Risk Assessment of Core Banking System Replacement based on ISACA Framework

Fenty Simanjuntak
Master of Information Technology, Swiss German University, Edu Town BSD City, Tangerang 15339, Indonesia
Email: Fenty_sim@yahoo.com

Bobby Suryajaya
Master of Information Technology, Swiss German University, Edu Town BSD City, Tangerang 15339, Indonesia
Email: bobby.suryajaya@gmail.com

Abstract

Many banks are looking for a better core banking system to support their business growth with a more efficient and flexible core banking system to improve their sales and services in the competitive market and to fulfill regulatory requirements. The decision of replacing the legacy core banking system is difficult due to the high IT investment cost required for banks because they are also trying to cut costs. But maintaining the legacy system is costly in terms of upgrade. Changing the core banking system is also a difficult process and increases risks. To have a successful Core Banking System implementation, risk assessment is required to be performed prior to starting any activities. The assessment can help project teams to identify the risks and then to mitigate the risks as part of the plan. In this research the Core Banking System replacement risks were assessed based on ISACA Framework for IT Risk. Fourteen risk scenarios related to Core Banking System Replacement were identified. The high and medium rated inherent risks can become medium and low residual risk after assessment by putting the relevant control in place. The result proves that by adding mitigation plan it will help to mitigate the Residual Risk to become low risk. There are still three residual risk which categorized as medium risk and should be further mitigated they are Software Implementation, Project Delivery and Selection/Performance of Third Party Suppliers. It is also found that COBIT 5 has considered some specific process capabilities that can be used to improve the processes to mitigate the medium risks.
Keywords: IT Risk; ISACA; COBIT; Residual Risk; Inherent Risk; Core Banking System

Introduction

A core banking system is the back-end data processing application for processing all transactions that have occurred during the day and posting updated data on account balances to the mainframe. Core systems typically include deposit account and CD account processing, loan and credit processing, interfaces to the general ledger and reporting tools [1].

Changing the core banking system is a difficult process and increases risk. To have a successful implementation, risk assessment is required to be conducted before selecting and implementing the new core banking system.

The Banking Systems Market Survey results for 2012/13 indicated the following IT trends in the banking industry [2]:

- Of the respondents, 34% intend to replace their platforms; of these, 74% intend to move to packages.
- The pressure on bank IT budgets over the past five and two years is notable.
- There is considerable activity within “satellite” systems, such as payments and channels.
- Banks are placing high importance on data warehousing and business intelligence technology.
- Social media is not making a great impact on most banks as yet (other than in Southeast Asia).

Risk management can have a positive impact on selecting projects, determining the scope of project, and developing realistic schedules and cost estimates [3].

The benefit of Core Banking System replacement will help the bank achieve its business growth plan and contribute to superior sales and services to customers [4]. They are:

1. Resolving the current system constraints such as:
   - Operational instability that impacts not just branches and customers, but also the growing importance of electronic channels in Internet and mobile banking.
   - Inability to support business growth: number of customers/CIFs, number of products per customer, and transaction volumes.
• Inability to support evolving products and services required for business growth.

2. Resolving regulatory pain points related to manual processes and lack of automated controls that lead to high operational risk, reconcilement issues with the enterprise GL, and regulatory reporting process.

3. Increasing the level of customer service by providing a sales and service platform that will enable bank’s customer-facing staff to improve customer experience and increased ability to develop Cross Products.

4. Improving electronic channel capability to meet the needs of the targeted customer segment.

5. Changing the business processes to be more productive and effective by automating manual processes and controls, improving the operational risk, providing opportunities for staff to perform more value-added activities and improving customer service.

**Research Framework**

In this paper, ISACA framework is used to do the risk assessment and COBIT5 is used to improve the process capability. ISACA framework is used because it provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues. The framework can be used to understand and manage all significant IT risk types, building upon the existing risk related components within the other ISACA frameworks, i.e., COBIT and Val IT [5].

