Bank Resona Perdania

KEBIJAKAN PENGGUNAAN PIHAK PENYEDIA JASA TI

THE USE OF IT SERVICE PROVIDER POLICY

Edisi ke-3, Februari 2023

3rd Edition, Februari 2023

BOD Approval No. 078/ITD/IT-PLN/III/2023

BOC Approval No. 041/BOC/III/2023-ITD/IT-PLN

DAFTAR ISI
Table of Content

Hal/*Page*

Bank Resona Perdania

I. PENDAHULUAN

A. Latar Belakang

Dalam rangka meningkatkan efektivitas dan efisiensi pencapaian tujuan strategis, Bank dimungkinkan menggunakan pihak penyedia jasa TI. Hal ini sesuai dengan Pasal 29 POJK No. 11/POJK.03/2022 Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum tentang Manajemen Risiko Teknologi Informasi yang mengatur bahwa penyelenggaraan Teknologi Informasi (TI) dapat dilakukan oleh Bank sendiri dan/atau pihak penyedia jasa TI". Yang dimaksud dengan menggunakan pihak penyedia jasa TI adalah penggunaan jasa pihak lain dalam menyelenggarakan kegiatan TI yang dapat menyebabkan Bank memiliki ketergantungan terhadap jasa yang diberikan secara berkesinambungan atau dalam periode tertentu.

Penggunaan pihak penyedia jasa TI dapat mempengaruhi risiko Bank antara lain risiko operasional, kepatuhan, hukum, dan reputasi. Risiko-risiko ini dapat timbul antara lain karena adanya kegagalan penyedia jasa TI dalam menyediakan jasa, pelanggaran hukum, atau ketidakmampuan untuk mematuhi hukum dan ketentuan peraturan perundang-undangan.

B. Acuan

1. Peraturan External :

   1. POJK No. 11 /POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum

   2. SEOJK No. 21 /SEOJK.03/2017 tanggal 6 Juni 2017 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

      SEOJK No. 21 /SEOJK.03/2017 ini dinyatakan masih tetap berlaku sesuai dengan ketentuan dalam POJK No. 11 /POJK.03/2022

   3. POJK No. 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi

I. INTRODUCTION

A. Background

In connection to improve effectiveness and efficiency of strategic goals, Bank is possible to use IT service provider. This is in line with article 20 POJK No. 38/POJK.03/2016 as amended by POJK No.13/POJK.03/2020 about Implementation of Risk Management in the use of Information Technology by Commercial banks about Information Technology Risk Management that regulate that IT activity can be performed by Bank and/or IT service provider. The meaning of using IT service provider is using third party in carrying out IT activity that can cause Bank to have dependence on service provided continuously or within certain period.

The use of IT service provider can affect Bank risk, including operation risk, compliance risk, legal risk and reputation risk. These risks because of IT service provider unable to provide service, legal violation, or unable to comply with laws and regulations.

B. Reference

1. External Rules :

   1. POJK No. 11/POJK.03/2022 about Implementation of Information Technology by Public Bank.

   2. SEOJK No. 21 /SEOJK.03/2017 dated June 6, 2017 about Implementation of Risk Management in the use of Information Technology by Commercial banks.

      SEOJK No. 21 / SEOJK.03/2017 is declared still valid in accordance with the provisions in POJK No. 11 /POJK.03/2022

   3. POJK No. 18/POJK.03/2016 about Implementation of Risk

Bank Umum.

Sejak 30 Okt 2021, Pasal 20, Pasal 21, Pasal 22, dan Pasal 24 dalam POJK No. 18/ POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum dinyatakan dicabut dan tidak berlaku oleh POJK No. 13/POJK.03/2021 tentang Penyelenggaraan Produk Bank Umum.

4. SEOJK No. 34/SEOJK.03/2016 tanggal 1 September 2016 perihal Penerapan Manajemen Risiko Bagi Bank Umum.
5. POJK No.9/POJK.03/2016 tentang Prinsip Kehati-hatian Bagi Bank Umum yang Melakukan Penyerahan Sebagian Pelaksanaan Pekerjaan Kepada Pihak Lain.

   POJK ini dan ketentuan pelaksanaannya dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.24 Tahun 2022 tentang Pengembangan Kualitas Sumber Daya
   Manusia Bank Umum.
6. SEOJK No.11/SEOJK.03/2017 tanggal 17 Maret 2017 tentang Prinsip Kehati-hatian Bagi Bank Umum yang Melakukan Penyerahan Sebagian Pelaksanaan Pekerjaan Kepada Pihak Lain.

2. Peraturan Internal :

   1. Kebijakan Tingkat Otorisasi
   2. Kebijakan Manajemen Risiko secara Umum (Individual).
   3. Kebijakan Manajemen Risiko Operasional.
   4. Kebijakan Manajemen Risiko Hukum.
   5. Kebijakan Manajemen Risiko Reputasi.
   6. Kebijakan Manajemen Risiko Stratejik.
   7. Kebijakan Manajemen Risiko Kepatuhan.
   8. Kebijakan Manajemen Risiko Teknologi Informasi.
   9. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem dalam

Management for Commercial banks.

Since 30 Oct 2021, Article 20, Article 21, Article 22, and Article 24 in POJK No. 18/ POJK.03/2016 concerning the Implementation of Risk Management for Commercial Banks was declared revoked and invalid by POJK No. 13/POJK.03/2021 concerning the Operation of Commercial Bank Products.

4. SEOJK No. 34/SEOJK.03/2016 dated September 1, 2016 about Management for Commercial banks.
5. POJK No. 9/POJK.03/2016 about Prudential Principles for Commercial Banks Delegating Part of the Work Implementation to Other Parties.

   This POJK and its implementation provisions are declared to remain valid as long as they do not conflict with the provisions in POJK No. 24 of 2022 concerning Human Resources Quality Development Commercial Bank Man.
6. SEOJK No.11/SEOJK.03/2017 dated March 17, 2017 about Prudential Principles for Commercial Banks that Transfer Part of the Implementation of Work to Other Parties.

2. Internal Rules :

   1. Leveling Authority Policy
   2. Individual General Risk Management Policy
   3. Operational Risk Management Policy.
   4. Legal Risk Management Policy.
   5. Reputation Risk Management Policy.
   6. Strategic Risk Management Policy.
   7. Compliance Risk Management Policy.
   8. Information Technology Risk Management Policy.
   9. Information Security and System Risk Management Policy in the use

Penggunaan Teknologi Informasi.

10. Kebijakan Manajemen Proyek dan Pengembangan Sistem.
11. Kebijakan Tugas & Wewenang.
12. Kebijakan Uraian Pekerjaan.
13. Kebijakan Audit Intern Teknologi Informasi.

C. Tujuan

Memastikan bahwa Bank memiliki manajemen risiko yang efektif terkait pihak penyedia jasa TI dalam menyelenggarakan kegiatan TI agar penggunaan pihak penyedia jasa TI tersebut sesuai dengan kompleksitas jasa TI yang dibutuhkan Bank.

