Bank Resona Perdania

KEBIJAKAN MANAJEMEN PROYEK DAN PENGEMBANGAN SISTEM

PROJECT MANAGEMENT AND SYSTEM DEVELOPMENT POLICY

Edisi ke-9, Januari 2023

9th Edition, Januari 2023

BOD Approval No. 072/ITD/IT-PLN/III/2023

BOC Approval No. 040/BOC/III/2023-ITD/IT-PLN

DAFTAR ISI
Table of Content

Hal/*Page*

Bank Resona Perdania

I. PENDAHULUAN

A. Latar Belakang

Perkembangan Teknologi Informasi (TI) terjadi dari waktu ke waktu seiring dengan bisnis Bank, perkembangan Teknologi Informasi, keperluan dari pihak regulator atau pemerintah dan juga untuk perbaikan dan peremajaan sistem berjalan. Seiring dengan hal tersebut, maka Bank senantiasa melakukan pengembangan, perubahan dan perbaikan pada Teknologi Informasinya. Suatu pengembangan, perubahan atau perbaikan Teknologi Informasi dapat menimbulkan risiko operasional Bank, bisnis Bank atau reputasi Bank. Untuk meminimalkan risiko yang ada, maka perlu dibuat suatu kebijakan yang memadai untuk menunjang keberhasilan akan pengembangan, perubahan dan perbaikan TI.

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. SEOJK No.29/SEOJK.03/2022 Tentang Ketahanan Dan Keamanan Siber Bagi Bank Umum
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

I. INTRODUCTION

A. Background

Information Technology (IT) development is happen from time to time in line with business Bank, Information Technology development, requirement from regulator or government as well as to repair and enhance existing system. Along with this, Bank always develops, enhance and improve its Information Technology. An Information Technology development, enhancement or improvement can raise Bank operational risk, business Bank or Bank reputation. To minimize risk, an adequate policy is made to support the success of IT development, enhancement and improvement.

B. Reference

1. External Rules :

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

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

3. SEOJK No.29/SEOJK.03/2022 Concerning Cyber Security and Resilience for Commercial Banks
4. POJK No. 18/ POJK.03/2016 concerning 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

Penyelenggaraan Produk Bank Umum.

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

invalid by POJK No. 13/POJK.03/2021 concerning the Operation of Commercial Bank Products.

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

2. Peraturan Internal :

1. Kebijakan Manajemen Risiko Teknologi Informasi
2. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem dalam Penggunaan Teknologi Informasi
3. Kebijakan Manajemen Risiko secara Umum (Individual).
4. Kebijakan Tugas & Wewenang.
5. Kebijakan Tingkat Otorisasi.
6. Kebijakan *Job Description.*
7. Kebijakan Komite Pengarah Teknologi Informasi.
8. Kebijakan Audit Intern Teknologi Informasi.

2. Internal Rules :

1. Information Technology Risk Management Policy.
2. Information Security and System Risk Management Policy in the use of Information Technology.
3. General Individual Risk Management Policy.
4. Duties & Authorities Policy.
5. Leveling Authority Policy.
6. Job Description Policy.
7. Information Technology Steering Committee.
8. Information Technology Internal Audit Policy.

C. Tujuan

1. Sebagai standar dan acuan Bank Resona Perdania (selanjutnya disebut Bank) untuk melakukan pengembangan, perubahan atau perbaikan Teknologi Informasi dan untuk melaksanakan manajemen proyek TI yang baik, berdasarkan SDLC (*System Development Life Cycle*).
2. Sebagai kontrol dan pengawasan untuk meminimalkan kesalahan dan peristiwa kerugian risiko yang timbul dari adanya pengembangan, perubahan atau perbaikan Teknologi Informasi.
3. Untuk memastikan bahwa pengembangan, perubahan atau perbaikan Teknologi Informasi dilakukan dengan struktur yang baik dan mengakomodasi kebutuhan user, baik dilakukan oleh internal Bank atau oleh vendor.

C. Purpose

1. 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.
2. As control and monitoring to minimize mistake and operational loss that raise from Information Technology development, enhancement, or improvement.
3. To ensure that Information Technology development, enhancement or improvement has been done with a suitable structure and accommodate user requirement, whether it conducted by Internal Bank or by vendor.

D. Ruang Lingkup

D. Scope

1. Kategori Proyek

   Implementasi, pengembangan, konversi, upgrade, penambahan fungsi atau *major patch* pada suatu sistem.

   Berikut adalah contoh yang dikategorikan sebagai proyek:

   a. Pembuatan, pembelian atau penggantian sistem.
   b. Pembuatan, pembelian atau penggantian sistem interface untuk menunjang pekerjaan dan operasional Bank.
   c. Implementasi sistem baru atau perubahan sistem sesuai dengan peraturan regulator dan pemerintah.
   d. Pengembangan dan penambahan fungsi baru pada sistem yang digunakan.
   e. Upgrade versi dari sistem yang digunakan
   f. Upgrade versi sistem operasi, database dan *software* pendukung yang digunakan oleh sistem berjalan.
   g. Update *hardware* (skala besar) dan *hardware* yang digunakan sistem kritikal Bank.
   h. Konversi data, media *backup* karena perubahan teknologi dan adanya waktu retensi atas media yang digunakan.

   Dasar pelaksanaan atas proyek yang berhubungan dengan Teknologi Informasi atau untuk mendukung kegiatan usaha Bank adalah sebagai berikut:

   a. Rencana Strategis TI.
   b. Adanya peraturan, sistem baru dan/atau perubahan dari pihak Regulator/Pemerintah dan lembaga lainnya.
   c. Kebutuhan user dan/atau kebutuhan pemilik sistem karena adanya *end of support* dan/atau upaya perbaikan sistem.
   d. Rekomendasi dan/atau hasil temuan dari Audit Internal

1. Project Category

   Implementation, development, conversion, upgrade, add function or major patch of a system.

   Following is example that categorized as project:

   a. Development, purchase or replacement of a system.
   b. Development, purchase or replacement of interface system to support Bank operational and activity.
   c. Implementation of new system or system replacement in line with regulatory regulation and government.
   d. Development and enhancement of new function for existing system.
   e. Upgrade version of existing system.
   f. Upgrade operating system version, database and supporting software that is use by existing system.
   g. Update hardware (major scale) and hardware that is use by Bank's critical system.
   h. Data conversion, media backup because of new technology and because limitation from media retention.

   Base for implementation that related to Information Technology project or to support Bank business activity are as follow:

   a. IT Strategic Plan.
   b. Regulation, new system and/or changes from Regulator/ Government and other institution.
   c. User requirement and/or requirement from system owner because there is end of support and/or as effort to improve system.
   d. Recommendation and/or finding from Internal and/or

dan/atau eksternal.

2. Kategori Non-proyek

Aktivitas di Divisi TI terkait instalasi, *user maintenance* atau *minor patch* sistem atau *hardware*. Berikut adalah contoh aktivitas yang dikategorikan sebagai non-proyek:

a. Pengujian sistem yang dilakukan di unit pengembangan atau unit DR.

b. Pemeliharaan, pembuatan, perubahan dan penghapusan hak akses (*User ID & Password*) dari suatu sistem.

c. Instalasi *hardware* dan *software* (skala kecil).

d. Proses harian seperti *Start of Day*, *End of Day*, distribusi laporan, monitor sistem atau sistem *helpdesk*.

e. Instalasi *software* yang mendukung pekerjaan dan yang tidak terkoneksi langsung dengan operasional Bank, seperti: *software* SPSS, Adobe Acrobat, Ms-Project, Photo Editor atau Visio.

f. Bersifat mendesak tetapi tidak merubah alur proses sistem, seperti permintaan informasi atau data untuk pekerjaan atau pemeriksaan.

g. Aktivitas terkait sistem yang sudah beroperasional, seperti *install program/patch* untuk validasi, *bugs fix*, perubahan yang bersifat minor, penambahan atau perubahan laporan. Dasar analisa dilihat dari risiko yang ada, biaya dan waktu yang diperlukan untuk penyelesaian aktivitas.

E. Definisi

1. *Patches* merupakan program yang berfungsi untuk memperbaiki permasalahan-permasalahan yang terjadi. *Patches* diberikan oleh pihak vendor selaku pemilik/prinsipal suatu sistem. Pemberian patches berdasarkan adanya kontrak

External Audit.

2. Non-project Category

Activity at IT Division related to installation, user maintenance or minor patch system or hardware. Following is example of activity that categorized as non-project:

a. System testing that is conducted at development or DR unit.

b. Maintenance, creation, modification and deletion of access right (User ID & Password) of a system.

c. Install hardware and software (small scale).

d. Daily process such as Start of Day, End of Day, reporting distribution, system monitor or helpdesk system.

e. Software installation that supports daily activity and that is not connecting directly with Bank operation, such as: software SPSS, Adobe Acrobat, Ms-Project, Photo Editor or Visio.

f. Urgent but not changing system workflow, such as request information or data for work or audit.

g. Activity related to system that is already operational, such as install program/patch for validation, bug fix, minor changes, add or change reporting. Analysis base on risk, cost and time required completing the activity.

E. Definition

1. Patches is a program that has function to fix errors happen. Patches is provided by vendor as owner/principal of a system. Patches provided based on maintenance agreement or transaction between vendor/principal and user.

pemeliharaan atau transaksi antara vendor/prinsipal dengan pengguna.

2. *Work Break-Down Structure* (WBS) adalah hirarki/urutan dari kegiatan yang menjabarkan rincian pekerjaan yang akan dilakukan oleh Tim Proyek. Dengan WBS, Tim Proyek dapat mengestimasi jangka waktu proyek dan setiap tahapan.

2. Work Break-Down Structure (WBS) is a hierarchy/sequence of an activity that describes detail activity that will be done by Project Team. By WBS, Project Team can estimate duration of project and each phase.

3. *Unit Test* (UT) adalah uji coba yang dilakukan oleh vendor (*programmer*) atas fungsi-fungsi yang ada didalam suatu sistem, seperti proses input data, output data and perhitungan.

3. Unit Test (UT) is testing conducted by vendor (programmer) of system functions, such as input data process, output data and calculation.

4. *System Integration Test* (SIT) adalah proses uji coba yang dilakukan untuk memastikan semua sistem terkait terintegrasi dan dapat beroperasi dalam lingkungan yang sama. Proses SIT biasanya dilakukan sebelum tahapan proses UAT

4. System Integration Test (SIT) is testing conducted to ensure that all related system is integrated and operates in the same environment. SIT process is conducted before UAT process.

