ICT Change Management Project Report
Credit Loan Offering in ING
Group 8

Aniruddha Vaidya
University of Twente
a.h.vaidya@student.utwente.nl

Marzieh Adineh
University of Twente
m.adineh@student.utwente.nl

Yi-Fang Tsai
University of Twente
y.tsai@student.utwente.nl

Jiayu Li
University of Twente
j.li-10@student.utwente.nl

Léo Sajas
University of Twente
l.b.t.sajas@student.utwente.nl

Abstract

This paper aims to provide three potential solutions in the processes of Credit Loan Offering (CLO) in ING with the newly initiated IT change project. The process of CLO is broken down into seven parts which are analyzed with literature review. Based on the findings from the literature review, three solutions are proposed for improving the project and different parts of the process.

Index Terms

Keywords— Change IT, FIS, LoanIQ, Business Process, Project Management, Credit Analysis

I. Introduction and Background

humanThe context of this paper is about an IT change project of the Credit Loan Offering application (CLO) in ING, a major bank in the Netherlands. All the background information is obtained through an interview with a project manager in ING, A CLO loan application is dedicated for large corporations such as Shell and Heineken. Currently, it takes ING around three weeks to assess and complete an application, and there are many manual processes involved in acquiring and analyzing data from clients. To reduce assessment time and to improve efficiency of processes such as data retrieval and analysis, ING has initiated a project, which we refer to as the FIS Project in this paper. The project has been conducted for over a year, and the teams in ING are still working on it. In this project, ING is using the FIS Commercial Lending Suite which includes several components that are highly configurable. They estimate that thousands of hours of work could be spared with the adoption of this new software suite. The FIS lending suite, however, is treated as a black box because there is no publicly available technical documentation about this software. So, in this paper we make assumptions about the IT systems and processes and attempt to identify parts of the project that can be improved based on the literature review and our analysis. Our goal is that our proposed solutions can provide insights to ING to improve the project and the loan assessment process.

II. The Main Research Question

What are the areas that can be addressed for the FIS project and for the CLO assessment process in ING in order to improve their efficacy and quality?

A. Sub Questions

There are several main problems in CLO applications.

Firstly, corporations have many bank partners. 65% of them work with 2-10 banks. 28% work with 11 or more banks. They have hundreds of accounts with costs and management effort associated with each. Secondly, letters of credit – which accounts for $1T in export transactions annually – remain paper-based and labor intensive. ING's contact also told us that they also acquire and extract data from doc files, pdf, and email from clients. Thirdly, average decision time for corporate lending is 3 to 5 weeks. In addition, there are integration problems with legacy IT systems [16].

According to ING, there are hundreds of data points to be collected for a single loan application, and roughly 5% of them will have various types of errors. So, it is vital to use appropriate methods to improve data collection speed and data quality. More importantly, the data is sensitive in nature and needs to comply with regulation and security requirements. Last but not least, certain project management methods could help speed up the testing phase of the newly implemented software, and investigation is made into what can be used for this purpose.

Based on the problems mentioned above, we devised the following sub-questions for our research and analysis.

1) How to improve the credit analysis process?
2) How to improve the speed and quality of the process of CLO applications in the FIS project by optimizing the IT architecture?
3) How to improve data quality?
4) How to improve project management by alternative managerial methodology?
5) Which regulation and security measures need to be taken into account when implementing the new software suite?

III. Literature Review

A. Project Management

While doing changes in IT perspective, there are a lot of aspects that need to be discussed. If the project is too big, there are some uncertainties. That is the reason why corporates should use a standard to assess different possibilities. According to Rodríguez et al (2018), when applying lean thinking to the software development, different aspect should be considered. For example, the effect of the software development is longer and unlimited. What's more, the role that human play is different. While human presence is mostly required to operate automated equipment in a production environment, people's creativity and knowledge are critical in software development. Taufiq et al (2020) did a case study for using Scrum as a software project management tools in a digital banking company. The project was re-defined as successful since it is in line with the company's strategy and adheres to the criteria set forth by the stakeholders. However, Dhevina et al (2021) lists the challenges may appear during the adoption process, and map them with the PMBOK (Project Management Body of Knowledge). The result shows that the most mentioned challenges come from project integration management and project resource management.

B. Data security and privacy

Technology has become inevitable in human life, especially the growth of Internet of Things (IoT), which enables communication and interaction with various devices. No matter what industry it is, while transferring data to the digital cloud, data security has been an issue that people awaring. Not to say, data security and vulnerability scanning are now key concerns in the banking industry(Tse et. al, 2013). Meng (2013) discuss cloud computing data security issues, including tile security of data transmission, storage, security and management of security. In order to meet the contribution, Mohammed et. al. (2017) conduct a systematic mapping study to identify the primary studies on the use of software security techniques in SDLC. Accordion to Kumar, K. N., Balaramachandran, P. R. (2018), for banks to preserve a competitive advantage and boost profitability, robotic process automation (RPA) is becoming a strategic goal. The main advantage of using RPA services in retail banking is that it allows banks to automate regular and repetitive procedures, allowing them to improve efficiency, accuracy, operate 24 hours a day, decrease costs, and provide innovative services and a better client experience.

C. Loan Application

Traditional banking systems use several weeks or even months to make sure if the customer is qualified to apply for a loan. Loans to individuals and businesses are both risky. A fuzzy logic model for loan applications is proposed by Mammadli, S. (2016). The fuzzy model has five input variables: "income," "credit history," "employment," "character," and "collateral condition," as well as a single output variable that shows credit standing. This kind of automation of loan processing has been applied by a lot of banks. Also, Zhan, Q., Yin, H. (2018) suggest a fraud detection method based on a knowledge graph and neural network. The methodology can help reduce the risk in the banking industry.

IV. Research and Analysis on the Sub Questions

A. Loan application Process

Generally speaking, there are two types of risks associated with a loan with a corporation. The first is credit risk and the second project risk [18]. Figure 1 shows the overview of risks.

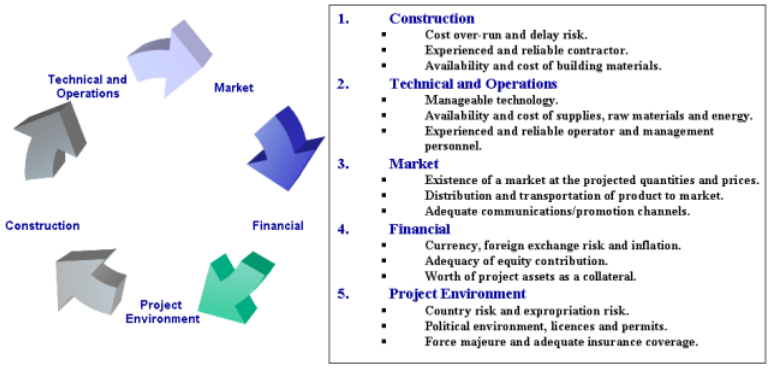

Fig. 1. risks associated with loans

Corporate loans can go bad because of multiple reasons- non-performance or project failures, market risks, diversion of funds, operational failures, bad structuring of finances, people/process issues in the company, management issues etc. [20].

The current (simplified) process as indicated by ING is as follows.

Customers send information via lending portal, docs, emails - Back office obtains, cleans and verifies data - LoanIQ (Finastra) containing hundreds of data points + calculation - Decision making.

To come up with alternative solution for improving loan application process, we found some examples of general lending process, as shown in the following three figures - figure 2, 3, and 4.

