TESIS – PM147501

AUDIT MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PERGURUAN TINGGI MENGGUNAKAN KERANGKA KERJA COBIT 5

IDA BAGUS GDE KRESNA ADI JAYA
NRP. 09211650053009

DOSEN PEMBIMBING
Dr.Tech. Ir. R. V. Hari Ginardi, M.Sc.
Dr. Rita Ambarwati S., S.E., M.MT.

PROGRAM MAGISTER MANAJEMEN TEKNOLOGI
BIDANG KEAHLIAN MANAJEMEN TEKNOLOGI INFORMASI
FAKULTAS BISNIS & MANAJEMEN TEKNOLOGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2018

(Halaman ini sengaja dikosongkan)

LEMBAR PENGESAHAN

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar

Magister Manajemen Teknologi (M.MT)

di

Institut Teknologi Sepuluh Nopember

Oleh :

IDA BAGUS GDE KRESNA ADI JAYA

NRP. 09211650053009

Tanggal Ujian : 21 Mei 2018

Periode Wisuda : September 2018

Disetujui oleh :

1. Dr. Tech. Ir. V. Hari Ginardi, M.Sc (Pembimbing I)
   NIP. 19650518 199203 1 003
2. Dr. Rita Ambarwati Sukmono, S.E., M.MT (Pembimbing II)
   NIDN. 0707048003
3. Dr. Eng. Febriliyan Samopa, S.Kom., M.Kom (Penguji)
   NIP. 19730219 199802 1 001
4. Faizal Mahananto, SKom, M.Kom., PhD (Penguji)
   NIPH. 5200201301010

Dekan Fakultas Bisnis dan Manajemen Teknologi,

Prof. Dr. Ir. Udisubakti Ciptomulyono, M.Eng. Sc.
NIP. 19590318 198701 1 001

(Halaman ini sengaja dikosongkan)

AUDIT MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PERGURUAN TINGGI MENGGUNAKAN KERANGKA KERJA COBIT 5

Nama	: Ida Bagus Gde Kresna Adi Jaya
NRP	: 09211650053009
Pembimbing	: Dr. Tech. Ir. R. V. Hari Ginardi, M.Sc.
Co-Pembimbing	: Dr. Rita Ambarwati, S., S.E., M.MT.

ABSTRAK

Berbagai persoalan muncul dalam implementasi teknologi informasi di perguruan tinggi, salah satunya adalah kurangnya pemahaman terkait risiko dalam implementasi TI. Tidak terkecuali di Politeknik Negeri Bali. Permasalahan yang terjadi saat penelitian berlangsung di Politeknik Negeri Bali adalah belum adanya dokumen profil risiko terkait TI.

Tujuan penelitian ini adalah memperoleh profil risiko terkait TI berdasarkan hasil penilaian risiko di Politeknik Negeri Bali. Fokus penilaian risiko dilakukan pada 7 proses bisnis di Unit Sistem Informasi Manajemen (SIM) Politeknik Negeri Bali. Masing-masing proses bisnis telah memiliki dokumen standar operasional prosedur. Kerangka kerja penilaian risiko TI menggunakan gabungan dari kerangka kerja ISO 31000 dan COBIT 5 *for Risk.* Pemrioritasan aksi respon terhadap risiko yang terdapat di tahapan penilaian risiko menggunakan Analytical Hierarchy Process (AHP).

Berdasarkan hasil kompilasi analisis risiko, didapat sejumlah 181 risiko yang berhasil diidentifikasi. 66 risiko masih dalam kategori yang dapat diterima, 105 risiko masih dalam batas toleransi risiko (perlu penanganan lebih lanjut) dan 10 risiko yang diluar batas toleransi risiko di Unit Sistem Informasi Manajemen (harus dihindari). Pemrioritasan respon risiko dibuat dalam 2 kategori, Tinggi dan Sedang. Berdasarkan hasil angket respon terhadap risiko, terdapat sejumlah 57 respon aksi risiko kategori "*Sedang*" dan 9 respon aksi risiko untuk kategori "*Tinggi*" yang belum terimplementasi, sehingga perlu untuk diprioritaskan menggunakan AHP. Berdasarkan perhitungan AHP, Memiliki server *backup* yang spesifikasinya sesuai dengan server yang digunakan saat ini memiliki prioritas tertinggi dari 9 risiko yang memiliki kategori nilai risiko "*Tinggi*". Sedangkan pada kategori nilai risiko "Sedang", *programmer* yang kurang paham dalam mengerti kemauan pemohon tersebut harus meminta bantuan kepada personel yang telah berpengalaman dalam memahami kemauan pemohon memiliki prioritas tertinggi dari 57 risiko. Implementasi dari penelitian ini adalah sebagai salah satu syarat pemenuhan tercapainya tujuan tata kelola TI sesuai dengan rencana strategis SI/TI Politeknik Negeri Bali.