COBIT 5 provides the next generation of ISACA’s guidance on the enterprise governance and management of IT. It builds on more than 15 years of practical usage and application of COBIT by many enterprises and users from business, IT, risk, security, and assurance community.

Other frameworks that were also considered to be used in this paper beside ISACA-COBIT were ITIL, COSO, ISO 31000:2009, ISO 27005:2008, etc. However, those frameworks may not be able to provide an end-to-end, comprehensive view of all risks related to Core Banking System replacement.

**Research Methodology**

This research consists of several stages, beginning with defining the research questions, and whether the risk assessment based on ISACA Framework can be used to identify risks and identify controls to reduce the risks.
Next, risk assessment was conducted based on The Risk IT Practitioner Guide [4] as shown in figure 2 and secondary data (project documentation) from Bank X.

Using ISACA Framework for IT Risk, the processes to identify risk are as follows:

- IT Risk Scenarios development
- Estimate Frequency and Impact
- Risk Response
- Risk Action Plan

ISACA in the IT Risk IT Practitioner Guide [5] provided the 36 (thirty six) IT Risk Scenarios (page 59). The risk scenarios relevant to the Core Banking System Replacement project were identified. Then the frequency and impact of each risk were calculated.

Frequency or Likelihood is number of times in a given period usually in a year that an event is likely to occur. Impact is the business consequence of the scenario. The frequency and impact and risk rating will be assessed using established operational risk guidelines of the bank.

For example, for the Major impact and Possible likelihood, the risk rating is High. Before putting control in place, the inherent risk was determined. After putting the control in place for the current situation, the residual risk became known.

For the residual risk that was identified, the risk response needed to be defined. Risk response will be in line with the risk appetite and tolerance of the bank. There are four types of risk response:

- Risk acceptance
- Risk sharing/transfer
- Risk mitigation
- Risk avoidance
Risk acceptance means the risk is recognized and loss is accepted but no action will be taken. Usually the risk is low with insignificant impact.

Risk sharing/transfer is reducing risk by transferring the risk to another party, such as insurance or outsourcing.

Risk mitigation is mitigation action needed to reduce the risk. Usually an action plan is needed for mitigating risk such as putting other control processes to reduce either the frequency of events and/or the business impact as defined by ISACA framework or strengthening the process capability as considered by COBIT5 [6].

Risk avoidance is to avoid risk by applying other activities or conditions when no other response is adequate.

Next, Subject Matter Expert of Bank X reviewed the risk assessment through interview and discussion. The results are summarized in the conclusion.

**Results & Analysis**

The first step was to identify the risk scenarios related to Core Banking System (CBS) replacement out of fourteen scenarios. From the fourteen scenarios, the likelihood and impact were determined. For example, High Level Risk Scenario is IT project economics risk. The negative example scenarios given are:

- Isolated project budget overrun
- Inconsistent and important IT projects budget overruns
- Absence of view on portfolio and project economics.

In terms of CBS replacement, this scenario is relevant. By choosing the CBS replacement as one of the IT programme, there may be risk associated with it. The impact
will be major, because it will impact Financial Loss and the inherent risk is High, using Bank X Operational Risk 5 by 5 Matrix [7].

Controls currently in place at the bank were identified, which reduced the likelihood and impact. It was found that there some essential controls are in place according to Bank X Operational Risk Report [8], such as:

- The bank has implemented a cost management process comparing actual costs to budgets. Costs are monitored and reported to the Steering Committee, which is composed of the President Director and member of the Board of Directors.
- The Steering Committee monitors and controls project execution, including project budget usage
  - There are also two working groups under the Steering Committee, which are the Executive Working Committee and the Executive Project Delivery Committee
  - Both committees will control project execution from an implementation and business requirement fulfillment perspective.
- Core Banking Software (CBS) project is one of the agenda for Board of Commissioner meeting to seek guidance from the commissioner member.
- There is a dedicated Financial Controller who strictly monitors the project budget and expenses. The Project Manager periodically reviews the project budget and expenses to avoid any unnecessary expenses.
- Minimum customization approach for CBS is to avoid additional implementation cost and reduce project delivery risk. Every customization needs to be approved by the Steering Committee.
- An external party as QA does a periodic review of internal project processes, including project expenses.
- Every unexpected expense that uses a contingency budget has to go through the approval process from the Steering Committee and other project governance bodies.
- Bank X periodically reviews of contingency budget to release part of contingency budget along with project execution where more detail information is gathered for more detailed project planning. Periodic review is held at the end of each phase.