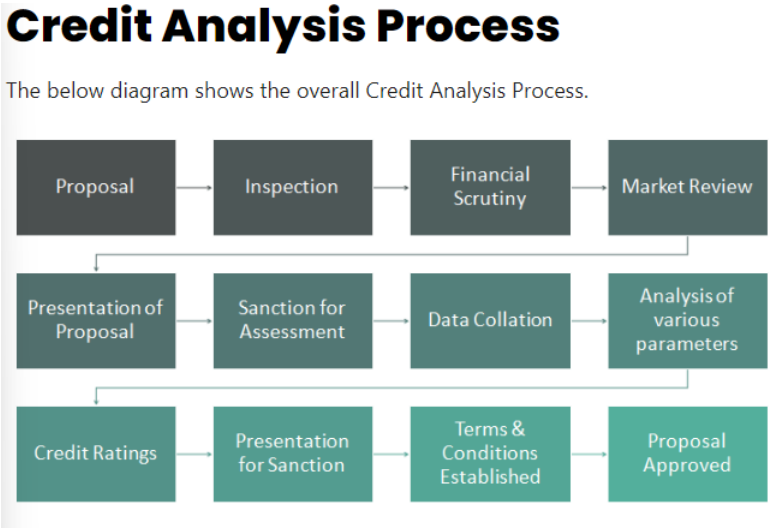

Fig. 2. process example from WallStreet Mojo [21]

Fig. 3. process example from Veripark [22]

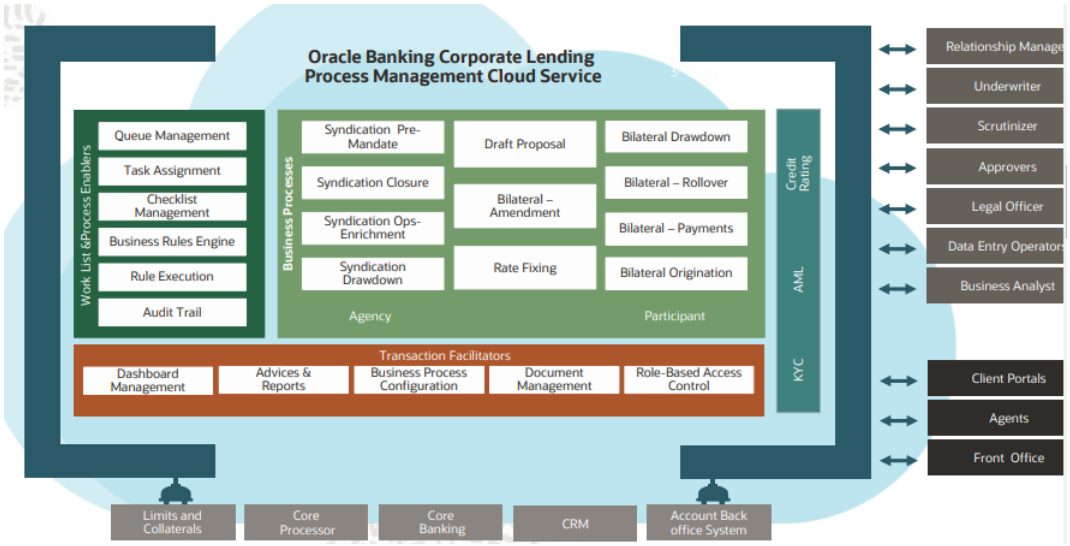

Fig. 4. process example from Oracle [17]

The figure 4 from Oracle shows the processes involved in corporate lending. It gives a structure of what tasks, which systems and which people are concerned. In the proposed solution chapter, we devised a business process diagram for loan application.

B. IT Architecture related to CLO application

ING mentioned that integration between the new FIS suite and other existing IT components poses a major challenge. Because we do not know the internal IT systems of ING, we sought some examples from other sources including Oracle, IBM, and Microsoft. They demonstrated generalized IT architecture. We assume one of the main reasons for the integration problem is that ING has many legacy IT infrastructure and applications, many of which do not have up-to-date standards for integrating with new IT applications.

To solve this issue, Microsoft offers an industry reference architecture. As indicated in the figure 5, in legacy systems, many applications and services are separate. Connecting them all and making them work together could be cumbersome. Any additional IT component being introduced will almost assuredly complicate the IT architecture. The new integrated platform, however, can effectively link all related IT components together and spare time for manual integration.

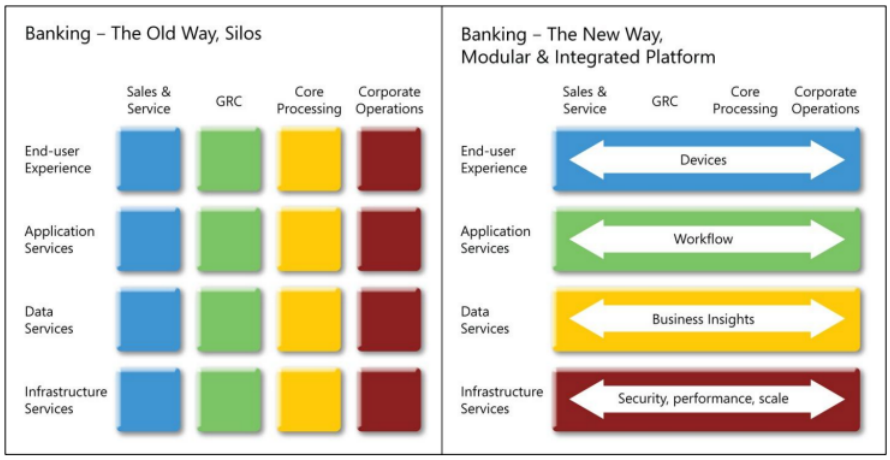

Fig. 5. The Old and New IT architecture [14]

Another advantage of using Microsoft's solution is the fact that there are many Partner Solutions with Microsoft. For example, Finastra's open platform announced last year called FusionFabric.cloud allows partners to develop on top of its core solutions via open APIs [13]. Figure 6 and 7 show this concept.

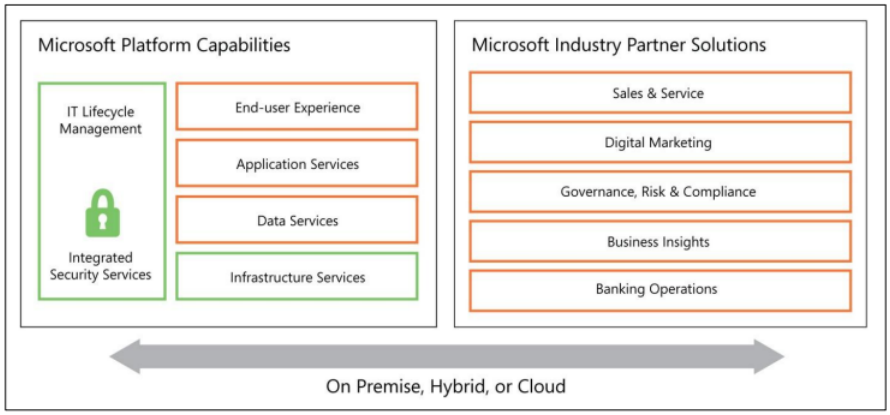

Fig. 6. Platform Capability - simplified [14]

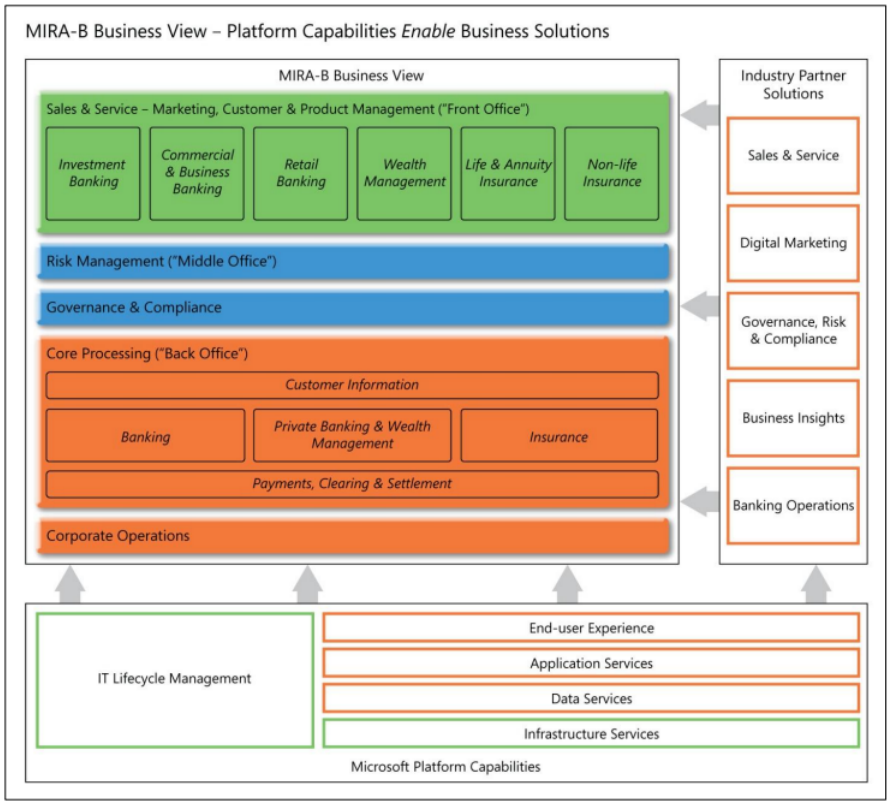

Fig. 7. Platform Capability - detailed [14]