Kata kunci: Manajemen risiko TI, Profil Risiko TI, COBIT 5, ISO 31000, AHP.

(Halaman ini sengaja dikosongkan)

INFORMATION TECHNOLOGY RISK MANAGEMENT AUDIT ON HIGHER EDUCATION USING COBIT 5 FRAMEWORK

Student Name	: Ida Bagus Gde Kresna Adi Jaya
Student Identity Number	: 09211650053009
Supervisor	: Dr. Tech. Ir. R. V. Hari Ginardi, M.Sc
Co-Supervisor	: Dr. Rita Ambarwati, S., S.E., M.MT.

ABSTRACT

Various problems arise in the implementation of information technology in universities, one of which is the lack of risk-related understanding in IT implementation. No exception at the Politeknik Negeri Bali. The problem that occurred during the research took place at Politeknik Negeri Bali is the absence of document of risk profile related to IT.

The purpose of this study was to obtain an IT-related risk profile based on risk assessment results at the Politeknik Negeri Bali. The focus of risk assessment is conducted on 7 business processes in the Unit Sistem Informasi Manajemen (Unit SIM) of the Politeknik Negeri Bali. Each business process has *Standard Operating Procedure* documents. The IT risk assessment framework uses a combination of ISO 31000 and COBIT 5 *for Risk* frameworks. Prioritizing the risk-responsive action in the risk assessment stage using the Analytical Hierarchy Process (AHP).

Based on the compilation of risk analysis, 181 risks were identified. 66 risks are still in an *Transferable* category, 105 risks are still within the *Risk Tolerance* limit (need further handling) and 10 risks beyond the *Risk Tolerance* limit in the Management Information System Unit (should be *Avoid*ed). Prioritizing risk responses is made in 2 categories, High and Medium. Based on the results of the risk-response questionnaire, there are a total of 57 "medium" category risk action responses and 9 risk action responses for the "High" category that have not yet been implemented, so it is necessary to prioritize using AHP. Based on AHP calculations, Having a *backup* server whose specifications correspond to the server currently used has the highest priority of the 9 risks that have the "High" risk rating category. Whereas in the "Moderate" risk category category, programmers who are not understood in understanding the willingness of the applicant should seek assistance to personnel who have experience in understanding the willingness of the applicant to have the highest priority of 57 risks. Implementation of this research is as one of the requirements of fulfillment of IT governance goals in accordance with the strategic plan SI / IT Politeknik Negeri Bali.

Keywords: IT Risk Management, IT Risk Assessment, COBIT 5, ISO 31000, AHP.

(Halaman ini sengaja dikosongkan)

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tesis yang berjudul "Audit Manajemen Risiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5". Tesis ini diajukan untuk memenuhi prasyarat untuk menyelesaikan studi magister di Program Studi Magister Manajemen Teknologi, Konsentrasi Manajemen Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya. Dalam penyelesaian Tesis ini, penulis telah mendapatkan banyak dukungan moral maupun material dari banyak pihak. Atas bantuan yang telah diberikan penulis ingin menyampaikan penghargaan dahn ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Ir. Udisubakti Ciptomulyono, M.Eng.Sc. selaku Dekan Fakultas Bisnis dan Manajemen Teknologi, Institut Teknologi Sepuluh Nopember.
2. Bapak Dr. Ir. Mokhamad Suef, MSc (Eng). selaku Kepala Departemen Manajemen Teknologi, Institut Teknologi Sepuluh Nopember.
3. Bapak Christiono Utomo, S.T., M.T., PhD. selaku Sekretaris Departemen Manajemen Teknologi, Institut Teknologi Sepuluh Nopember.
4. Bapak Dr. Tech, Ir. R. V. Hari Ginardi, M.Sc. selaku Kepala Program Studi Magister Manajemen Teknologi, Dosen Wali dan Dosen Pembimbing Tesis yang telah meluangkan waktu, tenaga dan pikiran dalam memberikan bimbingan, pengarahan, dan ilmu pengetahuan.
5. Ibu Dr. Rita Ambarwati S., S.E., M.MT. selaku Co. Pembimbing Tesis yang telah meluangkan waktu, tenaga dan pikiran dalam memberikan bimbingan, masukan, pengarahan, dan ilmu pengetahuan.
6. Seluruh dosen yang telah memberikan pengajaran dan ilmu yang begitu banyak. Serta seluruh karyawan MMT-ITS yang telah banyak membantu dalam berbagai hal selama masa perkuliahan. Terima kasih atas ilmu yang telah diajarkan kepada penulis.