D. Ruang Lingkup

1. Prinsip-prinsip penggunaan penyedia jasa TI
   a. Bank tetap bertanggung jawab terhadap aktivitas TI yang diselenggarakan oleh pihak penyedia jasa TI.
   b. Penggunaan penyedia jasa TI tidak menghambat proses pengawasan oleh Otoritas Jasa Keuangan.
   c. Keputusan penggunaan penyedia jasa TI harus sejalan dengan rencana strategis TI Bank.
   d. Setiap penggunaan penyedia jasa TI harus dituangkan dalam perjanjian tertulis.
   e. Penggunaan penyedia jasa TI harus memberikan manfaat lebih besar dibandingkan dengan biaya yang dikeluarkan Bank.
   f. Penggunaan penyedia jasa TI harus didasarkan pada hubungan kerja sama secara wajar (*arm's length principle*), dalam hal pihak penyedia jasa TI merupakan pihak terkait

of Information Technology.

10. Project Management and System Development Policy.
11. Duties & Authorities Policy.
12. Job Description Policy.
13. Information Technology Internal Audit Policy.

C. Purpose

Ensure that Bank has an effective risk management related to IT service provider in performing IT activity so the use of IT service provider is in line with the complexity of IT service that Bank needs.

D. Scope

1. Priciples of using IT service provider
   a. Bank still responsible for IT activity that perform by IT service provider.
   b. The use of IT service provider is not hinder the process of OJK supervision.
   c. Decision to use IT service provider must be in line with Bank IT strategic plan.
   d. Each use of IT service provider must be stated in agreement.
   e. The use of IT service provider must provide greater benefits compared to cost expense by the Bank.
   f. The use of IT service provider is base on fair relationship (arm's length principle), in the event that IT service providers are parties related to the Bank.

dengan Bank.

2. Keputusan penggunaan penyedia jasa TI pada dasarnya harus mempertimbangkan faktor efisiensi dan risiko. Oleh karena itu, penggunaan penyedia jasa TI harus memenuhi prinsip-prinsip penggunaan penyedia jasa TI dan hal sebagai berikut:

   a. Penggunaan penyedia jasa TI harus mendapat persetujuan Direksi.

   b. Pemilihan penyedia jasa TI harus melalui proses uji tuntas (*due diligence*).

   c. Pemilihan penyedia jasa TI untuk layanan TI harus melalui proses seleksi atau berdasarkan penunjukan langsung sesuai dengan Kebijakan Manajemen Proyek dan Pengembangan Sistem dan Pedoman Pengadaan Barang dan Jasa Terkait TI.

   d. Perjanjian penyedia jasa TI harus memungkinkan adanya klausula kondisi pengakhiran perjanjian sesuai dengan masa perjanjian maupun sebelum masa perjanjian berakhir.

2. The decision to use an IT service provider basically has to consider efficiency and risk factors. Therefore, the use of IT service providers must meet the principles of using IT service provider and the following:

   a. The use of IT service provider must get approval from Board of Directors.

   b. The selection of IT service provider must go through a due diligence process.

   c. The selection of IT service providers for IT services must go through a selection process or based on direct appointment in accordance with the Project Management Policy and System Development and Guideline for Procurement of Goods and Services Related IT.

   d. An IT service provider agreement must allow for a clause to terminate the agreement in accordance with the agreement period or before the end of the agreement.

II. TUGAS DAN TANGGUNG JAWAB

A. Direksi

1. Menetapkan kebijakan dan prosedur mengenai penggunaan pihak penyedia jasa TI.
2. Memastikan penyedia jasa TI memenuhi kebutuhan dan sesuai dengan rencana strategis Bank.
3. Memastikan Bank memiliki keahlian untuk mengevaluasi calon penyedia jasa TI dan keahlian untuk mengawasi penyedia jasa TI.
4. Memastikan terdapat perjanjian pemeliharaan dengan penyedia jasa TI dalam hal kerja sama pengadaan TI.
5. Memastikan bahwa Otoritas Jasa Keuangan diberikan akses untuk melakukan pemeriksaan terhadap layanan yang diselenggarakan penyedia jasa TI.

B. Divisi TI

1. Merumuskan Kebijakan Penggunaan Pihak Penyedia Jasa TI.
2. Mengevaluasi calon penyedia jasa TI berdasarkan ruang lingkup dan layanan yang akan diselenggarakan.
3. Memantau dan melakukan *risk assessment* secara berkala terhadap layanan yang diselenggarakan oleh penyedia jasa TI.

II. JOB AND RESPONSIBILITY

A. Board of Directors

1. Determine policy and procedure about the use of IT service provider.
2. Ensure that IT service provider fulfill Bank's need and in accordance with Bank's strategic plan.
3. Ensure Bank has the expertise to evaluate potential IT service provider and has the expertise to supervise IT service provider.
4. Ensure that there are maintenance agreements with IT service provider in terms of IT procurement.
5. Ensure that OJK is given access to conduct supervision regarding service that performed by IT service provider.

B. IT Division

1. Creating The Use of IT Service Provider Policy.
2. Evaluate prospective IT service providers based on the scope and services to be held.
3. Monitoring and conduct a regular basis risk assessment of service provider by IT service provider.

III. KEBIJAKAN DAN PROSEDUR

A. Aturan Umum

1. Penggunaan pihak penyedia jasa TI yang penting dan berskala besar, memerlukan standar pemilihan penyedia jasa TI. Hal ini untuk memastikan bahwa penggunaan pihak penyedia jasa TI tersebut sesuai dengan kompleksitas jasa TI yang dibutuhkan Bank dan sesuai dengan ketentuan peraturan perundangan dan tata kelola (*governance*) yang memadai. Standar tersebut mengacu ke kebijakan dan pedoman Bank yang berlaku.

2. Standar isi perjanjian kerja sama dengan pihak penyedia jasa TI meliputi:

   a. Cakupan pekerjaan atau jasa.

   b. Biaya dan jangka waktu perjanjian kerjasama.

   c. Hak dan kewajiban Bank maupun kesediaan pihak penyedia jasa TI dalam memenuhi kewajiban yang dimuat dalam perjanjian kerja sama.

   d. Jaminan pengamanan dan kerahasiaan data dan informasi mengenai Bank, pihak *stakeholder*, dan terutama data/informasi nasabah. Data hanya bisa diakses oleh pemilik data (Bank).

   e. Jaminan tingkat pelayanan (SLA), berisi mengenai standar kinerja seperti tingkat pelayanan yang diperjanjikan (service level) dan target kinerja.

      SLA tetap berlaku apabila terjadi perubahan kepemilikan baik pada Bank maupun penyedia jasa TI.

   f. Laporan hasil pemantauan kinerja penyedia jasa TI yang

III. POLICY AND PROCEDURE

A. General Rule

1. The use of important and large-scale IT service providers requires a standard selection of IT service providers. This is to ensure that the use of the IT service provider is in accordance with the complexity of the IT services needed by the Bank and in accordance with the provisions of the law and adequate governance. The standard refers to applicable Bank policies and guidelines.

2. The standard content of the agreement with IT service provider includes:

   a. Scope of work or services.

   b. Cost and duration of agreement.

   c. The rights and obligations of the Bank as well as the willingness of the IT service provider to fulfill the obligations contained in the cooperation agreement.

   d. Guarantee of security and confidentiality of data and information regarding the Bank, stakeholders, and especially customer data/information. Data can only be accessed by the data owner (Bank).

   e. Service level guarantee (SLA), contains performance standards such as service level and performance target.