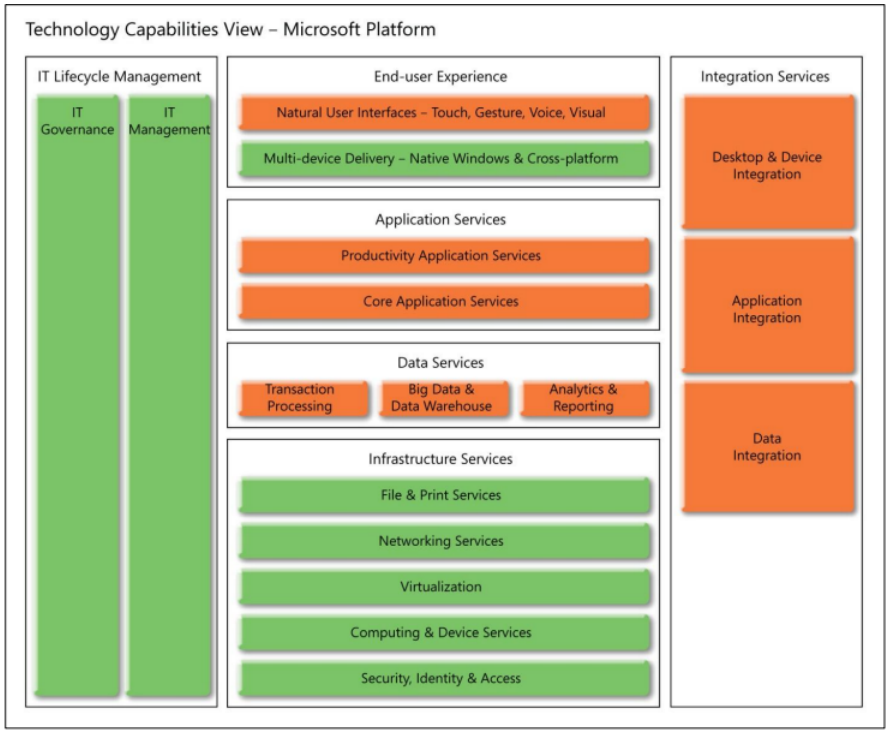

Fig. 8. Platform Capability - segments [14]

To look at the landscape with the technology capabilities view from Microsoft, FIS can be classified into Application

Services. It is linked to other IT components via integration services. Figure 8 illustrates this connection.

To conclude, The example from Microsoft is a useful reference for adapting IT systems for better integration in the future. Consider using software which is highly compatible with major IT service providers such as Microsoft, Oracle, and IBM.

C. Data Retrieval and Analysis

Data of a typical loan application can be classified as quantitative and qualitative data. There is also derived data from both types [7].

According to ING, they collect data from various channels including client portal, emails, documents, and pdfs. There could be dozens if not hundreds of documents to be reviewed for a loan application. So, to effectively extract usable data from them, ING devised their own version of natural language processing capability. Take another bank as example, JP Morgan Chase claims that it was able to extract 150 relevant attributes from 12,000 annual commercial credit agreements in seconds using their NLP software called COIN, although it cannot be verified as it uses COIN internally [3].

Figure 9 shows that NLP plays significant role in information retrieval.

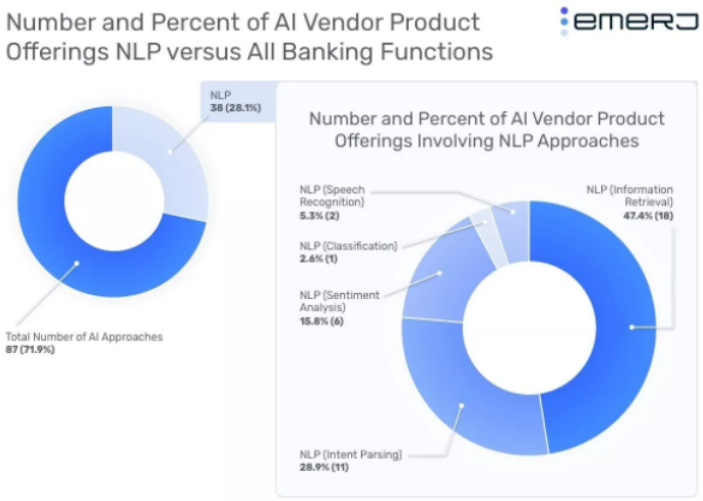

Fig. 9. NLP in information retrieval [3]

For data analysis, artificial intelligence algorithms are used in the field of credit, they are capable of simulating the behavior of a human expert and analyzing the risk of granting a loan to individuals, professionals or companies. The principle is to carry out an analysis of the risk of a request for financing according to business rules that respect the institution's risk policy and the sometimes more subjective rules of credit analysts. The tool gives an instant response, and a level of risk is associated with the credit request (e.g.: The request is favorable, unfavorable, to be examined further). The advantage of this system is that it is quick in its analysis and allows business leaders to make a decision in accordance with the delegated scheme. It has the advantage of accompanying the entrepreneur in his decision or, on the contrary, of providing him with elements enabling him to defend his case in the event of an unfavorable opinion, or to review the financing (increase in the contribution, reduction in financing, etc.), or even to refuse it. The distribution of loans is the core business of almost all banks. Today, many banks / finance companies approve a loan after a regressive verification and validation process. This involves mining the Big Data of past records of people who have applied for a loan.

Here is a scenario of using machine learning on a loan application. The training data set of a loan application is provided to the machine learning software. The software uses an automatic approach based on modeling: very common methods in data analysis are used, such as dimension reduction and clustering, in order to extract predictive variables that are as concise and representative as possible. Afterwards, based on the refined data set, various models can be used for supervised learning. The result of the supervised learning can be qualitative or quantitative. After training the data set, the algorithms optimise itself to fit input parameters into certain outcomes. When applying new data to the model, it then predicts whether the new applicant is a suitable case for loan approval or not based on the inference it makes from the optimisation.

V. Regulation and Security

The financial sector was the target of the most attacks. The banking industry has been targeted for two reasons: physical money theft and computer fraud. Hacking into servers to steal a customer's personally identifiable information (PII) is a type of cyber fraud. Cybersecurity is a technique that protects computers, servers, networks, and digital data in cyberspace from illegal access, damage, or attack. Banks rely on third-party platforms to provide a variety of digital services. As a result, they are reliant on systems over which they have little influence. This has made hackers and criminals more aware of technology vulnerabilities and flaws that could allow them to break into financial networks and steal vital data and dollars. Because of the rapid evolution of technology, cyber threats and attacks are difficult to detect. The following are some of the reasons why cyber security is critical for banks: 1. Loss of Customers When a bank is hit by a cyber assault, it not only hurts the bank's reputation, but it also results in the loss of assets belonging to its customers. When a user loses money due to card fraud, the money can usually be recovered from the bank. However, in situations like data theft, retrieving funds takes time, which is quite concerning for clients. Every bank must implement cyber security procedures to protect its clients' data in order to keep their data safe. 2. Bank Reputation Data breach is a serious problem for banks because it results in the loss of personal information. When a bank's clients' data is compromised, it becomes difficult for customers to trust the bank. The majority of data breaches occur as a result of inadequate cyber security measures. As a result, banks must have cyber security requirements in order to assess current security measures and secure critical data. 3. Digitization Almost everything has now been digitized, as we all know. We rely on multiple digital channels for everything from ordering things to scheduling meetings and sending money. This makes it critical for banks to improve their customer-facing banking activities, as hackers can quickly gain access to banking apps if suitable cyber security measures are not implemented.