5. *User Acceptance Test* (UAT) adalah proses uji coba untuk memastikan suatu sistem dapat menangani proses/prosedur sesuai dengan spesifikasi yang ditetapkan. Proses UAT merupakan proses akhir di tahapan pengujian untuk memutuskan bahwa sistem dapat diimplementasikan atau tidak.

5. User Acceptance Test (UAT) is testing process to ensure that system handle process/procedure according to defined specification. UAT process is a final process during testing phase to decide whether system can be implemented or not.

6. Manajer Proyek adalah seorang yang berwenang atas keseluruhan perencanaan dan eksekusi atas proyek pengembangan sistem. Penetapan Manajer Proyek ditentukan berdasarkan salah satu di bawah ini:

   a. Kepemilikan atas suatu sistem yang akan dikembangkan, yaitu orang yang bertanggung jawab atas aktivitas operasional sehari-hari sistem tersebut, atau

   b. Orang yang memahami keseluruhan proses input dan output sistem tersebut.

   c. Mampu mengkomunikasikan rencana proyek pengembangan sistem ke pihak vendor dan Direksi.

6. Project Manager is the person in overall charge of the planning and execution of a system development project. Determination of Project Manager is based on any of the below:

   a. Ownership of the system to be developed, that is responsible person of daily operational activity of the system, or

   b. Person who understand all input and output processes of the system.

   c. Able to communicate project plan of system development to vendor and Director.

7. Tim Proyek adalah orang-orang yang tergabung untuk melaksanakan proyek tertentu.

7. Project Team is person is collaborated in the project implementation.

8. *User* adalah orang-orang yang menggunakan atau mengoperasikan suatu sistem atau jaringan.	8. User is person that is use or operates system or network.

II. TUGAS DAN TANGGUNG JAWAB

A. Direksi

1. Menetapkan prosedur dan kebijakan manajemen proyek dan pengembangan sistem.
2. Menetapkan dan menerapkan prosedur dan metodologi pengembangan sistem secara konsisten.
3. Menerapkan manajemen proyek dalam pengembangan sistem yang utama.
4. Memastikan pengujian yang dilakukan pada saat pengembangan suatu sistem telah memadai.
5. Memastikan sistem yang dikembangkan sesuai kebutuhan user.
6. Memastikan kesesuaian satu sistem dengan sistem yang lain.
7. Memastikan adanya dokumentasi sistem yang dikembangkan dan pemeliharaannya.
8. Memastikan adanya manajemen perubahan sistem aplikasi.
9. Memastikan proyek sudah berjalan sesuai dengan rencana yang ditetapkan dan proses kontrol dan monitor sudah memadai.
10. Memastikan identifikasi, pengukuran dan pengendalian risiko terkait dengan proyek sudah dilakukan dan memadai.
11. Memastikan adanya prosedur pengembangan sistem dalam keadaan darurat.

B. Manajer Proyek

1. Membuat rencana proyek yang berisi latar belakang proyek, manajemen ruang lingkup, biaya, jadwal, struktur organisasi, tugas dan tanggung jawab internal dan vendor, manajemen komunikasi dan manajemen risiko proyek.
2. Memimpin dan mengatur proyek dan tim proyek.

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.
6. Ensure suitability of a system with other system.
7. Ensure the existence of documentation of system develop and its maintenance.
8. Ensure the existence of system application change management.
9. Ensure that project is running according to plan and process of control and monitor are adequate.
10. Ensure risk identification, measurement and control related to project is conducted and adequate.
11. Ensure the possession of system development procedure in emergency.

B. Project Manager

1. Create project plan consisting project background, scope management, project cost, schedule, organization structure, job and responsibility of internal and vendor, communication management and project risk management.
2. Lead and manage project and project team.

3. Memastikan proses yang dilakukan dalam proyek telah sesuai dengan standar dan aturan yang berlaku.
4. Memonitor perkembangan proyek dan biaya yang terjadi selama proyek berjalan.
5. Memastikan risiko proyek sudah diidentifikasi, dimitigasi dan dilaporkan ke Direksi.
6. Memberi saran dan pendapat atas permasalahan yang muncul terkait proyek dan melakukan eskalasi ke pihak manajemen jika permasalahan tidak dapat diselesaikan dan membutuhkan persetujuan manajemen.
7. Memastikan dokumentasi proyek sudah sesuai dengan standar dan aturan yang ditetapkan.
8. Melaporkan secara berkala kepada Direksi mengenai perkembangan, aktivitas, issue/masalah proyek dan usulan/rekomendasi terkait issue/masalah proyek yang terjadi.

C. Tim Proyek

1. Berkontribusi atas keseluruhan tujuan proyek.
2. Menyelesaikan tanggung jawab individual terkait proyek.
3. Memberikan bantuan pengetahuan dan ketrampilan.
4. Bekerja sama dengan user untuk menetapkan dan memenuhi kebutuhan bisnis.
5. Membuat dan memelihara dokumentasi proyek.

D. Komite Pengarah Teknologi Informasi

Mengacu ke Kebijakan Komite Pengarah Teknologi Informasi.

E. Fungsi Proyek TI

Membantu user dalam mendefinisikan spesifikasi yang diperlukan untuk proyek, seperti penggunaan perangkat keras, perangkat lunak, sistem operasi, database, sistem keamanan, jaringan serta koneksi/interface dengan sistem berjalan untuk memastikan hasil implementasi suatu proyek bisa digunakan secara efektif dan efisien

3. Ensure that process is conducted by following standard and regulation
4. Monitoring the progress of project and cost during project
5. Ensure project risk is identified, mitigated and reported to Board of Directors.
6. Give suggestion and opinion of problem raised related to project and escalate to management if problem could not be solved and requires management approval.
7. Ensure that project documentation is suitable with standard and regulation.
8. Report on regular basis to Board of Directors about project progress, activity, issue/problem and give suggestion/recommendation related issue/problem.

C. Project Team

1. Contributing to overall project objectives.
2. Completing individual responsibility.
3. Providing knowledge and expertise.
4. Working with user to establish and meet business needs.
5. Create and maintain project documentation.

D. Information Technology Steering Committee

Refer to Information Technology Steering Committee.

E. IT Project Function

Support user in define specification that is require for project, such as the use of hardware, software, operating system, database, security system, network includes connection/interface with existing system to ensure that the result of implementation is effective and efficient.

F. Fungsi Operasional & Dukungan TI

1. Bertanggung jawab atas *backup unit* produksi dan memastikan hasil backup bisa digunakan saat diperlukan.
2. Memonitor perubahan-perubahan yang terjadi pada unit produksi.

G. *User*

1. Bekerja sama dengan Manajer Proyek, Tim Proyek dan vendor dalam mendefinisikan kebutuhan bisnis dan fungsi sistem.
2. Bertanggung jawab melakukan proses UAT dan bertanggung jawab atas hasilnya.

H. Seksi Pengawas Keamanan Informasi dan Risiko Sistem

1. Membantu Manajer Proyek, Tim Proyek dan user dalam mengidentifikasikan persyaratan keamanan yang diperlukan dalam suatu sistem.
2. Melakukan pengawasan risiko internal dan eksternal terkait pengembangan sistem.
3. Melakukan pengawasan dan pengendalian atas penggunaan data Nasabah atau data rahasia Bank jika diperlukan untuk keperluan testing.

I. Audit Intern

1. Memberikan rekomendasi dan masukan ke Tim Proyek untuk memastikan kecukupan pengendalian proyek
2. Aturan lain yang berhubungan dengan kebijakan ini mengacu ke Kebijakan Audit Intern Teknologi Informasi.

J. Seksi Perencanaan TI

1. Membuat dan mengajukan perizinan untuk diajukan kepada direksi.
2. Berkoordinasi dengan tim proyek terkait dan pihak penyedia TI atas harga yang bisa ditawarkan oleh vendor / pihak ketiga.

F. IT Operation & Support Function

1. Responsible for production backup unit and ensure backup result can be used at any time.
2. Monitoring changes in production unit.

G. User

1. Cooperates with Project Manager, Project Team and vendor in defining business requirement and system function
2. Responsible to conduct UAT process and responsible about the result.

H. Information Security and System Risk Controller Section

1. Support Project Manager, Project Team and user in identify requirement for security that is necessary in a system.
2. Conduct supervisory of internal and external risk related to system development.
3. Conduct supervisory and control the use of Customer data or Bank confidential data if needed for testing.

I. Internal Audit

1. Give recommendation and suggestion to Project Team to ensure adequacy of project control
2. Other regulation related to this policy refers to Information Technology Internal Audit Policy.

J. IT Planning Section

1. Create and apply for permits to be submitted to the directors.
2. Coordinate with related project teams and IT providers for prices that can be offered by vendors / third parties.

III. KEBIJAKAN DAN PROSEDUR

A. Aturan Umum

1. Hal-hal yang harus mendapatkan persetujuan Presiden Direktur adalah implementasi (*go live*) suatu sistem yang terkait Nasabah dan sistem yang terkait regulator/otoritas (OJK, BI, Kantor Pajak, dan lain-lain).
2. Hal-hal yang harus mendapatkan persetujuan Direktur yang membawahi dan Direktur yang membawahi TI adalah implementasi (*go live*) suatu sistem yang digunakan oleh user internal Bank.
3. Hal-hal yang harus mendapatkan persetujuan Direktur yang membawahi TI adalah implementasi darurat pada sistem terkait Nasabah yang sudah beroperasional, karena terdapat masalah kritikal yang mengakibatkan sistem tidak dapat digunakan.
4. Terdapat pemisahan unit pengembangan dan unit produksi.
5. Sistem yang dikembangkan sebaiknya menggunakan *software* resmi untuk menghindari tuntutan hukum di kemudian hari dan juga pertimbangan atas *support software* tersebut. Penggunaan *software open source* harus berdasarkan rekomendasi dari vendor pelaksana dan/atau sudah ada mitigasi risiko terkait *software open source* tersebut.
6. Terdapat pemisahan kewenangan atau dual control untuk meningkatkan kualitas pengembangan sistem.
7. Penggunaan *checklist* Manajemen Proyek untuk memonitor tahapan proyek pada Lampiran 1.
8. Penggunaan *checklist* Kecukupan Implementasi (*Go Live*) untuk memutuskan kecukupan atas kesiapan implementasi (*go live*) suatu sistem yang terkait Nasabah pada Lampiran 2.

