

LAPORAN KERJA PRAKTEK

AUDIT SISTEM INFORMASI BERBASIS COBIT 5 PADA Bank BTPN Syariah



Oleh :

Kevin Giovanni Pradana

1301164677

PROGRAM STUDI S1 INFORMATIKA
FAKULTAS INFORMATIKA
UNIVERSITAS TELKOM
JULI 2019

LAPORAN KERJA PRAKTEK

AUDIT SISTEM INFORMASI BERBASIS COBIT 5 PADA Bank BTPN Syariah

Sebagai salah satu syarat dalam melaksanakan perkuliahan Mata Kuliah Kerja Praktek

Oleh :

Kevin Giovanni Pradana 1301164677

Bandung, 1 Agustus 2019

Menyetujui,
Dosen Pembimbing Akademik

Mahasiswa

Danang Triantoro Murdiansyah, S.Si., M.T.

Kevin Giovanni Pradana

NIP 14870045

NIM 1301164677

Mengetahui,
Ketua Program Studi S1 Informatika

Niken Dwi Wahyu Cahyani S.T.,M.Kom.,Ph.D.
NIP 00750052

ABSTRAK

Nama : Kevin Giovanni Pradana

Program Studi : S1 Informatika

Judul : Audit Sistem Informasi pada perusahaan Bank BTPN Syariah

Sistem Informasi dan Teknologi Informasi menjadi bagian yang tidak terpisahkan dalam operasi bisnis perusahaan. Sistem informasi ini membawa kemudahan dan efisiensi dalam operasi perusahaan namun juga membawa berbagai macam resiko baru. Sehingga dibutuhkan berbagai macam prosedur, metode, serta pengendalian untuk mengelola resiko tersebut. Audit sistem informasi dibutuhkan juga untuk mengkaji dan menguji efektifitas pengendalian-pengendalian yang ada di sebuah perusahaan. Laporan ini menjelaskan tentang audit sistem informasi yang dilaksanakan penulis selama menjalani program magang.

Kata Kunci :

Audit, Sistem Informasi, Bank, Laporan, Teknologi Informasi

KATA PENGANTAR

Puji syukur atas kehadiran Allah SWT yang telah melimpahkan rahmat, hidayah dan inayah-NYA sehingga penulis bisa menyelesaikan laporan kerja praktek di PT Bank BTPN Syariah.

Laporan ini dibuat sebagai salah satu syarat untuk memenuhi persyaratan tugas mata kuliah kerja praktek di program studi Informatika – S1 Universitas Telkom Bandung. Tujuan dibuatnya laporan magang ini yaitu untuk melaporkan segala sesuatu yang ada kaitannya dengan dunia kerja di PT BTPN Syariah Kuningan.

Dalam penyusunan laporan magang ini, tentu tak lepas dari arahan dan bimbingan dari berbagai pihak. Oleh sebab itu, penulis mengucapkan rasa hormat dan terima kasih kepada semua pihak yang telah membantu. Pihak-pihak yang terkait tersebut diantaranya sebagai berikut:

1. Dosen pembimbing akademik di program studi S1 Informatika – Bapak Danang
2. Bapak Gustiawan , selaku pembimbing kerja praktek lapangan
3. Bapak Ruhimat, selaku kepala divisi IT Security
4. Karyawan dan karyawan PT Bank BTPN Syariah yang memberikan pengarahan dan petunjuk selama program kerja praktek berlangsung
5. Orang Tua dan teman-teman yang selalu mendukung

Karena kebaikan semua pihak yang telah penulis sebutkan tadi, maka penulis bisa menyelesaikan laporan magang ini dengan sebaik-baiknya. Laporan magang ini memang masih jauh dari kesempurnaan, tetapi penulis sudah berusaha sebaik mungkin. Sekali lagi terima kasih, semoga laporan magang ini bisa bermanfaat bagi kita semua.

Jakarta, 5 Agustus 2019

Kevin Giovanni Pradana

DAFTAR ISI

ABSTRAK.....	3
KATA PENGANTAR	4
DAFTAR ISI	5
DAFTAR TABEL.....	7
DAFTAR GAMBAR	8
BAB I.....	9
PENDAHULUAN.....	9
1.1 Latar Belakang Kerja Praktek	9
1.2 Latar Belakang Judul	10
1.3 Rumusan Masalah.....	11
1.4 Tujuan	11
1.5 Manfaat	11
1.6 Waktu dan tempat pelaksanaan kerja praktek	12
BAB II.....	13
TINJAUAN TEORI.....	13
2.1 Teknologi Informasi	13
2.2 Sistem Informasi	13
2.3 Pengertian <i>Auditing</i>	13
2.4 Pengertian Audit Sistem Informasi.....	14
2.5 Tujuan Audit Sistem Informasi	14
2.6 Audit Internal.....	15
2.6.2 Fungsi Audit Internal.....	16
2.7 COBIT	16
2.8 COBIT 5	17
2.9 Prinsip COBIT 5	17
BAB III	19
PROFIL PERUSAHAAN.....	19
3.1 Deskripsi Perusahaan.....	19
BAB IV	20
PEMBAHASAN HASIL / PELAKSANAAN KERJA PRAKTEK	20
4.1 Ruang Lingkup Materi / Kegiatan.....	20
4.2 Bentuk Kegiatan.....	21
4.2.1 Kajian BAU	21
4.2.2 Kajian Tematik.....	21
4.2.3 Kajian Strategic.....	21
4.2.4 Kajian Improvement	22

4.3 Hasil Kerja Praktek	22
4.3.1 Tugas yang dikerjakan.....	22
4.3.1.4 Menerima dan mencari temuan yang sesuai dengan prosedur yang berlaku	22
4.3.2 Domain-domain COBIT 5 yang digunakan dalam melakukan mapping PRC.....	23
4.3.3 Pengerjaan kertas kerja	42
BAB V	59
PENUTUP	59
5.1 Kesimpulan	59
5.2 Saran	59
5.3 Daftar Pustaka	59
5.4 Lampiran-lampiran	60

DAFTAR TABEL

Tabel 1 hasil pemeriksaan bulan juni	55
Tabel 2 hasil pemeriksaan bulan juli	56

DAFTAR GAMBAR

Gambar 1 5 prinsip-prinsip COBIT 5	17
Gambar 2 EDM01	23
Gambar 3 EDM02	23
Gambar 4 EDM03	24
Gambar 5 EDM04	24
Gambar 6 EDM05	24
Gambar 7 APO01	25
Gambar 8 APO02	26
Gambar 9 APO03	26
Gambar 10 APO04	27
Gambar 11 APO05	27
Gambar 12 APO06	28
Gambar 13 APO07	28
Gambar 14 APO08	29
Gambar 15 APO09	29
Gambar 16 APO10	30
Gambar 17 APO11	30
Gambar 18 APO12	31
Gambar 19 APO13	31
Gambar 20 BAI01	32
Gambar 21 BAI02	33
Gambar 22 BAI03	33
Gambar 23 BAI04	34
Gambar 24 BAI05	34
Gambar 25 BAI06	35
Gambar 26 BAI07	35
Gambar 27 BAI08	36
Gambar 28 BAI09	36
Gambar 29 BAI10	37
Gambar 30 DSS01	37
Gambar 31 DSS02	38
Gambar 32 DSS03	38
Gambar 33 DSS04	39
Gambar 34 DSS05	39
Gambar 35 DSS06	40
Gambar 36 MEA01	40
Gambar 37 MEA02	41
Gambar 38 MEA03	41
Gambar 39	42

BAB I

PENDAHULUAN

1.1 Latar Belakang Kerja Praktek

Magang atau disebut kerja praktek bagi mahasiswa di perusahaan dan lembaga-lembaga pemerintah ataupun lembaga non pemerintah adalah salah satu mata kuliah dari Program Studi S1 Informatika Fakultas Informatika Universitas Telkom Bandung Jawa Barat yang wajib diikuti oleh mahasiswa semester VI dengan bobot 2 Satuan Kredit Semester (SKS).

Program magang di Universitas Telkom merupakan suatu proses belajar mengajar atau praktek langsung bagi mahasiswa untuk menambah wawasan, pengetahuan, keterampilan dan etika pergaulan khususnya pada lingkungan kerja nyata bagi mahasiswa sebelum mahasiswa tersebut memasuki dunia pekerjaan yang sebenarnya.

Perguruan tinggi sebagai institusi pendidikan memiliki peran yang sangat besar dalam upaya pengembangan sumber daya manusia (SDM) dan peningkatan daya saing bangsa. Agar peran yang strategis dan besar tersebut dapat dijalankan dengan baik maka lulusan perguruan tinggi haruslah memiliki kualitas yang unggul.

Dalam masa ini seorang mahasiswa bukan hanya dituntut berkompeten dalam bidang kajian ilmunya tetapi juga dituntut untuk memiliki jejaring yang luas, mampu mengambil keputusan, peka terhadap perubahan dan perkembangan yang terjadi di dunia pekerjaan dan luar.

Program kerja praktek ini dilaksanakan minimal 40 hari kerja dan maksimal 60 hari kerja sesuai dengan kurikulum di Universitas Telkom, mahasiswa akan memilih topik dan judul magang serta memilih tempat dan lokasi perusahaan swasta, lembaga-lembaga pemerintah maupun non pemerintah yang dituju.

Fakta yang terjadi menunjukkan bahwa mahasiswa dengan kualifikasi tersebut sulit ditemukan untuk hal tersebut maka dibutuhkan sebuah program Kerja Praktek (magang) sebagai sarana pembelajaran bagi mahasiswa Program Studi Informatika Universitas Telkom Bandung untuk memperoleh berbagai kompetensi *holistic* yang dibutuhkan setelah menyelesaikan pendidikan

Berdasarkan uraian diatas maka penulis tertarik melaksanakan program magang ini pada bidang sistem informasi salah satu bank yang ada di jakarta selatan, salah satu perusahaan bank PT Bank BTPN Syariah yang berkedudukan di menara BTPN kuningan, Jakarta Selatan yang bergerak dibidang perbankan.

Pada Bank BTPN Syariah terdapat divisi IT yang setiap bulannya harus menjalankan prosedur yang telah dibuat sebelumnya dan akan di laksanakan proses audit setiap bulannya untuk memastikan bahwa prosedur berjalan serta masalah-masalah atau insiden yang terjadi dapat diselesaikan dan ditanggulangi kedepannya.

1.2 Latar Belakang Judul

Dalam menjalankan kegiatan bisnisnya sehari-hari, setiap perusahaan sangat mengandalkan sistem informasi perusahaan yang mereka miliki. Mereka mengelola, menyimpan, dan memanfaatkan informasi yang mereka miliki dengan menggunakan sistem informasi dan teknologi informasi perusahaan tersebut. Sistem informasi perusahaan ini meliputi seluruh perangkat keras, perangkat lunak, basis data, jaringan, prosedur dan manusia yang dimiliki oleh perusahaan. Baik buruknya sebuah perusahaan juga bergantung dengan bagaimana sistem informasi atau teknologi informasi perusahaan mereka. Dengan sistem informasi atau teknologi informasi yang bagus dan sesuai, perusahaan bisa beroperasi lebih cepat, efektif, dan menguntungkan. Oleh karena itu perusahaan menghabiskan sumber daya yang tidak sedikit untuk merancang, membuat, dan mengelola sistem informasi yang mereka miliki.

Perusahaan seiring dengan berkembangnya teknologi informasi menjadi menyebabkan ketergantungan lebih terhadap teknologi informasi. Teknologi informasi merubah bagaimana cara perusahaan melakukan kegiatan bisnisnya. Seluruh aktivitas mulai dari transaksi, monitoring, feedback, keluhan dan lain sebagainya di perusahaan menjadi sangat tergantung dengan komputer.

Semua data mulai dari data pelanggan, transaksi, perubahan aplikasi dan lainnya disimpan dalam bentuk *cloud* atau disimpan didalamn *harddisk* pada *server* yang pasti menggunakan komputer. Sistem informasi perusahaan menjadi lebih kompleks, terdiri dari beberapa sistem terpisah yang terintegrasi menjadi satu dalam sebuah jaringan. Infrastruktur dan sumber daya teknologi informasi perusahaan menjadi sebuah aset penting yang perlu dikelola dengan baik. Di lain pihak ketergantungan perusahaan terhadap teknologi informasi ini juga membawa resiko-resiko baru. Data dan informasi perusahaan menjadi lebih rawan dari sisi keamanannya karena bentuk data *cloud* dan *harddisk* dapat sewaktu-waktu rusak, dimanipulasi, maupun hilang diambil atau dicuri oleh pihak tertentu. Maka dari itu dibutuhkan finansial dan perencanaan finansial yang besar dan baik. Dan dibutuhkan juga sumber daya manusia yang mumpuni untuk membangun dan mengelola sistem informasi tersebut. Dan yang tidak kalah penting adalah dibutuhkannya manajemen sistema informasi (*Management Information System* atau MIS) dan yang dibahas pada laporan ini yaitu tata kelola sistema informasi (*IT Governance*) yang baik dan efektif untuk mengelola dan mengatur infrastruktur teknologi informasi dan sistem informasi perusahaan.