      SLA remains valid if there is a change in ownership both at the Bank and IT service provider.

   f. Report on the results of monitoring the performance of IT service providers related to

terkait dengan SLA

SLA

g. Batasan risiko yang ditanggung oleh Bank dan penyedia jasa TI, diantaranya :

g. Risk limit borne by the Bank and IT service provider, including :

1) Risiko perubahan ruang lingkup perjanjian

1) Risk of changes in the scope of the agreement

2) Perubahan ruang lingkup bisnis dan organisasi perusahaan penyedia jasa TI;

2) Changes in the business scope and organization of IT service providers

3) Perubahan aspek hukum dan regulasi

3) Changes in legal and regulatory aspects

4) Aspek hukum yang meliputi hak cipta, paten dan logo atau merek (*trade mark*)

4) Legal aspects which include copyright, patent and logo or brand (trade mark)

h. Persetujuan Bank secara tertulis dalam hal pihak penyedia jasa TI melakukan pengalihan sebagian kegiatan (subkontrak) kepada subkontraktor. Selain itu, subkontraktor harus mempunyai standar penyelenggaraan TI yang memadai

h. Bank approval in writing in the event that the IT service provider transfers part of the activity (subcontracting) to the subcontractor. In addition, subcontractors must have an adequate standard of IT management.

i. Tersedianya sarana komunikasi yang terkoneksi dengan jaringan internet serta pengamanan terhadap akses dan transmisi data dari dan ke Pusat Data dan/atau Pusat Pemulihan Bencana

i. Availability of communication facilities connected to the internet network as well as security against data access and transmission from and to the Data Center and / or Disaster Recovery Center.

j. Pengaturan yang jelas mengenai rekam cadang (*back-up*) data, kebijakan saat keadaan yang mengancam kelangsungan operasional Bank (*contingency*), perlindungan terhadap data Bank (*record protection*) termasuk perangkat keras, perangkat lunak, dan perlengkapan (*equipment*), untuk menjamin kelangsungan penyelenggaraan TI

j. Clear arrangements regarding backup data, policies when conditions that threaten the continuity of the Bank's operations (contingency), protection of Bank data (record protection) including hardware, software, and equipment (equipment), to ensure continuity of operation IT.

k. Pengaturan mengenai pengamanan dalam pengiriman dokumen sumber (*source document*) yang diperlukan dari dan ke Pusat Data dan/atau

k. Arrangement regarding security in sending the required source document from and to the Data Center and / or Disaster Recovery

	Pusat Pemulihan Bencana. Pihak yang bertanggung jawab sebaiknya dilindungi asuransi yang cukup	Center. Responsible parties should be protected by adequate insurance
l.	Kesediaan diaudit baik oleh intern Bank, Otoritas Jasa Keuangan, dan/atau pihak ekstern yang ditunjuk oleh Bank maupun oleh Otoritas Jasa Keuangan dan tersedianya informasi untuk keperluan pemeriksaan, termasuk hak akses, baik secara *logic* maupun fisik terhadap data yang dikelola oleh penyedia jasa TI.	l. Willingness audited by Bank, OJK, and/or external party that assigned by Bank or OJK and the availability of information for examination purposes, including access rights, both logically and physically to data managed by IT service provider.
m.	Pihak penyedia jasa TI harus memberikan dokumen teknis kepada Bank terkait dengan jasa yang dikerjakan oleh penyedia jasa TI antara lain alur proses TI dan struktur Pangkalan Data (*Database*).	m. IT service providers must provide technical documents to the Bank related to services performed by IT service providers including IT process flow and Database structure.
n.	Pihak penyedia jasa TI harus melaporkan setiap kejadian penting (*critical*) yang dapat mengakibatkan kerugian keuangan dan/atau mengganggu kelancaran operasional Bank.	n. IT service providers must report every critical event that can result in financial losses and / or disrupt the smooth operation of the Bank.
o.	Khusus untuk penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan Pemrosesan Transaksi Berbasis Teknologi Informasi, pihak penyedia jasa TI harus menyampaikan kepada Bank laporan keuangan terkini yang telah diaudit setiap tahun. Penyedia jasa TI menyampaikan hasil audit TI yang dilakukan auditor independen secara berkala terhadap penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi, kepada Otoritas Jasa Keuangan melalui Bank.	o. Especially for organizing Data Centers, Disaster Recovery Centers and Information Technology-Based Transaction Processing, IT service providers must submit to the Bank the latest financial reports that have been audited annually. IT service providers deliver the results of IT audits conducted by independent auditors on a regular basis against the implementation of Data Centers, Disaster Recovery Centers, and / or Information Technology-Based Transaction Processing, to the OJK though Bank.
p.	Tanggung jawab penyedia jasa TI dalam menyediakan SDM yang memiliki kualifikasi dan kompetensi sesuai jasa yang disediakan agar operasional	p. Responsibility of IT service providers in providing HR who have qualifications and competencies according to the services provided so that the

	Bank tetap terjamin.	Bank's operations are guaranteed.
q.	Kepemilikan dan lisensi.	q. Ownership and license.
r.	Jaminan dari penyedia jasa TI bahwa penyediaan jasa masih akan diberikan kepada Bank selama periode tertentu setelah implementasi.	r. The guarantee from the IT service provider that the provision of services will still be provided to the Bank during a certain period after implementation.
s.	Mekanisme perubahan, pengakhiran, atau pemutusan perjanjian termasuk dalam hal ketika Otoritas Jasa Keuangan memerintahkan Bank menghentikan penyediaan jasa TI sebelum berakhirnya jangka waktu perjanjian.	s. Mechanism of changes, terminations, or termination of agreements including in the event that the Financial Services Authority orders the Bank to stop providing IT services before the end of the agreement period.
t.	Sanksi dan penalti terhadap alasan-alasan yang tidak jelas terhadap pembatalan perjanjian dan pelanggaran isi perjanjian.	t. Sanctions and penalties for unclear reasons for cancellation of the agreement and violation of the contents of the agreement.
u.	Kepatuhan pada hukum dan ketentuan peraturan perundang-undangan di Indonesia.	u. Compliance with laws and regulations in Indonesia.
v.	Standar pengamanan sistem yang harus dipenuhi oleh penyedia jasa TI.	v. System security standards that must be met by IT service provider.
w.	Standar tingkat pelayanan yang harus dipenuhi oleh penyedia jasa TI.	w. Service level standards that must be met by IT service provider.
x.	Standar laporan pemantauan kinerja penyedia jasa TI.	x. Standard IT service provider performance monitoring report
y.	Standar perjanjian penyimpanan dokumen (*escrow agreement*).	y. Standard document storage agreement (escrow agreement).
z.	Pihak penyedia jasa TI berkomitmen untuk menyampaikan hasil audit TI secara berkala yang dilakukan auditor independen atas penyediaan jasa TI kepada Bank. (Terutama untuk penyediaan jasa IT yang sifatnya kritikal, seperti Data Center/Data Recovery Center, kecuali ada tambahan penjelasan dari regulator di kemudian hari)	z. The IT service provider is committed to submitting the results of periodic IT audits conducted by independent auditors for the provision of IT services to the Bank. (Especially for the provision of IT services related to services that are critical, such as Data Centers/Data Recovery Centers, unless there is additional explanation from the regulator at a later date)

3. Bank hanya dapat melakukan Alih Daya atas pekerjaan penunjang pada alur kegiatan usaha Bank dan pada alur kegiatan pendukung usaha Bank. Pekerjaan penunjang paling sedikit memenuhi kriteria :
   a. Berisiko rendah.
   b. Tidak membutuhkan kualifikasi kompetensi yang tinggi di bidang perbankan.
   c. Tidak terkait langsung dengan proses pengambilan keputusan yang mempengaruhi operasional Bank.