A. Regulation and Security

Vulnerabilities

In the ICT section of the risk analysis, the biggest risks are: Insufficient monitoring and action on vulnerabilities,

- Malware,
- Hacking,
- Unsafe behavior of employees,
- Insufficient capacity and training for ICT.

In this list, the last two vulnerabilities are based on human errors. The second one, malware, is seen as a very important risk: indeed, it includes ransomware. Ransomware is the most known example of malware because of its availability to hackers: every hacker can buy ransomware as a service. Ransomware is capable of revealing data. In the case of banks, the data stored is information about the accounts, which is very sensitive.

B. Ransomware Attacks: Principle

Ransomware is a type of malware, which is a program or software that is executed in a system with the intent of causing damage or extracting information with the intent of causing damage to the system. In this case, one malware is installed into the system, which encrypts all data and renders files unreadable. The ransomware's creators then demand a ransom in exchange for decryption. On the one hand, if the ransom is not paid, hackers frequently threaten to sell or release the data or authentication information that has been stolen. The victims, on the other hand, have no guarantee that if they are paid, they will decrypt the files and not sell the information. Furthermore, if the corporation purchased insurance before the attack, it loses it.

C. Ransomware Attacks: Consequences

The bank's data is lost if there are no backups. Furthermore, if they are released, the company's reputation will be harmed. They can also have to pay a fine if they don't follow regulations like GDPR. A good way to understand to what extent ransomware can affect organizations is to present two examples of ransomwares: WannaCry (2017) and Conti (2019).

WannaCry is a ransomware containing worm-like features which allow it to spread across the IT system of the network. The $300 ransom had to be paid in bitcoin. If not paid after three days, it became $600. It affected more than 150 countries and 230 000 computers. The estimated amount of money earned is around $4 billion [11]..

Conti is a Ransomware-As-A-Service which targets big companies in the retail, manufacturing and construction sectors and governments from North America and Europe. The data stolen are published on their website [1]. According to [6] between July 2021 and November 2021 it made at least 130 victims and earned around 7$ millions in bitcoin.

D. Ransomware Attacks: the Attack Tree, or Origin of the Attack

We've decided to create an attack tree to show how a ransomware attack can happen in a bank. It's a type of conceptual graphic that shows how something could be attacked. The root of the problem is data encryption in order to beg for money. This occurs as a result of a ransomware assault. There are three ways for this type of attack to succeed, according to SocRadar [19], Barker [2], Mitre [15], and Challita [4]:

Downloading harmful files from compromised websites, spam, phishing, spear phishing, or guessing a user's password are all examples of social engineering (via social media or call for example).

Vulnerabilities in the IT system: a weakness in the network architecture, such as poor Internet segmentation, might cause this. The bank's website may also be vulnerable, allowing for attacks like SQL injection or XSS breaches. Vulnerabilities in the Remote Desktop Protocol (RDP) and Server Message Block (MB) protocols' configuration and use might also be a concern. Finally, brute force and Man-in-the-Middle assaults can be used to obtain an employee's credentials, allowing the attacker to install the ransomware.

Physical access to the IT system: if physical protection is inadequate, an attacker can break into the bank's building. Employees who aren't aware of the threat can use a malevolent person's hacked USB and portable media.

In order to explain which ransomware attacks and how can occur in the banking sector, an attack tree is created see Figure 10. An Attack tree is a conceptual diagram used to explain how an asset or target (e.g. a person or enterprise) might be attacked. The root of the tree in Figure 2 is the encryption of data in order to ask for money.

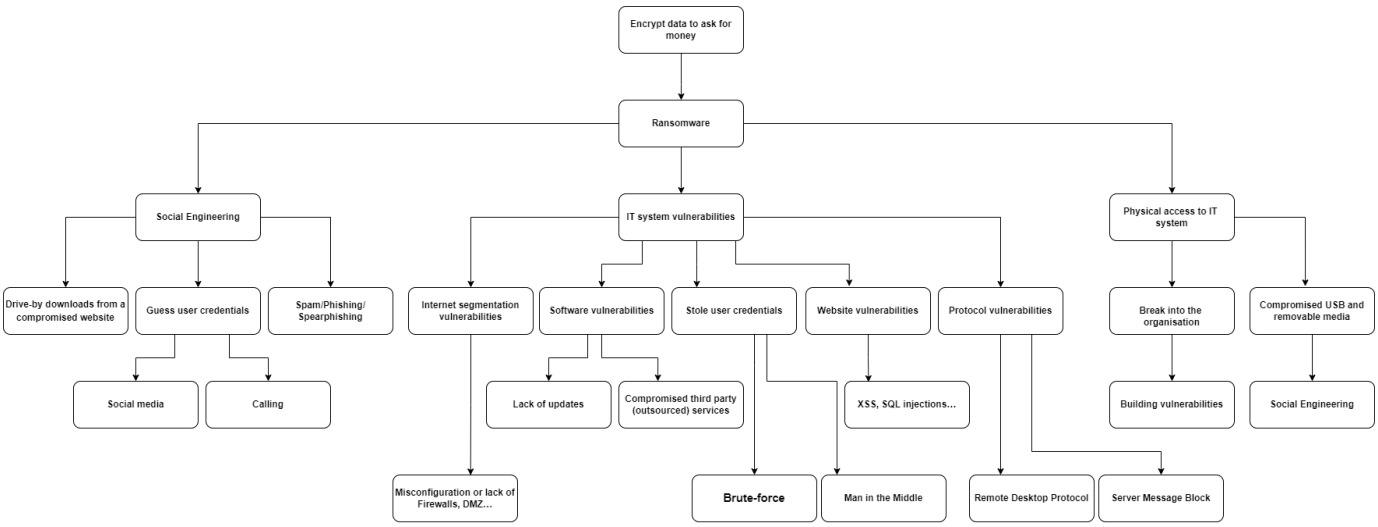

Fig. 10. Attack Tree

E. Cybersecurity Regulations in the Financial Industry

As a result of the increasing number of cyberattacks aimed at the financial industry, various mandatory cybersecurity legislation have been enacted. Regulatory compliance is one of the most successful ways for holding financial services accountable for their security posture, despite the fact that it is typically seen as an unneeded burden on security teams. Each of the following regulations increases customer data security and resilience against data breaches.

F. NIST

The National Institute of Standards and Technology (NIST) recently released the Cybersecurity Framework (CSF), which establishes a standardized framework for best practices in critical infrastructure sectors such as healthcare, government, and financial services. The financial sector has always relied on a certain level of trust between all parties, but now it is heavily reliant on technology, shifting that traditional trust structure between people to a more nebulous trust in the digital realm.

Cybercriminals are primarily interested in the financial sector, notably the rapidly increasing mobile banking sector, as we have already mentioned. The framework (NIST) serves as a de facto standard for enterprises combating cybersecurity risks. It's a framework that's both flexible and repeatable, and it provides a number of approaches for financial services firms to reduce their cyber risk by: Providing a common language: NIST provides a common language for all organizations to describe their current cybersecurity posture, define a target state, and identify where cybersecurity risk management gains and improvements can be made. Providing a consistent roadmap: Once an objective has been established, evaluating progress toward that goal is simple. Enabling communication: NIST can be used to communicate current cybersecurity concerns to internal and external

stakeholders, as well as the efforts being taken to address these risks. Flexibility: One of the framework's greatest assets is its adaptability. Its creators understand that each company's cybersecurity requirements are unique. NIST recognizes the various issues that financial institutions confront and does an excellent job of complementing rather than simply replacing what has already been developed. This reduces downtime and helps businesses to examine their present risk levels and improve them by following NIST's guidelines.