Meningkatnya ketergantungan perusahaan terhadap teknologi informasi dan sistem informasi juga membawa perubahan pada proses audit pada bagian *quality* sebuah perusahaan. Audit *quality managemet* memiliki tujuan untuk memberikan keyakinan bahwa laporan *quality* di berbagai aspek teknologi informasi perusahaan berjalan sesuai aturan dan prosedur yang berlaku saat itu. Dikarenakan proses transaksi, penyimpanan data, dan berbagai laporan lainnya menjadi terkomputerisasi, auditor menjadi sulit untuk tidak memperhatikan IT perusahaan dan harus mempertimbangkannya dalam proses audit

mereka. Oleh karena itu muncullah audit sistem informasi yang berfungsi untuk memberikan *assessment* dan *assurance* atas sistem informasi perusahaan.

Audit Sistem Informasi ini dilakukan oleh Auditor Sistem Informasi. Pada proses audit sistem informasi ini Auditor sistem informasi akan memberikan *assessment* dan evaluasi atas *IT Governance* perusahaan, kontrol-kontrol IT yang ada, dan prosedur serta keamanan dari sistem informasi perusahaan. Audit sistem informasi ini tidak hanya memberikan keyakinan bahwa auditor telah mempertimbangkan semua resiko dan control yang ada namun juga dapat mengurangi cakupan audit laporan *quality (Scope of The Audit)*.

Semakin pentingnya audit sistem informasi dalam sistem perusahaan menjadi alasan mengapa penulis memilih tema audit sistem informasi dalam laporan magang ini. Alasan lainnya adalah penulis juga mendapati betapa pentingnya audit sistem informasi secara langsung. Penulis selama magang mendapatkan penugasan untuk melakukan audit sistem informasi pada perusahaan Bank BTPN Syariah. Dalam penugasan ini penulis terlibat pada proses Audit *Incident* dan *Problem management* serta monitoring ticket dan lain sebagainya.

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat diuraikan rumusan masalah dari kegiatan kerja praktek ini yaitu apa prosedur dan bagaimana proses audit yang dilakukan oleh Bank BTPN Syariah ?

1.4 Tujuan

Adapun tujuan penulis dalam melakukan kegiatan magang ini adalah untuk mengetahui proses IT Audit dan prosedur serta *problema* dan *incident* yang ada dan mungkin terjadi kedepannya pada PT Bank BTPN Syariah.

1.5 Manfaat

Kerja praktek merupakan proses untuk mempelajari praktek-praktek pekerjaan yang nyata pada dunia perkantoran, sehingga diharapkan kerja praktek akan memberi manfaat sebagai berikut :

1. Bagi Penulis

Penulis dapat mengaplikasikan ilmu dan teori-teori yang telah dipelajari selama perkuliahan juga memberikan pengetahuan tentang suasana dunia kerja secara nyata dan memberikan pengalaman baru bagi penulis.

2. Bagi Perusahaan

Hasil audit ini bisa menjadi acuan bagi perusahaan untuk bagian ITQM (Information technology quality management) dalam memperbaiki kekurangan pada masalah terkait *incident* dan *problem* management dan berbagai hal lainnya sekaligus untuk membantu dokumentasi untuk peserta magang selanjutnya.

1.6 Waktu dan tempat pelaksanaan kerja praktek

Kegiatan kerja praktek ini dilaksanakan di PT. Bank BTPN Syariah yang beralamat di Menara BTPN Lt. 15 Kuningan RT.5/RW.2, Setia Budi, 12950 Jakarta Selatan. Pelaksanaan magang direncanakan berlangsung selama dua bulan atau 40 hari kerja. dengan hari kerja 5 hari seminggu dengan jam masuk dimulai dari jam 9.00 WIB hingga jam 17.00 WIB

BAB II

TINJAUAN TEORI

2.1 Teknologi Informasi

Teknologi Informasi (TI) menurut Sawyer (2007) adalah teknologi apapun yang membantu manusia dalam membuat, mengubah, menyimpan, mengomunikasikan dan/atau menyebarkan informasi. TI menyatukan komputasi dan komunikasi berkecepatan tinggi untuk data, suara dan video. Sedangkan dalam konteks bisnis menurut “Information Technology Association of America”, seperti yang dikutip oleh Dennis & Michael (1985), teknologi informasi adalah pengolahan, penyimpanan dan penyebaran vokal, informasi bergambar, teks dan numerik oleh mikroelektronika berbasis kombinasi komputasi dan telekomunikasi. Jadi bisa disimpulkan bahwa teknologi adalah kombinasi teknologi komputer dan telekomunikasi yang digunakan untuk mengolah informasi. Informasi sendiri mengandung suatu arti yaitu data yang telah diolah ke dalam suatu bentuk yang lebih memiliki arti dan dapat digunakan (Turban, Rainer, & Porter, 2005).

Peranan dan kegunaan teknologi dalam dunia bisnis adalah untuk melakukan otomisasi proses bisnis yang dilakukan perusahaan, pengolahan data dan informasi untuk pengambilan keputusan, menghubungkan antara perusahaan dengan konsumen serta supplier, dan menggunakannya sebagai alat untuk meningkatkan efektifitas perusahaan. Semakin berkembangnya teknologi komputer dan telekomunikasi menyebabkan Teknologi Informasi menjadi bagian yang tidak dapat dipisahkan bagian perusahaan saat jaman sekarang. [2]

2.2 Sistem Informasi

Sistem menurut McLeod dan Schell (2001) adalah sekumpulan elemen, baik itu proses, teknologi, atau aktivitas manusia, yang terintegrasi dan berkerja bersama-sama untuk mencapai tujuan atau obyektif yang sama. Sementara itu informasi adalah data yang telah diolah ke dalam suatu bentuk yang lebih memiliki arti dan dapat digunakan (Turban, Rainer, & Porter, 2005). Sehingga secara umum bisa dikatakan bahwa sistem informasi adalah sekumpulan teknologi informasi, proses, dan aktivitas manusia yang berkerja atau digunakan secara bersama-sama untuk mengolah data menjadi suatu bentuk yang lebih memiliki arti dan dapat digunakan. Dalam konteks bisnis, sistem informasi mengalami perluasan definisi dimana tidak hanya merujuk pada penggunaan organisasi teknologi informasi namun juga merujuk pada bagaimana cara orang memanfaatkan dan menggunakannya untuk mendukung proses bisnis perusahaan (Kroenke, 2008).[2]

2.3 Pengertian *Auditing*

Menurut Arens, Elder dan Beasley dalam buku berjudul *Auditing dan Jasa Assurance* (2011:4) audit adalah pengumpulan data dan evaluasi bukti tentang informasi

untuk menentukan dan melaporkan derajat kesesuaian antara informasi itu dan kriteria yang telah diterapkan. Audit harus dilakukan oleh orang yang kompeten dan independen

Sedangkan menurut Mulyadi (1998;7) auditing adalah “proses sistematis untuk memperoleh dan mengevaluasi bukti secara objektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang ditetapkan, serta menyampaikan hasilhasilnya kepada pemakai yang berkepentingan”.

Sukrisno Agoes (2004:4), auditing adalah “suatu pemeriksaan yang dilakukan secara kritis dan sistematis oleh pihak yang independen, terhadap laporan keuangan yang telah disusun oleh manajemen beserta catatan-catatan pembukuan dan bukti-bukti pendukungnya, dengan tujuan untuk dapat memberikan pendapat mengenai kewajaran laporan keuangan tersebut”.

2.4 Pengertian Audit Sistem Informasi

Menurut Ron Webber dalam buku berjudul *Information Systems Control and Audit* (1999) Audit sistem informasi ialah proses mengumpulkan dan mengevaluasi fakta untuk memutuskan apakah sistem computer yang merupakan asset bagi perusahaan terlindungi, integritas data terpelihara, sesuai dengan tujuan organisasi untuk mencapai efektifitas dan efisiensi dalam penggunaan sumber daya teknologi yang ada.

Dari kedua definisi tersebut dapat didefinisikan bahwa suatu proses pengumpulan dan pengevaluasian bahan bukti informasi yang didapat dengan segala kriteria yang telah ditentukan, pemeriksaan juga harus dilakukan oleh seorang yang berkompeten dalam bidang audit. Cakupan audit yang penulis gunakan yaitu hanya audit internal saja.[2]

2.5 Tujuan Audit Sistem Informasi

Audit sistem informasi, baik yang menjadi bagian dari audit eksternal atau audit internal, memiliki tujuan untuk memberika *assurance* atau ketenangan bahwa sistem informasi perusahaan yang ada sudah sejalan dengan IT *Governance* yang telah dibuat. Namun secara spesifik Weber (1999) mengatakan bahwa tujuan dari audit sistem informasi ada empat, yaitu :

1. Mengamankan Aset

Aset yang dimaksud disini adalah asset sistem informasi perusahaan yang berupa perangkat keras, perangkat lunak, fasilitas pendukung, sumber daya, data, perlengkapan, dan peralatan teknologi informasi lainnya. Semakin besar ketergantungan perusahaan terhadap sistem informasinya, pengendalian atas berbagai asset informasi tersebut menjadi semakin penting.

2. Memelihara Integritas Data

Integritas data adalah keandalan, kelengkapan, kebenaran dan keakuratan data. Integritas data yang buruk dapat merugikan perusahaan dikarenakan data mudah hilang, rusak, atau dimanipulasi sehingga bisa merugikan perusahaan secara finansial dan mengurangi kompetensi perusahaan. Audit sistem informasi bertujuan untuk menjaga integritas data ini. Selain itu keefektifan data juga termasuk integritas data yang memiliki peran penting dalam perusahaan.

3. Meningkatkan Efektivitas

Audit sistem informasi memiliki suatu tujuan untuk memastikan bahwa sistem informasi yang sudah ada telah berjalan secara efektif implementasinya. Apakah sudah bisa secara efektif mendukung proses bisnis perusahaan dalam mencapai tujuannya.

4. Meningkatkan Efisiensi

Pengguna sumber daya sistem informasi dalam kegiatan bisnis perusahaan untuk tujuannya dapat menjadi suatu tolak ukur keberhasilan suatu sistem informasi dalam kegiatan operasional perusahaan. Sistem informasi dikatakan efisien jika dengan penggunaan sumber daya yang minimal bisa memberikan hasil atau output yang dibutuhkan oleh perusahaan dalam melakukan kegiatan bisnisnya untuk mencapai tujuan perusahaan. [2]

2.6 Audit Internal

2.6.1 Pengertian Audit Internal

Audit internal hanya terdapat dalam perusahaan yang relative besar. Dalam perusahaan ini, pimpinan perusahaan membentuk banyak departemen, bagian, seksi, atau suatu organisasi yang lain dan mendelegasikan sebagian wewenangnya kepada kepala-kepala unit organisasi tersebut. Pendelegasian wewenang kepada sejumlah unit organisasi inilah yang mendorong perlunya dibentuk suatu audit internal.

Menurut Arens-loebbecke (2005) mengatakan “Internal auditor adalah seseorang yang bekerja sebagai karyawan suatu organisasi untuk melakukan audit bagi kepentingan manajemen”

Menurut Sukrisno Agoes (2004:13), internal audit (pemeriksaan intern) pemeriksaan yang dilakukan oleh bagian internal audit perusahaan, baik terhadap laporan keuangan dan catatan akuntansi perusahaan, maupun ketaatan terhadap kebijakan manajemen puncak yang telah ditentukan dengan ketentuan-ketentuan yang berlaku.

Dari uraian diatas dapat dikatakan bahwa Audit Internal adalah pemeriksaan yang dilakukan oleh bagian internal audit perusahaan terhadap laporan keuangan dan catatan keuangan perusahaan mengenai ketelitian, dapat dipercaya, efisiensi dan internal control pada perusahaan dengan fungsi penilaian yang independen dan aktivitas membantu manajemen yang meliputi audit dan penilaian terhadap operasi pada seluruh tingkat organisasi perusahaan.

2.6.2 Fungsi Audit Internal

Fungsi audit internal memerlukan pemeriksaan yang berkualitas tinggi. Fungsi audit internal tidak akan berhasil tanpa adanya orang-orang yang mempunyai pengetahuan yang cukup, mempunyai daya imajinasi yang kuat, serta berinisiatif dan mempunyai kemampuan untuk berhubungan dengan orang lain. Fungsi audit internal juga ditentukan oleh bantuan dan dorongan yang penuh dan nyata dari pimpinan tertinggi di perusahaan.

