MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATICS

DEPARTMENT OF INFORMATION TECHNOLOGY

NAME: HAMUN MOHAMED HASSAN

REGNO: SIT/B/01-55770/2020

COURSE CODE: BIT 315

COURSE TITLE: INFORMATION SECURITY AND ASSUARANCE I

TASK: ASSIGNMENT

1. Consider a given organization and activities of the organization

a. Propose the possible system to be used by that organization

The banking industry they use the banking system software.

Banking Software is a comprehensive term used for applications and software solutions for core banking, investment banking, financial services, and capital markets. This software provides tools to automate, manage, and simple corporate banking, SME banking, Wealth Management, Asset management, trading platforms, credit organizations, and more. Designed to make the life of bankers, banking clients, and employees easy, these tools have all features to run the core banking operations efficiently.

What are the different types of Banking Software?
Desktop-based/On-Premise

These types of banking system software are licensed, and banks can install them within their IT infrastructure. On-Premise banking management systems are highly customizable in nature. Banking organizations seeking banking software solutions for optimum results and who prefer keeping their data on their own servers can opt for desktop-based banking systems.

Web-based

These types of online banking platforms are hosted, and third-party digital banking solution providers offer these tools. Web-based online banking platforms are very popular as apart from the bank admins, customers, bank agents, and employees can also access these software solutions from anywhere with a login ID and the password provided by banks.

Cloud-based

These types of banking management software are hosted through third-party cloud service providers such as Amazon web service, Microsoft Azure, etc. These are popular with large banking organizations that require massive data storage capacity and extreme flexibility. The cloud-based banking software solution is a SaaS (Software as a Service) that allows banks and their customers to access the services using internet-enabled devices.

Open Source

These types of core banking software allow users to customize source code, modify inbuilt settings, and add extra plugins to enhance the capabilities, functionalities, and utility of the software. When banking organizations need to accommodate specific features in their banking software solutions that are unavailable with any vendor, then open source banking software can opt.

Why do you need Banking Software, and what will happen without it?
For ease of transactions

Banking software has made the lives of both bankers and customers easy. Banking software allows bank account holders to access banking services, in real-time. Implementing it means easing the transactional activity.

For 24/7 functionality

Without software, banks cannot provide 24/7 functionality and around-the-clock service.

Increasing account holder's trust:

When service requests, queries, fund transfer processing are in real-time, and loan sanctions are through a high-speed digitally automated process, the account holders are more likely to trust the banking organization.

Ensuring regulatory compliance:

The financial ministry of every nation and regulatory body frequently asks the banks to submit various financial documents and reports related to their transactions, customer bank account details, and related liquidity information. Mostly such requests are on an urgent basis. For example, if the finance ministry wants the banks to submit the details of all account holders having more than a million dollars in their current or saving accounts, then banks having banking software need not take any stress. They will just have to filter, segregate, and download the information with a few clicks, and information will be available in any format (PDF, CSV, Excel) they need.

To Safeguard valuable data:

Banks have records of account holders' personal details, financial assets data, copies of various identity proofs, and tax information that can be misused by fraudulent imposters or scammers if leaked. The two-factor authentication and password-protected layered security of banking software provide a shield to banks for safeguarding their valuable data and honoring their customer's privacy.

For Ensuring High-security

Stringent adherence to high-end security features is a foremost criterion for banking software. Double-factor authentication, multiple-layer of security, and encrypted networks make transactions secure and hacking-proof.

Management of corporate treasury

Since the 2008 financial crisis, a lot of changes have been made in the corporate treasury part of the banking business. Greater transparency to protect account holders' money is a fundamental aspect of banking laws. Banking software is essential to access financial market data and assess risky investments for corporate and institutional investors.

Improved bank workflow

With automated financial service solutions, progressive banks can improve their workflow and automate complex processes. With an automated classification of documents, extraction tools, advanced search features, and validating processes, banks can enjoy a faster and error-free workflow.

Centralized Banking

With every data, quantifiable information, and business process available to all employees of a bank, a uniform approach can be maintained across all branches. In decentralized banking processes, managers can provide loans considering the soft data such as the customer's relationship with the manager, but it can be very risky. A banking software centralizes

everything so that managers can adopt a quantifiable approach to credit assessment before sanctioning any loans.

Bank Treasury

Banking software keeps a record of all the capital that the bank's treasury possesses in real-time. It helps to control and manage the bank's money efficiently for daily operations.