G. GDPR (General Data Protection Regulation)

The General Data Protection Regulation (EU-GDPR) is a security framework created by the European Union to protect citizens' personal data. All businesses that process data about EU citizens, whether manually or through automated procedures, are subject to the GDPR. In order to secure the whole lifetime of user data, the GDPR specifies various security rules for both data processors and data controllers. The following are the most important principles and requirements that regulate the management of personal data: Limited Purpose: Customers' personal data should only be collected for legitimate, explicit, and precise purposes, and should never be used in a way that contradicts these objectives. Legitimacy, Fairness, and Transparency: Personal data should be processed in a legal, fair, and transparent manner. Storage Limitation: Personal data should only be kept for as long as is necessary for the purposes for which it is processed. Accuracy: When storing and managing personal data, it should be accurate and, when applicable, kept up to date. Integrity and Confidentiality: Personal data should be handled in a secure manner, including protection from unauthorized or unlawful processing, as well as accidental loss, destruction, or damage. Data Minimization: Personal data collection should be kept to a minimum, and data collected must be relevant to achieving a specific aim.

H. ISO/IEC 27001

Another standard for reducing security risks and preserving information systems is ISO/IEC 27001. ISO/IEC 27001 is an internationally recognized set of security policies and processes that give companies in any industry guidance on how to improve their security posture. Given its reputation as an internationally recognized benchmark for cyber attack resilience, financial institutions that want to demonstrate their exceptional cybersecurity procedures to stakeholders should pursue ISO/IEC 27001 accreditation. Another significant advantage of following this approach is that, when combined with an Information Security Management System, it can help your company comply with GDPR (ISMS).

I. Preventing Human Errors

Human errors can be thought of as lack of action by employees or users while engaging in software systems thereby causing security breaches. These breaches can be as simple as failing to use a strong and encrypted password to something as damaging as downloading a malware-infected attachment to the software systems. Data breaches at the banking sector can be crippling in terms of the costs that are incurred there-after, restructuring the intellectual property and realigning regulatory requirements.

According to the IBM Security Intelligence Index, human error is involved in more than 90% of security incidents (clicking on a phishing link, visiting a suspicious website, activating viruses or other advanced persistent threats). It is therefore important to bear in mind that attacks in the technical or cryptographic sector can be patched by better secure protocols. But the human factor will always remain a source of problems, difficult to prevent. More and more attackers are now turning to social engineering, which is a practice of psychological manipulation for the purpose of swindling. The most common human errors that are threatening to the data at any organization are listed below:

1) Ineffective means of handling sensitive data: Human errors often stem from slips and lapses that occur while doing routine tasks and activities. More often than not, these errors occur when the users handle large amounts of sensitive data that lead to data compromises and leaks out of carelessness. Some of the most common careless mistakes made by users include sending sensitive data via email to the wrong recipient, accidentally deleting important files, sharing confidential data to peers and colleagues via insecure applications, forgetting to backup critical data, etc.

Negligence among users can also lead to delaying software updates, disabling security features and using unauthorized systems. It is but natural for users who have no prior knowledge on the importance of following security protocols at workplaces to unintentionally compromise sensitive information.

Dismissing software updates can lead to ransomware attacks that affect systems running older versions of certain operating systems or applications. Unintentionally disabling security features at work could also put the organization's data at risk. This could be something along the lines of pressing pause on the antivirus feature update or browser security. Users can also download software applications that are unauthorized or don't conform to the software requirements of the organization giving leeway to malicious and ransomware attacks.

2) Not having enough knowledge on security standards: Employees and users lacking the basic knowledge on the importance of security protocols and cybersecurity measures can disclose sensitive information unintentionally. This gives way to bigger threats at the workplace like phishing emails and ransomware attacks on software systems. Phishing emails are convincing enough to make users on the other side of the screen give up their credentials and click on links that redirect them to some malicious content.

3) Weak password policy and credentials: When employees and users fail to follow a password management policy for access to sensitive data, they give leeway to hackers and malicious users to access accounts by performing brute-force attacks. These human errors can be as simple as storing passwords in plain text, using the same passwords for multiple accounts, using unsafe password managers that have weak encryption protocols.

J. Measures that can be taken to prevent human errors at the baking sector

The management at the banking sector should take it upon themselves to educate employees on the criticality of security protocols at workplaces to avoid human errors. This should stem from the management level where investing in good security practices should not be seen as an IT problem but an organization problem that is resolved cross-functionally across all departments. There needs to be a plan in place that can handhold employees and users to adhere to good security practices that can prevent human errors from happening. More often than not, users and employees are in the dark about taking the right course of action when handling sensitive information.

1) Formal Security Awareness and Training Program: Introducing an educational approach to train employees at the workplace on the risk of phishing emails, software system cyberattacks and malware behaviors is imperative to make everyone understand the importance of following well-structured IT policies and best practices. By doing this, banks can protect their reputation, reduce unnecessary incur of costs as part of cybersecurity issues and secure their IT infrastructure and data. This can be done by implementing a robust security awareness and training program that educates employees on cybersecurity best practices, information security, compliance and regulatory requirements.

2) Stronger Password Management Policy: Establishing and incorporating a secure password manager application allows employees and users using the software systems to create and save passwords without having to remember them every time or run the risk of writing them down on sticky notes and leaving them unattended on the desks. If users currently have a Two-Factor Authentication in place, they can go the extra mile and mandate the usage of a Dynamic Password Controller to strengthen secure access to accounts and confidential information. This is a viable solution to combat a weak password policy at the banking sector as it acts as a centralized vault to store all passwords in fully encrypted forms. It also provides visibility of the users and employees who access the systems thereby enabling authorized access to software systems and applications.

3) Privilege control and access management: By exerting control over the access and permissions granted to users, the management can ensure that employees only have access to data that is required for them to perform their daily functions. One way to do this is by establishing separate account access for administrative and other user accounts. This limits the exposure of information on a high-level and reduces the risk of attacks caused due to human errors and negligence.

K. Project Management methodology

The world around us is changing rapidly and computer technology is driving these changes. Loan applicants have an increasing number of options to contact those they do business with, which must be accessible 24/7 and provide a relevant, quality service. For ING, agility is intended to be the core of management methods. Agility is about flexibility and the ability of an organization to adapt quickly and move in a new direction. It is about minimizing handovers and bureaucracy, and empowering people. The aim is to create stronger and more complete professionals. Being agile is not just about changing the IT department or any other function in itself. The key is to work in multi-disciplinary teams, or squads, with a mix of marketers, product and sales specialists, user experience designers, data analysts and IT engineers. These are important sources of inspiration for developing a new way of working together and a new level of service to customers. This way of working requires a faster response to changing customer needs. This essentially means less handover between departments, fewer meetings and coordination, more space for initiative and higher levels of responsibility for both teams and individuals.

Based on information from ING, the fundamental unit in the organization is called the Squad, which are autonomous and self-regulating teams of up to 9 people fully responsible for their own specific client-related tasks. A Squad is structured around different disciplines and areas of expertise or background - such as colleagues specializing in marketing, management or IT - and there may be more of them in one area or another depending on the nature of the Squad's mission. Within each squad there is a product owner who is responsible for what the squad does, he or she is in charge of the backlog, making the list of tasks to be executed and determining priorities.

To ensure coordination between the squads, a tribe intervenes. This is a group of squads with interconnected tasks. Typically a tribe has less than 150 coordinated people who ensure that expertise and vision are shared, set priorities and allocate available budgets.

However, as this is not an approach that is suitable for all ING functions, therefore a certain amount of trial and error will help to determine what in practice works and what does not. The agile approach is not in itself permanently fixed. This is what makes it a useful tool for achieving ING's objectives.