Due to the high impact controls in place, the risk becomes minor therefore it is unlikely to happen. Therefore, the residual risk becomes low.

After assessing all the risks of Core Banking System replacement, the result is described in the Risk Heat Map figure below:

- 11-risks are inherently rated as High Risk
- 3-risks are inherently rated as Medium Risk
Fig 3. Inherent Risk of Core Banking System Replacement Heat Map

Risk is rated based on color from light to dark as Insignificant, Low, Medium, High, and Very High.

Fig 4. Residual Risk of Core Banking System Replacement Heat Map
After assessing the Control in Place for the High & Medium Risks, the Residual Risk becomes Medium & Low.

- 11-risks are rated as Low Risk
- 3-risks are rated as Medium Risk

Using COBIT 5, the Medium Residual Risk will be mitigated by adding some action plans. For example, to reduce the project delivery risk, the project team plans to monitor the performance of the overall project including the contributions of the business and IT functions of the project and report to the project steering committee in a timely, complete and accurate manner. Escalation to management team is needed for any deviation of the plan. This action is essential control and has High effect on Impact. The risk becomes low due to reduced impact to minor even though the likelihood is still possible.

The table below summarizes all the risks identified, the impact, the likelihood and the Residual Risk after analysis.

Table 1. Summary Residual Risk of Core Banking System Replacement

<table>
<thead>
<tr>
<th>No</th>
<th>Risks</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IT Programme selection</td>
<td>Minor</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>New Technologies</td>
<td>Minor</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Technology Selection</td>
<td>Minor</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>4</td>
<td>IT Investment decision making</td>
<td>Minor</td>
<td>Possible</td>
<td>Low</td>
</tr>
<tr>
<td>5</td>
<td>IT project termination</td>
<td>Minor</td>
<td>Possible</td>
<td>Low</td>
</tr>
<tr>
<td>6</td>
<td>IT project economics</td>
<td>Minor</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>7</td>
<td>Architecture agility and flexibility</td>
<td>Minor</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>8</td>
<td>Software implementation</td>
<td>Moderate</td>
<td>Unlikely</td>
<td>Medium</td>
</tr>
<tr>
<td>9</td>
<td>Project delivery</td>
<td>Moderate</td>
<td>Possible</td>
<td>Medium</td>
</tr>
<tr>
<td>10</td>
<td>Project quality</td>
<td>Minor</td>
<td>Possible</td>
<td>Low</td>
</tr>
<tr>
<td>11</td>
<td>Selection/performance of third party suppliers</td>
<td>Moderate</td>
<td>Possible</td>
<td>Medium</td>
</tr>
<tr>
<td>12</td>
<td>IT Staff</td>
<td>Minor</td>
<td>Possible</td>
<td>Low</td>
</tr>
<tr>
<td>13</td>
<td>IT expertise and skills</td>
<td>Minor</td>
<td>Possible</td>
<td>Low</td>
</tr>
<tr>
<td>14</td>
<td>Software performance</td>
<td>Minor</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
</tbody>
</table>

Some risks are low due to the bank already having some controls in place, such as:
1. CBS Replacement is aligned with enterprise strategy and priorities.
2. Design Review Board provides architecture guidelines and advice on the software application and to verify compliance.
3. The Steering Committee monitors the key project performance such as scope, schedule, quality, cost and risk.
4. A cost management process has been established to compare actual cost to budget. There is a dedicated financial controller to monitor the project cost.
5. Quality management plan is established that shows the project quality system and reviewed and agreed by all parties. The usage of Requirement Traceability Matrix is to ensure the solution are met with initial requirements.