7. Bapak I Ketut Suja selaku Ketua Unit Sistem Informasi Manajemen Politeknik Negri Bali, Ibu Kadek Cahya Dewi selaku Sekertaris Unit Sistem Informasi Manajemen dan Kepala Divisi yang tidak bisa saya sebutkan satu persatu yang telah banyak membantu dan memberikan banyak informasi yang dibutuhkan oleh penulis dan telah meluangkan waktunya untuk berdiskusi tentang banyak hal berkaitan dengan informasi organisasi.
8. Ida Bagus Made Sutedja Putra, S.H., selaku Ayah dan Ir. Ida Ayu Reni Setiawati selaku Ibu yang selalu memberikan dukungan baik melalui doa ataupun material untuk kesuksesan dan kelancaran penelitian ini.
9. Saudara Pande Gede Angga Prihardi Putra dan Djoko Cahyo Utomo Lieharyani selaku rekan seperjuangan penulis yang selalu bersama berbagi berbagai rasa baik selama menjadi mahasiswa kampus MMT-ITS ataupun dalam proses penyusunan Tesis ini. Terima kasih atas waktu, motivasi, bantuan dan dukungannya selama ini.
10. Saudari I Gusti Ayu Agung Mas Aristamy, S.TI. selaku rekan yang selalu memberikan motivasi dan dukungan kepada penulis dalam penyusunan tesis ini.
11. Teman-teman MTI angkatan 2016 yang selalu memotivasi, mengingatkan, memberi masukan, dan selalu memberi suntikan semangat kepada penulis dalam penyusunan tesis ini.
12. Semua pihak yang tidak dapat disebutkan satu persatu, yang telah banyak memberikan berbagai macam bantuan dalam penyusunan Tesis ini.

Akhir kata, penulis berharap tesis ini dapat memberikan manfaat kepada pembaca mengenai proses audit manajemen risiko TI pada perguruan tinggi menggunakan kerangka kerja COBIT 5. Penulis menyadari bahwa Tesis ini masih jauh dari kesempurnaan dan memiliki banyak kekurangan. Oleh karena itu, dengan kerendahan hati penulis mengharapkan masukan dan saran yang membangun dari pembaca untuk perbaikan ke depan.

Surabaya, 21 Mei 2018

Ida Bagus Gde Kresna Adi Jaya

DAFTAR ISI

(Halaman ini sengaja dikosongkan)

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab 1 menjelaskan tentang pendahuluan terkait penelitian yang meliputi latar belakang masalah, perumusan masalah, tujuan penelitian, manfaat penelitian dan batasan masalah, dan sistematika penulisan laporan penelitian dengan judul "Audit Manajemen Risiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5".

1.1 Latar Belakang

Penerapan teknologi informasi (TI) berkembang menjadi kebutuhan yang sangat penting dalam rangka peningkatan efektifitas, efisiensi dan produktivitas kinerja melalui tiap prosesnya (Aisha et al., 2016). Pemanfaatan TI tidak akan membuat proses kerja bisnis tercapai dengan baik jika tidak adanya tata kelola teknologi informasi yang baik (Adhitya, 2016). Menurut buku IT Governance karya Alan Carder di Tahun 2015, tata kelola TI adalah sebuah kerangka kerja untuk kepemimpinan, struktur organisasi dan proses bisnis, standar dan kepatuhan terhadap standar, yang memastikan bahwa sistem informasi organisasi mendukung dan memungkinkan pencapaian strategi dan sasarannya. Tujuan dari tata kelola TI untuk memastikan organisasi memiliki keselarasan antara teknologi informasi dengan tujuan bisnis organisasi (Calder & Watkins, 2015). Dalam rangka mencapai tujuan tata kelola TI, terdapat lima prinsip yang harus ada, antara lain: *IT strategic alignment*, *value delivery*, *risk management*, *resource management* dan *performance measurement* (IT Governance Institute, 2003).

