The Annual Conference on Management and Information Technology (ACMIT) 2016

Benefit and Risk Assessment for Having Disaster Recovery in Cloud Computing for Banking Industry: Go/No-Go Decision Making Model

Krisdian Eko Sutedja 3*
Swiss German University, EduTown BSDCity, Kav. II.1, Bumi Serpong Damai, Banten 15339, Indonesia

Abstract

Over the past year, we all have been showed many cloud-based solutions for so many purposes, starting from the public storage facilities to the disaster recovery solutions. We have learned that enterprises need to pay more attention to the cybersecurity, especially for the banking industry. The bank needs to encompass all that protects the bank from the attacks, breaches, disruptions, and incidents and also the consequences, but still need to reduce costs. So as the result, the solutions need to be aligned with all of the other aspects within the bank, which include the governance, management and risk assurance. The idea of having the disaster recovery in the cloud have to also consider the information security aspects, as the bank is trying to get the maximum benefit that the bank can get from the cloud like to minimize the cost needed by the bank’s activities, but still need to consider the results of the risk assessment as one of the requirement in implementing the cloud solutions. The other thing that the bank has to consider is the compliance aspect.

Keywords: Disaster Recovery; Cloud Computing; Risk Assessment

1. Introduction

Currently the Bank is facing tough economic times. Depreciation of Rupiah, Indonesian stocks continue to fall, and other economic problems that we currently have right now. In the very competitive business environment, The Bank is forced to increase efficiency but still need to improve flexibility and scalability, and the arising ideas are like how to cut costs, keep the trust from the clients by giving reliable services, and help the clients to maintain their good and even make closer relationship with their customers by maintaining the service level as agreed.

One of the things that can be improved to be more efficient is the resource usage. The cloud computing is claimed to be able to reduce recovery time and provide multi-site availability at a fraction of the conventional disaster recovery solutions cost.

* Corresponding author. Tel.: +62-21-3045-0045; fax: +62-21-3045-0001. E-mail address: krisdian.sutedja(at)sgu.ac.id.
As the bank industry is always required to meet the operational and regulatory requirements set by the regulator, in this case Otoritas Jasa Keuangan (OJK), the banks need to design and implement the cloud computing solution very carefully to make sure that it meets the requirements, or else, the project
will be failed to be delivered. We can learn from the cases like what happened in the Bank of Queensland case, where they were unable to meet the operational and regulatory requirements [2]. So, the implementation in banking industry is even trickier because of the regulatory requirements.

This research proposes a comprehensive benefit and risk assessment framework in which the objective hierarchy is constructed and the appropriate measurements are defined to provide the guidance for the assessment. Thus, the research is driven by this research question: How to decide whether the bank should go with the disaster recovery in the cloud project plan from the perspective of benefit and risk analysis?

2. Cloud-based Disaster Recovery Solutions: An Overview

Cloud-based disaster recovery solutions can be an attractive alternative for the companies, especially the small and medium-sized business (SMB), where the secondary infrastructure is only idling most of the times. It can reduce the need for spaces, and the resources that may lead to a significant cost reduction [3]. So it may enable the SMBs to have the disaster recovery solution options that were only available for the large enterprises because of the high cost. The cloud-based solution has another benefit that it make the disaster recovery process to become less complicated. But there are challenges in providing cloud-based disaster recovery solutions, that security is usually the top concern. The usual questions regarding the cloud-based solutions are like is the data stored and transferred securely in the cloud, how the user sessions are being authenticated, and as for the banks, they have the additional regulatory requirement considerations. The table below shows the three disaster recovery categories in term of the feature differences.