III. POLICY AND PROCEDURE

A. General Rule

1. Matter that must get approval from President Director are implementation (go live) for a system that related to Customer and system that related to regulator/authority (OJK, BI, Tax Office, etc)
2. Matter that must get approval from Director in charge and Director in charge of IT are implementation (go live) of a system that is used by internal Bank user.
3. Matter that must get approval from Director in charge of IT are emergency implementation on operational system that related to Customer because there is a critical problem that causing system cannot be used
4. There is a separation between development unit and production unit.
5. The developed system should use original software to avoid legal lawsuit in the future and to get software support. The use of open source software must base on recommendation from vendor and/or it already has risk mitigation for using the open source software.
6. There is segregation of duty or dual control to improve system development quality.
7. Use the Project Management checklist to monitor project phase in Appendix 1.
8. Use Implementation (Go Live) Sufficiency checklist to decide the sufficiency of implementation (go live) for a system that related to Customer in Appendix 2.

B. Tahapan Proyek

Ada beberapa metode yang digunakan dalam manajemen proyek diantaranya adalah metode *Waterfall*, yaitu proses dilakukan secara berurutan sesuai dengan tahapan proyek. Berikut adalah rincian tahapan proyek menggunakan metode *Waterfall*:

1. Tahap Inisiasi

Berikut adalah langkah-langkah yang dilakukan untuk pengembangan sistem terkait atau Nasabah:

a. Bank menyusun dokumen RFP (*Request for Proposal*) yang berisi identifikasi kebutuhan user dan/atau suatu sistem, tujuan dan manfaat yang diharapkan, kebutuhan fungsional dan non-fungsional dan risiko dan pengaruh ke proses bisnis dan perubahannya.

   Dokumen RFP (*Request for Proposal*) dikirimkan ke vendor dan menjadi dasar vendor menawarkan solusi.

b. Bank membuat dokumen Studi Kelayakan dengan memperhatikan sebagai berikut:

   1) Rencana strategis dan rencana bisnis Bank untuk memastikan permintaan sudah termasuk dalam rencana strategis TI dan rencana bisnis Bank.
   2) Analisis biaya dan manfaat.
   3) Analisis pemilihan vendor, yang dibuat berdasarkan dokumen yang disediakan oleh vendor, sebagai berikut:
      - Kesesuaian antara solusi yang ditawarkan dengan kebutuhan.
      - Kondisi laporan keuangan vendor 2 (dua) tahun terakhir.
      - Kewajiban untuk membuat *escrow agreement*

B. Project Phase

There is some methods use in project management, one of it is Waterfall method, when process is conducted sequentially following project phase. Following is project phase using Waterfall method:

1. Initiation Phase

Below is steps to be conducted development of a system that related to Customer:

a. Bank create RFP (Request for Proposal) that consisting user and/or system identification, purpose and expected benefit, functional and non-functional requirements, and risk and impact to business process and its changes.

   RFP document (Request for Proposal) is sent to vendor and vendor will use it as base to propose solution.

b. Bank creates Feasibility Study by consider the following:

   1) Strategic plan and bank business plan to ensure the request is included in IT strategic plan and business plan.
   2) Cost and benefit analysis.
   3) Vendor selection analysis, that is create based on document that provided by vendor, as follow:
      - Suitability between proposed solution and requirement
      - Vendor financial report for the last 2 (two) years.
      - Obligation to create a source code escrow agreement for system

penyimpanan *source code* untuk sistem yang dikembangkan oleh vendor dan sistem tersebut terkait Nasabah dan sistem yang terkait regulator/otoritas (OJK, BI, Kantor Pajak, serta sistem yang dianggap penting oleh Bank).

Escrow agreement dibuat sebagai antisipasi jika dukungan dari vendor terhenti. Untuk sistem yang tidak terkait Nasabah atau regulator/otoritas (OJK, BI, Kantor Pajak, dan lain-lain), maka tidak diwajibkan untuk pembuatan *escrow agreement*, kecuali terdapat analisis yang menyatakan sebaliknya.

that is developed by vendor and the system is related to Customer and system that related to regulator/authority (OJK, BI, Tax Office, also system that is considered important by Bank).

Escrow agreement is create as anticipation if vendor support stopped. For system that is not related to Customer or regulator/authority (OJK, BI, Tax Office, etc) is not mandatory to create escrow agreement, unless there's an analysis that stated the otherwise.

- Profil vendor yaitu referensi di Bank lain untuk sistem yang sama atau pernah memiliki pengalaman kerjasama sebelumnya dengan Bank.
- Tingkat layanan.
- Perbandingan harga yang termasuk harga implementasi dan harga pemeliharaan.
- *Hardware* dan *software* yang disarankan, perencanaan kapasitas (jaringan ataupun penyimpanan), metode pengembangan, operasional sistem (pemeliharaan).
- Kelayakan jadwal yang menjelaskan tentang jangka waktu dan batas waktu penyelesaiannya.

- Vendor profile, consisting of reference for the same system or has past expericense with Bank.
- Support level.
- Price comparison that includes price for implementation and maintenance.
- Recommended hardware and software, capacity planning (network or storage) development method, system maintenance.
- Schedule feasibility that explains about timeline and target date completion.

c. Membuat Rencana Proyek yang menjelaskan setiap aktivitas dan sumber daya yang dibutuhkan. Rencana Proyek ini menjadi acuan dalam pelaksanaan proyek dan harus dikinikan sesuai perkembangan proyek.

Rencana Proyek sekurangnya mencakup sebagai berikut:

1) Latar belakang dan tujuan proyek.
2) Struktur Organisasi.

   Struktur organisasi proyek berisi pengawas, pelaksana dan pengamat proyek. Manajer Proyek ditetapkan berdasarkan jenis dan aktivitas proyek yang akan dilakukan. Sedangkan Tim Proyek diwakili oleh para Pemangku Kepentingan yang terkait dengan proyek.
3) Jadwal atas setiap tahapan dan *cut off date* untuk pengalihan ke sistem baru.
4) Perkiraan biaya.
5) Kriteria hasil yang ditargetkan (*acceptance criteria*) yaitu pendefinisian kriteria yang harus dipenuhi sehingga suatu proyek dianggap selesai dan dapat diterima oleh Manajemen.

   Berikut adalah *acceptance criteria* secara umum:

   - Setiap hasil proyek (*High Level Project Deliverables*) telah dipenuhi sesuai dengan jadwal dan telah disetujui oleh Manager Proyek dan diketahui oleh Direktur yang membawahi.
   - Semua prosedur terkait telah dibuat dan/atau sudah diajukan ke Divisi terkait untuk mendapatkan persetujuan. Dalam kondisi tertentu terkait jadwal implementasi,

c. Creates Project Plan that defines each activity and resource needed.This Project Plan will be used as guideline in a project and should be updated as the project progresses.

Project Plan at least consisting the following:

1) Project background and purpose.
2) Organization structure

   Organization structure consisting project supervisor, implementer and observer. Project Manager is appointed base on project type and activity. Meanwhile Project Team represented by stakeholder related with project.
3) Schedule for each stage and cut off date for the transfer to the new system.
4) Cost estimation
5) Acceptance criteria, is defining criteria that must be met in a project to consider a project is completed and accepted by Management.

   Following is common acceptance criteria:

   - Each High Level Project Deliverable met within schedule and has been approved by Project Manager and aknowledge by Director in Charge.
   - All related procedures have been made and/or submitted to related Division in order to get approval. In some circumtances related to implementation

persetujuan atas prosedur terkait dapat diproses setelah tahap implementasi.

- Masalah setelah implementasi (*Go live*) yang mengakibatkan sistem dan/atau suatu fungsi sistem tidak dapat digunakan sudah diselesaikan dan sudah ditutup.

Acceptance criteria perlu disesuaikan dengan karakteristik proyek dan sesuai dengan perkembangan proyek.

6) *High Level Project Deliverables* (Hasil Proyek), yaitu daftar dokumen yang akan diserahkan per tahapan proyek. Jenis dokumen dan/atau jumlah dokumen disesuaikan dengan kriteria proyek.

   Contoh: Dokumen Pendefinisian Kebutuhan (*Requirement Definition*), dokumen FSD (*Functional Specification Document*) atau dokumen hasil pengujian.

7) Tugas dan Tanggung Jawab setiap anggota proyek (termasuk vendor).

8) Prosedur Manajemen Perubahan, yang menjelaskan prosedur perubahan selama proyek berlangsung.

9) Prosedur Komunikasi Proyek. yaitu pendefinisian atas metode pelaporan yang akan dilakukan rutin selama proyek berlangsung. Contoh: laporan per minggu ke Direktur yang membawahi dan/atau laporan ke Direksi di setiap *checkpoint*/*milestone*.

10) Manajemen Risiko yaitu pendefinisian risiko terkait proyek dan akan diupdate

schedule, approval of related procedure can be processed after implementation phase.

- Problem after implementation (Go Live) that causing system and/or system function cannot be used are resolved and closed.

Acceptance criteria should be adjusted according with project characteristic and as the project progresses.

6) High Level of Project Deliverables is a list of document deliverable at each project phase. Document type and/or number of document are adjusted according with project criteria.

   Example: Requirement Definition document, Functional Specification Document or document of testing result.

7) Job and Responsibility of each project member (includes vendor).

8) Change Management Procedure that defines change procedure during project.

9) Project Communication Procedure, which define a routine reporting method during project. Example: weekly report to Director in charge and/or report to Board of Directors at each checkpoint/milestone.

10) Risk Management, which define risk of project and will be updated according

berdasarkan perkembangan proyek.

Sedangkan untuk pengembangan sistem yang digunakan oleh user internal Bank mengacu pada SOP Pengadaan Barang dan Jasa.

2. Tahap Pendefinisian Kebutuhan

Pada tahapan ini Manajer Proyek dan Tim Proyek mendefinisikan secara rinci sebagai berikut:

a. Deskripsi atas sistem/fungsi/proses/ prosedur saat ini.

b. Masalah atas sistem/fungsi/proses/ prosedur saat ini.

c. Rincian kebutuhan fungsional dan non-fungsional.

d. Kebutuhan yang menjelaskan mengenai keinginan tentang input, output, proses bisnis, mekanisme kerja sistem dan prosedur penggunaan sistem.

Proses ini akan menghasilkan dokumen spesifikasi kebutuhan yang berisi tentang fungsional sistem yang akan dikembangkan, spesifikasi proses dan prosedur, baik dari segi software, hardware dan database.

Dokumen spesifikasi kebutuhan (*Requirement Definition*) harus lengkap, jelas, dapat diuji, konsisten dan merinci kebutuhan input, proses dan output.

3. Tahap Perancangan Sistem

Tahapan ini menterjemahkan kebutuhan dalam suatu dokumen *Functional Specification Document* (FSD) yang menggambarkan cara kerja sistem. Dokumen ini akan disiapkan oleh vendor. Dokumen ini setidaknya mencakup mengenai sistem parameter, menu, tampilan layar untuk input data, laporan yang dihasilkan, validasi yang dapat dilakukan sistem dan informasi struktur data (jika memungkinkan).