B. Prosedur Penggunaan Penyedia Jasa TI

Pemilihan penyedia jasa TI paling sedikit mencakup:

1. Pendefinisian Kebutuhan oleh Bank dengan menentukan hal seperti :

   a. Identifikasi secara spesifik mengenai fungsi atau aktivitas yang akan diserahkan penyelenggaraannya kepada pihak penyedia jasa TI.

   b. Jika sudah didapat identifikasi fungsi dan aktivitas yang dibutuhkan, maka Bank dapat membuat kriteria pihak penyedia jasa TI yang dibutuhkan.
   c. Bank perlu meneliti potensi calon pihak penyedia jasa TI.
   d. Proses penilaian risiko yang dapat timbul akibat penyerahan penyelenggaraan fungsi atau aktivitas tersebut.

   e. Penetapan dasar yang akan digunakan untuk mengidentifikasi pengukuran pengendalian yang memadai.

2. Tahap pendefinisian kebutuhan di atas harus menghasilkan suatu dokumen yang berisi gambaran secara rinci mengenai keinginan Bank terhadap jasa yang akan dikerjakan oleh pihak penyedia jasa TI. Isi dari dokumen tersebut mencakup beberapa komponen berikut ini:

   a. Cakupan dan karakteristik dari layanan dan teknologi yang

3. Banks may only conduct Outsourcing for supporting work in the Bank's business activity flow and in the Bank's business support activity flow. Support work at least meets the following criteria:
   a. Low risks.
   b. Does not require high competency qualifications in banking sector.
   c. Not directly related to the decision-making process that affects the Bank's operations.

B. The Use of IT Service Provider Procedure

Selection of IT service provider at leas covering:

1. Requirement Definition by Bank needs to specify things such as :

   a. Specific identification of the function or activity to be delivered to the IT service provider.

   b. If the identification of the required functions and activities has been obtained, the Bank can make criteria for the required IT service provider.
   c. Banks need to research potential IT service providers.
   d. Risk assessment process that can arise due to the delivery of the implementation of the function or activity.

   e. Base determination that will be used to identify adequate measurement of control.

2. The phase of defining the above needs must produce a document that contains a detailed description of the Bank's requiremment for services to be carried out by the IT service provider. The contents of the document include the following component:

   a. Coverage and characteristics of services and technology

digunakan serta dukungan kepada nasabah.

b. Tingkat layanan meliputi ketersediaan dan kinerja, manajemen perubahan (*change management*), kualitas layanan, keamanan, dan kelangsungan usaha.

c. Karakteristik minimal yang harus dipenuhi oleh penyedia jasa TI yang akan digunakan seperti pengalaman, arsitektur TI dan sistem, pengendalian proses, kondisi keuangan, dan referensi mengenai reputasi.

d. Pemantauan dan pelaporan meliputi kriteria yang akan digunakan dalam pemantauan dan pelaporan baik untuk Bank maupun untuk pihak ketiga.

e. Persyaratan yang harus dipenuhi baik dari sisi sistem, data maupun pelatihan personel saat transisi atau migrasi ke sistem yang disediakan pihak penyedia jasa TI.

f. Jangka waktu, penghentian, dan isi minimal dari perjanjian.

g. Perlindungan perjanjian terhadap kewajiban seperti pembatasan kewajiban dan ganti rugi serta asuransi.

Dalam hal penyelenggaraan kegiatan atau fungsi yang didefinisikan tersebut dipertimbangkan untuk dilakukan oleh pihak terkait Bank maka manajemen Bank harus memastikan bahwa persiapan yang dilakukan tidak berbeda apabila akan dilakukan oleh pihak tidak terkait dengan Bank.

3. Permintaan *Proposal*

Proses pemilihan penyedia jasa TI dimulai dengan permintaan *proposal* dari penyedia jasa TI. *Proposal* yang diajukan harus menjelaskan secara rinci kebutuhan Bank seperti cakupan dan jenis pekerjaan yang akan dilakukan, ekspektasi tingkat

used and support for customer.

b. Service levels include availability and performance, change management, service quality, security, and business continuity.

c. The minimum characteristics that must be met by IT service providers to be used such as experience, IT architecture and systems, process control, financial conditions, and references to reputation.

d. Monitoring and reporting includes criteria that will be used in monitoring and reporting for both the Bank and third parties.

e. Requirements that must be met both in terms of systems, data and personnel training during transition or migration to systems provided by IT service provider.

f. Duration, termination and minimum content of the agreement.

g. Protection of agreements on obligations such as restrictions on liabilities and compensation and insurance.

In the event that the implementation of the defined activities or functions is considered to be carried out by the Bank's related parties, the Bank's management must ensure that the preparations made are not different if they will be carried out by the parties not related to the Bank.

3. Request for Proposal

The process of selecting an IT service provider begins with a request for proposal from IT service provider. The proposed proposal must explain in detail the needs of the Bank such as the scope and type of work to be performed,

layanan, jangka waktu penyelesaian, rincian biaya layanan, pengukuran pekerjaan dan pengendaliannya, pengamanan, dan kelangsungan bisnis.

Bank harus dapat memastikan kebijakan pihak penyedia jasa TI yang terkait dengan kepentingan audit penyelenggaraan TI Bank untuk akses auditor intern, ekstern, maupun Otoritas Jasa Keuangan. Dengan demikian, data dan informasi yang diperlukan dari penyelenggaraan TI tetap dapat diperoleh secara tepat waktu setiap kali dibutuhkan meskipun TI tidak diselenggarakan oleh Bank.

4. Uji Tuntas (*Due Diligence*) Penyedia Jasa TI

Uji tuntas (*due diligence*) perlu dilakukan untuk menilai reputasi, kemampuan teknis, kemampuan operasional, kondisi keuangan, rencana pengembangan, dan kemampuan mengikuti inovasi TI di pasar, agar Bank mendapatkan keyakinan bahwa penyedia jasa TI mampu memenuhi kebutuhan Bank.

Uji tuntas (*due diligence*) yang dilakukan Bank selama proses pemilihan harus didokumentasikan dengan baik dan dilakukan kembali secara berkala sebagai bagian dari proses pemantauan.

Pada saat uji tuntas (*due diligence*), Bank harus mempertimbangkan antara lain:

a. Eksistensi dan sejarah perusahaan penyedia jasa TI.

b. Kualifikasi, latar belakang, dan reputasi pemilik perusahaan penyedia jasa TI.

c. Perusahaan lain yang menggunakan jasa yang sama dari penyedia jasa TI sebagai referensi.

d. Kemampuan dan efektivitas pemberian jasa, termasuk dukungan purna jual.

e. Teknologi dan arsitektur sistem

service level expectations, completion period, details of service costs, measurement of work and control, security, and business continuity.

Banks must be able to ensure the policies of IT service providers related to the audit interests of IT Bank operations for access to internal, external, and OJK. Thus, the data and information needed from the implementation of IT can still be obtained in a timely manner whenever needed even though IT is not held by the Bank.

4. Due Diligence of IT Service Provider

Due diligence needs to be done to assess reputation, technical capability, operational capability, financial condition, development plan, and ability to follow IT innovations in the market, so that the Bank can be assured that IT service providers are able to meet the Bank's needs.

Due diligence conducted by the Bank during the selection process must be well documented and periodically carried out as part of the monitoring process.