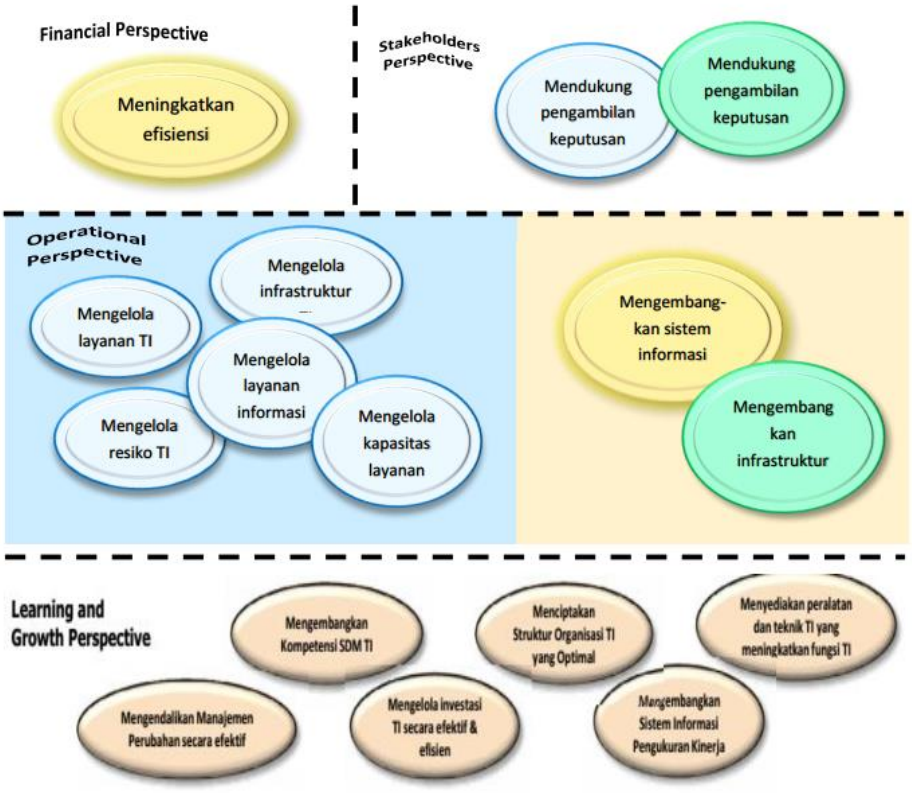
Pemerintah Indonesia melalui Departemen Komunikasi dan Informatika Republik Indonesia (Kominfo) telah menerbitkan sebuah panduan umum untuk tata kelola teknologi informasi dan komunikasi nasional yang ditetapkan pada Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/M.KOMINFO/ 11/2007 tanggal 19 November 2007(Departemen Komunikasi dan Informatika Republik Indonesia, 2007). Menurut Peraturan Menteri Pendidikan dan Kebudayaan Nomor 99 Tahun 2013 tentang Tata Kelola Teknologi Informasi dan Komunikasi di Lingkungan Kementerian Pendidikan dan Kebudayaan, perguruan tinggi

merupakan salah satu pengguna layanan TIK. Perguruan Tinggi sebagai salah satu lembaga pendidikan dengan tugas menyelenggarakan Tridharma Perguruan Tinggi yang meliputi penyelenggaraan pendidikan, penelitian, dan pengabdian masyarakat harus menyelenggarakan sistem informasi manajemen berbasis teknologi informasi dan komunikasi yang handal yang mendukung pengelolaan Tridharma Perguruan Tinggi, akuntansi dan keuangan, kepersonaliaan, kemahasiswaan dan kealumnian (diatur dalam Peraturan Menteri Pendidikan dan Kebudayaan Nomor 139 Tahun 2014 tentang Pedoman Statuta dan Organisasi Perguruan Tinggi).

Berbagai persoalan muncul dalam implementasi teknologi informasi di perguruan tinggi, salah satunya adalah kurangnya pemahaman terkait risiko dalam implementasi TI (Edi Nugroho, 2009). Risiko TI adalah risiko organisasi yang diakibatkan oleh penggunaan TI dalam organisasi, terdiri atas semua kejadian terkait TI yang berpotensi memiliki dampak para organisasi (ISACA, 2009). Disaat kehidupan perguruan tinggi masih belum tentu tergantung pada TI, permasalahan yang muncul masih bisa dimitigasi dengan solusi manual dengan kerugian yang masih dalam tahap *Transferable*. Skenario ini tidak akan berguna jika peran TI di perguruan tinggi semakin meningkat. Jika ada layanan TI yang mengalami masalah, tidak mudah untuk kembali ke prosedur manual karena infrastrukturnya sudah tidak ada lagi, karena semua sudah terkomputerisasi. Contohnya: proses KRS sudah sepenuhnya terkomputerisasi, tiba-tiba basis datanya *crash*, sementara tidak ada *backup* data yang memadai karena tidak terpikirkan selama ini dan *backup hardcopy* juga sudah tidak ada lagi (Edi Nugroho, 2009).