Manajer Proyek dan Tim Proyek melakukan review atas dokumen tersebut dengan cara

to progress of project

For development of a system that is used by internal Bank user refer to Procurement of Goods and Services SOP.

2. Requirement Definition Phase

Following is steps to be conducted in
this phase

a. Description of the existing system / function/ process/ procedure.

b. Problem of the existing system/ function/ process/ procedure.

c. Detail of functional and non-functional requirement.

d. Requirement that explain about expected input, output business process, system mechanism and procedure of system use.

This process will produce a document of requirement specification that consisting of system functional to be developed, process specification and procedure, all from software, hardware and database point of views

Requirement Definition document should be comprehensive, clear, tested,consistent and detailing about the requirement for input, process and output.

3. System Design Phase

This phase translates requirement in a Functional Specification Document (FSD) that describe system workflow. Document is prepared by vendor. This document should at least covers about system parameter, menu, input screen, report, system validation and structure data information (if possible).

Project Manager and Project Team to conduct document review by comparing with Requirement

membandingkan dengan dokumen *Requirement Definition*. Jika dokumen telah disetujui maka dokumen tersebut akan ditandatangani (*sign-off document*). Selanjutnya dokumen tersebut akan digunakan untuk tahap pemrograman.

Definition document. If document approved, the document should be sign (sign-off document). The approved document should be used for programming phase.

Catatan: Jika terdapat kesalahan dalam proses review dapat mengakibatkan keterlambatan proyek atau penambahan biaya

Note: if there's mistake in review process can cause project delay or additional cost

Hal-hal yang perlu diperhatikan selama proses review adalah sebagai berikut:

Things to consider during review process:

a. Kelengkapan informasi pada tampilan *input screen*, proses pada sistem, laporan yang dihasilkan dan panjang setiap input dan output.

a. Information completeness for input screen, system process, report and length for each input and output.

b. Ketersediaan sistem parameter untuk menghindari proses *hard code*, yang dapat meningkatkan ketergantungan pada vendor

b. Availability of system parameter to prevent hard code, which can cause dependency to vendor.

c. Kecukupan proses validasi atas informasi yang diinput oleh user untuk menghindari duplikasi data.

c. Adequacy of process validation of information that inputted by user to prevent data duplication.

d. Pengendalian proses untuk mengetahui *error* yang terjadi dalam sistem seperti *error message*, *error log*, *history log*, *audit log*, atau *email notification*.

d. Control process to understand about error occurred such as error message, error log, history log, and audit log or email notification.

4. Tahap Pemrograman dan Unit Test

4. Programming and Unit Test Phase

Sistem yang dibuat oleh vendor merupakan hak cipta/milik dari vendor tersebut, dimana informasi, dokumentasi terkait dengan *proses coding*/*source code* tidak dapat di-share ke pihak Bank, kecuali ada perjanjian khusus mengenai *source code* tersebut. Jika Bank tidak memiliki perjanjian terkait kepemilikan *source code*, maka perlu diatur suatu perjanjian *escrow agreement* dengan pihak vendor. Perjanjian ini bertujuan untuk melindungi Bank jika vendor tidak dapat memberikan jasa untuk pengembangan atau pemeliharaan dikemudian hari.

System made by vendor is copyright of vendor, whereas information, documentation related to coding/source code could not be shared to Bank except there is an agreement about source code. If Bank not have agreement about source code ownership, Bank need to make escrow agreement with vendor. Agreement purpose is to protect Bank if vendor could not support for future development or maintenance

Untuk memonitor kualitas dan stabilitas pemograman yang

To monitor programming quality and stability that conducted by vendor,

dilakukan oleh vendor, Bank dapat meminta dokumen hasil *Unit Test* (jika memungkinkan). *Unit Test* dilakukan untuk validasi atas komponen sistem dan memastikan komponen tersebut menangani input dan output dengan benar.

Jika sistem dibuat oleh internal, dokumentasi setidaknya mencakup halhal sebagai berikut:

a. Tujuan pembuatan

b. Nama unit yang digunakan (mesin, OS, *database*, *software*, bahasa pemograman)

c. Penjelasan mengenai proses dan perhitungan/formula yang digunakan (jika ada)

d. Hasil *Unit Test*

5. Tahap Pengujian

Proses pengujian pada tahapan ini dibagi sebagai berikut:

a. *System Integration Test* (SIT) adalah proses untuk memastikan fungsi sistem dan sistem terkait berjalan. Vendor bertanggung jawab untuk membuat skenario SIT. Jika diperlukan, stress testing juga dapat dilakukan di tahapan ini.

b. *User Acceptance Test* (UAT) adalah proses untuk memastikan proses bisnis sesuai dengan FSD. Sebelum melakukan UAT, vendor dan Tim Proyek melakukan pelatihan kepada user sehingga user memahami sistem yang akan digunakan. Vendor dan Tim Proyek bertanggung jawab untuk membuat skenario UAT.

c. Berikut adalah hal-hal yang dapat dipertimbangkan dalam pembuatan skenario uji coba:

   1) Dalam skenario SIT satu test case dibuat untuk satu fungsi. Skenario SIT digunakan untuk verifikasi FSD. Contoh:

Bank can request Unit Test result document (if possible). Unit test conducted to validate system component and to ensure its component handle input and output correctly.

If system made by internal, documentation should at least consist the following:

a. Purpose

b. Unit used (machine, OS, database, software, programming language)

c. Explanation about process and calculation/formula used (if any)

d. Unit Test result

5. Testing Phase

Testing process in this phase divided into the following:

a. System Integration Test (SIT) is process to ensure system function and existing system are working. Vendor is responsible to create SIT scenario. If needed, stress testing can be done in this phase.

b. User Acceptance Test (UAT) is process to ensure business process is suitable with FSD. Before conducting UAT, vendor and Project Team conducting training to user so user understand the system. Vendor and Project Team are responsible to create UAT scenario.

c. Following is things to consider in creating testing scenario:

   1) In SIT scenario one test case is made for one function. SIT scenario used to verify FSD. Example:

- Pengisian suatu *field* sudah sesuai dengan formatnya, misal: untuk jumlah transaksi diisi dengan angka saja, pengisian tanggal, penggunaan spesial karakter, hanya boleh diiisi huruf Y atau N saja.
- Pengisian suatu *field* harus divalidasi pada tabel/parameter lain, seperti pengisian sandi Bank, sandi negara, atau kode mata uang.
- Kebenaran perhitungan, misalnya perhitungan kecukupan saldo Nasabah, konversi dari mata uang asing ke Rupiah dan sebaliknya.
- Formula atau aturan sudah sesuai, seperti penggunaan standar format dan *special charge*, penggunaan kurs beli dan kurs jual.
- Memastikan integritas data yang diinput pada sebuah *field*.

2) Dalam skenario UAT, satu *test case* dibuat untuk satu bisnis proses. Skenario UAT digunakan untuk verifikasi bahwa *Requirement Definition* telah sesuai dengan FSD.

d. Selain SIT dan UAT, untuk menentukan apakah sebuah proyek dapat dilanjutkan ke tahap implementasi atau tidak, Bank meminta vendor untuk melakukan evaluasi kualitas uji coba untuk memastikan bahwa tidak ada isu dan untuk menyerahkan evaluasi atas kualitas uji coba. Evaluasi metode dapat ditentukan oleh vendor, tapi harus mencakup poin kualitatif dan kuantitatif sebagaimana dijelaskan di bawah ini:

- Filling out a field is suitable with its format, example: transaction amount fill out with only number, date, special character, can only fill out with Y or N.
- Filling out a field is validated at other table/parameter, such as Bank code filling, country code or currency code.
- Calculation correctness, such as balance availability checking, conversion from foreign exchange to Rupiah and vice versa.
- Formula or procedure is correct, such as using format standardization and special charge, buy rate and selling rate.
- Ensure the integrity of inputted data in a field

2) In UAT scenario, one test case is made for one business process. UAT scenario used to verify Requirement Definition is suitable with FSD.

d. Besides SIT and UAT, in order to determine whether the project can be continued to implementation phase or not, Bank request vendor to evaluate the quality of the testing to make sure there is no issues and to provide evaluation of testing quality. The evaluation method can be decided by vendor but it covers qualitative and quantitative points as described below:

1) Poin kuantitatif: vendor harus mengevaluasi secara kualitatif jumlah *test case* dan *bug* yang terjadi, kemudian memutuskan apakah *bug* yang terjadi sudah layak dan dapat ditoleransi jika dibandingkan dengan jumlah *test case* dan *bug* di proyek pengembangan sebelumnya (jika ada). Vendor dapat mengecek apakah jumlah *test case* sudah cukup atau tidak dan apakah *bug* yang ditemukan sudah dievaluasi sesuai dengan skala pengembangan. Jika ditemukan permasalahan, vendor melakukan analisa untuk menemukan sumber masalah, melakukan konfirmasi apakah permasalahan tidak terkait kualitas dan jika diperlukan vendor mengambil langkah tambahan untuk mengukur kualitas pengembangan.

1) Quantitative point: vendor should evaluate quantitatively number of test cases and occurred bugs, and decide whether they are still appropriate and tolerable by comparing with number of test cases and bugs of previously developed projects (if any). Vendor can check whether number of test case is enough or not and whether the bugs are sufficiently removed per development scale as methods of evaluation. In case problem found, vendor should analyze the root cases, confirm they are not problem for the quality and if necessary, vendor should take additional quality enhancement measures.

2) Poin kualitatif: vendor melakukan evaluasi atas seberapa rinci *test case* di setiap tahapan, seperti output dan input, variasi data dan koneksi ke sistem lain, kinerja sistem, skenario asumsi kegagalan, dampak ke sistem lain, aktivitas operasional (harian, mingguan, bulanan, tahunan, dan lain-lain), dan jam operasional. Vendor harus memastikan bahwa cakupan test sudah mencukupi.

2) Qualitative point: vendor should perform evaluation regarding how detailed the test case of each phase is, such as output and input, data variation, and connection to other systems, performance, assumed failure scenario, impact to other existing systems, operation activity (Daily, weekly, monthly, annually, etc), and service time. Vendor should ensure the coverage of each test is sufficient.