At the time of due diligence, the Bank must consider, among others:

a. The existence and history of IT service provider.

b. Qualifications, background, and owner reputation of IT service provider.

c. Other companies that use the same services from IT service providers as references.

d. Ability and effectiveness of service delivery, including support after sales.

e. Technology and system

architecture.

f. Lingkungan pengendalian intern, sejarah pengamanan, dan cakupan audit.

f. Internal control environment, security history, and audit scope.

g. Kepatuhan terhadap hukum dan ketentuan peraturan perundang-undangan.

g. Compliance with laws and statutory provisions.

h. Kepercayaan dan keberhasilan dalam berhubungan dengan sub kontraktor.

h. Trust and success in dealing with sub-contractor.

i. Jaminan pemeliharaan.

i. Maintenance guarantee.

j. Kemampuan untuk menyediakan pemulihan bencana dan keberlanjutan bisnis.

j. The ability to provide disaster recovery and business continuity.

k. Penerapan manajemen risiko.

k. Implementation of risk management.

l. Laporan hasil pemeriksaan pihak independen.

l. Report of audit result.

m. Kondisi keuangan termasuk kaji ulang atas laporan keuangan yang telah diaudit.

m. Financial report include a review of audited financial statement.

n. Kualifikasi dan kompetensi sumber daya manusia yang dimiliki oleh penyedia jasa TI.

n. Qualifications and competencies of human resources owned by IT service providers.

o. Kemampuan pihak penyedia jasa TI dalam memberikan harga terbaik untuk layanan jasa yang disediakan.

o. The ability of the IT service provider to provide services with the best price that may offered.

5. Penentuan Penyedia Jasa TI

Dalam menentukan penyedia jasa TI:

5. Selection of IT Service Provider

In select IT service provider:

a. Bank harus melakukan evaluasi atas penerapan manajemen risiko pihak penyedia jasa TI secara berkala untuk memastikan penggunaan pihak penyedia jasa TI tidak mengurangi tanggung jawab Bank dalam menerapkan manajemen risiko.

a. Bank must conduct a periodical evaluation for the implementation of risk management for IT service provider to ensure the use of IT service provider is not reducing Bank responsibility in implement risk management.

b. Bank harus memastikan bahwa laporan yang diperlukan untuk memantau kinerja pihak penyedia jasa TI telah memadai.

b. The Bank must ensure that the reports needed to monitor the performance of the IT service provider are adequate.

c. Bank dan Divisi TI harus

c. The Bank and IT Division must

melakukan analisis biaya dan manfaat untuk setiap alternatif yang akan dipilih.

conduct a cost and benefit analysis for each alternative that will be selected.

d. Bank harus memastikan bahwa pihak penyedia jasa TI dapat menyampaikan hasil audit atas penyediaan jasa TI yang dilakukan oleh pihak independen.

(Terutama untuk penyediaan jasa IT terkait Penyediaan Jasa yang sifatnya kritikal, seperti Data Center/Data Recovery Center, kecuali ada tambahan penjelasan dari regulator di kemudian hari)

d. Banks must ensure that the IT service provider can submit the results of the audit on the provision of IT services carried out by an independent party. (Especially for the provision of IT services related to services that are critical, such as Data Centers/Data Recovery Centers, unless there is additional explanation from the regulator at a later date)

e. Bank dapat memperoleh informasi dari berbagai sumber termasuk laporan tahunan pihak penyedia jasa TI dalam rangka memantau dan mengevaluasi kehandalan pihak penyedia jasa TI secara berkala, baik yang menyangkut kinerja, reputasi penyedia jasa TI, dan kelangsungan penyediaan layanan.

e. Banks can obtain information from various sources including the annual report of the IT service provider in order to monitor and evaluate the reliability of IT service provider on a regular basis, both concerning performance, IT service provider reputation, and continuity of service provision.

f. Bank harus memastikan akses terhadap Pangkalan Data (*Database*) dapat dilakukan oleh Otoritas Jasa Keuangan setiap saat baik untuk data terkini maupun untuk data yang telah lalu.

f. The Bank must ensure access to the Data Base (Database) can be carried out by the OJK at any time both for the latest data and for past data.

g. Bank harus menerapkan hubungan kerja sama secara wajar *(arm's length principle*) dengan pihak penyedia jasa TI termasuk pihak terkait dengan Bank. Bank harus melakukan proses seleksi dan didokumentasikan.

g. The Bank must implement a fair relationship (arm's length principle) with IT service provider including parties related to the Bank. Banks must carry out the selection process and be documented.

6. Perjanjian Kerja Sama dengan Penyedia Jasa TI

6. Agreement with IT Service Provider

Setelah memilih sebuah perusahaan penyedia jasa TI, manajemen membuat perjanjian tertulis dengan penyedia jasa TI sesuai standar perjanjian Bank. Dalam menyusun perjanjian, Bank harus memperhatikan hal-hal sebagai berikut:

After choosing an IT service provider company, management makes a written agreement with IT service providers according to the Bank's agreement standards. In preparing the agreement, the Bank must pay attention to the following matter:

a. Isi perjanjian sesuai dengan standar perjanjian Bank.

b. Melalui proses pembahasan dengan seksi Legal.

c. Mempertimbangkan adanya klausula khusus untuk pemutusan perjanjian sebelum berakhirnya perjanjian apabila penyedia jasa TI wanprestasi.

7. Klausula Khusus

a. Dalam perjanjian yang dibuat antara Bank dengan penyedia jasa TI harus dicantumkan klausula khusus sebagaimana mengacu pada Lampiran I mengenai kemungkinan mengubah, membuat perjanjian baru, atau mengambil alih kegiatan yang diselenggarakan oleh pihak penyedia jasa TI atau menghentikan perjanjian sebelum berakhirnya perjanjian. Termasuk dalam hal ini atas permintaan Otoritas Jasa Keuangan apabila diperlukan dengan pertimbangan bahwa penyelenggaraan oleh pihak penyedia jasa TI dapat mengganggu pelaksanaan tugas Otoritas Jasa Keuangan

b. Guna mengukur risiko selama penyelenggaraan layanan, terutama jika terdapat kondisi perubahan yang signifikan pada organisasi pihak penyedia jasa TI, Bank wajib melakukan penilaian ulang materialitas atas pihak penyedia jasa TI. Jika dari penilaian ulang materialitas tersebut didapat temuan kondisi sebagai berikut:

1) Hasil penilaian ulang materialitas menunjukan bahwa penyelenggaraan penyedia jasa TI berpotensi tidak berjalan efektif.

2) Memburuknya kinerja layanan TI oleh pihak penyedia jasa TI yang dapat berdampak signifikan pada kegiatan

a. Agreement in accordance with Bank agreement standard.

b. Through the process of discussion with Legal section.

c. Consider the existence of a special clause for termination of the agreement before the end of the agreement if the IT service provider default.

7. Special clause

a. In agreements made between the Bank and IT service providers, special clauses must be included as refer to Appendix I regarding the possibility of changing, entering into a new agreement, or taking over activities carried out by the IT service provider or terminating the agreement before the end of the agreement. Included in this case at the request of the OJK if necessary with the consideration that the implementation of the IT service provider may interfere with the implementation of the duties of the OJK.

b. In order to measure risks during services delivery, especially if there are significant changes inside IT service provider's organization, the Bank is required to reassess the materiality of the IT service provider. If the reassessment of materiality finds the following conditions:

1) The results of the materiality reassessment show that the implementation of IT service providers has the potential to be ineffective.
2) The deteriorating performance of IT services by IT service provider that can have a significant impact on the

usaha Bank.

