transfer

5. Main Important Assets

Money
is needed to offer financial services to customers.

- Foreign exchange reserves
  → To be on top of the market by offering services to customers in every country independent of the currency.
- Loans
  → Brings profit back to the bank
- Securities
  → Get more value from stocks by selling them → Get money from securities of other companies

Customers

- Customer Data
  → To ensure the company receives money from the customers in case of insolvency
  → Analytic / Statistics : To increase profit and improve process

- Holdings
  → Generate income:
    • Bank is dependent on holdings
    • Independency from single customers

Employees

- Qualified & trained
  → To keep and gain customers by providing good service
  → To analyse data efficiently and profitably

6. Threat scenarios & attack vectors compromising to the assets:

Threat Scenario: Data Breach

Data Breach is the loss of private/secure data by a company. The loss can occur mainly because of human beings. Often intentional by a hacker outside the company, but also unintentional by the staff or external staff. Furthermore force majeure can cause a data breach too.
Targeted assets: Customer data, employees

Security controls referring to ISO 27002:

A8.3.2 - Disposal of media
Control: Secure disposal of no longer needed media

- Media containing confidential information should be stored and disposed safely, for example shredded or incinerated.
- Procedures to identify data which is important to disposing securely are necessary, but it can be easier to collect all media items and dispose them then.
- Be careful with organizations which offer collection and disposal services of media, ideally do it yourself.

A12.3.1 - Information backup
Control: Regular backup of information, software and system images

- Accurate and complete records of the backup copies and documented restoration procedures should be produced.
- The extent and frequency of the backups should conform with the security requirements and the business requirements.
- The backups should be stored in a remote location, with a sufficient distance to the main location.
- In special situations where confidentiality is important, the backups should be protected additionally by encryption.

A13.2.1 - Information transfer policies and procedures
Control: Protecting the transfer of any information by formal transfer policies, procedures and cpntrols

- Procedures which prevent transferred information from getting intercepted, copied, modified, miss-routed or destroyed.
- Procedures for the detection and protection against malware.
- Use of cryptographic techniques to protect the confidentiality, integrity, and authenticity of information.
- Advising personnel to take appropriate precautions not to reveal confidential. information.
- Not leaving messages with confidential information on answering machines.

Threat Scenario: Exploitable Software Vulnerabilities

A vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability — a vulnerability for which an exploit exists.
A resource may have one or more vulnerabilities that can be exploited by a threat agent in a threat action. The result can potentially compromise the confidentiality, integrity or availability of resources belonging to an organization and/or other parties involved.
Targeted assets: Customers, Money

Security Controls referring to ISO 27001:

A12.2.1 - Controls against malware
Control: Protect information and information management facilities from malware and raise appropriate user awareness

- Implement detection, prevention, and recovery tools against malware by prohibiting unauthorized software via whitelisting.
- Installation of malware detection systems which scans all types of incoming files e.g. via network download or USB media, for malware, and which scans mail attachments when they enter the mail server and scan webpages for malware.
- Define procedures to deal with malware infection like reporting the incidents and executing an already implemented business continuity plan.

A12.6.1 - Management of technical vulnerabilities
Control: Gather and evaluate information about technical vulnerabilities and take appropriate measures to address them

- Prevent exploitation of technical vulnerabilities by defining management and monitoring roles for them.
- Patching and assessment of necessity by evaluating if patch fixes present vulnerability appropriately and if new risks arise by patching
- Patch testing before implementation in a safe environment and increase of monitoring and logging to track suspicious behavior and detect it in a timely manner
- Communication with incident management about vulnerabilities and risks by setting up emergency plans like backup servers and softwares.

A13.1.1 - Network Controls
Control: Ensure security of information in networks and the protection of connected services from unauthorized access.

- Separation from operational responsibility for networks by introducing a network operations center which is a specific department for network management, monitoring and controlling.

- Logging and monitoring of traffic and using intrusion detection and network security monitoring software, like security onion, forensics analysis of collected data to track suspicious behavior.
- Authentication of network systems by requiring login for a network action such as a file transfer and restricting access of systems connected to the internet

Attack Vector: Social Engineering

Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. Although it is similar to a typical confidence trick, the concept is applied to the trick of gathering login credentials, bank information or computer access, and it's commonly one of the many steps of a bigger scheme.

Initial Targeted Assets: Customers, employees and third parties' employees.
Goal Targeted Assets: Money, holdings, and securities.

Security Controls referring to ISO 27001:

A.7.2.2 – Information security awareness, education, and training.

Control: All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

- Conduct security training for new employees adapted to their role and access.
- Conduct security training for employees when they change area and level.
- Reinforce security with follow-up trainings on a regular basis.

A.7.2.3 – Disciplinary Process

Control: There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

- Establish different levels of disciplinary process based on nature and gravity of a breach, while ensuring correct and fair treatment of employees.
- Establish a reward system for employees that successfully follow security procedures.
- Include clauses in personal contracts for their understanding and acceptance of the disciplinary process.

A.9.2.2 – User Access Provisioning

Control: A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services

- Include clauses in personal and services contracts, regarding the acceptance of responsibilities for unauthorized use of access.
- Adapt and update access, so it is limited to the necessary business requirements according to the user role.
- Maintenance of a central record with access and activity information, to facilitate tracking the origin of any breach.