Fungsi audit internal menurut Hiro Tugiman (2007:25) menyatakan bahwa:

“Fungsi audit internal adalah suatu pengawasan yang memiliki lingkup tidak terbatas tidak pembatas sumber, informasi, kewenangan untuk memeriksa hal apapun pada saat kapan pun, kebebasan untuk menyatakan sesuatu, menguji, mengevaluasi kegiatan organisasi yang dilaksanakan, dan dukungan sepenuhnya dari pimpinan organisasi”.

Fungsi audit internal menurut Mulyadi (1998 : 204), yaitu :

“Fungsi audit internal memantau kinerja pengendalian internal entitas. Pada waktu auditor berusaha memahami struktur pengendalian intern, ia harus berusaha memahami fungsi audit intern untuk mengidentifikasi aktivitas audit intern yang relevan dengan perencanaan audit. Lingkup prosedur yang diperlukan untuk memahami nya bervariasi, tergantung atas sifat aktifitas atas audit intern tersebut”.

Dari pengertian di atas dapat diketahui bahwa fungsi audit internal merupakan kegiatan penilaian yang bebas, yang terdapat dalam organisasi, yang dilakukan dengan cara memeriksa akuntansi, keuangan, dan kegiatan lain. Untuk memberikan jasa bagi manajemen dalam melaksanakan tanggung jawab mereka. Dengan cara menganalisis, menilai, rekomendasi, dan komentar-komentar penting terhadap kegiatan manajemen, auditor internal menyediakan jasa tersebut. Audit internal berhubungan dengan semua kegiatan perusahaan, sehingga tidak hanya terbatas pada audit catatan-catatan akuntansi.

2.7 COBIT

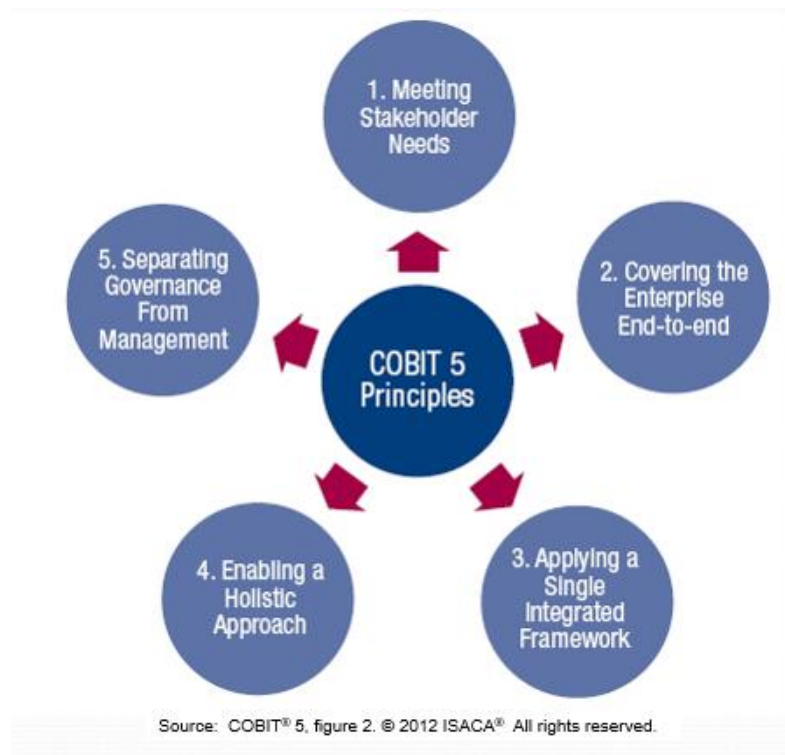
COBIT merupakan singkatan dari *Control Objectives for Information and Related Technology*, merupakan salah satu kerangka kerja (*framework*) dalam mendukung tata kelola teknologi informasi. Prinsip dasar pada *framework* COBIT adalah menyediakan informasi yang diperlukan untuk mencapai tujuan perusahaan atau organisasi. Perusahaan atau organisasi perlu mengatur dan mengatur sumber daya teknologi

informasi dengan menggunakan sekumpulan proses teknologi informasi yang terstruktur sehingga dapat memberikan informasi yang dibutuhkan [1]

2.8 COBIT 5

Cobit (*Control Objectives for Information and Related Technology*) diperkenalkan pada tahun 1996 oleh ISACA (*The Information System Audit and Control Association*). COBIT adalah kerangka kerja tata kelola IT (IT governance Framework) dan kumpulan perangkat yang mendukung dan memungkinkan para nanger untuk menjembatani jarak (gap) yang ada antara kebutuhan yang dikendalikan (control requirement), masalah teknis (*technical issues*) dan resiko bisnis (*business risk*). COBIT 5 adalah sebuah versi pembaruan yang menyatukan cara berpikir yang mutakhir di dalam teknik-teknik dan tata kelola TI perusahaan. Menyediakan prinsip-prinsip, praktek-praktek, alat-alat analisa yang telah diterima secara umum untuk meningkatkan kepercayaan dan nilai sistem-sistem informasi. Meningkatkan kepercayaan dan nilai sistem-sistem informasi. COBIT 5 dibangun berdasarkan pengembangan dari COBIT 4.1 dengan mengintegrasikan Val IT dan Risk IT dari ISACA, ITIL, dan standar-standar yang relevan dari ISO. [1]

2.9 Prinsip COBIT 5



Gambar 1 5 prinsip-prinsip COBIT 5

1. *Meeting stakeholders needs* (Memenuhi keinginan pemangku kepentingan)

Perusahaan menciptakan nilai bagi stakeholder dengan mempertahankan keseimbangan antara realisasi manfaat dan optimalisasi risiko serta penggunaan sumber daya.

2. *Covering the enterprise end-to-end* (Mencakup Enterprise End-to-end)

Mengintegrasikan tata kelola perusahaan TI dalam tata kelola perusahaan: mencakup semua fungsi dan proses dalam perusahaan menganggap semua tata kelola dan manajemen TI enabler untuk perusahaan.

3. *Applying a single integrated framework* (Menerapkan Single Framework yang Terpadu)

Berkaitan dengan IT standar dan praktik terbaik, masing-masing memberikan bimbingan pada subset dari kegiatan TI.

4. *Enabling a Holistic Approach* (Mengaktifkan tata Pendekatanyang menyeluruh)

Manajemen TI perusahaan yang efisien dan efektif memerlukan pendekatan yang menyeluruh, mempertimbangkan beberapa komponen yang berinteraksi. Cobit 5 mendefinisikan satu set enabler untuk mendukung pelaksanaan tata kelola yang komprehensif dan sistem manajemen TI untuk perusahaan.

5. *Separating Governance from Management* (Memisahkan Tata Kelola dari Manajemen)

Kerangka COBIT 5 membuat perbedaan yang jelas antara tata kelola dan manajemen. Kedua hal tersebut mencakup berbagai jenis kegiatan, memerlukan berbagai struktur organisasi dan melayani tujuan yang berbeda.

BAB III

PROFIL PERUSAHAAN

3.1 Deskripsi Perusahaan

BTPN terletak di Menara BTPN - CBD Mega Kuningan Jl. Dr. Ide Anak Agung Gde Agung, Kav. 5.5 - 5.6. BTPN Syariah merupakan salah satu dari anak perusahaan BTPN. Perusahaan BTPN bergerak di bidang perbankan dan menyediakan aplikasi untuk perbankan dan transaksi apapun. Perusahaan-perusahaan yang ada di BTPN antara lain :

1. Bank BTPN konvensional, bergerak didalam bidang perbankan konvensional dengan basis otoritas jasa keuangan
2. Bank BTPN Syariah, bergerak didalam bidang perbankan syariah
3. Jenius, program yang bergerak dalam aplikasi dan menyediakan transaksi yang mudah melalui *smartphone* untuk segala macam transaksi
4. BTPN WOW, bergerak dibidang transaksi melalui no telp tertentu seperti transaksi pulsa di *smartphone*

Lokasi kegiatan magang penulis ada di salah satu perusahaan BTPN, yakni BTPN Syariah . dan divisi yang dituju oleh penulis yaitu ITQM (*Information Technology Quality Management*).

BAB IV

PEMBAHASAN HASIL / PELAKSANAAN KERJA PRAKTEK

Pada bagian ini penulis akan menjelaskan tentang audit sistem informasi pada PT Bank BTPN Syariah secara lebih mendetail. Gambaran umum dari audit sistem informasi akan dijelaskan lalu diikuti dengan penjelasan yang mendetail atas kajian dan pengujian yang dilakukan selama audit sistem informasi berlangsung. Untuk gambaran umum audit sistem informasi yang dilakukan penulis akan menjelaskan beberapa hal berikut ini :

1. Fase perencanaan audit atau audit *planning* dari audit sistem informasi menggunakan perencanaan audit sebelum masuk tahun 2019
2. Tujuan dari audit sistem informasi
3. Ruang lingkup pemeriksaan
4. Prosedur umum audit sistem informasi
5. Pelaksanaan audit sistem informasi. Pada bagian ini akan dibahas secara mendetail mengenai incident dan problem yang mungkin terjadi dan yang sedang terjadi

Setiap bagian dari kajian dan pengujian akan dibahas tiap-tiap prosedur yang dilakukan, hasil atas kajian dan pengujian, serta kesimpulan dan analisis atas hasil kajian dan pengujian audit sistem informasi yang dilakukan.

4.1 Ruang Lingkup Materi / Kegiatan

Audit Sistem Informasi atas Bank BTPN Syariah dimulai dari dibentuknya program audit yang akan dijalankan sebelum masuk tahun 2019. Audit sistem informasi yang dilakukan tiap bulannya akan berbeda-beda bagian yang diperiksa. Untuk tiap bulan pengecekan akan dilakukan sesuai dengan kebutuhan yang diperlukan. Jika SKAI dan OJK akan datang pada bulan tertentu, audit sistem informasi akan dilakukan beberapa bulan sebelum OJK dan SKAI datang untuk melakukan audit ke BTPN Syariah untuk menghindari banyaknya perbaikan yang harus dilakukan nantinya. Selain itu, alasan adanya audit sistem informasi atas PT Bank BTPN Syariah adalah karena proses bisnis dalam bank ini sepenuhnya terintegrasi dengan sistem informasi perusahaan dan teknologi informasi perusahaan. Terutama pada proses pengadaan, pengelolaan, pencatatan asset, pelaporan *incident* dan problem yang sepenuhnya terintegrasi dengan IT perusahaan dan memiliki resiko paling besar. Ketika ada problem dan kebutuhan audit, tim auditor pada bidang masing-masing bersama-sama menentukan tujuan dan ruang lingkup dari Audit sistem informasi yang akan dilakukan. Timeline audit sistem informasi selama satu tahun yaitu pemahaman awal, pengumpulan data dan dokumen, review dan analisa, dan yang terakhir laporan hasil pemeriksaan. Karena proses magang hanya selama 2 bulan oleh karena itu saya akan membuat mapping audit untuk bulan juni dan bulan juli karena magang tidak sampai akhir agustus oleh karena itu data tidak lengkap jika tidak sampai akhir bulan dan karena data nya pun bersifat *confidential* sehingga data kalau tidak lengkap tidak diperbolehkan oleh ITQM. Pemeriksaan audit dilakukan untuk 3 tahap yang pertama audit bulanan, audit per-empat bulan sekali, audit pertengahan tahun dan audit tahunan.

4.2 Bentuk Kegiatan

Karena mata kuliah peminatan penulis di semester ini yaitu audit sistem informasi oleh karena itu penulis memilih divisi ITQM di Bank BTPN Syariah dengan bagian jobdesk audit sistem informasi untuk bagian incident dan problem untuk perbaikan kualitas IT di Bank BTPN. Bentuk kegiatan yang dilakukan selama proses kerja praktek diantaranya memahami terlebih dahulu konsep-konsep audit dan prosedur yang berlaku pada perusahaan Bank BTPN Syariah. Selama kegiatan magang berlangsung penulis banyak melakukan kegiatan atau pekerjaan yang jarang atau sebelumnya tidak pernah dilakukan. Hal tersebut membantu penulis untuk lebih memahami dunia audit sistem informasi langsung didalam kantor. Kerja praktek ini memiliki kaitan dengan mata kuliah audit sistem informasi (mata kuliah peminatan).

Dalam melaksanakan audit sistem informasi tim audit sistem informasi melakukan 3 kategori kajian, yaitu :

1. BAU
2. Tematik
3. Strategik
4. Improvement

Di bagian selanjutnya akan membahas tentang masing-masing kajian yang dilakukan.