<table>
<thead>
<tr>
<th>DR model</th>
<th>Data synchronization</th>
<th>Independency</th>
<th>Initial Cost</th>
<th>Ongoing cost</th>
<th>Cost of potential disasters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Depends</td>
<td>High</td>
</tr>
<tr>
<td>Distributed</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Depends</td>
<td>High</td>
</tr>
<tr>
<td>Cloud</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Depends</td>
<td>Low</td>
</tr>
</tbody>
</table>

Table 1. Disaster recovery models [4]

There are several different types of the cloud-based disaster recovery solutions that are available and can be used by the bank, as follow [5] [6]:

a. Both of the managed application and also managed disaster recovery solutions are in the cloud. By doing this, the bank can have the full benefits of the cloud computing, that are from having the cost based on usage, and further more in eliminating the needs of on-premise infrastructures. In this scenario, the most important thing to be addressed is the Service Level Agreement (SLA) with the vendor.

b. Backup in the cloud as the substitute for tape based off-site backup. In this scenario, the application and database are still remain on-premise, and the data is being backup into the cloud, in case when system failures/disasters occur, the on-premise systems are restored from the data taken from the cloud.

c. Backup to the cloud, and when needed, the restore is also done to the cloud. So in this scenario, when system failure/disaster is happened, the data that was backed up to the cloud, is restored to the virtual machine (VM) in the cloud.

d. Replication to the backup virtual machines in the cloud. In this scenario where the RPO (Recovery Point Objective) is the main objective, the data is replicated to the virtual machine in the cloud. This scenario can be used to replicate and protect both of the on-premise and backup system in the cloud.

3. The Benefits, Risks, and Costs of Cloud-based Disaster Recovery Solutions

The considerations in implementing the cloud-based disaster recovery solutions are basically the same as in the traditional disaster recovery solutions, that are about how long the systems can be down, how much data loss that is acceptable, what business parts that have to be up and when, and also about less downtime of the systems versus the greater disaster recovery solution costs. Or they can be defined as [7]:

- RTO (Recovery Time Objective): The time between the declaration and the service availability, it’s related to the time needed to restore the services to usable state.
- RPO (Recovery Point Objective) : The data in the system that is lost during the disaster time, it’s related to the amount of data that is entered into the system since the last backup of the system.
- TTO (Test Time Objective) : The time required in testing the recovery plans, it’s related to the resources that are used for the testing.

The RPO needs to be considered in choosing the disaster recovery solutions. Generally, the necessary RPO of a disaster recovery system is a business decision [7].

What we can see from the above diagram is that the longer the disruption is happening, more costly it will become for the company and the operation. The shorter the RTO, the recovery solution costs to implement will become more expensive [8].

In the disaster recovery system planning, after we’ve done the business impact analysis (BIA), the next step is to perform the risk assessment. What BIA can help is that the BIA helps in identifying the business processes that are the most critical and describes about the potential impact of the disruption to the processes, and then the risk assessment can identify both the internal and external situations that
may impact the critical processes negatively. The bank should have the Risk Management Policy, as a statement of the overall intentions and the direction of an organization which is related to risk management, including the risks related to the disaster recovery plans [9]. Moreover it can quantify the potential severity of the events like that and the likelihood of them to be occurred [10] [11].

4. Regulatory Challenges

For the banking industry in Indonesia, the regulators require the data to be located in local data centers, to be kept secure and integrity and confidentiality maintained. Failing to conform to the regulation may cause the bank to be penalized by the regulator. The impact may even include the loss of reputation, which may be then reflected in the market shares. So the increasing dependency on the external cloud-based disaster recovery solution can increase the non-compliance probability. That’s the reason of why compliance is also an important area of the cloud risk.

The current regulation, legislation, and standards that exist nationally and internationally that are related to the business continuity management and disaster recovery plan need to be checked against the plan that’s going to be defined by the company. One of the checklist of the regulation, legislation, and standards is published by Business Continuity Institute (BCI), that lists the legislations, regulations, standards, and good practices from many countries in the world. The example of the regulation from Indonesia is as follows:

Table 2. The business continuity related regulation in Indonesia [12]