3) Sebagai tambahan, jika *bug* terjadi, vendor harus mengidentifikasi di tahapan mana *bug* terjadi (kemungkinan *bug* terjadi di tahapan sebelumnya) dan vendor menganalisa sumber permasalahan (contoh: kesalahan rancangan, kesalahan manusia, dan lainlain). Vendor juga harus

3) In addition, when bugs have occurred, vendor should identify on which phase the bugs occurred (the cause of bugs are probably on the previous phase) and vendor analyze the root causes (example: mistake on design, human error, etc). Vendor should check others functions if

melakukan pengecekan di fungsi lain jika *bug* yang sama terjadi.

e. Jika diperlukan, Bank melakukan *rehearsal test* untuk memastikan kesesuaian rencana implementasi dan hasil *rehearsal test*. Berikut tujuan dilakukannya *rehearsal test*:

1) Verifikasi dan *review* rencana peralihan (*change over*).

2) Verifikasi dan *review* alokasi waktu (*time chart*).

3) Verifikasi dan *review fall back prosedur*.

4) Verifikasi dan *review* proses prosedur peralihan (*change over*) termasuk identifikasi permasalahan atau *error*

Hasil dari tahap pengujian digunakan untuk menentukan apakah dapat melanjutkan ke tahap implementasi atau perlu perpanjangan waktu pengujian.

Catatan: dokumen terkait hasil proses pengujian didokumentasikan untuk keperluan pengembangan/perubahan atau pemeriksaan di kemudian hari.

6. Tahap Implementasi

Berikut adalah 3 (tiga) jenis prosedur implementasi :

a. Prosedur implementasi untuk pengembangan sistem yang terkait Nasabah dan sistem yang terkait regulator/otoritas (OJK, BI, Kantor Pajak, dan lain-lain):

1) Proyek Manajer membuat dokumen persetujuan ke Presiden Direktur paling tidak 1 (satu) bulan sebelum tanggal implementasi yang berisi setidaknya sebagai berikut:

- Evaluasi kecukupan implementasi dengan

the same bugs also exist.

e. If necessary, Bank conduct rehearsal test to ensure suitability of implementation plan and result of rehearsal test. Following is purpose of rehearsal test:

1) Verification and review change over plan.

2) Verification and review time chart allocation

3) Verification and review fall back procedure.

4) Verification and review process of change over includes identification problem or error.

Result of testing phase is use to decide continue to implementation phase or need to extend testing period.

Note: document testing is documented for future development/enhancement or audit.

6. Agreement with IT Service Provider

Following is 3 (three) type of implementation procedures:

a. Implementation procedure for development of a system that related to Customer and system that related to regulator/authority (OJK, BI, Tax Office, etc):

1) Project Manager create approval document to President Director at least 1 (one) month before implementation date at least consisting as follow:

- Evaluation of implementation

menggunakan lampiran 2 - *Go live Sufficiency*.

- Rencana proyek/jadwal yang sudah di*update*.
- Tanggal implementasi.
- Rencana implementasi.
- Rencana pemberitahuan ke Nasabah. Tim Proyek sebaiknya melakukan pemberitahuan ke Nasabah mengenai rencana implementasi paling tidak 2 (dua) minggu sebelum implementasi.

  Pemberitahuan ke Nasabah juga dapat dikirim secara bertahap. Contohnya pemberitahuan awal 2 (dua) minggu sebelum implemetasi, pemberitahuan 1 (satu) minggu sebelum implementasi dan 1 (satu) hari sebelum implementasi.

2) Memberlakukan masa *freeze development* (tidak ada lagi tambahan fungsi/perubahan pemograman) untuk memastikan bahwa sistem/ program yang akan di-deploy ke unit produksi adalah sistem/program yang sudah teruji dan beroperasi dengan benar.

b. Prosedur Implementasi atas aktivitas dan/atau pengembangan sistem untuk digunakan di internal Bank:

1) Dokumen persetujuan diajukan ke Direktur yang membawahi TI paling lambat 3 (tiga) hari sebelum implementasi dengan melampirkan Formulir Identifikasi Perubahan Sistem (BRP-ISC-01).

   Jika pemilik atas sistem yang dikembangkan bukan

sufficiency using appendix 2 - Go Live Sufficiency

- Updated project plan/schedule.
- Implementation date.
- Implementation plan
- Notification plan to Customer. Project Team should notify Customer about implementation plan at least 2 (two) weeks before implementation.

  Notification to Customer can also be sent by stages. For example early notification at 2 (two) weeks before implementation, reminder notification at 1 (one) week before implementation and 1 (one) day before implementation

2) Set freeze development time (there is no additional function/program changing) to ensure system/program that will be deployed to production unit is system/program that is tested and running correctly.

b. Implementation Procedure of activity and/or system development for internal Bank:

1) Approval document submitted to Director in charge of IT at latest 3 (three) days before implementation by attach Identification of System Change Form (BRP-ISC-01).

   If owner of the developed system not from IT

dari Divisi TI, maka dokumen persetujuan harus mendapatkan persetujuan dari Direktur yang membawahi dan Direktur yang membawahi TI.

Dokumen tersebut setidaknya berisi sebagai berikut:

- Tujuan implementasi.
- Tanggal implementasi
- Penjelasan fungsi yang dikembangkan/diperbaiki/ patch/perubahan parameter yang dilakukan.
- Penjelasan dampak ke fungsi lain dan sistem terkait lainnya.
- Evaluasi vendor atas hasil pengujian.
- Hasil pengujian internal Bank (user).
- Tingkat risiko dan mitigasinya.
- Rencana notifikasi ke user terkait.

2) Setelah mendapatkan persetujuan PIC melakukan pemberitahuan ke user terkait sebelum melakukan implementasi.

3) PIC memastikan adanya prosedur *rollback* jika implementasi gagal.

4) PIC memastikan bahwa sistem/data sudah di*backup* sebagai *contingency* jika memerlukan proses *restore* ketika *deploy* gagal.

5) Setelah implementasi sudah dilakukan dan sistem berjalan stabil, PIC melakukan evaluasi atas implementasi yang terjadi dan hasil evaluasi dilaporkan ke Direktur yang membawahi dan Direktur yang membawahi TI.

Division, the approval document must get approval from Director in charge and Director in charge of IT.

The document at least consist of the following:

- Implementation purpose.
- Implementation date.
- Explanation of function that is developed/fixed/patch /parameter change.
- Explanation of impact to other function and other related system.
- Vendor evaluation of testing result
- Testing result from internal Bank (user).
- Risk level and its mitigation.
- Notification plan to related user.

2) After get approval, PIC notify to related user before conduct implementation.

3) PIC ensures the existence of rollback procedure if implementation fails.

4) PIC ensure that system/data is backup as contingency if require restore process when deploy fails.

5) After implementation is done and system is running stable, PIC conducts evaluation of implementation and report to Director in charge and Director in charge of IT.

c. Prosedur Implementasi Darurat

Implementasi ini dilakukan hanya jika terjadi masalah pada sistem yang sudah beroperasional dan harus dilakukan *bug fix*/*patch*/perubahan parameter segera. Jika tidak dilakukan segera maka sistem tersebut tidak dapat digunakan. Berikut adalah prosedur implementasi darurat:

1) PIC melakukan rencana keberlangsungan usaha berdasarkan persetujuan Direktur yang membawahi TI dengan mengacu ke Kebijakan sistem terkait.
2) PIC dan/atau vendor mencari sumber permasalahan/*error* yang terjadi.
3) Setelah PIC dan/atau vendor menemukan sumber permasalahan/*error*, PIC meminta persetujuan ke Direktur yang membawahi TI dengan menggunakan Formulir Identifikasi Perubahan Sistem (BRP-ISC-01). Formulir tersebut setidaknya berisi sebagai berikut:
   - Penjelasan sumber permasalahan/*error* yang terjadi.
   - Penjelasan fungsi yang akan diperbaiki/*patch*/ perubahan parameter yang dilakukan.
   - Penjelasan dampak ke fungsi lain dan sistem terkait lainnya.
   - Hasil pengujian vendor dan internal Bank (*user*).
   - Tingkat risiko dan mitigasinya.
4) Setelah implementasi sudah dilakukan dan sistem kembali normal, PIC dan/atau vendor melakukan evaluasi atas

c. Emergency Implementation Procedure

This implementation conducted if operational system is in trouble and need immediate bug fix/patch/change parameter. If not done immediately, the system could not be used. Following is procedure of emergency implementation:

1) PIC conduct contingency plan base on approval from Director in charge of IT by refer to related system Policy.
2) PIC and/or vendor finds out problem/error occurred.
3) After PIC and/or vendor found problem/error root cause, PIC immediately request approval from Director in charge of IT using Identification of System Change Form (BRP-ISC-01). The form at least consist the following
   - Explanation of problem/ error root cause.
   - Explanation of function that will be fixed/patch/ parameter change
   - Explanation of impact to other function and other related system.
   - Testing result from vendor and internal Bank (user).
   - Risk level and its mitigation.
4) After implementation is done and system is back to normal, PIC and/or vendor conducts evaluation about

permasalahan/*error* yang terjadi dan hasil evaluasi dilaporkan ke Direktur yang membawahi TI.

Terkait dengan kemungkinan implementasi darurat, maka jika memungkinkan parameter/*profile* unit pengembangan disamakan dengan parameter/profile unit produksi.

Berikut dapat menjadi pertimbangan dalam pemilihan metode implementasi:

a. Implementasi secara langsung/*Big Bang*

1) Keuntungan

- Bank tidak perlu menjalankan 2 (dua) sistem yang berbeda, sehingga operasional Bank menjadi lebih efisien
- Proses implementasi lebih cepat dan Bank dapat fokus pada kegiatan atau proyek lainnya.

2) Kerugian

- Meningkatnya risiko operasional dan/atau reputasi Bank jika implementasi sistem bermasalah.
- Memerlukan *resource* yang besar.

3) Hal-hal untuk dipertimbangkan

- Memastikan sistem dan *interface* dengan sistem terkait sudah berjalan dengan baik. Oleh karena itu pastikan hasil *testing* (UT, SIT dan UAT) dan hasil migrasi data (jika ada) sudah benar, tidak ada pengaruh ke sistem.
- Memastikan user sudah dapat mengooperasikan

problem/error occurred and the evaluation result report to Director in charge of IT.

Related with the possibility of emergency implementation, then if possible parameter/profile at development unit is the same as parameter/profile at production unit.

Following is consideration in selecting implementation method :

a. Big-Bang implementation

1) Advantage

- Bank not need to run 2 (two) different systems, so Bank operational is effective.
- Implementation process is quicker and Bank can focus to other activity or project.

2) Disadvantage

- Operational risk increase and/or Bank reputation if problem occurred during implementation.
- Require many resources.

3) Things to consider

- Ensure system and interface is running well.

