Bank Resona Perdania

KEBIJAKAN PENGGUNAAN PIHAK PENYEDIA JASA TI
THE USE OF IT SERVICE PROVIDER POLICY

Edisi ke-4, Februari 2024

4th Edition, February 2024

BOD Approval No. 091/ITD/IT-PLN/V/2024

BOC Approval No. 073/BOC/VI/2024-ITD/IT-PLN

DAFTAR ISI
Table of Content

Bank Resona Perdania

I. PENDAHULUAN

A. Latar Belakang

Dalam rangka meningkatkan efektivitas dan efisiensi pencapaian tujuan strategis, Bank dimungkinkan menggunakan 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.

Bank yang menggunakan pihak penyedia jasa TI wajib memiliki kemampuan dalam melakukan pengawasan atas pelaksanaan kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa TI.

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. POJK No. 17 Tahun 2023 tentang Penerapan Tata Kelola Bagi Bank Umum;

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

   POJK ini dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.17 Tahun 2023 tentang Penerapan Tata Kelola Bagi Bank Umum.

3. 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;

I. INTRODUCTION

A. Background

To increase the effectiveness and efficiency of achieving strategic goals, the Bank can use IT service providers. What is meant by using the services of an IT service provider is the use of the services of another party in carrying out IT activities which can cause the Bank to become dependent on the services provided continuously or within a certain period of time.

Banks that use IT service providers are required to have the ability to supervise the implementation of Bank activities carried out by IT service providers.

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. References

1. POJK No. 17 of 2023 concerning Implementation of Governance for Commercial Banks;

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

   This POJK is declared still valid as long as it does not conflict with the provisions in POJK Number 17 of 2023 concerning the Implementation of Governance for Commercial Banks.

3. 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;

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

   POJK ini dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.17 Tahun 2023 tentang Penerapan Tata Kelola Bagi Umum;

5. SEOJK No. 34/SEOJK.03/2016 tanggal 1 September 2016 perihal Penerapan Manajemen Risiko Bagi Bank Umum.

6. 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.

7. 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.

8. POJK No.21 Tahun 2023 tentang Layanan Digital Bank Umum

9. SEOJK No.24/SEOJK.03/2023 tanggal 14 Desember 2023 Tentang Penilaian Tingkat Maturitas Digital Bank Umum

10. POJK No.8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme, Dan Pencegahan Pendanaan Proliferasi Senjata Pemusnah Massal Di Sektor Jasa Keuangan.

11. Kebijakan Tingkat Otorisasi

4. POJK No. 18/POJK.03/2016 about Implementation of Risk 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;

   This POJK is declared still valid as long as it does not conflict with the provisions in POJK Number 17 of 2023 concerning the Implementation of Governance for Commercial Banks;

5. SEOJK No. 34/SEOJK.03/2016 dated September 1, 2016 about Management for Commercial banks.

6. 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 Development of the Quality of Human Resources for Commercial Banks.

7. 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.

8. POJK No.21 of 2023 concerning Commercial Bank Digital Services

9. SEOJK No.24/SEOJK.03/2023 dated 14 December 2023 concerning Assessment of Digital Maturity Levels of Commercial Banks

10. POJK No.8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector

11. Levelling Authority Policy

12. Kebijakan Manajemen Risiko Teknologi Informasi
13. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem dalam Penggunaan Teknologi Informasi
14. Kebijakan Manajemen Risiko Umum (Individual).
15. Kebijakan Manajemen Risiko Operasional.
16. Kebijakan Manajemen Risiko Hukum.
17. Kebijakan Manajemen Risiko Reputasi.
18. Kebijakan Manajemen Risiko Stratejik.
19. Kebijakan Manajemen Risiko Kepatuhan.
20. Kebijakan Manajemen Proyek dan Pengembangan Sistem.
21. Kebijakan Audit Intern Teknologi Informasi.
22. Kebijakan Tugas & Wewenang.
23. Kebijakan Uraian Pekerjaan.

C. Tujuan

1. Menetapkan prosedur yang mengatur proses penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI.
2. 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. Tata cara melakukan hubungan kerja sama dengan pihak penyedia jasa TI, mulai dari proses identifikasi kebutuhan sampai dengan proses pemilihan pihak penyedia jasa TI;
2. Proses manajemen risiko penggunaan pihak penyedia jasa TI;
3. Penilaian kinerja dan kepatuhan pihak penyedia jasa TI

12. Information Technology Risk Management Policy
13. Information Security and System Risk Management Policy in the use of Information Technology
14. Individual General Risk Management Policy
15. Operational Risk Management Policy.
16. Legal Risk Management Policy.
17. Reputation Risk Management Policy.
18. Strategic Risk Management Policy.
19. Compliance Risk Management Policy.
20. Project Management and System Development Policy.
21. Information Technology Internal Audit Policy.
22. Duties & Authorities Policy.
23. Job Description Policy.

C. Purpose

1. Define the procedures that govern the process of using IT service providers in IT Implementation.
2. 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. Cooperation procedures with IT service providers, starting from the requirement identification process to the IT service provider selection process;
2. Risk management process for using IT service providers;
3. IT service provider performance and compliance assessment procedures

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 OJK 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. Memastikan bahwa kontrak tertulis antara Bank dengan pihak penyedia jasa TI mencakup hal-hal yang diatur bagi penggunaan pihak penyedia jasa TI.
4. 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. Ensure that the written contract between the Bank and the IT service provider covers matters regulated regarding the use of the IT service provider
4. Monitoring and conduct a regular basis risk assessment of service provider by IT service provider.