Politeknik Negeri Bali merupakan salah satu perguruan tinggi vokasi yang menerapkan tata kelola TI sejak awal tahun 2017. Politeknik Negeri Bali memiliki peta strategi SI/TI yang terdiri dari empat perspektif, yaitu *financial perspective*, *stakeholder perspective*, *operational perspective* dan *learn and growth perspective* (Astawa et al., 2015). Permasalahan terkait Tata kelola TI di Politeknik Negeri Bali berdasarkan hasil wawancara awal dan observasi, ditemukan suatu masalah, yaitu: belum adanya dokumen profil risiko terkait TI, karena kurang jelasnya pemahaman tentang manajemen risiko TI di Politeknik Negeri Bali. Jika mengacu pada Gambar 1.1, Politeknik Negeri Bali mencantumkan "mengelola risiko TI" menjadi bagian dari *operational perspective*. Tahun 2015 lalu kabel *fiber optic* yang menjadi

backbone koneksi internet Politeknik Negeri Bali terputus karena suatu insiden saat proyek pelebaran jalan di Jimbaran, Bali sedang berlangsung. Kabel *fiber optic* tersebut menjadi *backbone* koneksi internet untuk dua perguruan tinggi, Universitas Udayana dan Politeknik Negeri Bali. Terputusnya kabel *fiber optic* membuat terganggunya aktifitas penginputan KRS di kedua perguruan tinggi. Kedua perguruan tinggi sudah melayangkan protes, namun pihak Universitas Udayana lebih dulu di diberikan *follow up* dan beberapa hari kemudian jaringan di Universitas Udayana dapat pulih kembali sedangkan Politeknik Negeri Bali masih mengalami gangguan. Pada awal peluncuran Sistem Informasi Akademik Online (SION) Politeknik Negeri Bali di tahun 2017, tampilan utama SION di *deface* oleh oknum internal Politeknik Negeri Bali yang tidak bertanggung jawab dengan memanfaatkan *file double extension*. Tidak ada SOP yang menjadi panduan bagaimana untuk memulihkan tampilan utama SION seperti semula. Langkah mitigasi yang dilakukan adalah dengan menunjuk salah satu pegawai yang mahir didalam jaringan untuk melakukan perbaikan.



Gambar 1.1 Peta Strategi SI/TI Politeknik Negeri Bali

Berdasarkan latar belakang permasalahan yang dijelaskan sebelumnya, peneliti akan melakukan penilaian risiko terkait TI melalui proses bisnis dengan menggunakan Kerangka Kerja COBIT 5 *for Risk*. Proses awal dalam melakukan penilaian risiko terkait TI adalah mengidentifikasi risiko TI. Proses berikutnya adalah melakukan analisis risiko berdasarkan hasil identifikasi risiko. Proses selanjutnya adalah pemrioritasan aksi respon terhadap risiko. pemrioritasan aksi respon terhadap risiko digunakan untuk memudahkan manajemen Politeknik Negeri Bali dalam melakukan aksi untuk mengontrol risiko. hasil akhir dari penilaian risiko TI adalah dokumen profil risiko TI. COBIT (Control Objective for Information and Related Technology) adalah sebuah kerangka kerja yang dibuat dengan mengintegrasikan banyak "*best practice*". Versi COBIT yang terbaru adalah COBIT 5 (ISACA, 2013b). Sedangkan COBIT 5 *for Risk* adalah kerangka kerja COBIT 5 yang khusus menangani risiko TI yang sifatnya generik yang terdapat di perusahaan atau organisasi (ISACA, 2013c).

Beberapa penelitian terdahulu menjadi acuan dalam penelitian ini. Penelitian pertama oleh Edwina Fiqhe Anandita pada Tahun 2014, yaitu: melakukan penyusunan mekanisme kerja identifikasi risiko TI yang bertempat di Departemen Pengelolaan Sistem Informasi Bank Indonesia. Latar belakang masalah yang diangkat adalah Bank Indonesia memiliki terlalu banyak profil risiko TI yang dihasilkan setiap tahunnnya. Sehingga Departemen Sistem Informasi Bank Indonesia mengalami kesulitan dalam memitigasi risiko. Sehingga peneliti memiliki tujuan untuk membuat mekanisme kerja identifikasi risiko TI yang sifatnya generik atau umum yang menggunakan penggabungan *best practice* ISO 31000 dan COBIT 5 *for Risk* (Anandita, 2014). Penelitian kedua yang dilakukan oleh Chitra Utami Putri pada Tahun 2017, yaitu: melakukan penilaian risiko proses TI pada *Helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember. Latar belakang yang diangkat adalah DPTSI ITS belum pernah melakukan identifikasi dan penilaian risiko terkait pengelolaan layanan dan insiden. Kerangka kerja yang digunakan adalah COBIT 5 for Risk.

Berdasarkan latar belakang permasalahan yang telah dijelaskan, penelitian ini akan membahas mengenai penilaian risiko TI melalui proses bisnis yang terdapat

di Unit Sistem Informasi Manajemen (SIM) Politeknik Negeri Bali untuk memperoleh profil risiko TI harapannya agar dapat memudahkan manajemen TI di Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen dalam melakukan penilaian risiko TI di kemudian hari.