Fig. 11. ING organization

VI. Proposed Solutions

A. *Methods for improving data quality*

Data collection, cleaning, validation, and feature engineering are vital steps for ensuring the quality of data that will eventually be fed into decision making algorithm. The two figures, figure 12 and figure 13 , in this section show the high-level view of the practise on improving data quality. Following the practise is the basic requirement. There are other ways to improve data quality.

For ING, the first solution to improving data quality would be to ask the client to systematically check the data he sends. However, this is a tedious task for the client, and will not prevent errors such as deliberate error.

The second, more realistic solution to this problem would be, knowing that a certain percentage of the data will inevitably

TABLE I
AUTOMATED DATA CLEANING

Type of data	Methods
Possible duplicates	Clustering
Standardised data such as ZIP code	Intelligent Suggesting, for example, deep learning.
Outliers	Profiling data by using dictionaries, statistical comparison, etc.

be corrupted, to manage to spot these corruptions. Some types of errors such as wrong ZIP code, data that is above or below three standard deviations from its mean can be detected using simple algorithms during data cleaning process. The table, table I, summarising some methods for automate data cleaning [23].

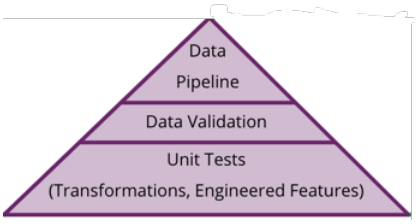

Fig. 12. Data Quality Control [5]

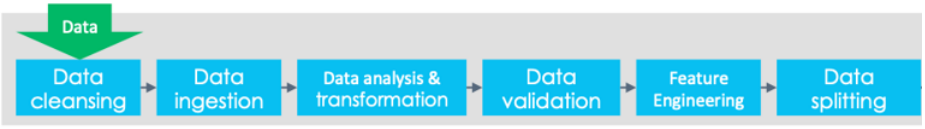

Fig. 13. Data Quality Control Process [10]

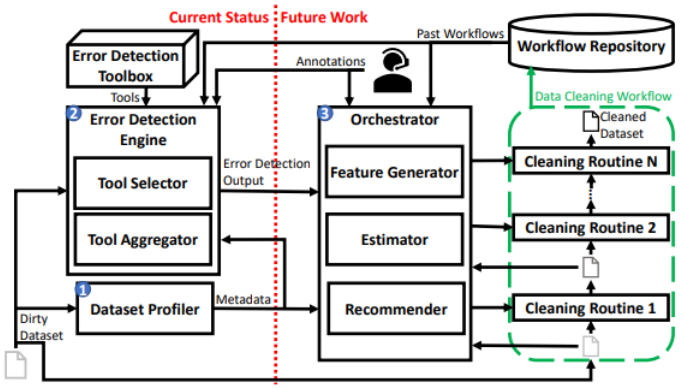

Fig. 14. Automated Data Cleaning Workflow [12]

To automate data cleaning through a workflow [12], figure 14 shows the high-level architecture of such mechanism. It could be useful for ING to look into this workflow, borrow the ideas, and try to test it on its own data cleaning workflow.

B. Project management method (Scrum)

The second aspect to improve the project is to implement some specific framework related to IT management. ING is currently using squads and tribes to manage their working team. However, from the IT management perspective, there are no specific framework to control the software development process. In this long-term project, there are still a lot of uncertainties. That is why the agile methodology is suitable. Agile governance is defined as "the 'means' by which strategic competitive advantages ought to be achieved and improved on the organizational environment, under an agile approach in order to deliver faster, better, and cheaper value to the business." (Luna et al., 2014)

Scrum is a framework for managing software development projects. It was developed by Ken Schwaber and Jeff Sutherland in the mid-1990s, but has since been widely adopted in organizations of all sizes. The Scrum framework consists of five roles: product owner, scrum master, team members (also called "scrum members"), development tasks (also called "work items") and iterations. The product owner works with stakeholders to define what they want from the project; this includes identifying business value, user stories and acceptance criteria. Once these have been defined, work can begin on creating an implementation.

There are several strengths of Scrum. First of all, Scrum's adaptable nature allows it to quickly adapt or merge new information, resulting in improved performance. ING has to keep looking for new information that can help the loan decision-making process. Second, The sprint retrospective phase in Scrum can be used to assess all iterative deliverables. Third, The individual effort of each team member is visible during daily scrum meetings. All of the above can be a benefit for ING. However, Scrum often leads to scope creep, due to the lack of a definite end-date. Also, the chances of project failure are high if individuals aren't very committed or cooperative. Moreover, adopting the Scrum framework in large teams is challenging and the framework can be successful only with experienced team members. ING needs to take into account of these factors.

In figure 15, we illustrate some activities within the scrum management process.

Daily Stand-up: Check progress and feedback from users and developers. Make adjustment to plans accordingly.

Continuous Integration: From data collection to decision making, break up the system/process into small parts and make them work one by one.

Continuous Testing: Implement the integration in the testing environment; perform unit testing, automated and manual testing; make sure each unit works as it should, and also the entire business process should work without error.

Continuous Delivery: Realise the changes from Continuous Testing phase into a prototype environment. The users will be using this environment to test out the loan application process.