III. PROSEDUR PENGGUNAAN PIHAK PENYEDIA JASA TI

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 kebijakan dan pedoman Bank yang berlaku.

A. Prinsip Penggunaan Pihak Penyedia Jasa TI

1. Bank tetap bertanggung jawab terhadap layanan TI yang diselenggarakan oleh pihak penyedia jasa TI;
2. Penggunaan penyedia jasa TI tidak menghambat proses pengawasan oleh OJK;
3. Keputusan penggunaan penyedia jasa TI harus sejalan dengan rencana strategis TI Bank;
4. Setiap penggunaan penyedia jasa TI harus dituangkan dalam perjanjian tertulis;
5. Penggunaan penyedia jasa TI harus memberikan manfaat lebih besar dibandingkan dengan biaya yang dikeluarkan Bank;
6. 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 dengan Bank;
7. Penggunaan penyedia jasa TI harus mendapat persetujuan manajemen;
8. Pemilihan penyedia jasa TI harus melalui proses uji tuntas;
9. Pemilihan penyedia jasa TI untuk layanan TI harus melalui proses seleksi dari beberapa penyedia jasa;
10. Perjanjian penyedia jasa TI harus memungkinkan adanya klausula kondisi pengakhiran perjanjian sesuai dengan masa perjanjian maupun sebelum masa perjanjian berakhir.

III. PROCEDURES FOR USING OF IT SERVICE PROVIDERS

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.

A. Principles For Use of IT Service Providers

1. Bank remains responsible for the IT services provided by the IT service provider;
2. The use of IT service providers does not hinder the supervision process by OJK;
3. The decision to use an IT service provider must be in line with the Bank's IT strategic plan;
4. Every use of an IT service provider must be stated in a written agreement;
5. The use of IT service providers must provide greater benefits than the costs incurred by the Bank;
6. The use of IT service providers must be based on a reasonable cooperative relationship (arm's length principle), in the event that the IT service provider is a party related to the Bank;
7. The use of IT service providers must be approved by management;
8. The selection of an IT service provider must go through a due diligence process;
9. Selection of IT service providers for IT services must go through a selection process from several service providers;
10. The IT service provider agreement must contain a clause regarding the conditions for ending the agreement in accordance with the term of the agreement or before the term of the agreement ends.

Dalam hal Bank melakukan Alih Daya atas pekerjaan penunjang pada alur kegiatan usaha Bank dan pada alur kegiatan pendukung usaha Bank, maka pekerjaan penunjang tersebut paling sedikit memenuhi kriteria :

1. Berisiko rendah;
2. Tidak membutuhkan kualifikasi kompetensi yang tinggi di bidang perbankan;
3. Tidak terkait langsung dengan proses pengambilan keputusan yang mempengaruhi operasional Bank.

In the event that a bank outsources supporting work in the flow of Bank business activities and the flow of Bank business support activities, then the supporting work at least following criteria below :

1. Low risk;
2. Does not require high competency qualifications in the banking sector;
3. Not directly related to the decision-making process that affects Bank operations.

B. Proses Pemilihan Penyedia Jasa TI

1. Identifikasi Kebutuhan

Sebelum menggunakan pihak penyedia jasa TI, Bank harus mendefinisikan terkait kebutuhan bisnis, diantaranya melalui:

1. Identifikasi secara spesifik mengenai fungsi atau aktivitas yang akan diserahkan penyelenggaraannya kepada pihak penyedia jasa TI;
2. Menyusun kriteria pihak penyedia jasa TI yang dibutuhkan;
3. Meneliti potensi calon pihak penyedia jasa TI;
4. Proses penilaian risiko yang dapat timbul akibat penyerahan penyelenggaraan fungsi atau aktivitas tersebut;
5. Penetapan dasar yang akan digunakan untuk mengidentifikasi pengukuran pengendalian yang memadai.

Pendefinisian kebutuhan tersebut akan 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:

1. Cakupan dan karakteristik dari layanan dan teknologi yang digunakan serta dukungan kepada Nasabah;
2. Tingkat layanan meliputi ketersediaan dan kinerja, manajemen perubahan *(change management)*, kualitas layanan, keamanan, dan kelangsungan usaha;
3. 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;
4. Pemantauan dan pelaporan meliputi kriteria yang akan digunakan dalam pemantauan dan pelaporan baik untuk Bank maupun untuk pihak ketiga;

B. IT Service Providers Selection Process

1. Requirement Identification

Before using an IT service provider, the Bank must determine related business needs, including through:

1. Specific identification of functions or activities to be assigned to the IT service provider;
2. Arrange criteria for required IT Service Providers;
3. Assess the potential of IT service providers;
4. Risk assessment process that may arise as a result of the delivery of the function or activity;
5. Determining the basis that will be used to identify adequate control measures

The requirements definition will produce a document containing a detailed description of the Bank's wishes for the services to be provided by the IT service provider. The content of the document includes the following components:

1. The scope and characteristics of the services and technology used and their support to Customers;
2. Service levels include availability and performance, change management, service quality, security and business continuity;
3. Minimum characteristics that must be met by the IT service provider to be used, such as experience, IT and system architecture, process control, financial condition, and references regarding reputation;
4. Monitoring and reporting includes the criteria that will be used in monitoring and reporting for both the Bank and third parties;

5. Persyaratan yang harus dipenuhi baik dari sisi sistem, data maupun pelatihan personel saat transisi atau migrasi ke sistem yang disediakan pihak penyedia jasa TI;
6. Jangka waktu, penghentian, dan isi minimal dari perjanjian; dan
7. Perlindungan perjanjian terhadap kewajiban seperti pembatasan kewajiban dan ganti rugi serta asuransi.