3) Tingkat solvabilitas pihak penyedia jasa TI tidak memadai, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan.

4) Terdapat pelanggaran terhadap ketentuan peraturan perundang-undangan mengenai rahasia Bank dan data pribadi nasabah.

5) Terdapat kondisi yang menyebabkan Bank tidak dapat menyediakan data yang diperlukan dalam rangka pengawasan yang efektif oleh Otoritas Jasa Keuangan.

6) Terdapat potensi munculnya gangguan atau terhentinya penyediaan jasa TI untuk Bank.

Pada temuan kondisi sebagaimana yang dimaksud diatas, maka Bank harus melakukan hal-hal:

1) Melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah kondisi tersebut di atas diketahui oleh Bank.

2) Memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penggunaan jasa TI apabila diperlukan.

3) Melaporkan kepada Otoritas Jasa Keuangan paling lama 3 hari kerja setelah Bank menghentikan penggunaan jasa TI sebelum berakhirnya jangka waktu perjanjian.

c. Untuk menjaga kelangsungan usaha Bank dalam hal

Bank's business activities.

3) The solvency level of IT service provider is inadequate, in the process of going to liquidation, or bankrupt by the court.

4) There is a violation of the provisions of the legislation concerning bank secrets and customers' personal data.

5) There are conditions that cause the Bank to not be able to provide the data needed for effective supervision by the OJK.

6) There is a potential for disruption or obstruction to the provision of IT services to the Bank.

In the event that the Bank finds the matters referred to above, the Bank must conduct the following:

1) Report to the OJK at the latest 3 (three) working days after the conditions mentioned above are known by the Bank.

2) Decide on the follow-up that will be taken to overcome the problem, including the termination of the use of IT services if needed.

3) Report to the OJK max. 3 working days after the Bank stops using IT services before the end of the agreement period.

c. To maintain the continuity of the Bank's business in the

penghentian penggunaan jasa TI dilakukan sebelum berakhirnya perjanjian maka Bank harus memiliki rencana tindak lanjut yang teruji dan memadai (*contingency plan*) dalam keadaan kahar (*force majeure*).

event that the termination of the use of IT services is carried out before the end of the agreement, the Bank must have a proven and adequate follow-up plan (force majeure).

d. Dalam hal Bank akan menghentikan penggunaan pihak penyedia jasa TI, Bank wajib:
   1) Menyusun rencana penghentian penggunaan pihak penyedia jasa TI;
   2) Melakukan penilaian atas kelangsungan layanan dan data terkait dengan kegiatan yang diserahkan kepada pihak penyedia jasa TI serta pengujianatau simulasi terhadap kelangsungan kegiatan usaha dan/atau operasional Bank; dan
   3) Memastikan penghentian penggunaan pihak penyedia jasa TI tidak menimbulkan gangguan pada kegiatan usaha dan/atau operasional Bank.

d. In the event that the Bank will stop the use of IT service providers, the Bank must:
   1) Prepare a plan to stop the use of IT service providers;
   2) Conduct an assessment of the continuity of services and data related to the activities submitted to the IT service provider as well as testing or simulating the continuity of the Bank's business activities and/or operations; and
   3) Ensure that the termination of the use of IT service providers does not cause disruption to the Bank's business activities and/or operations.

8. Penilaian Kinerja dan Kepatuhan

8. Performance and Compliance Assessment

Selama penggunaan layanan penyedia jasa TI, Bank berhak untuk melakukan penilaian kinerja dan kepatuhan yang sudah dijalankan oleh penyedia jasa TI selama periode pelaksanaan pekerjaan berlangsung. Pemantauan ini dilaksanakan untuk menghindari terjadinya risiko kepatuhan atau ketidaksesuaian pelaksanaan dengan perjanjian dan SLA yang disepakati. Hal yang perlu diperhatikan oleh Bank antara lain :

During the use of IT service providers, the Bank has the right to carry out performance and compliance assessments that have been carried out by IT service providers during the period of implementation of the work. This monitoring is carried out to avoid the risk of compliance or non-compliance with the agreed agreements and SLAs. Things that need to be considered by the Bank include:

a. Pemantauan dan evaluasi keandalan pihak penyedia jasa TI yang secara berkala terkait kinerja, reputasi pihak penyedia jasa TI, dan kelangsungan penyediaan layanan.

a. Monitoring and evaluating the reliability of the IT service provider on a regular basis related to the performance, reputation of the IT service provider, and continuity of service provision.

b. Penerapan pengendalian TI

b. Implementation of adequate IT

secara memadai oleh pihak penyedia jasa TI, yang dibuktikan dengan hasil audit dan/atau penilaian yang dilakukan oleh pihak independen.

c. Penyelenggaraan layanan dan pelaksanaan tanggung jawab oleh pihak penyedia jasa TI sudah sesuai dengan perjanjian tingkat layanan antara Bank dan pihak penyedia jasa TI.

9. Penggunaan Penyedia Jasa TI di Luar Wilayah Indonesia

Bank yang merencanakan penggunaan penyedia jasa TI di luar wilayah Indonesia tidak boleh menghambat pengawasan atau pemeriksaan oleh Otoritas Jasa Keuangan. Sama halnya dengan penggunaan penyedia jasa TI domestik, penggunaan jasa TI pihak asing atau yang berlokasi di luar wilayah Indonesia harus melalui prosedur yang sama yaitu mulai dari uji tuntas, pemilihan penyedia jasa TI, pembuatan perjanjian dan pengawasan, namun karena terkait dengan perbedaan yurisdiksi maka terdapat persyaratan lain yang harus diperhatikan oleh Bank. Penggunaan pihak penyedia jasa TI di luar wilayah Indonesia harus terlebih dahulu mendapatkan persetujuan Otoritas Jasa Keuangan.

control by IT service providers, as evidenced by the results of audits and/or assessments conducted by independent parties.

c. The implementation of services and the implementation of responsibilities by the IT service provider is in accordance with the service level agreement between the Bank and the IT service provider.

9. Use of IT Services Provider Outside Indonesian Territory

Bank that plan the use of IT service provider outside the territory of Indonesia may not hinder supervision or inspection by the OJK. As with the use of domestic IT service providers, the use of foreign party IT services or those located outside Indonesia must go through the same procedures, from due diligence, selection of IT service provider, agreement and supervision, but because they are related to different jurisdictions there are other requirements that must be attention by the Bank. The use of IT service provider outside the Indonesian territory must first obtain the approval of the OJK.