<table>
<thead>
<tr>
<th>TITLE</th>
<th>AUTHORITY</th>
<th>SUMMARY</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circular Letter No. 9/30/DPNP - Risk Management in the Use of Information Technology by Commercial Banks (March 31st, 2008)</td>
<td>Regulation Bank Indonesia (Central Bank)</td>
<td>Requires SCP documentation and at least annual testing with focus on Bank Indonesia RTGS system. Requires internal audit to conduct an audit at least annually and provide report to Bank Indonesia.</td>
<td><a href="http://www.bi.go.id/web/bi/o/PeraturanPerbankan/Sea_093007.htm">http://www.bi.go.id/web/bi/o/PeraturanPerbankan/Sea_093007.htm</a></td>
</tr>
</tbody>
</table>

5. Evaluating Cloud-Based Disaster Recovery Solutions For Banking: A Case Study

The virtualization technology, the cloud computing and cloud storage of data are among the top main concerns for the companies regarding the required knowledge. The companies need the knowledge about cloud computing in order to explore the more possibilities in deploying the cloud computing and getting more benefits from it [13]. According to the Forrester/DRJ study, 42% of the companies are using some sort of outsourced disaster recovery services [14], and 78% of enterprises have stated that the disaster recovery capabilities improvement is their high priority, in order to be better in identifying and quantifying the risks, in understanding the economic impact, and having less tolerance for the downtime and the data loss [15]. The CEOs (Chief Executive Officers) and business owners are already realized that they can get more of the money with outsourcing. In line with the global IT transformation focus and survey, the bank tries to find the disaster recovery solution that’s more cost effective compared to continuing the current conventional way in doing the disaster recovery plan, that’s by adding new servers and network devices into the available space at the disaster recovery site. The cost to rent the private space for the servers and network devices is another big issue for the bank, and the needed space is even growing, in line with the growing of the on-premise/production data center site. In doing so, the bank is developing the model about how to decide if the bank should go with the cloud-based disaster recovery solution for each of the systems. So the cloud-based disaster recovery solution can be used for a new banking system, or for the old systems that need to be moved to the cloud, due to
the high maintenance costs, for example. The move to the cloud for the old systems’ disaster recovery plan is also to improve the RTO and RPO.

First the bank needs to set the BIA. The bank defines the critical level of the business processes in the BIA into four tiers as follows [16]:

a. Tier 1: Mission-Critical
   Mission-critical business processes/activities are those that have the greatest impact on company's operations and potential for recovery. Tolerable downtime for mission-critical process is 0 to 6 hours top. Process must be maintained in top priority under any circumstances.

b. Tier 2: Vital
   Vital business processes/activities are deemed very important and should be addressed immediately after the mission-critical processes. Tolerable downtime for vital process is 7-24 hours top.

c. Tier 3: Important
   Important business processes/activities will not stop the business from operating in the near-term but they usually have a longer-term impact if they were missing or disabled. Tolerable downtime for important process is more than 1 day.

d. Tier 4: Minor
   Minor business processes/activities do not need to wait for any system/facility to recover. They are going to not to be missed in the near-term and that certainly not while business operations are being recovered. They may resume business with workaround that requires minimal effort.

Based on the critical level, the BIA form was then distributed to the each of the business units in the bank, the example of the result is as follows:

<table>
<thead>
<tr>
<th>No.</th>
<th>Critical Business Process</th>
<th>Critical Level Tier</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
<th>Tier 4</th>
<th>Dependencies on IT Group Software/Hardware</th>
<th>Dependencies on other Biz/SU/Vendor</th>
<th>Min. Resource Required</th>
<th>Potential Financial Impact</th>
<th>Legal / Compliance Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IBM and TL as window person for customers, internal department and decision maker</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>N/A</td>
<td>Loan Ops and IRMID</td>
<td>N/A</td>
<td>2</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>Credit Proposal preparation until obtain final approval</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>CRMG</td>
<td>N/A</td>
<td>3</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- server folder</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Core Banking System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- counter party related</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Loan documentation process</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>N/A</td>
<td>Legal, Loan Ops, IRMID</td>
<td>N/A</td>
<td>2</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Agreement signing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Drawdown process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Repayment schedule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Cash Management</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Operation Group and IT</td>
<td>Low</td>
<td>2</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>- FBS system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Internet Banking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

From the BIA results, the requirements from people, process, and technology aspects in order to support the critical business functions can be defined. Like for example, how can the available people related resources owned by the bank support the disaster recovery plan, such as the skills and knowledge needed, the amount of staff, etc.