2. 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 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 sendiri oleh Bank.

3. Uji Tuntas (Due Diligence)

Bank juga perlu melakukan uji tuntas *(due diligence)* 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.

Hal-hal yang perlu dipertimbangkan dalam proses uji tuntas *(due diligence)* antara lain :

1. Eksistensi dan sejarah perusahaan penyedia jasa TI;
2. Kualifikasi, latar belakang, dan reputasi pemilik perusahaan penyedia jasa TI;
3. Perusahaan lain yang menggunakan jasa yang sama dari penyedia jasa TI sebagai referensi;
4. Kemampuan dan efektivitas pemberian jasa, termasuk dukungan purna jual;
5. Teknologi dan arsitektur sistem;

5. Requirements that must be met in terms of systems, data and personnel training when transitioning or migrating to a system provided by an IT service provider;
6. Term, termination and minimum contents of the agreement; and
7. Liability protection agreements such as limitation of liability and compensation and insurance.

2. Proposal Request

The selection process for an IT service provider begins with a request for proposals from the service provider. Proposals must explain in detail the bank's requirements, such as the scope and type of work to be carried out, the level of expectations for services, the completion time period, details of service costs, measurement and control of work, security, and business continuity.

Banks must be able to ensure that IT service providers policies regarding audit needs for bank IT operations can be accessed by internal and external auditors and the Financial Services Authority. Therefore, the data and information required for IT operations can still be obtained on time whenever needed, even though IT is not managed by banks.

3. Due Diligence

Banks also need to do due diligence to assess the reputation of technical capabilities, operational capabilities, financial conditions, development plans, and ability to follow IT innovations in the market, so the Banks can gain confidence that IT service providers are able to fulfill Banks requirements.

Things that need to be considered in the due diligence process include:

1. Existence and history of IT service provider companies;
2. Qualifications, background and reputation of the owner of the IT service provider company;
3. Other companies that use the same services from the IT service provider as a reference;
4. Service delivery capabilities and effectiveness, including after-sales support;
5. Technology and system architecture;

6. Lingkungan pengendalian intern, sejarah pengamanan, dan cakupan audit;
7. Kepatuhan terhadap hukum dan ketentuan peraturan perundang-undangan;
8. Kepercayaan dan keberhasilan dalam berhubungan dengan sub kontraktor;
9. Jaminan pemeliharaan;
10. Kemampuan untuk menyediakan pemulihan bencana dan Keberlanjutan bisnis;
11. Penerapan manajemen risiko;
12. Laporan hasil pemeriksaan pihak independen;
13. Kondisi keuangan termasuk kaji ulang atas laporan keuangan yang telah diaudit.

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

4. Pemilihan Penyedia Jasa TI

Hal-hal yang harus diperhatikan dalam proses pemilihan penyedia jasa TI :

1. Kualifikasi dan kompetensi pihak penyedia jasa TI, termasuk sumber daya manusia yang dimiliki.
2. Analisis biaya dan manfaat dengan mengikutsertakan satuan kerja penyelenggara TI Bank;
3. Prinsip kehati-hatian dan manajemen risiko;
4. Prinsip hubungan kerja sama secara wajar jika pihak penyedia jasa TI merupakan pihak terkait dengan Bank. Bank harus melakukan proses seleksi dan didokumentasikan.

5. Perjanjian Kerjasama

Dalam melakukan hubungan kerjasama dengan pihak penyedia jasa TI, Bank wajib memiliki perjanjian kerjasama dengan pihak penyedia jasa TI dengan memperhatikan paling sedikit :

1. Kualifikasi dan kompetensi sumber daya manusia yang dimiliki pihak penyedia jasa TI;
2. Komitmen pihak penyedia jasa TI dalam menjaga kerahasiaan data dan/atau informasi Bank serta Nasabah Bank;
3. Komitmen pihak penyedia jasa TI untuk menyampaikan hasil audit TI secara berkala yang dilakukan auditor independen atas penyediaan jasa TI kepada Bank;
4. Pengalihan sebagian kegiatan atau subkontrak oleh pihak penyedia jasa TI dilakukan atas persetujuan Bank yang dibuktikan dengan dokumen tertulis;

6. Internal control environment, safeguards history, and audit coverage;
7. Compliance with laws and regulations;
8. Trust and success in dealing with sub contractors;
9. Maintenance guarantee;
10. Ability to provide disaster recovery and business continuity;
11. Implementation of risk management;
12. Independent inspection report;
13. Financial condition includes a review of audited financial reports.