  Therefore testing result (UT, SIT and UAT) and result of data migration (if any) is correct and there is to impact to system.
- Ensure user able to operates new system

sistem baru tersebut.

- Memastikan *personnel* yang akan bertanggung jawab dalam menangani permasalahan.

b. Implementasi secara *parallel*

1) Keuntungan

- Risiko kegagalan sistem dapat dimitigasi, karena hanya berpengaruh pada sistem baru saja.
- Tidak memerlukan *resource* yang besar

2) Kerugian

- Operasional Bank menjadi tidak efisien karena harus memelihara sistem yang berbeda.
- Proses implementasi menjadi lebih lama karena dilakukan secara bertahap.

3) Hal-hal untuk dipertimbangkan

- Pemilihan user/Nasabah yang dapat bekerja sama dengan untuk mendapatkan *feedback*.
- Membuat jadwal dan menetapkan target implementasi secara keseluruhan.

- Ensure personnel to handle problem.

b. Parallel implementation

1) Advantage

- Risk of system failure can be mitigated because impact to new system only.
- Not require many resources.

2) Disadvantage

- Bank operation is not efficient because have to maintain different system.
- Implementation process is longer because conducted in stages.

3) Things to consider

- Select user/Customer that can cooperate in order to get feedback.
- Create schedule and define overall implementation target.

7. Tahap Kaji Ulang

Tujuan proses kaji ulang adalah untuk meninjau tingkat kesuksesan dari suatu proyek serta sebagai pembelajaran untuk pelaksanaan proyek lainnya.

Tingkat keberhasilan suatu proyek dinilai dari kesesuaian antara rencana proyek dengan hasil implementasi.

Laporan *Post Implementation Review* setidaknya berisi:

a. Hasil kaji ulang kinerja sistem (*system performance review*).

b. Kesesuaian dengan *user requirement*.

c. Masalah yang terjadi dan solusi atau eskalasi atau langkah penyelesaian yang dilakukan.

d. Efektivitas pengamanan yang ditetapkan.

Laporan tersebut akan dilaporkan ke Direksi.

8. Tahap Pemeliharaan

Untuk menjaga sistem berjalan baik, Bank perlu melakukan pemeliharaan dan monitor atas sistem yang digunakan. Proses pemeliharaan dapat dilakukan oleh Bank atau vendor dengan memperhatikan hal-hal berikut

a. Pemeliharaan Sistem

1) Tersedianya sumber daya manusia Bank yang memadai.

2) Tersedianya akses pada kode sumber (jika memungkinkan)

3) Apakah sistem memiliki ketergantungan yang tinggi pada pihak vendor.

4) Ruang lingkup dan biaya, misal apakah hanya tebatas pada proses *backup* dan *restore* saja, hanya menangani *bug fixing* atau hal-hal yang dapat dilakukan pihak Bank atau vendor lainnya.

Berikut adalah pertimbangan

7. Review Phase

The purpose of post implementation review is to review success level of a project and as a lesson for future project.

Success level of a project is measure from suitability between project plan and result of implementation.

Post Implementation Review report at least consist of the following:

a. System performance review.

b. Conformity with user requirement.

c. Problem occurred and solution or escalation that have been conducted.

d. Effectiveness of the determined security.

The report will be submitted to Board of Directors.

8. Maintenance Phase

To maintain system is running well, Bank conduct maintenance and monitoring the system. Maintenance process can be done by Bank or vendor by consider the following:

a. System Maintenance

1) Availability of human resource adequacy.

2) Access to source code (if possible).

3) System has high dependency to vendor

4) Scope and cost, example limited to backup and restore process, only bug fixing or activity conducted by Bank or vendor.

Following is consideration in

terkait perjanjian jika pemeliharaan diserahkan ke vendor:

1) Ruang lingkup pemeliharaan, seperti *bug fixing*, dukungan *upgrade* atas sistem, dukungan atas *software* yang digunakan, dan lain-lain.
2) Jangka waktu pemeliharaan, seperti 7x24 jam atau terbatas selama jam kerja.
3) Biaya, apakah bersifat tetap atau direview setiap tahunnya. Jika dimungkinkan, dasar kenaikan sudah ditetapkan dalam perjanjian atau berdasarkan kesepakatan yang wajar.
4) Waktu kunjungan pemeliharaan secara rutin, untuk menghindari kerusakan sistem yang fatal yang dapat mengganggu operasional Bank.
5) *Service Level Agreement*, termasuk *response time* sejak permasalahan dilaporkan sampai dengan batas waktu penyelesaiannya.

b. Dukungan Sistem

1) Tersedia dukungan teknikal yang memadai untuk memastikan operasional Bank berjalan dengan baik dan permasalahan yang terjadi telah ditangani dengan tepat
2) Divisi TI harus dapat memberikan dukungan yang memadai kepada user dan/atau Nasabah.
3) Dalam memberikan dukungan pada tingkatan awal setelah implementasi, jika diperlukan perlu dibentuk *help desk* yang bertugas untuk mendokumentasikan dan

making agreement if maintenance handle by vendor:

1) Maintenance scope, such as bug fixing, upgrade system support, software support and others.
2) Maintenance schedule, such as 7x24 hours or limited to working hour.
3) Cost, fixed cost or need review every year, increment base is stipulated at agreement or base on reasonable agreement.
4) Regular onsite maintenance, to prevent system failure that can impact to Bank operational.
5) Service Level Agreement; include response time of problem reported until time resolution.

b. System Support

1) Availability of an adequate technical support to ensure Bank operational running well and problem is handling correctly.
2) Information Technology Division gives an adequate support to user and/or customer.
3) In giving early support after implementation, if needed establish help desk to support and documented problem at early stage after implementation. If help desk not able to

menangani permasalahan yang terjadi pada tingkat awal setelah implementasi. Jika help desk tidak dapat menangani, akan dilakukan eskalasi ke tingkatan berikutnya, seperti: Tim Proyek atau Vendor. Proses dokumentasi harus dilakukan dengan jelas dan benar, sehingga masalah yang sama dapat diantisipasi. Selain itu dokumentasi dapat dijadikan sebagai referensi bagi karyawan baru atau karyawan lainnya

handle problem, it should be escalated to the next level such as Project Team or Vendor. Documentation should be clear and accurate so the same problem could be anticipated. Other than that documentation can be a reference for new employee or other employee.

4) Dalam memberikan dukungan ke *user*, help desk harus mempunyai pengetahuan yang memadai mengenai sistem yang diimplementasikan.

4) In support user, help desk should have adequate knowledge about the implemented system.

c. Manajemen *Patch*

Tujuan manajemen *patch* adalah untuk menjaga tingkat keamanan sistem terkait kerentanan OS dan/atau middleware. Informasi *patch* dapat diperoleh dari regulator, vendor, internet dan/atau konsultan keamanan TI.

Seksi Sistem TI dan Seksi Pengawas Keamanan Informasi dan Risiko Sistem menganalisis tingkat kerentanan sistem dan tingkat prioritas kerentanan sistem terhadap operasional dan bisnis Bank sebagai berikut:

c. Patch Management

The purpose of patch management is to maintain security level of system related to vulnerability of OS and/or middleware. Patch information can be obtained from regulator, vendor, internet and/or IT security consultant.

IT System Section and Information Security and System Risk Controller Section analyze system vulnerability level and priority level towards operational and business Bank as follow:

1) Matriks evaluasi tingkat kerentanan sistem:

1) Matrix of system vulnerability level:

Level kerentanan		Tingkat kesulitan serangan			
		Mudah	Sedang	Sulit	N/A
Akibat terhadap operasional dan/atau bisnis bank	Sangat besar	Tinggi	Sedang	Rendah	Tidak ada
	Besar	Sedang	Rendah	Rendah	Tidak ada
	Kecil	Rendah	Rendah	Rendah	Tidak ada

Berikut adalah penjelasan atas tingkat kesulitan serangan:

- Mudah: mudah untuk menyerang kerentanan.
- Sedang: memungkinkan untuk menyerang kerentanan.
- Sulit: sangat sulit untuk menyerang kerentanan.
- N/A: tidak ada akibat ke unit sistem.

Below is explanation for level of attack difficulties:

- Easy: easy to attack vulnerability
- Medium: possible to attack vulnerability
- Difficult: difficult to attack vulnerability
- N/A: no impact to system environment

2) Matriks evaluasi tingkat prioritas:

2) Matrix of priority level:

Evaluation		Tingkat kesulitan penanganan		
		Mudah	Sedang	Sulit
Level kerentanan	Tinggi	Secepatnya	Secepatnya	Jangka menengah : membuat rencana Jangka pendek: Mitigasi risiko
	Sedang	Secepatnya	Normal	
	Rendah	Normal	Normal	
	Tidak Ada	-	-	-

Berikut adalah penjelasan atas tingkat kesulitan penanganan:

Below is explanation for difficulty level of handling:

		Mudah	Sedang	Sulit
Kesulitanan penanganan	Terkait produk	Ringan dengan menggunakan aplikasi PTF (product temporary fix)	Cukup dengan menggunakan aplikasi PTF (product temporary fix)	Back up, service pack diperlukan, patch tidak tersedia, dll
	Terkait langkah yang harus dilakukan	Ringan dengan melakukan perubahan setting	Cukup dengan melakukan perubahan setting	Ada pengaruh keseluruhan service yang terkait dan tidak dapat melakukan perubahan setting

Berikut adalah prosedur manajemen *patch*:

1) Seksi Perencanaan TI dan Seksi Pengawas Keamanan Informasi dan Risiko Sistem melakukan identifikasi terhadap kerentanan sistem dengan bekerja sama dengan vendor dan/atau konsultan keamanan TI. Identifikasi ini wajib dilakukan secara berkala terhadap sistem

Below is procedure of patch management:

1) IT Planning Section and Information Security and system Risk Controller Section conduct identification for system vulnerability by coordinate with vendor and/or IT security consultant. This identification is mandatory to conduct on regular basis for system related to

terkait Nasabah.

2) Berdasarkan hasil identifikasi, Seksi Perencanaan TI dan Seksi Pengawas Keamanan Informasi dan Risiko Sistem membuat rencana tahunan proses implementasi *patch* dan mengajukan persetujuan ke Direktur yang membawahi TI.

3) Implementasi *patch* untuk sistem terkait regulator dilakukan berdasarkan perintah dari regulator.

4) Jika permintaan rencana implementasi *patch* disetujui, Seksi Perencanaan TI dan Seksi Pengawas Keamanan Informasi dan Risiko Sistem bekerja sama dengan vendor terkait untuk melakukan ujicoba di unit *development*. Ujicoba dilakukan untuk memastikan sistem tetap dapat digunakan setelah implementasi *patch*. Jika diperlukan ujicoba dapat melibatkan *user*.

