Information Security Policy

1) Purpose:

Information Security is ensures that all the digital and non-digital data is secured by implementing, maintaining and improving information security management systems to provide secure, well-maintained business. ISMS is ensures that all the data kept by bank organization, servers and other assets are secured against external and internal threats to ensure integrity and confidentiality and all assets are available to ensure business continuity by accordance to business strategy, regulations and contracts.

2) Business Model:

Business model of banking is providing financial support to car/truck manufacturing by offering

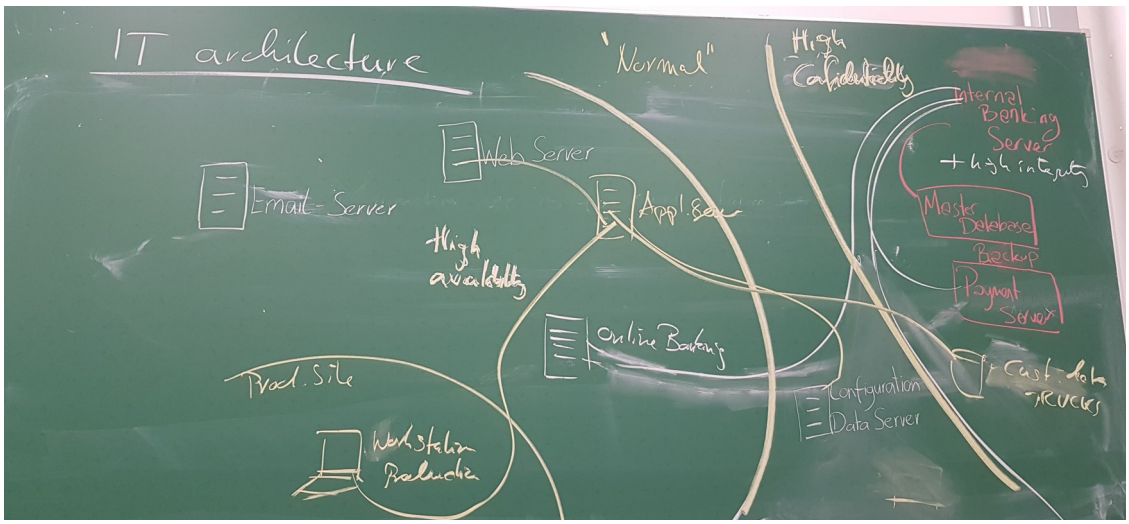
-Leasing options to customers and companies to avoid third party financial services,
-Saving accounts to provide financial liquidity to manufacturing and development departments,
-Online banking.

Income of the Bank can be used to invest back into the business, e.g. expansion of business unit and better R&D.

3) Assets in bank:

-User Data,
-Employee/Employer Data,
-Financial Data,
-Servers: Web Server, Internal Banking Server, Master & Slave Database Servers, Backup Server
-Transaction Logs,
-Network infrastructure
- Backup System & off-site Backups
-Proprietary Softwares,
-ATMs,
-Offices computer equipment,
-Call center & telephone/eMail system & online form
-Software Licenses/Patents

3) IT Architecture:



Each department of the company has their own IT Architecture for efficiency of the business. Each of them has different priorities and requirements according to business. Therefore main computer centers are segregated into their needs.

Banking department, main computer center should be located at somewhere provides high integrity.

Cars and Trucks department, main computer centers should be located at somewhere provides high availability for continuous manufacturing.

Publicly accessible servers get physically separated from internal servers with high confidential data and only connect through interfaces to the internal servers which require authentication and access control. These internal Servers are in their own DMZ network and isolated from the rest of the company.
High Availability servers such as e-Mail, Web and Online-Banking (front-end) are distributed across the world and internal across the manufacturing departments to provide fail-over and 24/7 Service. Configuration and Slave Database servers offering less-confidential but still critical data get are local to the public services to minimize latency.