The due diligence carried out by the Bank during the selection process must be documented properly and re-conducted periodically as part of the monitoring process.

4. Selection of IT Service Providers

The following should be considered in the IT Service providers selecting process :

1. Qualifications and competencies of IT service providers, including human resources.
2. Cost and benefit analysis involving the Bank's IT management work unit;
3. Principles of prudence and risk management;
4. Principles of a reasonable cooperative relationship if the IT service provider is a party that has a special relationship with the Bank. Banks must carry out a selection process and document it.

5. Cooperation Agreement

In establishing a cooperative relationship with an IT service provider, you must have a cooperation agreement with the IT service provider, at least by paying attention to:

1. Qualifications and competencies of human resources owned by IT service providers;
2. Commitment of IT service providers to maintain the confidentiality of Bank and Bank Customer data and/or information;
3. Commitment of IT service providers to submit the results of regular IT audits conducted by independent auditors regarding the provision of IT services to the Bank;
4. The transfer of part of the activities or subcontracts by the IT service provider is carried out with the approval of the Bank as evidenced by written documents;

5. Mekanisme pelaporan kejadian kritis oleh pihak penyedia jasa TI kepada Bank;
6. Mekanisme penghentian perjanjian kerja sama jika terdapat penghentian perjanjian sebelum jangka waktu perjanjian berakhir;
7. Pemenuhan ketentuan peraturan perundang-undangan atas penyediaan jasa TI oleh pihak penyedia jasa TI;
8. Kesediaan pihak penyedia jasa TI untuk memenuhi kewajiban dan/atau persyaratan yang dimuat dalam perjanjian kerja sama;
9. Kesediaan pihak penyedia jasa TI untuk memberikan akses kepada Otoritas Jasa Keuangan dan/atau pihak lain yang berwenang untuk melakukan pemeriksaan terhadap kegiatan penyediaan jasa TI yang diberikan sesuai dengan ketentuan peraturan perundang-undangan.

Dalam penyusunan perjanjian tertulis dengan penyedia jasa TI harus memerhatikan hal-hal sebagai berikut :
1. Isi penjanjian sesuai dengan standar perjanjian Bank;
2. Melalui proses pembahasan dengan satuan kerja hukum;
3. Mempertimbangkan adanya klausula khusus untuk pemutusan perjanjian sebelum berakhirnya perjanjian apabila penyedia jasa TI wanprestasi.

Standar isi perjanjian kerja sama dengan penyedia jasa TI, meliputi:
1. Cakupan pekerjaan atau jasa;
2. Biaya dan jangka waktu perjanjian kerja sama;
3. Hak dan kewajiban Bank maupun pihak penyedia jasa TI;
4. Jaminan pengamanan dan kerahasiaan data, terutama data Nasabah. Data hanya bisa diakses oleh pemilik data (Bank);
5. Jaminan tingkat pelayanan (SLA), berisi mengenai standar kinerja seperti tingkat pelayanan yang diperjanjikan *(service level)* dan target kinerja;
6. SLA tetap berlaku apabila terjadi perubahan kepemilikan baik pada Bank maupun penyedia jasa TI;
7. Laporan hasil pemantauan kinerja penyedia jasa TI yang terkait dengan SLA;
8. Batasan risiko yang ditanggung oleh Bank dan penyedia jasa TI, diantaranya:
   - risiko perubahan ruang lingkup perjanjian;

5. Critical incident reporting mechanism by IT service providers to the Bank;
6. Mechanism for terminating the cooperation agreement if the agreement is terminated before the agreement period ends;
7. Fulfillment of statutory provisions regarding the provision of IT services by IT service providers;
8. Willingness of the IT service provider to fulfill the obligations and/or requirements stated in the cooperation agreement;
9. Willingness of IT service providers to provide access to the Financial Services Authority and/or other authorized parties to carry out inspections of IT service provision activities provided in accordance with statutory provisions.

Following should be considered when making agreement with an IT service providers :
1. The contents of the agreement are in accordance with the Bank's agreement standards;
2. Through a discussion process with the legal work unit;
3. Consider a special clause to terminate the agreement before the end of the agreement if the IT service provider experiences default.

Standard contents of cooperation agreements with IT service providers include:
1. Scope of work or services;
2. Costs and term of the cooperation agreement;
3. Rights and obligations of Banks and IT service providers;
4. Guarantee security and confidentiality of data, especially customer data. Data can only be accessed by the data owner (Bank);
5. Service level guarantee (SLA), containing performance standards such as agreed service levels and performance targets;
6. The SLA remains in effect if there is a change in ownership of either the Bank or the IT service provider;
7. Report on the results of monitoring the performance of IT service providers regarding SLA;
8. Risk limits borne by the Bank and IT service providers, include:
   - risk of changes in the scope of the agreement;

- perubahan ruang lingkup bisnis dan organisasi perusahaan penyedia jasa TI;
- perubahan aspek hukum dan regulasi; dan
- aspek hukum yang meliputi hak cipta, paten dan logo atau merek *(trade mark)*;