5) Seksi Perencanaan TI dan Seksi Pengawas Keamanan Informasi dan Risiko Sistem mengajukan persetujuan ke Direktur yang membawahi yang berisi hasil ujicoba dan rencana jadwal implementasi *patch* ke unit produksi.

6) Seksi Perencanaan TI dan/atau vendor melakukan installasi *patch* ke sistem terkait dengan menggunakan Formulir Identifikasi Perubahan Sistem (BRP-ISC-01) dan atas sepengetahuan Fungsi Operasional & Dukungan Teknologi Informasi

7) Dokumen perubahan *patch* harus dikelola dan

Customer.

2) Base on identification result, IT Planning Section and Information Security and System Risk Controller Section create annual plan for patch implementation process and request for approval to Director in charge of IT.

3) Patch implementation for system that related to regulator is conducted base on instruction from regulator.

4) If plan for patch implementation is approved, IT Planning Section and Information Security and System Risk Controller Section coordinates with related vendor to conduct test in development unit. Testing is conducted to ensure system run normal after patching. If necessary, test involving user.

5) IT Planning Section and Information Security and System Risk Controller Section request for approval to Director in charge that consisting testing result and schedule plan of patching into production unit.

6) IT Planning Section and/or vendor install patch to related system using Identification of System Change Form (BRP-ISC-01) and with acknowledge of IT Operation & Support Function.

7) Patch management document is well

disimpan dengan baik.

documented and maintained.

d. Pemusnahan

Beberapa pertimbangan dalam untuk pemusnahan sistem:

1) Sistem sudah tidak digunakan lagi oleh Bank.
2) Tidak tersedianya dukungan perangkat keras dan perangkat lunak untuk menjalankan sistem tersebut.

Catatan: Jika suatu sistem memiliki versi lama tetapi masih digunakan untuk pengecekan data, maka sistem tersebut harus dipelihara.

d. Disposal

Following is consideration for system disposal:

1) System is no longer use by Bank.
2) No hardware or software support.

Note: If the system is old version but still require for data checking, the system has to be maintained.

Berikut adalah prosedur pemusnahan sistem:

1) Setiap proses pemusnahan sistem harus mendapat persetujuan dari Direktur yang membawahi TI.
2) Setiap proses pemusnahan sistem harus dilakukan diawasi oleh Seksi Pengawas Keamanan Informasi & Risiko Sistem dan atau Divisi Audit.
3) Setiap proses pemusnahan sistem harus dibuatkan berita acara pemusnahan yang jelas seperti nama sistem, No. persetujuan Direksi dan tanggalnya, tanggal dan tempat pelaksanaan, mekanisme pemusnahan, nama pelaksana, saksi dan PIC lainnya yang terlibat serta informasi penting lainnya. Laporan berita acara pemusnahan akan dilaporkan ke Direktur yang membawahi TI.

Following is system disposal procedure:

1) Every system disposal has to get approval from Director in charge of IT.
2) Every process of system disposal is supervised by Information Security and System Risk Controller Section and Audit Division.
3) Every process of system disposal has a news event of disposal consist of system name, Board of Directors approval's number and its date, date and place of implementation, disposal mechanism, implementer name, witness and other PIC that involve in the disposal process. The disposal news event will be reported to Director in charge of IT.

IV. MANAJEMEN RISIKO DALAM MANAJEMEN PROYEK DAN PENGEMBANGAN SISTEM

Manajemen memastikan bahwa risiko internal dan eksternal dalam pelaksanaan proyek telah diidentifikasi, dinilai, dilaporkan, ditinjau dan dimitigasi dengan baik disetiap tahapan SDLC. Dalam mitigasi risiko yang teridentifikasi mengharuskan organisasi untuk mengembangkan strategi risiko yang dapat diterima, dimitigasi, ditransfer atau kombinasinya.

Berdasarkan SEOJK 29 /SEOJK.03/2022 tentang Ketahanan Dan Keamanan Siber Bagi Bank Umum menyebutkan bahwa Penerapan manajemen risiko terkait keamanan siber mencakup 4 (empat) aspek, yaitu :

a) Tata kelola risiko terkait keamanan siber, yang meliputi kecukupan pengawasan aktif oleh Direksi dan Dewan Komisaris, perumusan tingkat risiko terkait keamanan siber yang akan diambil (risk appetite) dan toleransi risiko terkait keamanan siber (risk tolerance), serta budaya dan kesadaran risiko terkait keamanan siber;

b) Kerangka manajemen risiko terkait keamanan siber, yang meliputi strategi manajemen risiko, kecukupan perangkat organisasi, serta kecukupan kebijakan, prosedur, dan penetapan limit risiko, terkait keamanan siber;

c) Proses manajemen risiko, kecukupan sumber daya manusia (SDM), serta kecukupan sistem informasi manajemen risiko, terkait keamanan siber; dan

d) Sistem pengendalian risiko terkait keamanan siber, yang meliputi kecukupan sistem pengendalian intern dan kecukupan kaji ulang.

A. Jenis Risiko terkait Aktivitas Proyek dan Pengembangan Sistem

Ada beberapa risiko terkait aktivitas proyek dan pengembangan sistem, yaitu:

1. Risiko Operasional. Pada umumnya terjadi karena spesifikasi kebutuhan yang tidak jelas dan memadai, kelemahan pada sistem yang dikembangkan, proses *testing* (UT, SIT dan UAT), kesalahan pada saat proses migrasi data serta tidak

IV. RISK MANAGEMENT IN PROJECT MANAGEMENT AND SYSTEM DEVELOPMENT

Management ensure that internal and external risk in project implementation has been identified, measured, reported, reviewed and mitigated properly at each SDLC phase. In risk mitigation that identified enforce organization to develop strategy risk that is tolerable, mitigated, transferred or the combination.

Based on SEOJK 29/SEOJK.03/2022 concerning Resilience and Cybersecurity for Commercial Banks, it states that the implementation of risk management related to cybersecurity includes 4 (four) aspects, namely:

a) Governance of risks related to cybersecurity, which includes adequacy of active oversight by the Board of Directors and Board of Commissioners, formulation of risk levels related to cybersecurity to be taken (risk appetite) and risk tolerance related to cybersecurity (risk tolerance), as well as culture and awareness of related risks cybersecurity;

b) Risk management framework related to cybersecurity, which includes risk management strategies, adequacy of organizational tools, as well as adequacy of policies, procedures and risk limit setting, related to cybersecurity;

c) Adequacy of risk management processes, human resources (HR), and risk management information systems, related to cybersecurity; And

d) Risk control system related to cybersecurity, which includes the adequacy of the internal control system and the adequacy of reviews.

A. Risk Level Related to Project Activity and System Development

Following is risk related to project activity and system development:

1. Operational Risk. Usually happen because of unclear and insufficient requirement specification, system weakness, testing process (UT, SIT and UAT), mistake in data migration process include unavailability of resource and regulation that

tersedianya *resource* dan aturan untuk mendukung kegiatan operasional.

2. Risiko Reputasi. Pada umumnya terjadi karena kurang tanggap/pengabaian permasalahan yang terjadi, yang mengakibatkan permasalahan yang sama akan terus terjadi.
3. Risiko Strategik. Pada umumnya terjadi karena sistem yang dikembangkan gagal memenuhi kebutuhan bisnis Bank atau kebutuhan Nasabah
4. Risiko Kepatuhan. Pada umumnya terjadi karena kegagalan Bank dalam mengikuti regulasi atau peraturan yang berlaku atas proyek yang dikerjakan.

Pada proses pengembangan, Manajemen harus memperhatikan risiko terkait berikut:

1. Ruang lingkup sistem yang dikembangkan meliputi sensivitas data yang diakses, dilindungi atau dikendalikan, volume transaksi dan tingkat pentingnya aktivitas dan fungsi tersebut terhadap bisnis Bank.
2. Teknologi yang digunakan meliputi kehandalan, keamanan, ketersediaan dan ketepatan waktu serta kemampuan mengikuti perkembangan teknologi dan perubahan ketentuan

B. Pengendalian Risiko pada Pengadaan

Berikut adalah pedoman untuk pengendalian risiko pada pengadaan:

1. Melakukan perbandingan atas produk sejenis, seperti kesesuaian fungsi dengan kondisi Bank, harga, kualitas, waktu penyerahan dan komitmen dalam memberikan dukungan (jumlah karyawan dan tugasnya, ruang lingkup bisnis yang dijalankan dan lain-lain).
2. Pemilihan infrastruktur untuk sistem yang akan digunakan sudah teruji. Tanyakan ke pihak vendor mengenai *platform* yang disarankan untuk digunakan oleh sistem tersebut.
3. Memastikan proposal dan perjanjian telah mengatur secara jelas persyaratan minimum yang

supports operational activity.

2. Reputation Risk. Usually happen because not responsive/neglect problem that is happen and cause the same problem will always happen.
3. Strategic Risk. Usually happen because developed system is fail to fulfill requirement of business Bank or Customer requirement.
4. Compliance Risk. Usually happen because Bank fails to follow rule or regulation during project.

In development process, Management pay attention following risk:

1. System scope that covers data sensitivity that is accessed, protected or controlled, transaction volume and importance level of activity and function to business Bank.
2. Technology covers reliability, security, availability and timeliness includes capability to follow development of technology and changes of regulation.

B. Risk Control in Procurement

Following is guideline to control risk in procurement:

1. Compare the same product, such as function suitability with Bank condition, price, quality, schedule and support commitment (number of employee and its job description, scope business and other)
2. Select system infrastructure that has been tested. Ask to vendor about platform suggestion to use for the system.
3. Ensure the proposal and agreement has stipulate clearly about minimum requirement, such as:

ditetapkan, seperti

a. Lisensi sistem atau *software*
   1) Jangka waktu
   2) Penggunaan secara eksklusif atau tidak
   3) Perhitungan lisensi (Jumlah pengguna atau Transaksi atau lainnya) yang diatur
   4) Lokasi penggunaan
   5) Berlaku untuk *offsite backup* atau tidak

b. Pemeliharaan
   1) Periode pemeliharaan
   2) Biaya pemeliharaan, mekanisme pembayaran serta dasar kenaikannya
   3) Ruang lingkup.

c. Garansi
   1) Tidak melanggar hak kekayaan intelektual.
   2) Tidak mengandung kode rahasia/terbatas yang tidak diungkapkan/pembatasan otomatis pada perjanjian.
   3) Akan bekerja sesuai spesifikasi/tanggung jawab vendor bila terjadi masalah.
   4) Perjanjian lisensi tetap berlaku bila terjadi merger/perubahan pemilikan pada Bank/Vendor.

d. Penyelesaian Perselisihan

   Memastikan klasul penyelesaian perselisihan pada kontrak dan perjanjian lisensi.