Adapun yang menjadi motivasi pada penilitian ini adalah sebagai berikut: pertama, memberikan masukan kepada Politeknik Negeri Bali tentang cara melakukan identifikasi risiko TI sampai penilaian risiko berbasis TI pada proses bisnis yang ada di Unit Sistem Informasi Manajemen, kedua, mendapatkan profil risiko TI kepada Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan, maka rumusan masalah dalam penelitian ini, antara lain:

1. Bagaimana hasil integrasi antara ISO 31000:2009 dengan proses TI APO12 di COBIT 5 sebagai dasar metode penelitian untuk melakukan penilaian risiko TI.
2. Bagaimana hasil identifikasi risiko TI pada proses bisnis di Unit SIM Politeknik Negeri Bali.
3. Bagaimana hasil analisis risiko TI berdasarkan skenario risiko TI yang telah dibuat pada proses bisnis di Unit SIM Politeknik Negeri Bali.
4. Bagaimana hasil pemrioritasan dari respon terhadap risiko TI pada proses bisnis di Unit SIM Politeknik Negeri Bali.
5. Bagaimana hasil profil risiko TI pada proses bisnis di Unit SIM Politeknik Negeri Bali.

1.3 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini, antara lain:

1. Menggunakan hasil integrasi antara ISO 31000:2009 dan proses TI APO12 di COBIT 5 sebagai dasar metode penelitian untuk melakukan penilaian risiko TI.

2. Memperoleh skenario risiko TI dengan menggunakan pendekatan *top-down* dan *bottom-up* pada proses bisnis di Unit SIM Politeknik Negeri Bali.
3. Memperoleh peta risiko TI berdasarkan hasil analisis risiko TI yang telah didapatkan dari skenario risiko TI pada proses bisnis di Unit SIM Politeknik Negeri Bali
4. Memperoleh hasil pemrioritasan dari respon terhadap risiko TI menggunakan *Analytical Hierarchy Process* (AHP) pada proses bisnis di Unit SIM Politeknik Negeri Bali.
5. Memperoleh dokumen profil risiko TI berdasarkan skenario risiko TI, hasil analisis risiko TI dan pemrioritasan dari respon terhadap risiko TI menggunakan *Analytical Hierarchy Processing* (AHP) pada proses bisnis di Unit SIM Politeknik Negeri Bali.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat akademik adalah untuk memenuhi salah satu syarat dalam memperoleh gelar Strata Dua (S2) pada Program Magister Manajemen Teknologi, Bidang Keahlian Manajemen Tekologi Informasi, Institut Teknologi Sepuluh November Surabaya
2. Manfaat kepada Politeknik Negeri Bali adalah mendapatkan informasi mengenai cara melakukan penilaiain risiko TI pada proses bisnis dan memperoleh dokumen profil risiko TI.
3. Manfaat kepada Perusahaaan/ Organisasi/ Instansi/ Kalangan Profesional/ Akademisi lainnya adalah dapat menggunakan penelitian ini sebagai acuan dalam melakukan penilaian risiko TI menggunakan gabungan dari ISO 31000 dan COBIT 5 for Risk.

1.5 Batasan Masalah

Batasan masalah yang ditentukan dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini mengambil studi kasus pada Politeknik Negeri Bali.
2. Fokus dari pelaksanaan penilaian risiko TI di Politeknik Negeri Bali adalah pada proses bisnis yang didapat melalui dokumen *Standar Operasional*

Prosedur Unit Sistem Informasi Manajemen Politeknik Negeri Bali menggunakan gabungan kerangka kerja ISO 31000 dan COBIT 5 for Risk.

3. Fokus dari penelitian adalah memperoleh profil risiko terkait TI berdasarkan hasil penilaian risiko TI di Politeknik Negeri Bali, khususnya di Unit Sistem Informasi Manajemen.

1.6 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan pada peneltian ini:

Bab I Pendahuluan

Bab ini menyajikan mengenai latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, metodologi, dan sistematika penulisan

Bab II Kajian Pustaka dan Dasar Teori

Bab ini menyajikan tentang kajian pustaka terkait dokumen Politeknik Negeri Bali, penelitian sebelumnya yang telah dilakukan yang mendasari penelitian dan dasar teori yang terkait dengan penelitian.

Bab III Metode Penelitian

Bab ini menyajikan metode dan langkah-langkah yang dilakukan oleh penulis dalam melakukan penelitian ini.