9. 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;
10. 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;
11. 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;
12. Pengaturan mengenai pengamanan dalam pengiriman dokumen sumber *(source document)* yang diperlukan dari dan ke Pusat Data dan/atau Pusat Pemulihan Bencana. Pihak yang bertanggung jawab sebaiknya dilindungi asuransi yang cukup;
13. Kesediaan diaudit baik oleh intern Bank, OJK, dan/atau pihak ekstern yang ditunjuk oleh Bank maupun oleh OJK dan tersedianya informasi untuk keperluan pemeriksaan, termasuk hak akses, baik secara logic maupun fisik terhadap data yang dikelola oleh penyedia jasa TI;
14. 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);*
15. Pihak penyedia jasa TI harus melaporkan setiap kejadian penting *(critical)* yang dapat mengakibatkan kerugian keuangan dan/atau mengganggu kelancaran operasional Bank;

- changes in the business scope and organization of IT service provider companies;
- changes in legal and regulatory aspects; and

9. Approval from the Bank in the event that the IT service provider transfers some activities (subcontracting) to subcontractors. In addition, subcontractors must have adequate IT implementation standards;
10. Availability of communication facilities connected to the internet network as well as secure access and data transmission to and from the Data Center and/or Disaster Recovery Center;
11. Clear arrangements regarding data backup (back-up), policies for situations that threaten the continuity of Bank operations (contingency), protection of Bank data (record protection) including hardware, software and equipment, to ensure continuity of IT operations;
12. Arrangements regarding the security of sending required source documents to and from the Data Center and/or Disaster Recovery Center. Responsible parties must be covered by adequate insurance;
13. Willingness to be audited either by internal Bank, OJK, and/or external parties appointed by the Bank or by OJK and availability of information for audit purposes, including access rights, both logically and physically to data managed by IT service providers;
14. IT service providers are required to provide technical documents to the Bank related to the services provided by IT service providers, including IT process flow and Database structure;
15. IT service providers are required to report every important (critical) event that could result in financial losses and/or disrupt the smooth operation of the Bank;

16. 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 OJK melalui Bank yang bersangkutan;
17. Tanggung jawab penyedia jasa TI dalam menyediakan SDM yang memiliki kualifikasi dan kompetensi sesuai jasa yang disediakan agar operasional Bank tetap terjamin;
18. Rencana pelatihan SDM, baik jumlah yang dilatih, bentuk pelatihan maupun biaya yang diperlukan. Pihak penyedia jasa TI harus melakukan transfer ilmu kepada Bank, sehingga terdapat personel satuan kerja TI di Bank yang memahami TI yang digunakan Bank terutama mengenai alur proses TI dan struktur Pangkalan Data *(Database)* dari sistem yang disediakan oleh pihak penyedia jasa TI tersebut;
19. Kepemilikan dan lisensi;
20. Jaminan dari penyedia jasa TI bahwa penyediaan jasa masih akan diberikan kepada Bank selama periode tertentu setelah implementasi;
21. Perubahan, pengakhiran, atau pemutusan perjanjian termasuk dalam hal OJK memerintahkan Bank menghentikan penyediaan jasa TI sebelum berakhirnya jangka waktu perjanjian;
22. Sanksi dan penalti terhadap alasan-alasan yang tidak jelas terhadap pembatalan perjanjian dan pelanggaran isi perjanjian;
23. Kepatuhan pada hukum dan ketentuan peraturan perundang-undangan di Indonesia;
24. Standar pengamanan sistem yang harus dipenuhi oleh penyedia jasa TI;
25. Standar tingkat pelayanan yang harus dipenuhi oleh penyedia jasa TI;
26. Standar laporan pemantauan kinerja penyedia jasa TI; dan
27. Standar perjanjian penyimpanan dokumen *(escrow agreement).*

16. Specifically for the implementation of Data Centers, Disaster Recovery Centers and Information Technology-Based Transaction Processing, IT service providers are required to submit to the Bank the latest audited financial reports every year. IT service providers submit the results of IT audits carried out by independent auditors periodically regarding the implementation of Data Centers, Disaster Recovery Centers, and/or Information Technology Based Transaction Processing, to the OJK through the Bank concerned;
17. Responsibility of IT service providers in providing human resources who have qualifications and competencies in accordance with the services provided so that Bank operations remain guaranteed;
18. HR training plan, including the number of people to be trained, the form of training and the costs required. IT service providers must transfer knowledge to the Bank, so that there are IT work unit personnel at the Bank who understand the IT used by the Bank, especially regarding the IT process flow and system database structure provided by the IT service provider;
19. Ownership and licensing;
20. Guarantee from the IT service provider that the service will continue to be provided to the Bank for a certain period of time after implementation;
21. Changes, termination or termination of the agreement, including in the event that the OJK orders the Bank to stop providing IT services before the agreement period ends;
22. Sanctions and fines without clear reasons for canceling the agreement and violating the contents of the agreement;
23. Compliance with laws and regulations in Indonesia;
24. System security standards that must be met by IT service providers;
25. Service level standards that must be met by IT service providers;
26. Standards for IT service provider performance monitoring reports; and
27. Standard document storage agreement (escrow agreement).