4.2.1 Kajian BAU

Dalam kajian ini tim Audit sistem informasi melakukan review terhadap *process, risk, and control* (PRC) berdasarkan prosedur-prosedur dan kejadian yang akan terjadi dan sudah terjadi saat ini. Dengan target PRC telah disusun berdasarkan standar IT oleh unit kerja IT Risk.

4.2.2 Kajian Tematik

Dalam kajian ini tim audit sistem informasi melakukan Review SKAI dan IT direction 2019. Review berdasarkan rencana kerja SKAI & KSI yang terdiri dari 3 hal :

- Application Development
- Operation TI
- Pendampingan Tes DR

4.2.3 Kajian Strategic

Dalam kajian ini tim audit akan melakukan kunjungan ke KFO dan Wisma serta kantor-kantor cabang. Untuk mengawasi proses-proses dan problem-problem yang terjadi, hal-hal yang dilakukan pada kajian ini diantaranya :

- Standar KFO & Wisma
- Survey Layanan IT (CSAT)

- Implementasi Mobile Prospera

4.2.4 Kajian Improvement

Dalam kajian ini tim audit akan melakukan review berbagai hal mengenai IT dan melakukan mapping berdasarkan cobit 5 dan memberikan masukan perbaikan dan melakukan review pencapaian kinerja IT berdasarkan Cobit 5. Dalam cobit 5 terdapat beberapa domain yang terdiri atas banyak proses untuk tiap domainnya. Improvement terjadi apa bila proses dianggap cukup, kurang baik, kurang sehingga diperlukan perbaikan yang signifikan. Untuk dihasilkan improvement yang perlu dilakukan maka perlu dilakukan mapping terhadap cobit 5 sesuai domain dan process yang berlaku,

Yang penulis jalankan selama masa kerja praktek yaitu hanya PRC (BAU) karena waktu yang singkat.

4.3 Hasil Kerja Praktek

4.3.1 Tugas yang dikerjakan

4.3.1.1 Memahami kertas kerja dan planning ITQM

Pada minggu pertama dan kedua, pekerjaan yang diberikan yaitu membaca dan memahami kertas kerja beserta ITQM planning untuk tahun 2019 dengan tujuan untuk mempermudah penulis untuk mengerjakan dan mengolah data-data perusahaan dan melakukan mapping terhadap COBIT 5.

4.3.1.2 Menerima data process, risk, control untuk bulan juni 2019 dan juli 2019

Pada minggu kedua pertengahan penulis diberi data yang bersifat confidential untuk diolah dan dijadikan media pembelajaran untuk melakukan mapping terhadap COBIT 5.

4.3.1.3 Membaca dan memahami framework COBIT 5

Untuk dapat melakukan mapping terhadap data yang telah diberikan perusahaan, maka perlu memahami cobit 5 beserta 5 domain dan process-process nya secara menyeluruh sehingga saat proses pe-mappingan penulis tidak kesulitan

4.3.1.4 Menerima dan mencari temuan yang sesuai dengan prosedur yang berlaku

Untuk melakukan audit sistem informasi maka yang diperlukan pertama-tama yaitu pertanyaan dan bukti-bukti yang membuktikan apakah prosedur dan peraturan dalam berbagai aspek perusahaan telah berjalan semestinya sesuai dengan peraturan dan prosedur saat ini

4.3.1.5 Melakukan mapping COBIT 5 terhadap PRC juni 2019

Setelah memahami PRC dan tiap hal yang di audit, dan telah memahami domain-domain COBIT dan proses-prosesnya . maka dapat dilakukan mapping secara teliti untuk tiap hal yang diaudit dan memilih key management processnya juga karena belum tentu sub-proses pada tiap proses digunakan seluruhnya.

4.3.2 Domain-domain COBIT 5 yang digunakan dalam melakukan mapping PRC

4.3.2.1 Evaluate, Direct & Monitor (EDM)

EDM01.01 Evaluate the governance system.
EDM01.02 Direct the governance system.
EDM01.03 Monitor the governance system.

Gambar 2 EDM01

a. EDM01

Mengevaluasi *governance system* dan melakukan *maintenance*. Proses ini cenderung berkaitan dengan tata kelola it yang diterapkan dalam perusahaan

EDM02.01 Evaluate value optimisation.
EDM02.02 Direct value optimisation.
EDM02.03 Monitor value optimisation.

Gambar 3 EDM02

b. EDM02

Berdasarkan penjelasan dalam COBIT 5, dapat disimpulkan bahwa proses ini berkaitan dengan optimasi value untuk bisnis proses, *IT service* dan *IT assets*.

EDM03.01 Evaluate risk management.
EDM03.02 Direct risk management.
EDM03.03 Monitor risk management.

Gambar 4 EDM03

c. EDM03

Proses ini menjelaskan tentang manajemen resiko untuk mengurangi dan mencegah resiko yang mungkin terjadi, manajemen resiko juga dapat menentukan apakah suatu resiko layak dibiarkan atau ditindaklanjuti.

EDM04.01 Evaluate resource management.
EDM04.02 Direct resource management.
EDM04.03 Monitor resource management.

Gambar 5 EDM04

d. EDM04

Proses ini menjelaskan tentang manajemen sumber daya (manusia, teknologi dan proses) untuk mendukung *enterprise* perusahaan.

EDM05.01 Evaluate stakeholder reporting requirements.
EDM05.02 Direct stakeholder communication and reporting.
EDM05.03 Monitor stakeholder communication.

Gambar 6 EDM05

e. EDM05

Proses menjelaskan tentang proses memastikan performansi dan kesesuaian *enterprise IT* bersifat transparan, dengan tambahan *stakeholders* telah menyetujui tujuan dan *metrics* dan aksi penting lainnya.

4.3.2.2 Align, Plan and Organise (APO)

AP001.01 Define the organisational structure.
AP001.02 Establish roles and responsibilities.
AP001.03 Maintain the enablers of the management system.
AP001.04 Communicate management objectives and direction.
AP001.05 Optimise the placement of the IT function.
AP001.06 Define information (data) and system ownership.
AP001.07 Manage continual improvement of processes.
AP001.08 Maintain compliance with policies and procedures.

Gambar 7 APO01

a. APO01

Proses ini menjelaskan tentang klarifikasi dan mempertahankan tata kelola IT *enterprise* dalam sisi visi dan misi.

AP002.01 Understand enterprise direction.
AP002.02 Assess the current environment, capabilities and performance.
AP002.03 Define the target IT capabilities.
AP002.04 Conduct a gap analysis.
AP002.05 Define the strategic plan and road map.
AP002.06 Communicate the IT strategy and direction.

Gambar 8 APO02

b. APO02

Proses ini menjelaskan tentang keseluruhan view dari bisnis dan IT *environment*, perencanaan kedepan dan inisiatif untuk masa depan.

AP003.01 Develop the enterprise architecture vision.
AP003.02 Define reference architecture.
AP003.03 Select opportunities and solutions.
AP003.04 Define architecture implementation.
AP003.05 Provide enterprise architecture services.

Gambar 9 APO03

c. APO03

Proses ini menjelaskan tentang hal-hal yang berkaitan dengan manajemen arsitektur *enterprise*.

AP004.01 Create an environment conducive to innovation.
AP004.02 Maintain an understanding of the enterprise environment.
AP004.03 Monitor and scan the technology environment.
AP004.04 Assess the potential of emerging technologies and innovation ideas.
AP004.05 Recommend appropriate further initiatives.
AP004.06 Monitor the implementation and use of innovation.

Gambar 10 APO04

d. APO04

Mengatur dan menjaga *awareness of information technology* dan *service trends* terkait. Secara umum proses ini bertujuan untuk membuat, menjaga, mengatur, merubah dan mengembangkan inovasi dalam perusahaan.

AP005.01 Establish the target investment mix.
AP005.02 Determine the availability and sources of funds.
AP005.03 Evaluate and select programmes to fund.
AP005.04 Monitor, optimise and report on investment portfolio performance.
AP005.05 Maintain portfolios.
AP005.06 Manage benefits achievement.

Gambar 11 APO05

e. APO05

Proses ini bertujuan untuk mengoptimalkan portofolio dalam perusahaan secara keseluruhan

AP006.01 Manage finance and accounting.
AP006.02 Prioritise resource allocation.
AP006.03 Create and maintain budgets.
AP006.04 Model and allocate costs.
AP006.05 Manage costs.

Gambar 12 APO06

f. APO06

Proses ini menjelaskan tentang anggaran dan *costs* untuk IT dalam suatu perusahaan.

AP007.01 Maintain adequate and appropriate staffing.
AP007.02 Identify key IT personnel.
AP007.03 Maintain the skills and competencies of personnel.
AP007.04 Evaluate employee job performance.
AP007.05 Plan and track the usage of IT and business human resources.
AP007.06 Manage contract staff.

Gambar 13 APO07

g. APO07

Proses ini menjelaskan tentang mengoptimalkan sumber daya manusia agar sesuai dengan *enterprise objectives*.

AP008.01 Understand business expectations.
AP008.02 Identify opportunities, risk and constraints for IT to enhance the business.
AP008.03 Manage the business relationship.
AP008.04 Co-ordinate and communicate.
AP008.05 Provide input to the continual improvement of services.

Gambar 14 APO08

h. APO08

Proses ini menjelaskan tentang hubungan antara bisnis dengan IT dalam cara yang transparan dan formal untuk mencapai suatu tujuan secara efektif.

AP009.01 Identify IT services.
AP009.02 Catalogue IT-enabled services.
AP009.03 Define and prepare service agreements.
AP009.04 Monitor and report service levels.
AP009.05 Review service agreements and contracts.

Gambar 15 APO09

i. APO09

Proses ini bertujuan untuk memastikan bahwa IT *services* dan *services level* memenuhi kebutuhan *enterprise*.

AP010.01 Identify and evaluate supplier relationships and contracts.
AP010.02 Select suppliers.
AP010.03 Manage supplier relationships and contracts.
AP010.04 Manage supplier risk.
AP010.05 Monitor supplier performance and compliance.

Gambar 16 APO10

j. APO10

Proses ini bertujuan untuk meminimalisasi resiko terkait dengan non-performing suppliers dan memastikan pricing tetap kompetitif

AP011.01 Establish a quality management system (QMS).
AP011.02 Define and manage quality standards, practices and procedures.
AP011.03 Focus quality management on customers.
AP011.04 Perform quality monitoring, control and reviews.
AP011.05 Integrate quality management into solutions for development and service delivery.
AP011.06 Maintain continuous improvement.

Gambar 17 APO11

k. APO11

Proses ini bertujuan untuk mengatur kualitas sesuai *requirements* yang berlaku

AP012.01 Collect data.
AP012.02 Analyse risk.
AP012.03 Maintain a risk profile.
AP012.04 Articulate risk.
AP012.05 Define a risk management action portfolio.
AP012.06 Respond to risk.

Gambar 18 APO12

l. APO12

Proses ini bertujuan untuk mengintegrasikan manajemen IT risk dengan ERM secara keseluruhan, beserta keseimbangan dan cost dari pengaturan *IT-related enterprise risk*.

AP013.01 Establish and maintain an ISMS.
AP013.02 Define and manage an information security risk treatment plan.
AP013.03 Monitor and review the ISMS.

Gambar 19 APO13

m. APO13

Proses merupakan definisi, mengoperasikan dan memonitor sebuah sistem untuk informasi *security management*

4.3.2.3 Build, Acquire and Implement (BAI)

BAI01.01 Maintain a standard approach for programme and project management.	BAI01.03 Manage stakeholder engagement.
BAI01.02 Initiate a programme.	BAI01.04 Develop and maintain the programme plan.
	BAI01.05 Launch and execute the programme.
	BAI01.06 Monitor, control and report on the programme outcomes.
	BAI01.07 Start up and initiate projects within a programme.
	BAI01.08 Plan projects.
	BAI01.09 Manage programme and project quality.
	BAI01.10 Manage programme and project risk.
	BAI01.11 Monitor and control projects.
	BAI01.12 Manage project resources and work packages.
	BAI01.13 Close a project or iteration.
	BAI01.14 Close a programme.

Gambar 20 BAI01

a. BAI01

Proses melakukan pemeliharaan untuk berbagai program dan analisa terhadap keuntungan bisnis dan pengurangan resiko delay yang tidak dapat diprediksi serta mencegah pengurangan value di perusahaan.

BAI02.01 Define and maintain business functional and technical requirements.
BAI02.02 Perform a feasibility study and formulate alternative solutions.
BAI02.03 Manage requirements risk.
BAI02.04 Obtain approval of requirements and solutions.

Gambar 21 BAI02

b. BAI02

Proses ini berisi identifikasi solusi dan analisis *requirements* sebelum akuisisi untuk memastikan bahwa tiap *requirements* sesuai dengan *enterprise strategic requirements* mencakup proses bisnis, aplikasi, informasi/data, infrastruktur dan servis.