Trading

Today banks are involved in large-scale transactions of gold, stocks, bonds, and debt instruments for trading purposes. A banking system can be used to set algorithms to help banks in buying and selling profitably.

Friction-free back-office operations

With robust automation features of banking software, the back-office staff can work efficiently without hassle. It has a module to handle and automate back-office operations such as clearance of cheques, drafts, customer applications, etc.

Without banking software, banks would not be in a position to analyze the data of their customers to come up with meaningful conclusions. It would be difficult to manage the mammoth work manually. Banks won’t be able to efficiently tackle regulatory changes, operational requirements, and customers’ demands. Without a robust banking system, mapping customer demographics to come up with new products, or meet dynamic business demands is not feasible.

A banking software solution is capable of handling the following functions:

- Core banking
- ATM
- Internet Banking
- Mobile Banking
- Payments network
- SMS Based banking
- Card management system
- Trading services by Investment banks (Capital markets)
- Financial data management
- Multi-currency management
- Wealth management
- Customer management
- other banking products

What are the benefits of banking software?
Customer satisfaction and robust customer experience

One foremost benefit of the banking software is that you equip all your bank employees with the necessary information to deal with clients' issues. For instance, a customer who has called the bank to enquire about a deducted charge from his savings account abruptly asks a random question for his loan information too. His call is not transferred to the loan department; rather, the bank official solves the query. You can imagine how satisfied the customer would be to know that the bank knows his profile thoroughly. A single database available to all employees and Omnichannel banking solutions using the banking software can work wonders for your banking business.

Increasing productivity

Bank managers can automate tasks related to everyday core banking operations, service request proceedings, sending marketing emails to the customers, and enabling self-service portals for clients. When banks can complete a lot of tasks without the customers having to either contact the bank or visit the branch, it increases the productivity of the bank and saves time and employee cost.

Reduced need for workforce

Banking software reduces the need for the human resource required at individual branches to run its operations.

Multi-branch activities from one point

Banking software brings all branches of the bank on a single interactive platform. All core banking services can be monitored and controlled from a single dashboard.

Banks get assistance in all core operations of the banks, such as:

- Everyday banking transactions
- ATM transactions
- Internet Banking
- Fund transfers
- Account opening and closing
- Mobile Banking
- Payments network
- SMS Based banking
- Card management system
- Multi-currency transactions
- Customer service requests

b. Determine security issues of that organization

1. Unencrypted Data
This is a very basic yet crucial part of good cyber security. All data stored on computers within your financial institution and online should be encrypted. Even if your data is stolen

by hackers, it cannot be immediately used by them if it's encrypted – if left unencrypted, hackers can use the data right away, creating serious problems for your financial institution.

2. Malware
End user devices – such as computers and cell phones – that have been compromised by malware pose a risk to your bank's cyber security each time they connect with your network. Sensitive data passes through this connection and if the end user device has malware installed on it, without proper security, that malware could attack your bank's networks.

3. Third Party Services that Aren't Secure
Many banks and financial institutions employ third party services from other vendors in an effort to better serve their customers. However, if those third-party vendors don't have good cyber security measures in place, your bank could be the one that suffers. It's important to look into how you can protect from security threats imposed by third parties before you deploy their solutions.

4. Data That Has Been Manipulated
Sometimes hackers don't go in to steal data – they simply go in to change it. Unfortunately, this type of attack can be difficult to detect right away and can cause financial institutions to incur millions of dollars in damages, if not more. Because the altered data doesn't necessarily look any different than unaltered data on the surface, it can be challenging to identify what has and hasn't been altered if your bank has been attacked in this manner.

5. Spoofing
A newer type of cyber security threat is spoofing – where hackers will find a way to impersonate a banking website's URL with a website that looks and functions exactly the same. When a user enters his or her login information, that information is then stolen by hackers to be used later. Even more concerning is that new spoofing techniques do not use a slightly different but similar URL – they are able to target users who visited the correct URL.

c. Determine possible solution to those issues

- **Encrypt your data.** This should be your first step. As we stated before, should your data be stolen, hackers will have a difficult time unpacking and using it if it's encrypted.
- **Employ multi-factor authentication.** Another excellent tactic is taking more steps toward using multi-factor authentication if you haven't already. This grants access to

users who present two or more login credentials when prompted, including PINs, passwords, and/or fingerprints.