The metrics like the RTO and RPO can then be obtained and the most critical systems and data can be mapped, which areas of the business that can be down for a longer period without causing the adverse effects. The tiered services can be customized with the availability of the cloud computing, making the disaster solutions to become more flexible, as the bank can get more options for the solutions.
In the above diagram, the gap between the disaster and the RPO is the data/transactions of the bank that will be lost as the result of the disaster/system failure. The RTO required can then be mapped to the cloud-based disaster recovery service level that’s provided by the vendor. The example of the cloud based disaster recovery packages can be seen as follows:

Table 4. Disaster recovery service level differences from IBM [18]

<table>
<thead>
<tr>
<th>IBM SmartCloud recovery service</th>
<th>Recovery time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>1 minute</td>
<td>For mission-critical applications</td>
</tr>
<tr>
<td>Silver</td>
<td>30 minutes</td>
<td>For rapid recovery</td>
</tr>
<tr>
<td>Bronze</td>
<td>6 to 24 hours</td>
<td>Assisted failover and failback</td>
</tr>
</tbody>
</table>

The return on investment (ROI) of the disaster recovery solutions can be calculated to see the value of the disaster recovery options. The example about how to calculate the ROI is as follows: If the bank had been shutdown for the few days because of disaster, they might lose $900,000 in revenue, for example. Let’s say that the bank has an annual cloud-based disaster recovery solution from a vendor that costs about $50,000 per year in order to protect all of the bank’s tier 1 and 2 servers. And then, when a disaster hits the bank’s business, the bank then fail over to the cloud-based disaster recovery solution and the process takes about three hours total. Because of the successful fail over process, the bank does not suffer any significant productivity lost, that the bank still can serve their customers and continue to earn the revenues. Which means, the ROI can be counted as ($900,000 - $50,000) / $50,000 which equals to 1,700% [19].

The cost of investment and savings comparison from having the legacy disaster recovery solution with the cloud-based disaster recovery solution can be projected as follows:

Table 5. The example of the bank’s cumulative investment and savings data

<table>
<thead>
<tr>
<th>PT. Bank XYZ</th>
<th>Cumulative Investment and Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy Environment</td>
<td>$518,593</td>
</tr>
<tr>
<td>Year 1</td>
<td>$518,593</td>
</tr>
<tr>
<td>Year 2</td>
<td>$377,352</td>
</tr>
<tr>
<td>Year 3</td>
<td>$447,973</td>
</tr>
<tr>
<td>Cloud Environment</td>
<td>$56,698</td>
</tr>
<tr>
<td>Year 1</td>
<td>$25,053</td>
</tr>
</tbody>
</table>
The next step when considering the cloud-based disaster recovery solutions is to do the risk assessment. There are three main things that need to be considered for the cloud-based disaster recovery solutions [20]:

a. Data security. When the data of the company is starting to enter the cloud computing providers, there are always concerns regarding the security aspects. How the cloud computing service providers manage the security aspects of the systems needs to also be monitored, and the bank should have the visibility and certainty into the security elements that are used by the providers of the cloud computing.

b. Service reliability. The network connectivity from the bank to the cloud computing provider and vice versa may have problems and the cloud computing service provider systems may be down sometimes that affects the reliability of the bank’s services, so the network dependency and reliability have to be addressed carefully.

c. Software management. The fact that the bank may not have the full control over the software management and development, that causes the editing and updating of the softwares and the bug fixing processes to become more complex compared to if the softwares are hosted in the bank’s own premises.