BAI03.01 Design high-level solutions.	BAI03.07 Prepare for solution testing.
BAI03.02 Design detailed solution components.	BAI03.08 Execute solution testing.
BAI03.03 Develop solution components.	BAI03.09 Manage changes to requirements.
BAI03.04 Procure solution components.	BAI03.10 Maintain solutions.
BAI03.05 Build solutions.	BAI03.11 Define IT services and maintain the service portfolio.
BAI03.06 Perform quality assurance.	

Gambar 22 BAI03

c. BAI03

Proses ini untuk melakukan solusi yang dapat membantu *enterprise strategic* dan *operational objectives*.

BAI04.01 Assess current availability, performance and capacity and create a baseline.
BAI04.02 Assess business impact.
BAI04.03 Plan for new or changed service requirements.
BAI04.04 Monitor and review availability and capacity.
BAI04.05 Investigate and address availability, performance and capacity issues.

Gambar 23 BAI04

d. BAI04

Proses ini bertujuan untuk menjaga ketersediaan service, efisiensi sumber daya dan optimisasi dari performa sistem dan kapasitas sistem secara keseluruhan.

BAI05.01 Establish the desire to change.
BAI05.02 Form an effective implementation team.
BAI05.03 Communicate desired vision.
BAI05.04 Empower role players and identify short-term wins.
BAI05.05 Enable operation and use.
BAI05.06 Embed new approaches.
BAI05.07 Sustain changes.

Gambar 24 BAI05

e. BAI05

Proses ini bertujuan untuk tahap persiapan dan komitmen terhadap perubahan bisnis dan mengurangi resiko kegagalan.

BAI06.01 Evaluate, prioritise and authorise change requests.
BAI06.02 Manage emergency changes.
BAI06.03 Track and report change status.
BAI06.04 Close and document the changes.

Gambar 25 BAI06

f. BAI06

Proses ini membahas tentang manajemen perubahan untuk setiap hal berkaitan dengan IT dalam perusahaan

BAI07.01 Establish an Implementation plan.
BAI07.02 Plan business process, system and data conversion.
BAI07.03 Plan acceptance tests.
BAI07.04 Establish a test environment.
BAI07.05 Perform acceptance tests.
BAI07.06 Promote to production and manage releases.
BAI07.07 Provide early production support.
BAI07.08 Perform a post-Implementation review.

Gambar 26 BAI07

g. BAI07

Proses ini mendeskripsikan tentang *acceptance* dan *transitioning* serta membuat solusi baru terkait operasional, termasuk implementation planning, sistem dan konversi data, etc.

BAI08.01 Nurture and facilitate a knowledge-sharing culture.
BAI08.02 Identify and classify sources of information.
BAI08.03 Organise and contextualise information into knowledge.
BAI08.04 Use and share knowledge.
BAI08.05 Evaluate and refine information.

Gambar 27 BAI08

h. BAI08

Deskripsi proses ini yaitu mempertahankan ketersediaan dari pengetahuan yang terkait pada saat ini yang sudah dilegalisasi dan bisa dipercaya agar dapat mendukung aktivitas proses pembuatan keputusan.

Tujuan dari proses ini adalah memfasilitasi pengetahuan yang diperlukan agar dapat mendukung seluruh orang yang terkait di dalam aktivitas pekerjaan tersebut dan juga agar dapat meningkatkan produktivitas.

BAI09.01 Identify and record current assets.
BAI09.02 Manage critical assets.
BAI09.03 Manage the asset life cycle.
BAI09.04 Optimise asset costs.
BAI09.05 Manage licences.

Gambar 28 BAI09

i. BAI09

Deskripsi dari BAI09 yaitu mengelola aset pada siklus hidupnya agar memastikan aset dapat memberikan nilai pada anggaran yang optimal, dicatat dan dilindungi secara fisik, serta aset yang penting untuk mendukung kemampuan layanan yang ada. Mengelola lisensi *software* agar memastikan

mendapatkan nomor optimal, dan *software* yang diinstal telah sesuai dengan kesepakatan lisensi.

BAI10.01 Establish and maintain a configuration model.
BAI10.02 Establish and maintain a configuration repository and baseline.
BAI10.03 Maintain and control configuration items.
BAI10.04 Produce status and configuration reports.
BAI10.05 Verify and review integrity of the configuration repository.

Gambar 29 BAI10

j. BAI10

Deskripsi dari BAI10 yaitu mendefinisikan dan mempertahankan gambaran dan hubungan antara sumber daya kunci dan keahlian yang diperlukan untuk penyampaian layana IT. Sperti pengumpulan informasi tentang konfigurasi, penetapan *baseline*, *memverifikasi* dan audit informasi konfigurasi,serta memperbarui *repository* konfigurasi.

4.3.2.4 Deliver, Service and Support

DSS01.01 Perform operational procedures.
DSS01.02 Manage outsourced IT services.
DSS01.03 Monitor IT infrastructure.
DSS01.04 Manage the environment.
DSS01.05 Manage facilities.

Gambar 30 DSS01

a. DSS01

Deskripsi dari DSS01 yaitu koordinasi pelaksanaan kegiatan dan prosedur operasional yang dibutuhkan untuk menyediakan layanan bagi pihak internal maupun eksternal, termasuk juga pengawasan pelaksanaan prosedur operasional standard.

DSS02.01 Define incident and service request classification schemes.
DSS02.02 Record, classify and prioritise requests and incidents.
DSS02.03 Verify, approve and fulfil service requests.
DSS02.04 Investigate, diagnose and allocate incidents.
DSS02.05 Resolve and recover from incidents.
DSS02.06 Close service requests and incidents.
DSS02.07 Track status and produce reports.

Gambar 31 DSS02

b. DSS02

Deskripsi proses ini yaitu memberikan respon yang tepat waktu dan efektif untuk permintaan pengguna dari semua jenis insiden. Pemulihan setelah insiden terjadi, dengan melakukan merekam, menyelidiki, mendiagnosa dan menyelesaikan insiden.

DSS03.01 Identify and classify problems.
DSS03.02 Investigate and diagnose problems.
DSS03.03 Raise known errors.
DSS03.04 Resolve and close problems.
DSS03.05 Perform proactive problem management.

Gambar 32 DSS03

c. DSS03

Deskripsi dari proses ini yaitu identifikasi dan klasifikasi permasalahan dan akar penyebab yang kemudian memberikan solusi yang tepat guna untuk mencegah insiden berulang. Juga memberikan rekomendasi untuk perbaikan

DSS04.01 Define the business continuity policy, objectives and scope.	DSS04.05 Review, maintain and improve the continuity plan.
DSS04.02 Maintain a continuity strategy.	DSS04.06 Conduct continuity plan training.
DSS04.03 Develop and implement a business continuity response.	DSS04.07 Manage backup arrangements.
DSS04.04 Exercise, test and review the BCP.	DSS04.08 Conduct post-resumption review.

Gambar 33 DSS04

d. DSS04

Deskripsi dari proses ini yaitu pembangunan dan pemeliharaan rencana bisnis dan TI dalam menanggapi insiden dan gangguan demi kelanjutan operasional proses bisnis juga menjaga ketersediaan informasi pada tingkat yang dapat diterima oleh perusahaan.

DSS05.01 Protect against malware.
DSS05.02 Manage network and connectivity security.
DSS05.03 Manage endpoint security.
DSS05.04 Manage user identity and logical access.
DSS05.05 Manage physical access to IT assets.
DSS05.06 Manage sensitive documents and output devices.
DSS05.07 Monitor the Infrastructure for

Gambar 34 DSS05

e. DSS05

Perlindungan informasi perusahaan untuk mempertahankan tingkat risiko keamanan informasi dititik minimum sesuai dengan kebijakan keamanan. Membangun dan mempertahankan peran keamanan informasi dan hak akses serta melakukan pemantauan keamanan.

DSS06.01 Align control activities embedded in business processes with enterprise objectives.
DSS06.02 Control the processing of information.
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.
DSS06.04 Manage errors and exceptions.
DSS06.05 Ensure traceability of information events and accountabilities.
DSS06.06 Secure information assets.

Gambar 35 DSS06

f. DSS06

Deskripsi dari proses ini yaitu pendefinisian dan pemeliharaan kontrol bisnis proses yang tepat dalam memastikan informasi yang terkait, baik yang diproses oleh in-house maupun outsource. Juga mengidentifikasi persyaratan kontrol informasi yang relevan dan mengelola dan kontrol pengoperasian yang memadai untuk memastikan bahwa telah memenuhi persyaratan.

4.3.2.5 Monitor, Evaluate and Assess

MEA01.01 Establish a monitoring approach.
MEA01.02 Set performance and conformance targets.
MEA01.03 Collect and process performance and conformance data.
MEA01.04 Analyse and report performance.
MEA01.05 Ensure the implementation of corrective actions.

Gambar 36 MEA01

a. MEA01

Deskripsi dari proses ini yaitu mengumpulkan, memvalidasi dan mengevaluasi bisnis, IT dan tujuan proses dan metrik. Memantau bahwa proses berkinerja terhadap kinerja dan kesesuaian tujuan dan metrik persetujuan dan memberika pelaporan yang sistematis dan tepat waktu.

MEA02.01 Monitor internal controls.
MEA02.02 Review business process controls effectiveness.
MEA02.03 Perform control self-assessments.
MEA02.04 Identify and report control deficiencies.
MEA02.05 Ensure that assurance providers are independent and qualified.
MEA02.06 Plan assurance initiatives.
MEA02.07 Scope assurance initiatives.
MEA02.08 Execute assurance initiatives.

Gambar 37 MEA02

b. MEA02

Proses mengevaluasi lingkungan kontrol secara berkala, dengan cara penilaian mandiri dan penilaian dari pihak ketiga yang memungkinkan manajemen untuk mengidentifikasi inefisiensi kontrol atau penggunaan yang berlebihan serta untuk menginisiasi perbaikan, dan perencanaan, pengaturan dan perawatan standar untuk selalu melakukan penilaian kontrol dari dalam dan aktivitas penilaian dari luar.

MEA03.01 Identify external compliance requirements.
MEA03.02 Optimise response to external requirements.
MEA03.03 Confirm external compliance.
MEA03.04 Obtain assurance of external compliance.

Gambar 38 MEA03

c. MEA03

Deskripsi proses ini yaitu menilai bahwa proses TI dan proses bisnis IT yang didukung telah sesuai dengan undang-undang, peraturan dan persyaratan kontrak. Memperoleh keyakinan bahwa persyaratan telah diidentifikasi dan dipenuhi, dan mengintegrasikan IT *compliance* dengan kepatuhan perusahaan secara keseluruhan.

4.3.3 Pengerjaan kertas kerja

RATING	Nilai Rating	Hasil Pemeriksaan
BAIK	>85%	Diterapkan secara menyeluruh
CUKUP	$75\% < X \leq 85\%$	Diterapkan sebagian
KURANG	$50\% < X \leq 75\%$	Dalam perencanaan atau penerapan
BURUK	$\leq 50\%$	Tidak ada atau tidak dilakukan

4.3.3.1 Penjelasan untuk tiap angka penilaian

a. Buruk

Penilaian ini berlaku apabila tidak ada kontrol atau prosedur yang dilakukan sama sekali dan banyak temuan yang bersifat merugikan perusahaan

b. kurang

Penilaian ini berlaku apabila kontrol dan prosedur dijalankan tetapi hanya beberapa atau sebagian kecil dari keseluruhan kontrol dan prosedur-prosedur yang berlaku saat ini.

c. Cukup

Penilaian ini berlaku apabila sebagian kontrol sudah ada tetapi masih bersifat lemah atau dapat disebut belum berjalan baik

d. Baik

Penilaian ini berlaku apabila kontrol sudah dilakukan dengan baik tanpa ada kelemahan dan tanpa hambatan.

4.3.3.2 Melakukan Wawancara

Pada tahap ini kita harus menemukan temuan terlebih dahulu sebelum membuat PRC (process, risk dan control), tetapi sebelum mendapatkan temuan harus dilakukan tahap wawancara untuk menggali informasi pada tiap divisi dan hal yang dituju. Berdasarkan hal-hal yang harus diperiksa maka terbentuk berbagai jenis pertanyaan yang diolah sedemikian rupa agar user mengerti apa yang sedang ditanyakan.

4.3.3.3 PRC bulan Juni

4.3.3.3.1 Service Delivery

Menjelaskan tentang service secara keseluruhan yang terdapat dalam bank BTPN syariah. Dengan proses-proses diantaranya Ticket Management, Incident management, problem management, pengelolaan asset di user, rollout MMS dan pengelolaan mobile device prospera.