Bank dalam penyelenggaraan layanan digital dapat menggunakan pihak penyedia jasa TI dalam proses verifikasi nasabah dan/atau calon nasabah secara tatap muka atau tidak tatap muka secara elektronik. Pihak penyedia jasa TI yang menyediakan jasa perangkat lunak dan/atau perangkat keras tersebut harus memenuhi kriteria dan persyaratan sebagai berikut :

1. Penyedia jasa TI merupakan perseroan terbatas atau koperasi yang tercatat, terdaftar, memiliki izin dan/atau memperoleh persetujuan dari Otoritas Jasa Keuangan;
2. Penyedia Jasa TI wajib memiliki perjanjian kerja sama dengan kementerian atau lembaga yang menyelenggarakan urusan kependudukan dan pencatatan sipil untuk memperoleh hak akses dan/atau memfasilitasi hak akses data kependudukan pada kementerian atau lembaga tersebut, sistem elektronik yang dimiliki oleh penyedia jasa TI terhubung dengan sistem elektronik terkait akses data kependudukan yang dimiliki oleh kementerian atau lembaga dimaksud.

Dalam hal Bank menggunakan pihak penyedia jasa TI sebagaimana dimaksud diatas, maka Bank wajib memiliki perjanjian kerja sama yang paling sedikit mencakup :

1. Nama, alamat, dan identitas para pihak;
2. Hak dan kewajiban para pihak;
3. Ruang lingkup perjanjian kerja sama;
4. Kepemilikan data pelaksanaan verifikasi sepenuhnya menjadi milik Bank;
5. Ketentuan mengenai pelindungan data Nasabah;
6. Mekanisme sharing data secara seamless dalam verifikasi melalui mekanisme pertemuan tatap muka secara elektronik dan/atau verifikasi melalui mekanisme tidak tatap muka antara Bank dan Pihak Penyedia Jasa TI;
7. Ketentuan terkait subkontrak yang mengatur bahwa Pihak Penyedia Jasa TI dapat melakukan pengalihan sebagian kegiatan (subkontrak) berdasarkan persetujuan Bank yang dibuktikan dengan dokumen tertulis;
8. Mekanisme pelaporan kejadian kritis yang diakibatkan kondisi kahar oleh pihak penyedia jasa TI pada Bank ;
9. Pengakhiran perjanjian; dan
10. Mekanisme untuk menyelesaikan perselisihan yang timbul antara Bank dan pihak penyedia jasa TI.

Banks in providing digital services can use IT service providers in the process of verifying customers and/or prospective customers electronically, both face-to-face and non-face-to-face. IT service providers providing software and/or hardware services must meet the following criteria and requirements:

1. IT service providers are limited liability companies or cooperatives that are registered, licensed and/or have received approval from the Financial Services Authority;
2. IT Service Providers are required to have a cooperation agreement with the ministry or institution that administers population and civil registration affairs to obtain access rights and/or facilitate access rights to population data at that ministry or institution. Electronic systems owned by IT service providers are connected to the system. electronically related to access to population data held by the relevant ministry or institution.

In the event that the Bank uses an IT service provider as referred to above, the Bank is required to have a cooperation agreement that at least contains:

1. Name, address and identity of the parties;
2. Rights and obligations of the parties;
3. Scope of the cooperation agreement;
4. Ownership of verification implementation data fully belongs to the Bank;
5. Provisions regarding Customer data protection;
6. Smooth data sharing mechanism for verification through electronic face-to-face meeting mechanisms and/or verification through non-face-to-face mechanisms between the Bank and IT Service Providers;
7. Provisions related to subcontracts which stipulate that the IT Service Provider can transfer part of the activities (subcontract) based on the Bank's approval as evidenced by written documents;
8. Mechanism for reporting critical incidents due to force majeure conditions by IT service providers at the Bank;
9. Termination of agreement; and
10. Mechanism for resolving disputes that arise between the Bank and IT service providers.

C. 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 OJK. 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 OJK.

D. Penghentian Penggunaan Pihak Penyedia Jasa TI

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 pengujian atau 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.

C. Use of IT Service Providers Outside Indonesian Territory

Banks that plan to use IT service providers outside Indonesian territory may not obstruct the supervision or inspection of the Financial Services Authority. As with the use of domestic IT service providers, the use of IT services from foreign parties or those located outside Indonesian territory must go through the same procedures, starting with due diligence, selecting an IT service provider, making agreements, and supervision. But because it is related to differences in jurisdiction, there are other requirements that the bank must pay attention to. The use of IT service providers outside the territory of Indonesia must first obtain approval from the Financial Services Authority.

D. Termination of Using IT Service Providers

In the event that the Bank will stop using an IT service provider, the Bank is obliged to:

1. Develop a plan to terminate the use of IT service providers;
2. Conduct an assessment of the continuity of services and data related to activities submitted to IT service providers as well as testing or simulating the continuity of the Bank's business and/or operational activities; 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.

IV. MANAJEMEN RISIKO PENGGUNAAN PIHAK PENYEDIA JASA TI

A. Penerapan Manajemen Risiko

Dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko, Bank harus mempertimbangkan:

a. Terkait dengan aktivitas dan fungsi yang diselenggarakan oleh penyedia jasa TI meliputi sensitivitas data yang 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; dan;
c. Terkait dengan teknologi yang digunakan meliputi keandalan *(reliability)*, keamanan *(security)*, ketersediaan *(availability),* dan ketepatan waktu *(timeliness)* serta kemampuan mengikuti perkembangan teknologi dan perubahan ketentuan peraturan perundang-undangan.

1. Identifikasi Risiko

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.