4. Perubahan Perjanjian

   Perubahan harus disetujui oleh kedua belah pihak.

5. Keamanan
   a. Hasil kaji ulang kinerja sistem (*system performance review*).
   b. Kesesuaian dengan *user requirement*.

a. System software license
   1) Schedule
   2) Exclusive use or not
   3) License calculation (number of user or number of transaction)
   4) Location of use
   5) Includes offsite backup or not

b. Maintenance
   1) Maintenance period.
   2) Maintenance cost, payment mechanism, cost increase base.
   3) Scope.

c. Warranty
   1) Not violate copyright
   2) Not have back door code and should be stipulated in the agreement.
   3) Will work following specification/vendor responsibility if occur problem.
   4) License agreement is valid if Vendor/Bank change ownership/merger

d. Dispute Resolution

   Ensure the dispute resolution is stipulated at agreement and license agreement.

4. Agreement Amendment

   Amendment is agreed by both parties

5. Security
   a. Vendor responsibility to always keep Bank confidential information.
   b. Prohibit vendor to disclose Bank information without Bank approval.

c. Masalah yang terjadi dan solusi atau eskalasi atau langkah penyelesaian yang dilakukan.

d. Efektivitas pengamanan yang ditetapkan.

6. Sub Kontrak ke Pihak Ketiga

Vendor dilarang melakukan sub-kontak kepada pihak lain tanpa persetujuan Bank, bila terdapat kondisi yang mengharuskan proses sub kontrak maka harus mendapat persetujuan dari Bank.

7. SLA

a. *Service Level Agreement* (SLA) ditetapkan untuk semua sistem

b. Standar kinerja seperti waktu tanggap

c. Tingkat kinerja

d. SLA tetap berlaku apabila terjadi perubahan kepemilikan pada Bank dan atau penyedia jasa

e. Laporan rutin dari vendor terkait dengan kinerja sistem

C. Dokumentasi

Dokumen-dokumen yang harus disimpan selama pengembangan/pengadaan:

1. *Problem Report*. *Problem report* dibuat sebagai dokumentasi dari semua masalah atau kesalahan yang terjadi. *Problem report* harus terdokumentasi dengan baik dan teratur, sehingga dapat menjadi bahan perbaikan pada proyek berikutnya.

2. Meeting mingguan dan status laporan. Meeting mingguan diadakan sebagai media untuk membahas permasalahan yang ada dan pekerjaan berikutnya. Meeting mingguan dilakukan secara teratur dan didokumentasikan dengan baik.

3. Laporan status proyek mingguan digunakan untuk mencatat perkembangan proyek dalam satu minggu. Laporan disampaikan ke

c. Vendor warranty about the software does not contain back door that enables unauthorized party to use Bank system.

d. Vendor is not using function that can cause software not functioned.

6. Sub Contract to Third Party

Vendor is not allowed to sub contract to third party without Bank approval, if condition should happen, the process of sub contract should get Bank approval.

7. SLA

a. Service Level Agreement (SLA) is stipulated for all systems

b. Standard performance such as response time

c. Performance Level

d. SLA is valid even though there is a change in Bank or vendor ownership.

e. Regular report from vendor related to system performance

C. Documentation

Document that should be maintained during development/procurement:

1. Problem Report. Problem report is made as documentation from all problems or mistake happened. Problem report should be well and properly documented.

2. Weekly meeting and report status. Weekly meeting is held as media to discuss problem and next action. Weekly meeting is held regularly and well documented.

3. Report of weekly project status is use to record progress of project in a week. Report is reported to Director in charge.

Direktur yang membawahi

4. Dokumen hasil pengujian (SIT dan UAT).
5. Dokumen serah terima. Setiap tahapan proyek harus disertakan dengan dokumen serah terima yang ditandatangani oleh kedua belah pihak (Vendor, Tim Proyek, PMO, User dan Manajer Proyek). Manajer Proyek memastikan bahwa semua pihak telah melakukan setiap tahapan dengan sukses sebelum ditandatangani.
6. Laporan lainnya/Memo. Izin pembelian perangkat keras dan perangkat lunak dan izin implementasi sistem
7. Laporan ke pihak regulator, meliputi rencana dan realisasi implementasi sistem baru.

Dokumen terkait perubahan setidaknya mencakup hal-hal berikut:

1. Informasi penting yang menjadi prioritas.
2. Identifikasi sistem, database dan satuan kerja yang terpengaruh.
3. Nama PIC yang melakukan perubahan.
4. Kebutuhan sumber daya.
5. Perkiraan biaya
6. Perkiraan tanggal penyelesaian dan Implementasi.
7. Pertimbangan Keamanan dan Kehandalan.
8. Hasil test.
9. Prosedur implementasi.
10. Perkiraan *Downtime* saat implementasi.
11. Prosedur *Backup*.
12. Pengkinian dokumentasi yang terkait seperti rancangan program, *script*, topologi jaringan, manual pengguna, rencana keberlangsungan dan lain-lain.

D. Manajemen Perubahan

Dalam pelaksanaan suatu proyek dimungkinkan adanya perubahan pada proyek yang sudah direncanakan karena beberapa alasan, seperti perubahan

4. Testing document (SIT and UAT).
5. Deliverables document. Each project phase has document deliverables that is sign by both parties (vendor, Project Team, PMO, User and Project Manager). Project Manager ensure that all parties has conduct every phase before sign off.
6. Other report/Memo. Approval to purchase hardware and software and approval to implement system.
7. Report to regulator, consisting about plan and implementation realization of the new system.

Document related to changes at least consist of the following:

1. Important information that become priority.
2. System identification, database and related unit work
3. PIC name
4. Human resource needed.
5. Cost estimation
6. Estimation of completion date and implementation
7. Consideration of security and capability
8. Test result
9. Implementation procedure
10. Downtime estimation during implementation.
11. Backup procedure
12. Update related document such as design program, script, network topology, user manual and contingency plan and others.

D. Change Management

Changes are possible in project implementation that is cause by organization changes, regulation changes and other. The changes should

organisasi, perubahan aturan, dan sebagainya. Perubahan tersebut harus disetujui oleh seluruh pihak yang terkait karena dapat berakibat pada jadwal dan biaya proyek.

be agreed by related party because impact to project schedule and cost.

Ada beberapa faktor yang menyebabkan terjadinya perubahan, diantaranya adalah sebagai berikut:

Following is factor that causing changes:

1. Tidak didefinisikannya kebutuhan atau pengertian pada tahapan awal.
2. Salah dalam menginterprestasikan kebutuhan atau suatu pengertian.
3. Faktor luar seperti peraturan pemerintah yang menciptakan permintaan baru.
4. Perubahan didalam organisasi, seperti *merger* atau akuisisi.
5. Adanya teknologi yang lebih baik.
6. Perubahan organisasi, budaya dan/atau proses bisnis.
7. Kebutuhan baru.
8. Adanya pengurangan biaya proyek atau permintaan penyelesaian proyek yang lebih cepat.

1. Undefined requirement or description at initiation phase.
2. Mistake in interpret requirement or description.
3. External factor such as government regulation that creates new requirement.
4. Organization structure changes such as merger or acquisitions.
5. Better technology
6. Changes in the organization, culture and/or business process.
7. New Requirement
8. Cost reduction or request to implement project faster than planned.

Pelaksanaan suatu manajemen perubahan perlu diatur suatu prosedur agar perubahan yang terjadi bisa dimonitor dan dikendalikan sesuai dengan prioritas kebutuhannya. Adapun prosedur dari manajemen perubahan adalah sebagai berikut:

Change management implementation is stipulated in a procedure so changes is monitored and controlled according to requirement priority. Following is change management procedure:

1. Permintaan perubahan dari user.
2. Permintaan perubahan tersebut dievaluasi oleh Tim Proyek dan disetujui oleh Manajer Proyek. Evaluasi mencakup:
   a. Alasan perubahan
   b. Alasan penolakan (jika ditolak)
   c. PIC dari Bank
   d. PIC dari Vendor
   e. Duplikat source code (jika ada)
   f. Tanggal dan waktu perubahan
3. Proyek Manajer akan membuat dokumen persetujuan dari Direksi.
4. Setelah mendapat persetujuan Direksi, perubahan diajukan ke pihak internal/vendor untuk dilaksanakan.

1. Change request from user.
2. Change request is evaluated by Project Team and approved by Project Manager. Evaluation consist of the following:
   a. Reason of change request
   b. Reject reason (if rejected)
   c. Bank PIC
   d. Vendor PIC
   e. Source code duplicate (if any)
   f. Date and time implementation
3. Project Manager will create request for approval to Board of Directors.
4. After get approval from Board of Directors, changes is submit to internal/vendor to be implemented.

5. Proses perubahan dilakukan di unit pengembangan.
6. Proses pengujian di unit pengembangan tetap dilakukan secara bertahap (UT, SIT dan UAT).
7. Sebelum perubahan diimplementasikan, PIC Bank meminta persetujuan dengan mengacu ke tahapan implementasi dan kaji ulang.

5. Changes are conducted at development unit.
6. Testing process at development unit still conducted in stages (UT, SIT and UAT).
7. Before implements changes, Bank PIC request approval by refers to implementation phase and review.

V. PENUTUP

Kebijakan Managemen Proyek dan Pemgembangan Sistem Edisi 9 ini diterbitkan dalam Bahasa Indonesia dan Bahasa Inggris, dan bilamana terjadi perbedaan penafsiran antara keduanya maka yang menjadi acuan adalah Bahasa Indonesia

Kebijakan mulai berlaku sejak memperoleh persetujuan Presiden Direktur pada tanggal 21 Maret 2023 dan Dewan Komisaris pada tanggal 5 April 2023 dan mencabut Kebijakan Manajemen Proyek dan Pengembangan Sistem Edisi 8, November 2020.

Kebijakan 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

This 9th Edition of Project Management and System Development Policy is published in Indonesian and English, and if there is a difference in interpretation between the two, the reference is Indonesian.

The policy comes into effect since obtaining the approval of the President Director on March 21st, 2023 and the Board of Commissioners on April 5th, 2023 and revoking the Project Management and System Development Policy Edition 8, November 2020

This policy will be reviewed at latest every 2 (two) years or if needed as an improvement effort following the business development and the need of Bank or following the changes of base regulation.