4.3.3.3.2 Service level management

Menjelaskan tentang service level agreement management secara keseluruhan dari bank BTPN syariah. Dengan proses-proses diantaranya Service catalog management, SLA management, SLA monitoring dan survei.

4.3.3.2.2 Pengelolaan kapasitas

Menjelaskan tentang capacity management secara keseluruhan lebih tepatnya capacity planning beserta monitoring capacity juga.

4.3.3.4 Proses dan Pertanyaan-pertanyaan yang diajukan (PRC Juni 2019)

4.3.3.4.1 Service Delivery

a. Ticket management

1. Sub proses : penerimaan & verifikasi informasi/permohonan pembuatan tiket
Pertanyaan : apakah form yang diajukan kepada IT helpdesk telah valid dan disetujui oleh pejabat berwenang?
2. Sub proses : pembuatan tiket (Incident, Problem, Request)
Pertanyaan :

1. apakah batas waktu penyelesaian atas laporan yang diajukan user telah diberlakukan sesuai dengan ketentuan SLA yang berlaku?
2. Apakah setiap tiket yang dibuat telah dicatat dalam backlog email?
3. Sub proses : Monitoring status tiket
Pertanyaan : apakah IT helpdesk telah melakukan monitoring dan follow up tiket ke supporting level setiap hari?
4. Sub proses : penyelesaian/penutupan tiket
Pertanyaan :
 1. Apakah IT Helpdesk telah melakukan konfirmasi atas solusi yang diberikan dengan disertai bukti kepada user?
 2. Apakah telah dilakukan follow up tiket ke supporting level setiap hari?

b. Incident management

1. Sub proses : Penerimaan, Klasifikasi & Diagnosa insiden
Pertanyaan : Apakah solusi sementara yang diberikan telah dikoordinasikan dengan tim terkait (Operation/Asset)?
2. Sub proses : menetapkan solusi
Pertanyaan : Apakah pengklasifikasian insiden telah sesuai dengan panduan tertulis yang tersedia?
3. Sub proses : eskalasi insiden
Pertanyaan :
 1. Apakah solusi yang diberikan telah sesuai dengan panduan tertulis yang tersedia?
 2. Apakah aging tiket telah dimonitor setiap hari oleh service delivery officer?
 3. Apakah solusi atas tiket yang telah berstatus closed tercatat dalam database Smartdesk?
4. Sub proses : implementasi solusi & PIR (Post Implementation Review)
Pertanyaan :
 1. Apakah solusi yang akan diimplementasikan pada aplikasi/server/network telah melalui pengujian (UAT)?
 2. Apakah pemantauan hasil implementasi telah dilakukan sesuai dengan periode PIR?

c. Problem management

1. Sub proses : Identifikasi & menentukan penyebab masalah

Pertanyaan :

1. Apakah dalam Problem Report telah mengidentifikasi masalah dan penyebab problem?
2. Apakah Problem Report telah diperiksa oleh Div Head terkait?
3. Apakah terdapat problem report yang disusun dan dilaporkan setiap bulannya?

2. Sub proses : Pelaporan masalah

Pertanyaan :

1. Apakah Problem Report telah direview oleh Service Delivery Dept Head dan IT Operations, Infrastructure & Service Delivery Head?
2. Apakah dalam aplikasi Tiket TI telah tercantum solusi problem yang diberikan?

3. Sub proses : implelementasi solusi

Pertanyaan :

1. Apakah solusi yang diberikan telah melewati tahapan testing sebelum diberikan?
2. Apakah aging tiket tercatat dalam sistem?

d. Pengelolaan asset di user

1. Sub proses : penerimaan asset TI

Pertanyaan :

1. Apakah telah dilakukan pemeriksaan kesesuaian antara PO, DO dan fisik aset yang diterima?
2. Apakah aset yang disimpan telah dicatat sesuai dengan Juknis Pencatatan Aset TI?
3. Apakah IT Infrastructure telah memeriksa hasil pemasangan jaringan? Jika dilakukan
4. Apakah BAST sudah dilengkapi setelah pengerjaan sesuai dengan PO dan SPK?

2. Sub proses : pengeluaran asset IT

Pertanyaan :

1. Apakah FPPPT dilakukan validasi dan ketersediaan aset yang dibutuhkan sesuai?
 2. Apakah aset yang tidak tersedia tercatat ke dalam Log antrian barang untuk proses pengadaan?
 3. Apakah aset yang sudah dilakukan staging dilakukan pengujian?
 4. Apakah pengiriman aset sudah disertai dengan BAST?
3. Sub proses : perbaikan aset TI
Pertanyaan :
1. Apakah aset sudah diperiksa dan coba diperbaiki sebelum aset dikirim ke pusat?
 2. Apakah data aset diperiksa masa garansinya sebelum mengajukan klaim atau pengadaan aset baru?
4. sub proses : pengembalian atau penarikan asset
pertanyaan :
1. Apakah data aset telah di validasi sebelum dilakukan penarikan aset?
 2. Apakah BAST dan kondisi aset telah diperiksa kesesuaiannya?
5. Sub proses : peremajaan/penghapubukuan
Pertanyaan : Apakah request hapus buku telah sesuai dengan catatan aset rusak dan hilang?
- e. Pengelolaan Mobile Device prospera
1. Sub proses : Penerimaan dan distribusi aset
Pertanyaan :
1. Apakah aset telah sesuai dengan PO dan telah dicatat sesuai dengan juknis pencatatan aset TI?
 2. Apakah aset telah melalui Quality Control dan didaftarkan ke MDM?
 3. Apakah pengiriman aset ke KFO dilengkapi dengan BAST?
 4. Apakah tablet yang diterima di verifikasi dan disimpan dalam ruang khasanah?
 5. Apakah data aset di update setelah BAST aset dari MMS dikirim ke pusat?
2. Sub proses : aktivasi tablet
Pertanyaan :
1. Apakah aktivasi tablet sudah melalui Service Now?

2. Apakah profile pada MDM sudah diupdate?
3. Sub proses : penanganan insiden tablet
Pertanyaan :
 1. Apakah insiden pada tablet tercatat pada tiket?
 2. Apakah ada catatan perbaikan pada tablet yang rusak?
 3. Apakah tablet rusak sudah tersimpan di khasanah KFO dan dicatat pada logbook?
 4. Apakah tablet yang di wipe terdaftar pada grup wipe?
4. Sub proses : pengelolaan tablet backup
Pertanyaan :
 1. Apakah request tablet backup telah divalidasi dan diverifikasi?
 2. Apakah tablet backup telah terdaftar pada MDM?
 3. Apakah tablet yang akan dikirim telah melalui tahap testing?
 4. Apakah BAST sudah dikirimkan kembali setelah tablet backup diterima?
 5. Apakah data aset diupdate setelah BAST diterima?

4.3.3.4.3 Service level management

- a. Service catalog management
 1. Sub proses : Identifikasi service
Pertanyaan :
 1. Apakah service catalogue yang telah diperbarui dan sudah disetujui telah disosialisasikan?
 2. Apakah dokumen service catalog telah direview oleh IT service Delivery dan Management IT?
 2. Sub proses : update catalog
Pertanyaan : Apakah dokumen service catalog telah sesuai dengan format dokumentasi yang berlaku?
- b. SLA Management
 1. Sub proses : menyusun SLA
Pertanyaan :
 1. Apakah SLA yang disusun oleh IT Service Desk telah disepakati oleh pihak berwenang dari Kepala Divisi IT Service Delivery dan Manajemen TI serta pihak bisnis/operations dan user?

2. Apakah dokumen OLA telah digunakan dalam menentukan SLA?

2. Sub proses : Menepakati dengan user
Pertanyaan : Apakah SLA telah disepakati bersama dengan User dan di-review oleh Management TI?

3. Sub proses : Sosialisasi
Pertanyaan : Apakah SLA terbaru yang telah disetujui oleh IT dan user telah disosialisasikan?

c. SLA Monitoring

1. Sub proses : Menyusun service report
Pertanyaan : Apakah service report telah di-review oleh IT Service Delivery dan IT Ops, Infra & SD Head?

2. Sub proses : Distribusi Service Report
Pertanyaan : Apakah service report telah dipresentasikan kepada management TI sebulan sekali?

3. Sub proses : Identifikasi Action Plan
Pertanyaan : Apakah dokumen action plan telah dilaporkan sebulan sekali dan di-review oleh IT Service Delivery dan Management TI?

4. Sub proses : Sosialisasi action plan
Pertanyaan : Apakah action plan telah disosialisasikan?

5. Sub proses : Survei
Pertanyaan :

1. Apakah survey mengenai tingkat layanan TI telah dilakukan secara berkala?
2. Apakah hasil survey telah diberikan kepada IT Ops, Infra & SD dan dilakukan review. serta dilaporkan kepada management TI secara berkala?

4.3.3.4.3 Pengelolaan kapasitas

a. Capacity planning

1. Sub proses : Capacity planning
Pertanyaan : Apakah hasil analisis kebutuhan kapasitas telah sesuai dengan dokumen BRD beserta data-data lainnya?

2. Sub proses : capacity monitoring
Pertanyaan :

1. Apakah IT Operations telah menerima laporan penggunaan kapasitas dan melakukan pemantauan setiap bulan?
2. Apakah laporan capacity monitoring telah dievaluasi oleh Management TI?

4.3.3.5 PRC bulan Juli 2019

4.3.3.5.1 Operational

Bagian ini merupakan bagian IT yang secara garis besar membahas tentang pengamanan fisik data center, *patch management*, Media & Hardware Disposal, Database management, Maintenance dan request lainnya.

4.3.3.5.2 Backup restore EOD

Bagian ini merupakan bagian mengenai backup data, yang membahas tentang regular backup, end of day (EOD), retrieve tape, store tape dan restore & ad-hoc backup

4.3.3.5.3 Change Management

Bagian ini merupakan bagian mengenai change request, deployment, implementasi solusi di MMS, infrastruktur installation dan CMDB Library.

4.3.3.6 Proses, sub proses dan pertanyaan-pertanyaan yang diajukan

4.3.3.6.1 Operational

- a. Pengamanan Fisik Data Center (DC)
 1. Sub proses : Pengamanan Akses (keluar-masuk) DC
Pertanyaan :
 - a. Apakah logbook pengunjung DC sesuai dengan surat tugas?
 - b. Apakah daftar nama pada log access fingerprint telah sesuai dengan hak akses DC?
 2. Sub proses : pengamanan atas penggunaan asset & fasilitas pendukung yang ada di ruang DC
Pertanyaan :
 - a. Apakah perawatan berkala telah dilaksanakan sesuai jadwal?
 - b. Apakah sign board larangan telah terpasang di pintu masuk DC?
 - c. Apakah loker di dekat DC dalam kondisi baik?
 - d. Apakah Formulir Exit/Entry Aset DC telah divalidasi oleh pihak yang berwenang secara lengkap?
 - e. Apakah CCTV DC berfungsi dengan baik dan terdapat history rekamannya?
 - f. Apakah terdapat identifikasi aset milik Bank dan aset milik penyedia jasa?
 - g. Perangkat pengendalian lingkungan seperti temperatur, kelembapan, dan api? Selain maintenance juga apakah berfungsi dengan baik?
 - h. Penunjang listrik (power dan batre UPS)?

- i. Apakah aset Bank dan penyedia jasa ditempatkan secara terpisah?

3. Sub proses : Perubahan asset DC

Pertanyaan :

- a. Apakah setiap perubahan aset di DC telah dianalisis oleh petugas terkait?
- b. Apakah perubahan aset DC telah dilengkapi dengan formulir yang telah divalidasi oleh pihak yang berwenang?
- c. Apakah perubahan aset DC telah dicatat oleh Change Management?

- b. Patch Management

1. Sub proses : identifikasi patch baru

Pertanyaan : Apakah RFC patching telah dicatat dan sesuai dengan patch logbook?

2. Sub proses : analisa patch

Pertanyaan : Apakah RFC patching telah divalidasi oleh pihak yang berwenang dengan lengkap?

- c. Media & Hardware Disposal

1. Sub proses : Pengajuan, evaluasi dan persetujuan permohonan disposal

Pertanyaan : Apakah proses disposal telah dilengkapi dengan formulir pengajuan yang telah divalidasi oleh pihak yang berwenang secara lengkap?

2. Sub proses : Persiapan disposal (pra-disposal)

Pertanyaan : Apakah telah tersedia backup terhadap data yang terdapat di dalam media yang akan di-dispose?

3. Sub proses : Eksekusi disposal

Pertanyaan :

- a. Apakah terdapat klausa terkait kerahasiaan data dalam PKS dengan vendor pelaksana disposal media yang telah disetujui oleh kedua belah pihak?
- b. Apakah permohonan disposal media telah didaftarkan melalui tiket Helpdesk?