Everytime the bank tries to consider the cloud-based solution for their disaster recovery plan based on the BIA and tiering, the above risks need to be assessed [21]. Like for example, when the bank is thinking about choosing the cloud-based solution for one of their application, the data confidentiality contained in the application needs to be assessed first, and the risks need to be accepted before the bank can then move the disaster recovery plan for the application into the cloud, and the controls need to be defined and implemented to secure the data. Regarding the service reliability, for example for the network connectivity issues that need to be considered in choosing the right cloud-based disaster recovery solution. If the bank’s connectivity to the cloud computing vendor is not reliable or the
bandwidth is too small, the bank should consider the other options, or to choose the cloud-based disaster recovery solution that does not require very big network connection bandwidth. The solution that requires the data transfer from the vendor site to bank’s site, may depends on how big is the data. For the situation that the network bandwidth is very limited, the option to put both of the production and disaster recovery systems at the cloud that’s managed by the same vendor can be choosen.

And finally, before running the implementation of the cloud-based disaster recovery solution, the bank will need to check against the regulation. Regulators may not that keen on the cloud computing, fearing that any data breach may have devastating consequences for the bank customers, so the effect is not only for the bank themselves. Regulators don’t allow the bank to use the third-party vendors from outside of the country to store the bank customer data abroad, again for the security concerns. And the cloud computing vendor may not support the actually needed national, international, or industry standards and regulations in providing the cloud-based solutions for banking industry.

Considering the benefit and cost of the cloud-based disaster recovery solution for one of the bank’s application, in this case the bank chose to put both the primary server and disaster recovery system server into the cloud-computing vendor sites. In the case like this, the bank needs to make sure about the SLA since the process of activating the disaster recovery system will be much depending on the vendor’s SLA.

Regarding the vendor selection, there are several things need to be checked, like the support from vendor (Specialized knowledge & skills), how the disaster recovery (DR) drilling will be done including to state it in the contract, how is the vendor’s ability in supporting multiple customers when disaster happens, make sure that the vendor separate the location for the DR from the production servers location, make sure that remote access is provided to the DR servers, the SLA is agreed, and review the certifications that the vendor have, for example the certification from International Organization for Standardization (ISO).

![Diagram of the bank’s cloud-based disaster recovery system](image)

**Fig. 7.** The network diagram of the bank’s cloud-based disaster recovery system

6. **Conclusion**

While a cloud-based disaster recovery solution is often favourable because of the cost consideration, and especially to the smaller banks, there may still be significant benefits in maintaining the separate data centers, that the larger banks can’t also ignore. The banks may explore all of the options, while
still considering the risks caused. Nevertheless, the risks may do change over the project lifetimes, which may be caused by the system modification and operation changes, and the advancement in technology.

The main challenges are like the security and compliance, where SLAs are a must, and the banks need to demand the safety measures from the service providers, and to ensure that the applications meet the latest and most rigorous standards of security. And then about the reliability, in ensuring that the application and data are always available in the natural disaster or unpredictable events. The management of the cloud-based solution is one of the challenges, where achieving visibility and performance measurement are harder to be done in the cloud-based environment, especially when the bank use the cloud services for both internal and external services, that require the bank to handle multiple security systems. The interoperability is also a challenge as the bank need to ensure that the data and application can be moved as needed across the cloud environments from the different service providers, that a single interface and layer management need to be developed, internally and externally. The regulation needs to be understood clearly on where the data is kept. In order to guarantee the successful of the DR in the cloud plan, several things need to be checked, like the use of multiple ISPs (Internet Service Providers) in order to avoid single point of failure, evaluate the list of the applications with their specific requirements, understand about the capability of the vendor, make sure to test everything with the vendor especially for the critical applications, plan for the geographical locations, make sure about the access to the DR servers, and of course to make sure to get the main benefits from the cloud-based disaster recovery plans.

![Diagram](image)

Fig. 8. The cloud-based disaster recovery benefit and risk assessment for banking industry: Go/No go decision making model

7. Future Works

Cloud-based disaster recovery may help in ensuring the high reliability of the data, low cost of backup, and short recovery time, but it still depends on the strategies that are proposed, and suitable for the bank’s different kinds of disaster recovery scenarios. So the bank needs to study further about the implementation in the bank, and do risks assessment based on the solution that’s chosen by the bank. The adoption rate is increasing continously though, and that now the cloud-based disaster recovery solution is a more viable option for the bank, just need more studies in the future regarding the options and the risks.
References