6. A change management plan is established in line with organizational change management. Training and transfer knowledge is delivered to the users and IT team.

7. Suppliers were selected according to procurement policy and procedure. The performance is monitored to ensure the suppliers are meeting the business requirements.

8. IT personnel recruitment processes are in line with HR policies and procedures. The needs of external/vendor is to supplement the lack of IT related skills within IT due to new technologies.

9. Monitoring tools will be implemented to monitor the performance and capacity of IT resources. Perform the non-functional test, regression test, and production simulation and rehearsal test to ensure the software performance.

There are 3 (three) residual risks that still need to be mitigated, which are:

1. Software implementation risk
2. Project delivery risk
3. Selection/performance of third party suppliers risk

To mitigate the above risks, COBIT5 as described in Appendix C. Mapping Examples Risk Scenarios to COBIT5 Processes, page 67-70 [6] has considered some improvement in the relevant processes for each risk. For Software implementation risk, there are 8 (eight) COBIT5 process capabilities that can be improved.

<table>
<thead>
<tr>
<th>COBIT 5 Process Capabilities</th>
<th>Process to be improved</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO11</td>
<td>Consistent and effective quality management activities</td>
</tr>
<tr>
<td>BAI01</td>
<td>Project management</td>
</tr>
<tr>
<td>BAI02</td>
<td>Requirements definitions</td>
</tr>
<tr>
<td>BAI03</td>
<td>Solution development</td>
</tr>
<tr>
<td>BAI05</td>
<td>Managing organizational changes with regards to software implementation</td>
</tr>
<tr>
<td>BAI06</td>
<td>Change management</td>
</tr>
<tr>
<td>BAI07</td>
<td>Extensive solution testing</td>
</tr>
<tr>
<td>BAI08</td>
<td>Knowledge support</td>
</tr>
</tbody>
</table>

**Conclusion**

Bank X has assessed the risk of Core Banking System Replacement prior to the project starting and is documented in the Business Case.
Based on discussion with Subject Matter Expert, out of fourteen risks identified using ISACA Risk Scenarios, there are still three medium residual risks should be further mitigated: Software Implementation, Project Delivery and Selection/Performance of Third Party Supplier Risk.

Risk Assessment using ISACA Framework is proven to be capable of identifying the risks for Core Banking Replacement and help the company to identify some controls to mitigate the risks. The risks scenarios will depend on the current condition of the bank.

It is also found that COBIT5 has some specific process capabilities that can be used to improve the processes to mitigate the medium risks.

Recommendations

More research is required for further analysis of the IT risks using different framework and adding more risks scenarios for a successful Core Banking System project.

Meanwhile, Surveys from other banks, which had similar experiences can help to improve the risks scenarios and risks mitigation.

Further research may also need to focus on responding to medium risks based on missing or inadequate as suggested by COBIT5 processes.

Acknowledgments

The authors wish to thank the Head of Core Banking System Transformation Program, the Head of IT Architect & Design and the Head of Operational Risk of Bank X for their full support in this research.

References


**Glossary**

**Business Case** is a document to describe the business background, reason and objectives for initiating a project. It is often presented in a well-structured written document about the project strategy, project scope, high-level business stakeholder requirements, benefit realization, financial summary, and project delivery approach and organization change management of a proposed project.

**COBIT** is a framework created by ISACA for information technology (IT) management and IT governance. It is also provided by a supporting toolset that allows managers to identify the gap between control requirements, technical issues and business risks.

**Core Banking System (CBS)** is the back-end system which processing banking customer transactions of banking products/services and interfaces to other systems, such as general ledger, payment, reporting tools, etc.

**Heat Map** is a two-dimensional representation of data in which values are represented by colors, usually using darker colors to indicate high risk and brighter colors to indicate low risk.

**Inherent Risk** is the risk when no controls have been put in place.

**ISACA** is a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance.

**Residual Risk** is the risk remains after putting controls in place.