IV. MANAJEMEN RISIKO DALAM PENGGUNAAN PIHAK PENYEDIA JASA TI

A. Identifikasi Risiko

Identifikasi risiko paling sedikit memperhatikan hal-hal sebagai berikut:

1. Penggunaan pihak penyedia jasa TI lain dalam menyelenggarakan TI Bank dapat memberikan kontribusi terhadap beberapa jenis risiko, yaitu:
   a. Risiko operasional yaitu ketidakmampuan penyedia jasa TI dalam memenuhi perjanjian
   b. Risiko hukum yaitu ketidakpastian hukum atas perselisihan dengan pihak penyedia jasa TI, pihak ketiga, dan/atau tuntutan nasabah atas penyalahgunaan data nasabah oleh pihak penyedia jasa TI
   c. Risiko reputasi yaitu ketidakpuasan nasabah karena ketidakmampuan penyedia jasa TI memenuhi SLA;
   d. Risiko stratejik yaitu ketidakcocokan TI yang digunakan Bank dengan tujuan dan rencana strategis Bank yang dibuat untuk mencapai tujuan tersebut
   e. Risiko kepatuhan yaitu ketidakmampuan Bank memenuhi ketentuan peraturan perundang-undangan
   f. Risiko negara (*country risk*) – kondisi di negara asing yang dapat mempengaruhi kemampuan penyedia jasa TI dalam memenuhi standar pemberian jasa.
2. Dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko, Bank harus mempertimbangkan
   a. Terkait dengan aktivitas dan fungsi yang diselenggarakan oleh pihak penyedia jasa TI meliputi sensitivitas data yang

IV. RISK MANAGEMENT IN PROCUREMENT OF GOODS AND SERVICES RELATED IT

A. Risk Identification

Risk identification at least consider the following:

1. The use of other IT service providers in conducting IT Banks can contribute to several types of risks, such as:
   a. Operational risk is the inability of IT service provider to fulfill the agreement.
   b. Legal risk is legal uncertainty over disputes with IT service provider, third party, and/or customer demands for misuse of customer data by IT service provider.
   c. Reputation risk is customer dissatisfaction due to the inability of IT service provider to meet the SLA
   d. Strategic risk is the incompatibility of IT used by the Bank with the Bank's strategic objectives and plans that are made to achieve these objectives.
   e. Compliance risk is the inability of the Bank to comply with the provisions of laws and regulations.
   f. Country risk - conditions in a foreign country that can affect the ability of IT service providers to meet service delivery standards.
2. In identifying, measuring, monitoring and controlling risks, the Bank must consider:
   a. Related to the activities and functions held by IT service providers, the sensitivity of data accessed, protected, or

diakses, dilindungi, atau dikendalikan oleh penyedia jasa TI, volume transaksi, dan tingkat pentingnya aktivitas dan fungsi tersebut terhadap bisnis Bank.

b. Terkait dengan penyedia jasa TI seperti misalnya kondisi keuangan, kompetensi tenaga kerja, perputaran manajemen dan tenaga kerja, pengalaman pihak penyedia jasa TI, dan profesionalitas.

c. Terkait dengan teknologi yang digunakan meliputi keandalan (*reliability*), keamanan (*security*), ketersediaan (*availability*), dan ketepatan waktu (*timeliness*) serta kemampuan mengikuti perkembangan teknologi.

d. Perubahan ketentuan peraturan perundang-undangan.

controlled by IT service providers, transaction volume, and the level of importance of these activities and functions to the Bank's business.

b. Associated with IT service providers such as financial conditions, workforce competencies, management turnover and workforce, experience of IT service providers, and professionalism

c. Associated with the technology used includes reliability, security, availability and timeliness and the ability to keep abreast of technological developments

d. Changes to the provisions of the legislation.

B. Pengukuran Risiko

Setelah risiko diidentifikasi, Bank harus mengukur risiko tersebut untuk mengetahui tingkat risiko yang dihadapi. Pengukuran risiko penggunaan penyedia jasa TI harus terintegrasi dengan pengukuran risiko terkait TI lainnya dengan menggunakan pendekatan pengukuran risiko yang sama.

Hasil pengukuran risiko penggunaan penyedia jasa TI ini harus menghasilkan suatu tingkat risiko yang selanjutnya menjadi salah satu parameter untuk penilaian risiko TI Bank secara keseluruhan.

B. Risk Measurement

After the risk is identified, the Bank must measure the risk to determine the level of risk faced. The measurement of the risk of using IT service provider must be integrated with other IT-related risk measurement using the same risk measurement approach.

The results of measuring the risk of using this IT service provider must result in a level of risk which then becomes one of the parameters for the Bank's overall IT risk assessment.

C. Mitigasi Risiko

Dari hasil pengukuran risiko, Bank mengetahui tingkat risiko yang dihadapi. Selanjutnya, Bank harus menetapkan strategi mitigasi risiko sesuai dengan tingkat risiko tersebut. Tindakan mitigasi risiko yang dilakukan Bank harus efektif untuk mengendalikan risiko.

1. Contoh tindakan mitigasi risiko yang dapat dilakukan Bank antara lain menerapkan kontrol untuk mengurangi kemungkinan terjadinya

C. Risk Mitigation

From the results of risk measurement, the Bank knows the level of risk faced. Furthermore, the Bank must establish a risk mitigation strategy in accordance with the level of risk. Risk mitigation measures undertaken by the Bank must be effective for controlling risks.

1. Examples of risk mitigation actions that can be carried out by the Bank include applying controls to reduce the possibility of risk occurrence, such as:

risiko, seperti:

a. Perjanjian penyedia jasa TI yang memadai

b. Memantau kinerja penyedia jasa secara berkala

c. Pemilihan penyedia jasa TI yang andal

2. Tindakan mitigasi risiko lainnya adalah mengurangi dampak kerugian apabila risiko yang telah diidentifikasi terjadi seperti asuransi dan Rencana Pemulihan Bencana.

3. Bank harus memastikan bahwa risiko ketergantungan pada pihak penyedia jasa TI dapat dimitigasi sehingga Bank tetap mampu menjalankan bisnisnya apabila penyedia jasa TI mengalami wanprestasi, pemutusan hubungan, atau dalam proses likuidasi. Mitigasi risiko yang dapat dilakukan mencakup:

a. Memastikan bahwa pihak penyedia jasa TI memiliki Rencana Pemulihan Bencana sesuai dengan jenis, cakupan dan kompleksitas aktivitas atau jasa yang diberikan.

b. Secara aktif mendapatkan jaminan kesiapan Rencana Pemulihan Bencana milik pihak penyedia jasa TI seperti pengujian secara berkala atas Rencana Pemulihan Bencana.

c. Memiliki perjanjian penyimpanan program kode sumber (*escrow agreement)*, jika Bank tidak memiliki kode sumber dari program aplikasi yang diselenggarakan oleh pihak penyedia jasa TI.

d. Pemberian jaminan dari penyedia jasa TI kepada Bank bahwa kelangsungan aplikasi didukung oleh pejabat pengembang perangkat lunak dalam hal kode sumber tidak dimiliki oleh penyedia jasa TI.

a. An adequate IT service provider agreement

b. Monitor the performance of service providers regularly

c. Selection of reliable IT service provider

2. Other risk mitigation measures are reducing the impact of losses if the identified risks have occurred such as insurance and Disaster Recovery Plan

3. The Bank must ensure that the risk of dependence on IT service provider can be mitigated so that the Bank is still able to run its business if the IT service provider experiences default, termination, or in the process of liquidation. Risk mitigation that can be done includes

a. Ensure that IT service provider have a Disaster Recovery Plan according to the type, scope and complexity of the activities or services provided.

b. Actively secure the readiness of the IT service providers' Disaster Recovery Plans such as periodic testing of the Disaster Recovery Plan

c. Have an agreement to save the source code program (escrow agreement), if the Bank does not have the source code of the application program organized by the IT service provider.

d. Providing guarantees from IT service providers to the Bank that the continuity of the application is supported by software developer officials in the event that the source code is not owned by IT service provider.