- **Perform routine cyber-risk assessments.** A defense system is only good if it works. It's important to test your cybersecurity measures occasionally to ensure that you're properly protected. Doing so can help you prioritize areas you need to shore up.
- **Bolster various endpoints.** Banks have several endpoints to take into account, including smartphones, tablets, personal computers, and even servers to ATMs. If a hacker is able to access your network via a compromised ATM, for example, it could cause an ineffable amount of damage.
- **Invest in solid software security measures.** A solid medley of software security solutions can do a world of good! Investigate and invest in firewalls, antivirus, anti-malware software, and hardware security (hardsec) devices to help develop a strong infrastructure against cybercriminals.
- **Train your employees.** Your employees should all be kept up to date about best practices in cybersecurity in your financial institution. Ensure that they receive the proper training to identify threats and minimize the chances of data breaches. Consider adding refresher trainings once or twice a year (or however often you see fit).
- **Educate your customers.** It doesn't hurt to reach out to your happy customers to inform them about cyber safety! Construct a helpful email or newsletter educating them about cybersecurity and what to look out for.

e. How will they address security vulnerability?

1. Addressing the risks in mobile apps and web portals

Consumers are increasingly choosing cashless payment alternatives. As a result, banks are investing in mobile and web-based solutions that make payments and transfers easier. And such applications create new vulnerabilities that banks will need to address.

2. Examining third-party services

Another key area for cybersecurity concerns in banking is the monitoring of third parties and their cybersecurity practices. If banks lose control over their ingress and egress points, they might leave their critical infrastructure exposed to threats. Third parties are already causing their security environments to fragment.

3. Technical debt and cybersecurity in banking

Even if many financial institutions have been investing plenty of resources into building modern software systems and infrastructures, there's still a massive amount of legacy technology being used in the sector. The ATM industry is a great example. The majority of operating systems used there rely on Windows 7. And Microsoft stopped supporting the system in January 2020.

Moreover, banks looking to deploy new controls will have to re-examine their legacy systems. They will consider potential strategies for protecting their aging technology and choosing potential candidates for innovation.

4. Artificial intelligence for fraud prevention

Artificial Intelligence (AI) technologies are going to play a greater part in customer behaviour monitoring for fraud detection and prevention. What is the greatest strength of AI-powered platforms? They can unify a variety of channels such as digital banking, authentication, card banking, and open banking with a greater intelligence feed. For example, it no longer makes sense to monitor the login and payment activity separately. That way, banks might be left vulnerable to attack. As AI technologies improve and become more commonplace, they will enable in-depth behavioural monitoring and individual profiling of customers across their locations, devices, and authentication methods. Based on the observed

behaviour, the software will provide actionable intelligence with recommended decisions and accurate risk score.

5. Cryptocurrency regulations

The recent years have brought us a number of scams and fraudulent schemes associated with cryptocurrencies. In particular, the Initial Coin Offerings (ICOs) have generated a heated debate about this type of asset trading and investment.

So far, regulators assumed that the sums of money involved are less significant than in traditional banking, in the scheme of global finance. That's why they have used a light-touch approach to regulate the industry. Moreover, governments also wanted to welcome new technologies because they could potentially benefit from tax income in this rising sector.

However, as tech giants begin to enter the space, regulators are going to enforce new laws covering cryptocurrencies. Much stricter enforcement of regulations is going to be the topic for the crypto scene.

6. The rise of open banking

Until recently, banks had full control over the customer's journey. With the emergence and spread of open banking, this is going to change. Consumers now take advantage of banking services through third-party applications that lay outside the control of banks. That's why open banking is such an important trend for cybersecurity. Fraud monitoring with AI and machine learning capabilities will play a crucial role here. By combining the information about the user's normal behavior with parameters about the safety of user devices, the fraud monitoring solutions will accurately flag user behavior deemed as suspicious.

7. Adoption of IoT and 5G

We expect 5G networks to roll out and show their true potential to every industry, including the financial services sector. What’s more, we’re going to witness an increase in the use of connected Internet of Things (IoT) devices.

However, smart connected devices present a range of new risks. In particular, these devices may increase the network’s vulnerability to large-scale multifactor fifth-generation cyber-attacks. IoT devices and their connections to networks are still the weak links in these implementations. The ever-growing value of personal data processed by these devices will need security against potential breaches.

That's why banks are going to take on a holistic approach to IoT security to combine both traditional and new controls and protect the growing IoT network across the industry.