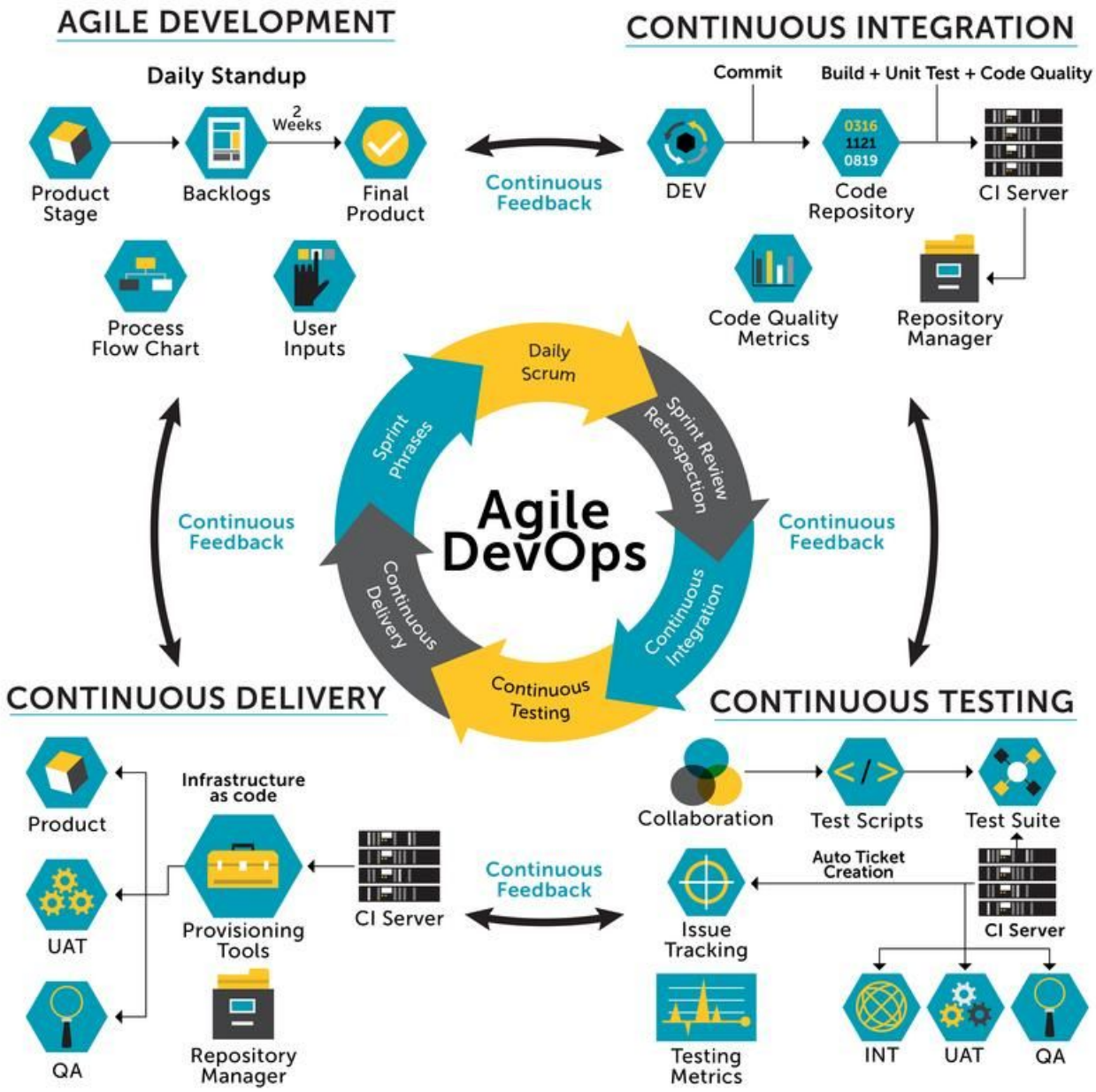

Fig. 15. CI/CD with Scrum

C. Credit Analysis Process

We created our business process model to show the basics of how the whole process for lending and credit analysis works [9].The big companies mostly have the people who takes care of the whole loan process but the ING can have an internal method to work on the application process.The loan application is intiated with checking the application and later transfering it to the further departments if the application satisfies all the data required and processing requirements.Furthermore the data is stored in the data storage which is collected, cleaned and anaylzed for further processing of the application.If the application is complete the credit history of a company is checked and the assessed credit risk should be taken into consideration while providing a loan. Also a collateral is considered one of the biggest part of the risk assessment which in the model it is stated as appraise property.Furthermore every analysis that takes place is considered for the eligibility of a company for the loan lending and the loan is approved.

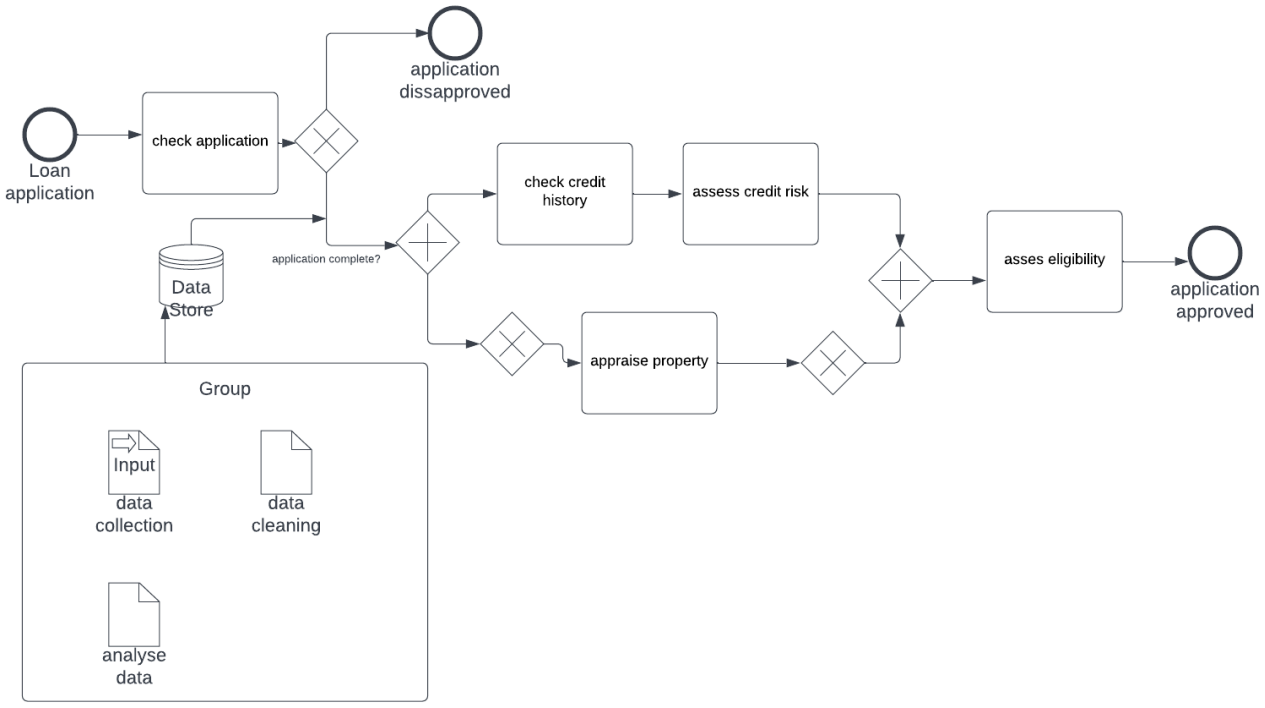

Fig. 16. Loan process

Credit evaluation is the identity of dangers in conditions wherein a capacity for lending is discovered through the Banks. Both quantitative and qualitative evaluation paperwork part of the general appraisal of the clients (company/individual). This, in general, enables to decide the entity's debt-servicing potential or its capacity to repay [8]. Ever questioned why bankers ask such a lot of questions and make you fill such a lot of paperwork whilst you observe for a loan. Don't a number of them sense intrusive and repetitive, and the entire procedure of submission of diverse files appears cumbersome. You simply attempt to fathom as to what they do with all this information and what they're really seeking to ascertain! It is without a doubt now no longer best your lethal attraction and appealing persona that makes you a great capacity borrower; obviously, there may be extra to that story. For this we have the 5 'c of the credit analysis [9]. Those are as Conditions, collateral, capital, capacity, character.

1) Character: This is the element wherein the overall impact of the protecting borrower is analyzed. The lender bureaucracy a completely subjective opinion approximately the trustworthiness of the entity to pay off the loan. Discrete inquiries, background, revel in level, marketplace opinion, and diverse different reassets may be a manner to accumulate qualitative information, after which an opinion may be formed, wherein he could make a choice approximately the individual of the entity.

2) Capital: Capital refers back to the cap potential of the borrower to carrier the mortgage from the income generated through his investments. This is possibly the maximum critical of the 5 factors. The lender will calculate precisely how the compensation is meant to take place, coins glide from the business, the timing of compensation, possibility of a hit compensation of the mortgage, fee history, and such factors, are taken into consideration to reach on the in all likelihood capability of the entity to pay off the mortgage.

3) Capacity: Capacity is seen as the borrowers worth to borrow and repay the money. This can be one of the aspect which is based on the capital as well.

4) Collateral: Collateral can be a mean of security where the borrower keeps something as a form of security to the lender so if in case the borrower is not able to repay the amount of the borrowed money, the lender has the right to seize the collateral that the borrower has given to the lender.Here the guarantees are the documents promising of the loan.In most cases the guarantees are the family members, friends or the person belonging in the same business if it is commercial. Sometimes collateral security is also used to offset some unpleasant factor that may have come to the front during the assessment process of the loan.

5) Conditions: This describes the purpose of the loan as well as the terms and conditions for the sanction of the loan. Purposes can be working environment, lending to the company, inventory.

TABLE II
FEATURES OF LOAN APPLICATION

Category	Feature	Qualitative/Quantitative
Companyś history	Market Data	Quantitative and Qualitative
	Financial Information	Quantitative
Judgment	Company Rating	Quantitative and Qualitative
	Credit History	Quantitative
	Analysis of market	Quantitative and Qualitative
Ratio	Liquidity Ratios	Quantitative
	Solvency ratios	Quantitative
	Profitability ratios	Quantitative
	Efficiency ratios	Quantitative
	Cash flow and projected cash flow	Quantitative
	Collateral analysis	Quantitative

In banking, it is important that the decision making is based on explainable inputs. Therefore, it is worthwhile to devise simpler models, put in the data ,and test them out using historical data. Use regression analysis to see whether the simplified versions are as good as the complex version. With hundreds of data points, it is a good practice to divide data points into sections; each section gives a score, and combining the score would yield a final score that can be used for decision making.