Bab IV Hasil Penelitian dan Pembahasan

Bab ini menyajikan mengenai pembahasan hasil penelitian yang telah dilakukan dan analisis hasil penelitian yang diperoleh.

Bab V Kesimpulan dan Saran

Bab ini menyajikan kesimpulan dan saran yang didapatkan dari pembahasan hasil penelitian.

(Halaman ini sengaja dikosongkan)

BAB II
KAJIAN PUSTAKA DAN DASAR TEORI

Bab ini menjelaskan mengenai kajian pustaka yang menitikberatkan pada hasil-hasil penelitian terdahulu yang relevan dengan masalah yang sedang dikaji, penelaahan beberapa dokumen Politeknik Negeri Bali dan dasar teori penunjang yang digunakan acuan dalam pembuatan laporan penelitian dengan judul "Audit Manajemen Risiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5"

2.1 Kajian Pustaka

Kajian pustaka menurut Suyatna adalah bahan bacaan yang secara khusus berkaitan dengan objek penelitian yang sedang dikaji (Suyatna, 2015). Berdasarkan pengertian kajian pustaka tersebut, kajian pustaka dalam penelitian ini merupakan dasar pijakan penelitian yang didapatkan dari hasil-hasil penelitian yang relevan dengan permasalahan yang sedang dikaji dan penelaahan beberapa dokumen terkait di Politeknik Negeri Bali.

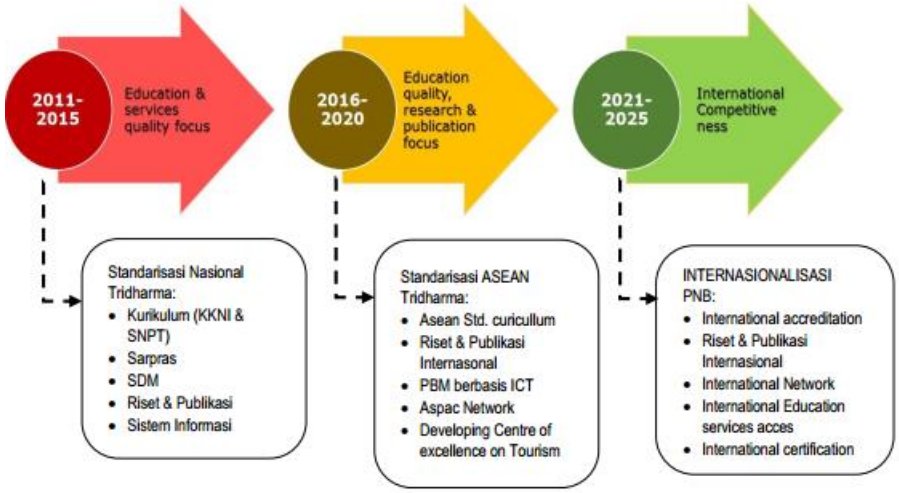
2.1.1 Profil Politeknik Negeri Bali

Politeknik Negeri Bali semula bernama Politeknik Universitas Udayana di tahun 1984. Pimpinan Politeknik Negeri Bali saat itu adalah Ir. Ketut Kinog dan Drs. Abdullah Jawas. Setelah melakukan persiapan-persiapan dan dianggap cukup siap maka tanggal 5 Oktober 1987 Politeknik Universitas Udayana memulai kuliah perdananya. Berdasarkan Peraturan Pemerintah No. 30 tahun 1990 tentang Perguruan Tinggi yang telah direvisi menjadi PP No. 57 tahun 1998, dinyatakan Politeknik seharusnya berdiri sendiri. Persiapan menjadikan Politeknik mandiri dilakukan sejak tahun 1994, yaitu dengan mempersiapkan Statuta, pembentukan Senat Politeknik, dan administrasi lainnya. Politeknik Negeri Bali (PNB) secara resmi dilembagakan pada tanggal 28 April 1997 berdasarkan Keputusan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 081/O/1997 tentang Pendirian Politeknik Negeri Bali. Peresmian dan penandatanganan prasasti papan Politeknik Negeri Bali dilakukan tanggal 12 September 1997 oleh Sekretaris

Jenderal Pendidikan Tinggi. Politeknik Negeri Bali adalah penyelenggara pendidikan tinggi vokasi yang berfokus pada pengembangan keilmuan dan keterampilan pada bidang IPTEKS terapan. Sasaran pendidikan diarahkan pada pembangunan insan cerdas komprehensif dengan mengutamakan pada pembangunan sumberdaya manusia yang profesional, dengan memberikan pendidikan berdasarkan kebutuhan pasar dan industri (Politeknik Negeri Bali, 2017b).