3.1) CIA Analysis:

Bank unit:		Confidentiality	Integrity	Availability
transaction servers for business costumers:		10	10	0
public web servers for new costumers:		0	0	10
online banking servers for private costumers:		5	0	7
administration servers for support/dev:		0	9	1
backend servers for information management(CMS):				
	master:	10	10	10
	slave:	8	3	5
distributed storage & backup servers:		5	5	10
truck unit:				
production:				
	web server (order placement):	0	0	10
	order database:	0	4	10
manufacturing:				
	information exchange server:	0	0	10
	costumer database:	10	0	10
service:				
	telemetry services:	0	0	10
car unit:				
costumer	web server & Database (order placement):	5	2	7
production	Manufacturing & automation	0	6	10
development	computer aided design & simulations	8	6	2

Banks:
- Servers for account transactions and the master database server require max priority for integrity/confidentiality over availability to ensure data can't be modified without authorization, accountability and financial data will not leak into public.
- Public web servers for new customers and the distributes storage & backup systems require highest availability and failover systems to ensure business continuity
- Internal online banking (app) require high confidentiality to ensure the security of private data and back-end servers for support of the online services and support require high integrity and some fail over
- Slave database servers provide higher availability while still maintaining confidentiality via authorization but easier and therefore lower priority on integrity through read-only mechanisms and checks with other servers in the network required to agree to modification

Trucks:
- production services like web server and database back-end for it require high availability and fail-over to ensure business continuity while the latter requires also integrity because it contains only non-personal order information
- the manufacturing services require high availability to ensure business continuity in the manufacturing of trucks, the costumer database required for fulfilling the orders and distributing the products requires high confidentiality because it contains personal data, integrity priority is low because this information can be presented read-only

- the telemetry services for existing customers require high availability with fail-over to ensure 24/7 connectivity to guarantee no outage in service of the trucks

Cars:
- production services like web server and database back-end for it require high availability and fail-over to ensure business continuity while the latter requires also integrity because it contains only non-personal order information
- the manufacturing services require high availability to ensure business continuity in the manufacturing of trucks, the costumer database required for fulfilling the orders and distributing the products requires high confidentiality because it contains personal data, integrity priority is low because this information can be presented read-only
-Cloud service servers require availability and integrity because of safety of customer.

4. Threat scenarios & Attack vectors compromising to the assets:

Threat Scenario: Data Breach

Data Breach is the loss of private/secure data by a company. It has a big importance for both customer and business side. 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. Data breaches are more result than attack but they still have a big effect of business confidentiality. The breached data might include sensitive information about customers, employees, business.
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 controls

- Procedures which prevent transferred information from getting intercepted, copied, modified, miss-routed or destroyed.
- Procedures for the detection and protection against malware.
- Use of cryptography 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: Software Vulnerabilities

A vulnerability is a weak point of the software or operation system which can be exploited by threat actor. This vulnerabilities can be exploited by using malware or remote code executions. For example a hacker can use ransomware type malware to encrypt all the data on the computer and by exploiting a vulnerability in the network it can spread over all the network. This type of attack may damage databases and will have effects on availability. An other possibility is remote access tools, which can give access to malicious persons to manipulate data or to reach customer data. This kind of attack will have effects on integrity of the servers.

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.

Threat Scenario: Social Engineering

Social engineering is using psychology to get data such as login credentials, bank information and computer access by human interaction. Example scenario of an attack is impersonating a new employee of the bank to gain physical access. This type of attack will cause an effect on integrity of

the bank. Another attack scenario is impersonating a customer or employee to steal their credentials. This type of attack will cause effects on confidentiality and integrity of the bank.
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.

Risk Analysis of Threats:

Risk Matrix	Negligible	Minor	Moderate	Significant	Severe
Very Likely	**Low**	**Moderate**	**High**	**High**	**High**
Likely	**Low**	**Moderate**	**Moderate**	**High**	**High**
Possible	**Low**	**Low**	**Moderate**	**Moderate**	**High**
Unlikely	**Low**	**Low**	**Moderate**	**Moderate**	**Moderate**
Very Unlikely	**Low**	**Low**	**Low**	**Moderate**	**Moderate**

Risk = Possiblity * Impact of Threat

Social Engineering : Moderate Risk
Software Vulnerabilities / Data Breach : High Risk