IV. RISK MANAGEMENT OF USE OF IT SERVICE PROVIDERS

A. Risk Management Implementation

In identifying, measuring, monitoring and controlling risks, the Bank must consider:

a. Related to the activities and functions carried out by the IT service provider including the sensitivity of the data accessed, protected or controlled by the IT service provider, the volume of transactions, and the level of importance of these activities and functions to the Bank's business;
b. Related to IT service providers, such as financial condition, workforce competency, workforce management and turnover, IT service provider experience, and professionalism; and
c. Regarding the technology used, including reliability, security, availability and timeliness as well as the ability to follow technological developments and changes in statutory provisions.

1. Risk Identification

a. Operational Risk, is the inability of the IT service provider to fulfill the agreement;
b. Legal Risk is legal uncertainty regarding disputes with IT service providers, third parties, and/or Customer claims for misuse of Customer data by IT service providers;
c. Reputation risk, namely customer dissatisfaction due to the inability of IT service providers to meet SLAs;
d. Strategic Risk is incompatibility of the IT used by the Bank with the Bank’s objective and the strategic plans made to achieve these objectives;
e. Compliance Risk is the Bank’s inability to comply with statutory provisions;
f. Country risk – conditions in a foreign country that may affect an IT service provider's ability to meet service delivery standards.

2. 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.

3. 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.

B. Penyediaan Rencana Pemulihan Bencana Yang Teruji dan Memadai

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.

C. Pemantauan Terkait Pemenuhan Keamanan Data

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 :

2. Risk Measurement

Once the risk is identified, the Bank is obliged to carry out risk measurements to determine the level of risk faced. Measuring the risk of using an IT service provider must be integrated with measuring other IT-related risks using the same risk measurement approach.

The result of measuring the risk of using an IT service provider must produce a risk level which then becomes one of the parameters for arressing the Bank's overall IT Risk

3. 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.

B. Provide a Tested and Adequate Disaster Recovery Plan

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.

C. Monitoring Related to Data Security

Even though banks and IT service providers use sophisticated systems, irregularities are still possible, for example human error, weak implementation of procedures, and theft by employees. Banks must ensure security controls are in place to mitigate risks and include:

a. Pihak penyedia jasa TI harus melakukan penelitian latar belakang para pegawainya;
b. 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;
c. Memastikan pihak penyedia jasa TI memahami dan dapat memenuhi tingkat pengamanan yang dibutuhkan Bank untuk masing-masing jenis data berdasarkan sensitivitas kerahasiaan data;
d. Memastikan biaya yang dikeluarkan untuk masing-masing pengamanan sebanding dengan tingkat pengamanan yang dibutuhkan dan sesuai dengan tingkat toleransi risiko yang telah ditetapkan oleh Bank.

a. IT service providers must conduct background research on their employees;
b. Ensure that the IT service provider's obligation to carry out security controls over all IT facilities used and the data processed and the resulting information has been stated in the agreement;
c. Ensure that IT service providers understand and can meet the level of security required by the Bank for each type of data based on the sensitivity of data confidentiality;
d. Ensure that the costs incurred for each security are proportional to the level of security required and in accordance with the risk tolerance level set by the Bank.

V. PENILAIAN KINERJA DAN KEPATUHAN PIHAK PENYEDIA JASA TI

A. Penilaian Kinerja Pihak Penyedia Jasa TI

Bank dalam melakukan penilaian kinerja dan kepatuhan memperhatikan paling sedikit :

1. Pemantauan dan Evaluasi keandalan pihak penyedia jasa TI secara berkala terkait kinerja, reputasi pihak penyedia jasa TI, dan kelangsungan penyediaan layanan.

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

3. Pemenuhan tingkat layanan sesuai dengan perjanjian tingkat layanan antara Bank dan pihak penyedia jasa 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.

Bank harus melakukan kaji ulang sebelum dan setelah pekerjaan penyedia jasa TI untuk memastikan bahwa kebijakan, standar, dan prosedur manajemen risiko Bank telah dilakukan secara efektif. Selanjutnya, *performance review* dan pencapaian SLA dilakukan secara berkala yang didokumentasikan dalam bentuk laporan. Pemantauan harus dilakukan terhadap laporan hasil pemeriksaan penyedia jasa TI.

Dalam hal terdapat perubahan yang signifikan terhadap organisasi dari pihak penyedia jasa TI, Bank wajib melakukan ulang materialitas terhadap pihak penyedia jasa TI.

Dalam hal terdapat kondisi berupa :

1. Hasil penilaian ulang materialitas menunjukkan bahwa kinerja pihak penyedia jasa TI berpotensi tidak berjalan dengan efektif;
2. Memburuknya kinerja penyelenggaraan TI oleh pihak penyedia jasa TI yang berpotensi menimbulkan dan/atau mengakibatkan

V. IT SERVICE PROVIDERS PERFORMANCE AND COMPLIANCE ASSESSMENT

A. Performace Assessment IT Service Providers

In conducting performance and compliance assessments, banks pay at least:

1. Regular monitoring and evaluation of the reliability of IT service providers regarding performance, reputation of IT service providers and continuity of service delivery.

2. Implementation of adequate IT controls by IT service providers as proven by the results of audits and/or assessments carried out by independent parties; and

3. Fulfillment of service levels in accordance with the service level agreement between the Bank and the IT service provider.