4. Sub proses : Pemantauan/verifikasi paska disposal

Pertanyaan :

- a. Apakah media yang telah di-dispose sudah tidak terdaftar dalam database inventory?
 - b. Apakah pelaksanaan media disposal dilengkapi dengan Berita Acara yang ditandatangani oleh pelaksana disposal?
- d. Database Management
 - 1. Sub proses : Pengajuan permohonan terkait data (perubahan/permintaan data) oleh unit pemohon
Pertanyaan :
 - a. Apakah Formulir Permohonan Standar Operasional telah divalidasi oleh pihak yang berwenang dengan lengkap, yaitu:
 - Pemohon
 - IT Operations Center
 - IT Security (untuk upload dan download data production)
 - b. Apakah permohonan terkait data telah didaftarkan di IT Helpdesk?
 - 2. Sub proses : Eksekusi permohonan (pengambilan data dan/atau perubahan data)
Pertanyaan : Apakah data nasabah yang digunakan untuk pengujian telah diacak (scrambled)?
 - 3. Sub proses : Penyampaian hasil permohonan yang telah diproses
Pertanyaan : Apakah Formulir Permohonan Standar Operasional yang diajukan telah dicatat oleh IT Helpdesk dan memiliki nomor tiket?
- e. Other Request
 - 1. Sub proses : Pengajuan dan persetujuan permintaan
Pertanyaan : Apakah Formulir Other Request telah disetujui oleh pihak yang berwenang?
 - 2. Sub proses : Eksekusi permintaan
Pertanyaan : Apakah Formulir Other Request yang diajukan telah dicatat oleh IT Helpdesk dan memiliki nomor tiket?
- f. Maintenance
 - 1. Sub proses : Pelaporan kegiatan pemeliharaan
Pertanyaan :
 - a. Apakah telah terdapat laporan hasil maintenance yang telah divalidasi oleh pihak yang berwenang?
 - b. Apakah aplikasi/tool untuk memantau environment devices di DC berfungsi dengan baik?

4.3.3.6.2 Backup Restore EOD

- a. Regular backup

1. Sub proses : persiapan pelaksanaan regular backup

Pertanyaan :

- a. Apakah schedule backup telah di-set up sesuai dengan ketentuan pada aplikasi/sistem yang telah ditetapkan?
- b. Apakah laporan backup telah direview oleh IT System & Continuity?
- c. Apakah instruksi backup telah melalui job ticket?

2. Sub proses : Eksekusi Backup

Pertanyaan : Apakah hasil backup telah di-verifikasi berdasarkan ketentuan yang berlaku?

b. End of Day (EOD)

1. Sub proses : Verifikasi COB (Cut of Business)

Pertanyaan : Apakah proses COB untuk masing-masing CBS telah mematuhi waktu cutoff setiap harinya?

2. Sub proses : Eksekusi EOD (End of Day)

Pertanyaan : Apakah checklist EOD telah diisi dengan lengkap dan divalidasi oleh supervisor?

3. Sub proses : Verifikasi dan konfirmasi paska EOD

Pertanyaan : Apakah ada verifikasi atas EOD yang telah selesai dilakukan?

c. Retrieve Tape

1. Sub proses : Penerimaan dan verifikasi permohonan

Pertanyaan : Apakah permohonan retrieve tape telah ditandatangani oleh pihak yang berwenang dengan lengkap?

2. Sub proses : Proses Retrieve Tape

Pertanyaan : Apakah perpindahan tape telah dilengkapi dengan bukti serah terima yang diverifikasi oleh pihak yang berwenang dengan lengkap dan tercatat dalam logbook?

3. Sub proses : Pemenuhan permintaan/ penyampaian tape kepada pemohon

Pertanyaan : Apakah SLA penyediaan/pemenuhan permintaan tape selalu terpenuhi?

d. Store Tape

1. Sub proses : Pengajuan penyimpanan tape ke Vendor (offsite)

Pertanyaan : Apakah penyimpanan tape di DC telah disertai dokumen tertulis (formulir permohonan penyimpanan)?

2. Sub proses : Serah terima store tape kepada Vendor (offsite)

Pertanyaan :

- a. Apakah proses perpindahan tape telah dilengkapi dengan dokumen delivery work order yang telah divalidasi oleh pihak yang berwenang?
- b. Apakah proses serah-terima tape dengan vendor telah dicatat dalam logbook/tape inventory?

- c. Apakah PKS dengan vendor penyimpanan tape telah mengatur tentang tanggung jawab vendor atas kehilangan/kerusakan tape pada saat pengangkutan dan penyalahgunaan tape yang dilakukan oleh Vendor?
- d. Apakah ada laporan tertulis dari vendor secara berkala terkait daftar tape yang disimpan pada lokasi penyimpanan vendor?
- 3. Sub proses : Pelaksanaan proses penyimpanan tape di DC (onsite)
Pertanyaan : Apakah ketentuan retensi penyimpanan tape telah dilakukan sesuai dengan standar backup yang berlaku?
- 4. Sub proses : Pengelolaan tape di tempat penyimpanan (onsite/offsite)
Pertanyaan : Apakah stock opname tape telah dilakukan secara berkala?
- e. Restore & ad-hoc Backup
 - 1. Sub proses : Penerimaan dan verifikasi pengajuan permohonan restore/adhoc backup
Pertanyaan :
 - a. Apakah proses restore/adhoc backup telah dilengkapi dengan formulir yang telah divalidasi dan disetujui oleh pihak yang berwenang?
 - b. Apakah permohonan User terkait dengan restore/backup adhoc telah tercatat oleh IT Helpdesk dan memiliki nomor tiket?
 - 2. Sub proses : Eksekusi/pelaksanaan restore/adhoc backup
Pertanyaan :
 - a. Apakah pengujian restore tape telah dilakukan secara periodik dan didokumentasikan secara tertulis?
 - b. Apakah SLA pengambilan tape dari vendor tape storage selalu terpenuhi?
 - c. Apakah tape backup onsite telah disimpan di lemari besi yang selalu terkunci dan hanya dapat diakses oleh pihak yang berwenang?

4.3.3.6.4 Operational

- a. Change Request
 - 1. Sub proses : Melakukan verifikasi dan validasi request perubahan
Pertanyaan :
 - a. Apakah RFC (dan ICR) telah dilengkapi dengan dokumen pendukung perubahan?
 - b. Apakah RFC (dan ICR) telah di-review dan disetujui oleh pihak yang berwenang?
 - 2. Sub proses : Implementasi Perubahan dan review atas hasil perubahan
Pertanyaan :

- a. Apakah implementasi ke production telah dilakukan sesuai dengan jadwal yang berlaku?
- b. Apakah implementasi ke production telah dilakukan sesuai dengan petunjuk teknis yang berlaku? (Implementasi aplikasi (Juknis Deployment), implementasi infrastruktur (Juknis Infrastructure Installation))

b. Deployment

1. Sub proses : Melakukan verifikasi implementation plan

Pertanyaan :

- a. Apakah perubahan yang akan dilakukan telah melalui tahap pengujian?
- b. Apakah Implementation plan beserta dokumen pendukung telah sesuai?

2. Sub proses : Deployment

Pertanyaan :

- a. Apakah versioning tools telah digunakan untuk menjaga versi aplikasi yang akan naik ke production?
- b. Apakah RFC telah diupdate sesuai dengan hasil implementasi?
- c. Apakah RFC telah didokumentasikan ke dalam CMDB Library, service katalog dan masukan untuk Juknis PIR?

c. Implementasi Solusi di MMS

1. Sub proses : Melakukan persiapan implementasi

Pertanyaan :

- a. Apakah package atau solusi telah terverifikasi sesuai dengan kebutuhan implementasi di MMS?
- b. Apakah backup file database MMS telah di validasi oleh tim IT Production Support dan dibuatkan file patching sync MMSnya? (Jika diperlukan backup sebelum implementasi)

2. Sub proses : Implementasi solusi dan restore database MMS

Pertanyaan : Apakah manager dan wakil manager sentra mengetahui testing setelah dilakukannya implementasi?

d. Infrastruktur installation

1. Sub proses : Instalasi dan pasca instalasia

Pertanyaan :

- a. Apakah setiap perubahan infrastruktur komunikasi data dan server dilengkapi dengan RFC/ICR yang telah disetujui oleh pihak yang berwenang?
- b. Apakah RFC/ICR telah diupdate sesuai dengan hasil implementasi?
- c. Apakah dilakukan PAT dan UAT setelah instalasi selesai?

e. CMDB Library

1. Sub proses : CMDB Library

Pertanyaan :

- a. Apakah setiap perubahan configuration item telah tercatat dalam CMDB yang diupdate secara berkala?
- b. Apakah dokumen CMDB telah ditandatangani oleh pihak-pihak yang terkait?

4.3.3.7 Temuan dan Analisis hasil kerja praktek (PRC)

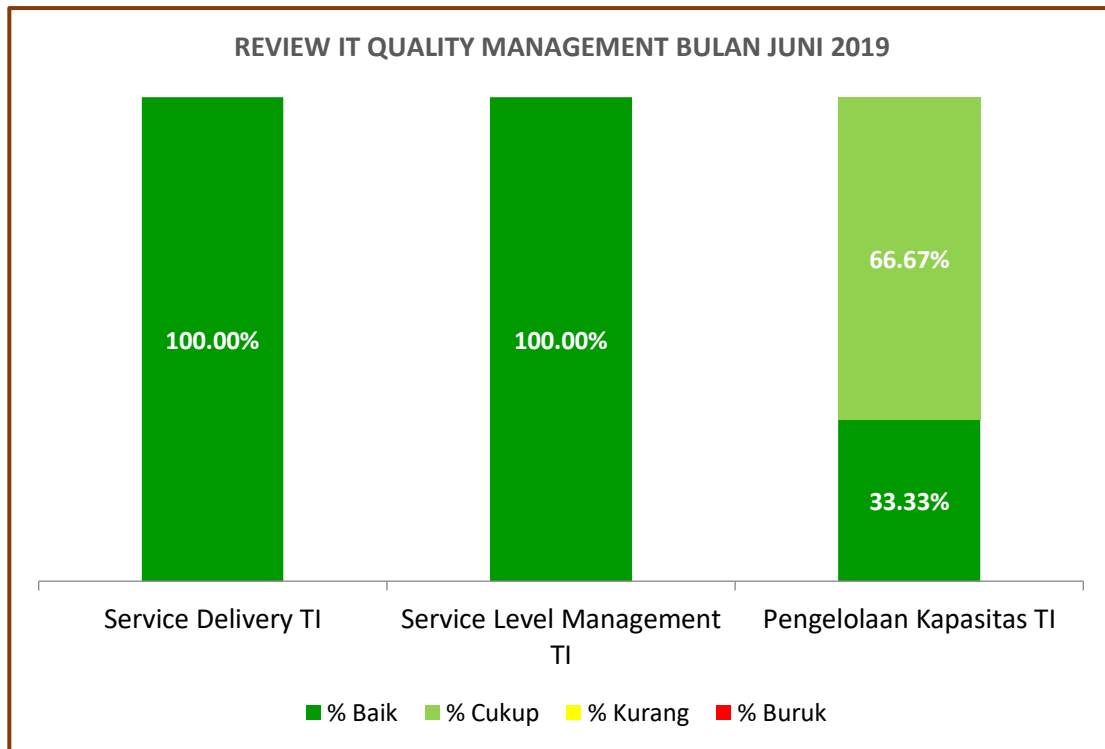
4.3.3.7.1 PRC Juni 2019

Temuan terdapat pada bagian pengelolaan kapasitas mengenai capacity monitoring belum dibuatkan laporan secara menyeluruh dan lengkap untuk tiap bulannya masih ada beberapa laporan yang belum terpenuhi.