4. Dalam rangka menjamin fungsi dan efektifivitas Rencana Pemulihan Bencana, Bank harus menyusun dan melakukan pengujian Rencana Pemulihan Bencana secara berkala, lengkap, dan mencakup hal-hal yang signifikan yang didasarkan atas jenis, cakupan, dan kompleksitas aktivitas atau kegiatan yang dilakukan oleh penyedia jasa TI. Disamping itu pihak penyedia jasa TI harus melakukan pengujian Rencana Pemulihan Bencana di pihak penyedia jasa sendiri untuk sistem atau fasilitas TI maupun pemrosesan transaksi yang diselenggarakan tanpa melibatkan pihak Bank. Hasil pengujian Rencana Pemulihan Bencana oleh pihak penyedia jasa TI tersebut digunakan Bank untuk mengkinikan Rencana Pemulihan Bencana yang dimiliki Bank.

4. In order to guarantee the function and effectiveness of the Disaster Recovery Plan, the Bank must prepare and test the Disaster Recovery Plan periodically, completely, and cover significant matters based on the type, scope and complexity of the activities or activities carried out by the service provider IT. In addition, IT service providers must test the Disaster Recovery Plan on their own service provider for IT systems or facilities as well as transaction processing carried out without involving the Bank. The results of the testing of the Disaster Recovery Plan by the IT service providers were used by the Bank to update the Disaster Recovery Plan owned by the Bank.

D. Pengendalian Risiko Lainnya

Meskipun Bank maupun pihak penyedia jasa TI sudah menggunakan sistem yang canggih namun masih memungkinkan adanya penyimpangan misalnya kesalahan manusia, penerapan prosedur yang lemah dan pencurian oleh pegawai. Bank harus memastikan adanya pengendalian pengamanan untuk memitigasi risiko dan mencakup hal-hal:

1. Pihak penyedia jasa TI harus melakukan penelitian latar belakang para pegawainya.

2. Memastikan kewajiban pihak penyedia jasa TI melakukan pengendalian keamanan terhadap seluruh fasilitas TI yang digunakan dan data yang diproses serta informasi yang dihasilkan telah dicantumkan dalam perjanjian.

3. Memastikan pihak penyedia jasa TI memahami dan dapat memenuhi tingkat pengamanan yang dibutuhkan Bank untuk masing-masing jenis data berdasarkan sensitivitas kerahasiaan data.

4. Memastikan biaya yang dikeluarkan untuk masing-masing pengamanan sebanding dengan tingkat pengamanan yang dibutuhkan dan sesuai dengan tingkat toleransi risiko

D. Other Risk Control

Even though the Bank and IT service providers have used sophisticated systems but still allow irregularities such as human error, the application of weak procedures and theft by employees. The bank must ensure that there are security controls to mitigate risks and cover following matter:

1. The IT service provider must research the background of its employees.

2. Ensuring the obligation of the IT service providers to control the security of all IT facilities used and the data processed and the information produced has been included in the agreement.

3. Ensure that IT service providers understand and can meet the level of security required by the Bank for each type of data based on data confidentiality sensitivity.

4. Ensure the costs incurred for each security are proportional to the level of security required and in accordance with the level of risk tolerance set by the Bank.

yang telah ditetapkan oleh Bank.

E. Pengendalian Intern dan Audit Intern

1. Pemantauan dan Pengawasan Penyedia Jasa TI.

   Dalam hal penyelenggaraan TI Bank dilakukan oleh pihak penyedia jasa TI, Bank tetap harus memiliki satuan kerja TI dan pejabat tertinggi yang memimpin satuan kerja TI.

   Bank harus memiliki program pemantauan untuk memastikan penyedia jasa TI telah melaksanakan pekerjaan atau memberikan jasa sesuai dengan perjanjian. Sumber daya untuk mendukung program ini dapat bervariasi tergantung pada kritikalitas dan kompleksitas sistem, proses, dan jasa yang dikerjakan penyedia jasa TI.

2. Audit Intern

   Bank melaksanakan fungsi audit terhadap pihak penyedia jasa TI secara berkala, baik dilakukan oleh Divisi Audit (SKAI) maupun pihak Audit ekstern yang ditunjuk oleh Bank. Ruang lingkup audit sesuai dengan cakupan jasa sebagaimana tertuang dalam perjanjian. Area yang diaudit antara lain:

   a. Sistem TI

   b. Keamanan data

   c. Kerangka kerja pengendalian intern

   d. Rencana Pemulihan Bencana

      Bank harus memastikan bahwa Otoritas Jasa Keuangan atau pihak lain yang ditugaskan oleh Otoritas Jasa Keuangan memiliki hak akses ke penyedia jasa TI untuk mendapatkan catatan dan dokumen transaksi, serta informasi Bank yang disimpan atau diproses oleh penyedia jasa TI serta hak akses terhadap laporan dan temuan audit terhadap penyedia jasa TI yang terkait dengan jasa TI.

E. Internal Control and Internal Audit

1. Monitoring and Supervision of IT Services Provider

   In the event that the implementation of Bank IT is carried out by an IT service provider, the Bank must still have an IT work unit and the highest official who leads the IT work unit.
   Banks must have a monitoring program to ensure IT service providers have carried out work or provided services in accordance with the agreement. Resources to support this program can vary depending on the criticality and complexity of the system, process, and services that conducted by IT service provider.

2. Internal Audit

   The Bank carries out audit functions on the part of IT service providers on a regular basis, both carried out by the Audit Division (SKAI) and the external Audit party appointed by the Bank. The scope of the audit is in accordance with the scope of services as stated in the agreement. Areas audited include:

   a. IT System

   b. Data security

   c. Internal control framework

   d. Disaster Recovery Plan

      The Bank must ensure that the OJK or other parties assigned by the Financial Services Authority have access rights to IT service providers to obtain transaction records and documents, as well as Bank information stored or processed by IT service providers and access rights to audit reports and findings against IT service providers related to IT services.

V. PENUTUP

Kebijakan Penggunaan Pihak Penyedia Jasa TI ini diterbitkan dalam 2 (dua) Bahasa yaitu Bahasa Indonesia dan Bahasa Inggris, dan bilamana terjadi perbedaan penafsiran antara keduanya maka yang menjadi acuan adalah Bahasa Indonesia.

Kebijakan Penggunaan Pihak Penyedia Jasa TI ini mulai berlaku sejak memperoleh persetujuan Presiden Direktur pada tanggal 24 Maret 2023 dan Dewan Komisaris pada tanggal 5 April 2023 serta mencabut Kebijakan Penggunaan Pihak Penyedia Jasa TI Edisi 2, November 2020.

Kebijakan Penggunaan Pihak Penyedia Jasa TI ini akan dikaji ulang secara berkala paling lambat setiap 2 (dua) tahun sekali atau jika diperlukan sebagai upaya penyempurnaan sesuai dengan perkembangan usaha dan kebutuhan Bank atau perubahan peraturan yang mendasarinya.

V. CLOSING

IT Service Provider Use Policy is establish in 2 (two) languages, Indonesian Language and English Language, and if there is a difference in the interpretation it will refer to Indonesian Language.

This IT Service Provider Use Policy is effective as obtain approval by President Director March 24th, 2023 and Board Of Commisioner April 5th, 2023 and revoke IT Service Provider Use Policy 2nd Edition, November 2020.

This IT Service Provider Use Policy will be reviewed periodically at least by 2 (two) times a year or if necessary as the efforts of improvement in accordance with the development of Bank's business and necessity or changes to the underlying regulatory.