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 may vary depending on the criticality and complexity of the systems, processes, and services provided by the IT service provider.

Banks are required to conduct before and after reviews of IT service providers' work to ensure that the Bank's risk management policies, standards, and procedures have been implemented effectively. Furthermore, performance reviews and SLA achievements are carried out periodically and documented in the form of reports. Monitoring should be carried out on IT service provider inspection reports.

If there are significant changes to the IT service provider organization, the Bank is obliged to re-examine the materiality of the IT service provider.

If there are conditions such as:

1. The results of the materiality reassessment indicate that the IT service provider's performance is potentially ineffective;
2. Worsening IT implementation performance by IT service providers which has the potential to cause and/or have a significant

dampak yang signifikan pada kegiatan usaha dan/atau operasional Bank;
3. Pihak penyedia jasa TI menjadi insolven, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan;
4. Terdapat pelanggaran oleh pihak penyedia jasa TI terhadap ketentuan peraturan perundang-undangan mengenai rahasia Bank dan/atau data pribadi nasabah;
5. Terdapat kondisi yang menyebabkan Bank tidak dapat menyediakan data yang diperlukan untuk pengawasan oleh Otoritas Jasa Keuangan; dan/atau
6. Terdapat kondisi lain yang menyebabkan terganggunya atau terhentinya penyediaan jasa TI dari pihak penyedia jasa TI kepada Bank.

Maka Bank wajib melakukan tindakan tertentu :

1. Melaporkan kepada OJK paling lama 3 (tiga) hari kerja setelah kondisi sebagaimana dimaksud diatas diketahui oleh Bank;
2. Memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penggunaan pihak penyedia jasa TI dalam hal diperlukan; dan
3. Melaporkan kepada OJK paling lama 3 (tiga) hari kerja setelah Bank menghentikan penggunaan pihak penyedia jasa TI sebelum berakhirnya jangka waktu perjanjian, dalam hal Bank memutuskan untuk menghentikan penggunaan pihak penyedia jasa TI.

Dalam hal penggunaan pihak penyedia jasa TI atau rencana penggunaan pihak penyedia jasa TI menyebabkan atau diindikasikan akan menyebabkan kesulitan pengawasan yang dilakukan oleh OJK, OJK dapat:
1. Memerintahkan Bank untuk menghentikan penggunaan pihak penyedia jasa TI sebelum berakhirnya jangka waktu perjanjian; atau
2. Melarang rencana penggunaan pihak penyedia jasa TI oleh Bank.

impact on the Bank's business activities and/or operations;
3. The IT service provider is declared bankrupt, is in the process of liquidation, or is declared bankrupt by a court;
4. There is a violation by the IT service provider of the provisions of laws and regulations regarding the confidentiality of personal data of the Bank and/or customers;
5. There are conditions that cause the Bank to be unable to provide data required for supervision by the Financial Services Authority; and/or
6. There are other conditions that cause disruption or cessation of providing IT services from IT service providers to the Bank.

So the Bank is obliged to take certain actions:

1. Report to the OJK no later than 3 (three) working days after the condition referred to above becomes known to the Bank;
2. Decide what follow-up actions will be taken to resolve the problem, including terminating the use of the IT service provider if necessary; and
3. Report to the OJK no later than 3 (three) working days after the Bank stops using the IT service provider before the end of the agreement period, in the event that the Bank decides to stop using the IT service provider.

In the event that the use of an IT service provider or the planned use of an IT service provider causes or is indicated to cause difficulties in supervision carried out by the OJK, the OJK can:
1. Order the Bank to stop using the IT service provider before the end of the agreement period; or
2. Prohibit Bank plans to use IT service providers.

B. Audit Intern

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

1. Sistem TI;
2. Keamanan Data;
3. Kerangka Kerja Pengendalian Intern; dan
4. Rencana Pemulihan Bencana

Bank harus memastikan bahwa OJK atau pihak lain yang ditugaskan oleh OJK 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.

B. Internal Audit

Bank carries out the audit function of IT service providers on a regular basis, both by the Internal Audit Division and external audit parties appointed by the Bank. The scope of the audit is in accordance with the scope of services stated in the agreement. Areas audited include:

1. IT Systems;
2. Data Security;
3. Internal Control Framework; and
4. Disaster Recovery Plan

Banks must ensure that OJK or other parties appointed by JK 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. IT service provider audit reports and findings regarding IT services

VI. 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 3 Juni 2024 dan Dewan Komisaris pada tanggal 10 Juni 2024 serta mencabut Kebijakan Penggunaan Pihak Penyedia Jasa TI Edisi 3, Februari 2023.

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.

VI. CLOSING

This IT Service Provider Use Policy is published in 2 (two) languages, namely Indonesian and English, and if there are differences in interpretation between the two, Indonesian will be the reference.

This IT Service Provider Use Policy comes into effect after obtaining approval from the President Director on June 3rd, 2024 and the Board of Commissioners on June 10, 2024 and revokes the IT Service Provider Use Policy, Edition 3 February 2023.

This IT Service Provider Use Policy will be reviewed periodically no later than once every 2 (two) years or if necessary as an effort to improve it in accordance with business developments and Bank needs or changes in underlying regulations.