Dashboard Hasil Pemeriksaan ITQM Bulan Juni 2019

Hasil Pemeriksaan	Jumlah Review	Persentase	Penilaian	Hasil Pemeriksaan
Service Delivery TI	51	100,00%	Baik	Service Delivery TI
Service Level Management TI	13	100,00%	Baik	Service Level Management TI
Pengelolaan Kapasitas TI	3	90,00%	Baik	Pengelolaan Kapasitas TI
Total	67	96,67%	Baik	Total

Tabel 1 hasil pemeriksaan bulan juni



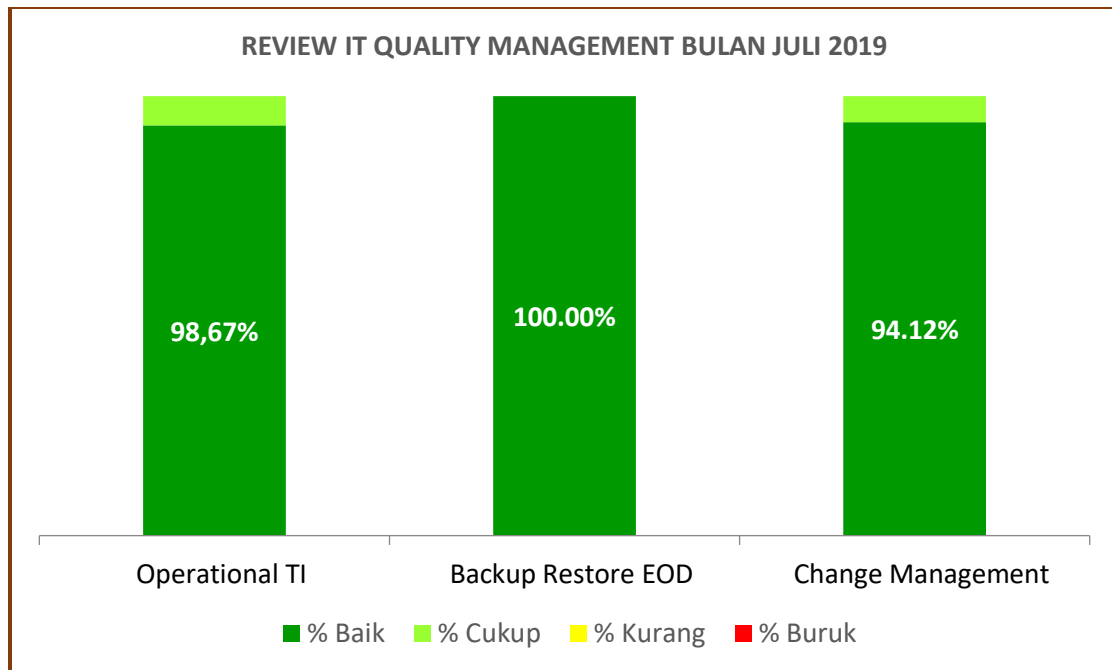
4.3.3.7.2 PRC Juli 2019

Temuan terdapat di bagian operational dan change management saja dalam PRC Juli 2019 ini, diantaranya :

1. Untuk history rekaman CCTV bagian NVR1 nya masih menggunakan HDD EKsternal.
2. Baterai UPS memiliki voltage yang tidak stabil
3. Patching di bulan juli 2018 tidak terdapat ICR dan hingga saat ini belum dilakukan patching kembali
4. Perubahan diakaukan melalui tahap pengujian tetapi tidak menyeluruh.

Hasil Pemeriksaan	Jumlah Review	Persentase	Penilaian
Operational	30	98,83%	Baik
Backup	22		
Restore EOD		100,00%	Baik
Change Management	17	99,00%	Baik
Total	69	99,27%	Baik

Tabel 2 hasil pemeriksaan bulan juli



4.3.3.8 Rekomendasi dan *improvement initiatives* (COBIT 5) Temuan pada kedua PRC

4.3.3.8.1 Rekomendasi dan *improvement initiatives* Operational

- a. **Temuan** : CCTV masih menggunakan HDD eksternal pada bagian NVR1.
Rekomendasi: Penggantian HDD dan reset default Webpam POE.
Acuan COBIT 5 : BAI09
 1. Merancang ulang proses manajemen insiden.
 2. Menerapkan problem management dan knowledge management.
- b. **Temuan** : Penunjang Listrik (UPS) dan Genset dalam kondisi normal akan tetapi terjadi unbalanced voltage pada baterai UPS nya
Rekomendasi: Penyetabilan voltage pada UPS
Acuan COBIT 5 : BAI09
 1. Merancang ulang proses manajemen insiden.
 2. Menerapkan problem management dan knowledge management.
- c. **Temuan** : Patching di bulan juli 2018 tidak terdapat ICR dan saat ini belum dilakukan patching kembali.
Rekomendasi: RFC tercatat oleh IT Change Management
Acuan COBIT 5 : BAI09
 1. Merancang ulang proses manajemen insiden.
 2. Menerapkan problem management dan knowledge management.

4.3.3.8.2 Rekomendasi dan *improvement initiatives* Change management

- a. **Temuan** : Perubahan diakaukan melalui tahap pengujian tetapi tidak menyeluruh.

Rekomendasi: Dilakukan pengujian untuk tiap perubahan yang terjadi mulai dari dokumen hingga perangkat

Acuan COBIT 5 : BAI06

1. Meningkatkan kemampuan untuk melakukan evaluasi dan assessment terhadap perubahan yang diajukan.
2. Memperbaiki test environment, test plan, dan test methods.

4.3.3.8.3 Rekomendasi dan *improvement initiatives* Pengelolaan kapasitas

- a. **Temuan** : Monitoring Capacity dilakukan oleh team data center, yang apabila terdapat informasi error pada aplikasi manage engine akan diinformasikan ke IT Operation. (tetapi proses monitoring ini belum dibuatkan laporan setiap bulannya)

Rekomendasi : ada laporan untuk tiap proses monitoring yang dilakukan jika diperlukan

Acuan COBIT 5 : BAI04

1. Melakukan assessment terhadap aspek kapasitas dan availability aplikasi dan infrastruktur yang ada saat ini.
2. Melakukan monitoring dan evaluasi terhadap kapasitas yang ada saat ini secara berkala.

- b. **Temuan** : Belum dilakukan evaluasi terhadap penggunaan kapasitas setiap bulannya secara menyeluruh

Rekomendasi: dilakukan evaluasi untuk penggunaan kapasitas tiap bulan

Acuan COBIT 5 : BAI04

1. Melakukan assessment terhadap aspek kapasitas dan availability aplikasi dan infrastruktur yang ada saat ini.
2. Melakukan monitoring dan evaluasi terhadap kapasitas yang ada saat ini secara berkala.

BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil analisis dan pemetaan data dapat disimpulkan bahwa Bank BTPN syariah untuk PRC Juni dan Juli temuannya tidak terlalu beresiko karena rata-rata untuk tiap proses berada pada angka 95% keatas dengan temuan-temuan yang baik dan sesuai dengan juknis perusahaan (petunjuk teknis). Dengan pengaplikasian cobit 5 belum semua proses berkaitan dengan proses pada cobit 5 dengan alasan perusahaan tidak harus sepenuhnya menyamakan proses-proses sesuai dengan cobit 5 melainkan menyesuaikan proses dengan kebijakan OJK (otoritas jasa keuangan) dan SKAI (Satuan Kerja Audit Intern). Proses audit ini melewati serangkaian agenda diantaranya melakukan planning di awal tahun sebelum audit IT dilakukan, setelah itu dilakukan proses wawancara melalui pertemuan langsung dan meeting, yang terakhir dilakukan pemetaan hasil temuan berdasarkan hasil jawaban wawancara yang telah dilakukan dan evaluasi jika diperlukan.

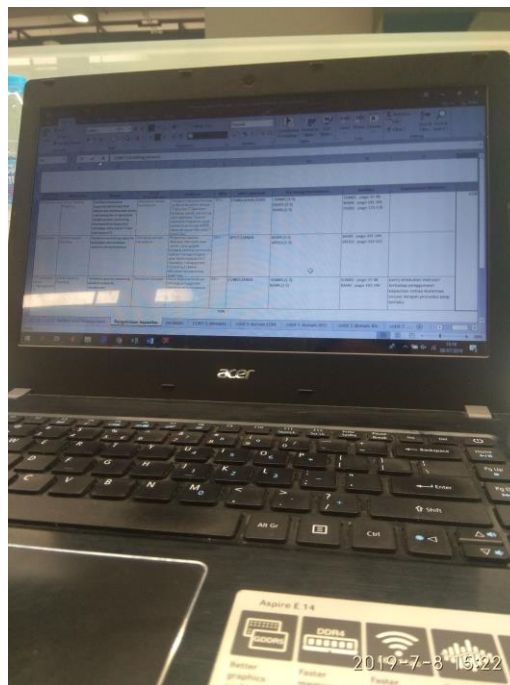
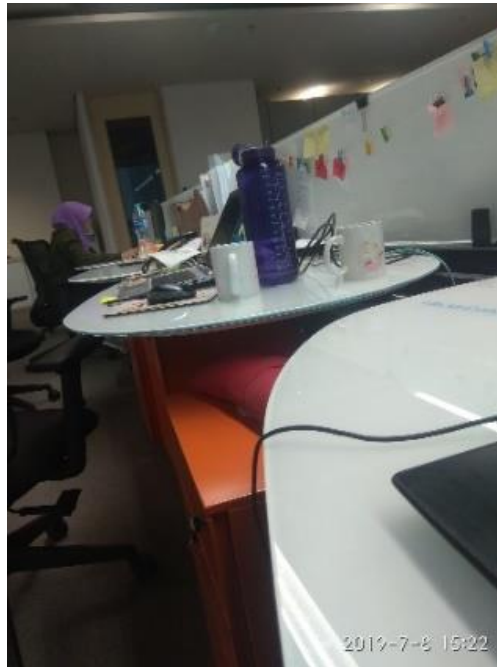
5.2 Saran

Kinerja perusahaan semoga menjadi lebih baik dalam segala sektor dan lebih banyak lagi mahasiswa atau mahasiswi yang melakukan kerja praktek di BTPN Syariah kedepannya. Sistem audit menggunakan COBIT 5 di kembangkan lagi kedepannya.

5.3 Daftar Pustaka

- [1] A. Al-Rasyid, "Analisis Audit Sistem Informasi Berbasis COBIT 5 Pada Domain Deliver, Service, and Support (DSS) (Studi Kasus: SIM-BL di Unit CDC PT Telkom Pusat. Tbk)," Bandung, 2011.
- [2] L. Sugeng Ivan, "Audit Sistem Informasi Pada Perusahaan Pengelola Jalan Tol PT JKLM (Studi Kasus: Perusahaan pengelols jalan tol PT JKLM),"Depok, 2013.
- [3] ISACA. 2012. *COBIT 5 Enabling Processes*. USA: IT Governance Institute
- [4] Audit Sistem Informasi Menggunakan Cobit 5.0 Domain DSS pada PT Erajaya Swasembada, Tbk
- [5] Application COBIT 5 DSS (Deliver, Service, and Support) Domain for information Technology Infrastructure Audit FMS PT Grand Indonesia, Adi Nuratmojo1, Eko Darwiyanto, ST. MT.2 , Gede Agung Ary Wisudiawan, S.Kom., MT.3

5.4 Lampiran-lampiran



FORMULIR APLIKASI PKL

☐ PENGAJUAN PRIBADI

☒ PENGAJUAN DARI SEKOLAH/UNIVERSITAS

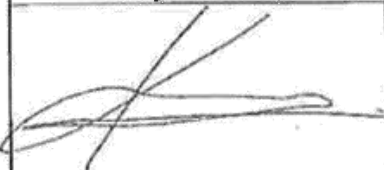


Nama : KEVIN GIOVANNI PRA DAMA
 Usia : 21 Th (K P)
 Nomer Identitas : 32 76 01 04 039 80011
 (Nomer Induk Siswa / Mahasiswa/KTP/SIM)*
 Nomer Telpon / HP : 0822 16643620
 Asal Sekolah/Universitas : TELKOM UNIVERSITY (UNIVERSITAS TELKOM)
 Tingkat Pendidikan* : ☐ SMU sederajat ☐ D1/D2 ☐ D3 ☒ S1
 Bidang studi / Jurusan : S1 INFORMATIKA
 Divisi yang dituju / Lokasi : ITQM
 Orang yang dikenal di BTPN :
 Alasan Pengajuan* : ☐ Tugas akhir siswa/ mahasiswa
☒ Kuliah Kerja Nyata
☐ Karya Ilmiah (Skripsi/Tesis/Paper/Desertasi)
 Tanggal PKL : 11 JUNI 2019 sampai dengan 11 AGUSTUS 2019

DIISI OLEH HC RESOURCING

Penempatan PKL

Lokasi PKL : Menara BTPN, Lantai 15
 Atasan Langsung : R. Ruhimat
 Divisi / Departemen : IT Planning, Strategy, & Governance
 Sasaran Tugas Individu : IT Process, Risk, and Governance.

- Memahami proses Incident dan problem management di organisasi IT.
- Melakukan audit atas kepatuhan pelaksanaan incident/problem mgt.
- Menyusun dan mempresentasikan laporan hasil audit.

Diajukan oleh,	Diketahui oleh,	Disetujui oleh,
		
(Peserta PKL)	Pembimbing dari BTPN Syariah	(Resourcing Head)
Tgl: 12 JUNI 2019	Tgl: 25 JUNI 2019	Tgl: 1

*1) Pilih salah satu

Lampirkan surat pengantar dari Sekolah / Universitas