Here is another simplified version of data points for loan assessment [21] as shown in table II. ING can reduce number of data points by using trimmed versions like this and compare the performance among different versions.

VII. Conclusions

In this paper, we obtained and analysed the information about the ongoing CLO change project in ING. We have identified some problems they are facing, and proposed some solutions to parts of the project. Firstly, we found that that an up-to-date IT architecture is paramount for doing an IT change project, and choosing software that is highly compatible with major providers such as Microsoft and Oracle is recommended. Secondly, we outlined regulation and security requirements that need to be conformed during the project. Thirdly, we proposed solutions for improving data quality, project management, and loan application process. The goal of this paper is to inform our findings and some of our proposed solutions may provide insight for ING as to where and how to improve the FIS project as well as the loan application process.

VIII. APPENDIX

A. Interview Summary

Date: 18-03-2022 1:45 PM-2:30 PM Name: Marcel van Hal (ING Wholesale Banking Tech - IT Manager) Participants in the group: Jia-Yu Li, Yi-Fang Tsai, Léo Sajas

Q1: Is there any IT change case in the company? A1: There are many kinds of changes. For example, change in the software, change in the platform. Also, there are some commercial packages that are highly configurable, so we can change the config settings.

Q2: What's the current method to manage the changes you mentioned? A2: We try to make this in a engineering way, and reduce manual work. In order to standardize the process, we push the changes through CI/CD pipeline and test them automatically. Finally put them into production.

Q3: Could you share a project that you're currently working on? A3: The project is called "CLO", which stands for Credit Loan Offering. This project started a year ago. It's a highly configurable software, so we need to make a shift to run on our platform.

Q4: Will this software run on a website or on an APP? A4: It will run in our ING process cloud. It's the base of all our new softwares and then it's made available to our front office.

Q5: Who is the user of the this software? A5: The front office is the people who are serving our customers. They are account managers so they will closing the deals to our customers.

Q6: Who is the exact customers? A6: Large corporates such as Shell and Heineken. However, there are still some smaller companies that we are serving.

Q7: What is the benefits of this new package? A7: We have two slogans to build our business cases. Time to yes and Time to cash. Time to yes is when we come to an agreement with the customers and Time to cash is we provide the money. For complex deals, they can easily take a few weeks. Also, there might exist some contracts that are impacted by the Europe current situation. We want to know what our customer's expectations are. What we're trying to do is to make more information available for the front office and accelerate the process. Also, we want to apply some machine learning, so the decision-making process time might be reduced to a few days or even hours.

Q8: What is the current software you use now? A8: For the front office, we don't use that much software. It's primarily Microsoft Office such as Excel and Words. Once the deal is closed, it moves to the back office, and they key the information into the interface of loan IQ to assess it.

Q9: How much time could you save for using this software? What is your expectation? A9: Thousands of hours for the front and back office per year. It's equivalent to ten to twenty full-time employees. This software can also improve the user experience because they don't need to type as much data as before.

Q10: What could go wrong in the deals? A10: Some normal banking risks such as counterparty risk. It's all included in pricing. The riskier the deal, the higher their interest is. From an IT perspective, the mistake of the data could go wrong but we don't assess it properly. 5% of the data could be incorrect, and this will influence the risk calculation.

Q11: Is there any budget limit to this project? A11: No, it's based on the tribe and it's a long term project. We don't have the fixed goal and the fixed timeline for this. The budget is flexible.

Q12: Can you talk about the integration between the software and the internal or the external systems? A12: We use the Dutchpoint architecture and it's an API framework. This regulates how our internal application should interconnect with each other. PSD2 is also a nice example. For the external communication, it really depends. It could be an PDF file in an mail. We also build a lending portal to get the data form customers directly.

Q13: What data is getting by the CLO? A13: The past loan application and trade. The data format could be everything. The email sent by the customers or the data form lending portal are all possible. We also apply NLP (Natural Language Processing) to deal with the unformatted data. However, part of the data still need to be processed manually.

Q14: Have you tested the NLP system before? A14: Yes, it's already run for a few years and it's getting better and better. We also try to combine machine learning. Once the data is extracted from the document, we have some self-learning algorithms to apply to it. The engineers in the ING design and develop the algorithms.

B. Reflection

During the process of this project, we have faced several challenges. For example, information collection is hard for student groups like us. During the interview with the ING IT manager, we can't go deep into their processing details since there are some confidential concerns. This results in the fact that we couldn't narrow our research question to a more specific issue. We can only try to see what we can do from a comprehensive point of view. Nonetheless, by doing this kind of project practically, students get more chances to connect theoretical knowledge with the practical process. Also, depending on the corporate they chose, students can explore their horizons to different industries and get some domain knowledge.

REFERENCES

[1]
[2] William C. Barker, Karen Scarfone, William Fisher, and Murugiah Souppaya. Cybersecurity framework profile for ransomware risk management. Technical report.
[3] Raghav Bharadwaj. Natural language processing in banking – current applications. October 2019. https://emerj.com/ai-sector-overviews/natural-language-processing-banking-current-applications/.
[4] Antonio Challita. The four most popular methods hackers use to spread ransomware.
[5] Christoph Windheuser Danilo Sato, Arif Wider. Continuous delivery for machine learning. September 2019. https://martinfowler.com/articles/cd4ml.html.
[6] Elliptic. Conti ransomware nets at least $25.5 million in four months.
[7] Jerry Grimlund Ferguson. Guide to corporate loan evaluation for commercial banks. 1970. https://scholarworks.umt.edu/cgi/viewcontent.cgi?article=5879context=etd.
[8] family=Vaidya given i=D.C., given=Dheeraj Cfa. Credit analysis.
[9] family=Bouteille given i=S., given=Sylvain and family=Coogan-Pushner given i=D., given=Diane. *The Handbook of Credit Risk Management: Originating, Assessing, and Managing Credit Exposures (Wiley Finance)*. Wiley, 2 edition.
[10] Ian Hellström. A tour of end-to-end machine learning platforms. July 2020. https://www.kdnuggets.com/2020/07/tour-end-to-end-machine-learning-platforms.html.
[11] Kaspersky. What is wannacry ransomware?
[12] Mohammad Mahdavi, Felix Neutatz, Larysa Visengeriyeva, and Ziawasch Abedjan. Towards automated data cleaning workflows. 09 2019. https://www.researchgate.net/publication/335136628$_{T}owards_{A}utomated_{D}ata_{C}leaning_{W}orkflows$.
[13] Microsoft. Microsoft for financial services: Empowering intelligent banking. https://blogs.partner.microsoft.com/mpn/financial-services-how-customer-challenges-spur-partner-opportunity/.
[14] Microsoft. Microsoft industry reference architecture for banking (mira-b). 2012. https://news.microsoft.com/download/presskits/msfinancial/docs/MIRAB.pdf.
[15] Mitre. Input capture: Web portal capture.
[16] Oracle. Digital roadmap: Accelerate the digitization of corporate banking. November 2020. https://www.oracle.com/a/ocom/docs/industries/financial-services/accelerate-corp-banking-ebook.pdf.
[17] Oracle. Corporate lending process management in the cloud. 2021. https://www.oracle.com/a/ocom/docs/industries/financial-services/corporate-lending-process-management-cloud-br.pdf.
[18] Savvides Savvakis. Corporate lending and the assessment of credit risk. March 2011. https://papers.ssrn.com/sol3/papers.cfm?abstract$_{i}d = 1813013$.
[19] SOCRadar. Top five causes of ransomware attacks.
[20] Reghunathan Sukumara. Corporate credit appraisals and decision making. March 2018. https://www.finextra.com/blogposting/15169/corporate-credit-appraisals-and-decision-making.
[21] Dheeraj Vaidya. Credit analysis. https://www.wallstreetmojo.com/credit-analysis/.
[22] Veripark. Corporate loan origination. https://www.veripark.com/products/veriloan/corporate-loan-origination.
[23] Zara Ziad. Using machine learning to automate data cleansing. March 2021. https://dzone.com/articles/using-machine-learning-to-automate-data-cleansing.