Politeknik Negeri Bali memiliki visi 2015-2019, yaitu: "Menjadi lembaga pendidikan tinggi vokasi terdepan penghasil lulusan professional berdaya saing internasional pada tahun 2025". Makna dari pernyataan visi Politeknik Negeri Bali dapat dijabarkan sebagai berikut (Politeknik Negeri Bali, 2010):

1. Terdepan memiliki makna bahwa PNB menjadi institusi pendidikan yang responsif dan adaptif terhadap perkembangan IPTEKS, serta bercita-ita maju.
2. Berdaya saing Internasional memiliki makna bahwa lulusan PNB diharapkan memiliki kompetensi dalam bidang Ipteks dengan standar mutu asia-pasifik dalam bidangnya,
3. Profesional memiliki makna bahwa lulusan PNB menjadi insan yang bertanggung jawab terhadap tugas yang diembannya, berintegritas, dan memiliki karakter dan budaya kerja berbasiskan pada nilai-nilai kearifan lokal



Gambar 2.1 Rencana Pengembangan Jangka Panjang PNB Tahun 2011-2025

Didalam meraih visi PNB pada tahun 2025 mengacu pada Gambar 2.1, perencanaan pengembangan PNB dibagi dalam tiga periode, yaitu (RIP PNB 2011-2025):

1. Periode I (2011-2015), merupakan periode "Standarisasi Nasional Tri Dharma Pendidikan Tinggi" dalam rangka penguatan mutu layanan yang mengacu pada pemenuhan Standar Nasional Pendidikan Tinggi (SNPT). Penguatan tata kelola PNB sebagai lembaga pendidikan tinggi vokasi yang mampu menghasilkan lulusan berkualitas dan relevan dengan kebutuhan industri yang berpegang teguh pada nilai-nilai kearifan lokal dan berorientasi pada pengembangan karakter bangsa (Nation Character Building), menjamin proses dan iklim pembelajaran yang kondusif, didukung oleh SDM yang kompeten dalam bidang tridharma, serta pemanfaatan sistem informasi berbasis IT,
2. Periode II (2016-2019), merupakan periode "Standarisasi Asia-Pasifik dalam Tri Dharma Pendidikan Tinggi" dalam rangka penguatan daya saing regional (Asia-Pasifik). pengembangan diarahkan pada penguatan layanan pendidikan yang memiliki mutu sama dengan mutu pendidikan ASEAN. PNB berupaya mencapai kesetaraan mutu pendidikan dengan mendapatkan pengakuan di kawasan ASEAN (akreditasi Asean), memiliki kemampuan riset dan publikasi regional, pengembangan sistem pembelajaran berbasisi ICT, memperluas akses kerjasama dalam lingkup kawasan regional Asean, serta mengembangkan daya saing institusi dengan membangun keunggulan sebagai pusat pendidikan dan pelatihan IPTEKS yang berpayung pada bidang kepariwisataan,
3. Periode III (2021-2025), merupakan periode "Internasionalisasi Politeknik Negeri Bali" dalam rangka penguatan daya saing internasional dengan menjadikan sektor pariwisata sebagai payung unggulan institusi (RIP PNB 2011-2025).

Sedangkan misi dari Politeknik Negeri Bali, antara lain (RIP PNB 2011-2025):

1. Menyelenggarakan pendidikan vokasi yang dapat diakses secara merata dan berkesetaraan bagi masyarakat.
2. Menyelenggarakan pendidikan bidang vokasi yang berkarakter kebangsaan dengan standar mutu nasional dan regional Asia-Pasifik
3. Melaksanakan penelitian bertaraf internasional pada bidang keilmuan dan teknologi terapan
4. Melaksanakan pengabdian kepada masyarakat yang berlandaskan pada penerapan keilmuan dan teknologi
5. Menyelenggarakan kerja sama di kawasan regional aspac
6. Mengembangkan sistem tata kelola yang inovatif, transparan, dan akuntabel didukung oleh sumber-sumber daya yang bertaraf internasional
7. Membangun keunggulan lembaga yang berorientasi pada kepariwisataan

2.1.1.1 Struktur Organisasi Politeknik Negeri Bali

Politeknik Negeri Bali (PNB) merupakan salah satu dari 43 Politeknik Negeri yang ada di Indonesia yang menyelenggarakan pendidikan tinggi vokasi pada berbagai bidang iptek terapan dibawah naungan Kementerian Riset, Teknologi, dan Pendidikan Tinggi RI (Kemristekdikti). Sesuai dengan amanat UU No.12 tahun 2012 tentang pendidikan tinggi, bahwa penyelenggaraan pendidikan vokasi diarahkan untuk menghasilkan lulusan yang memiliki pengetahuan terapan, keterampilan yang memadai, serta sikap professional (Politeknik Negeri Bali, 2017c). Politeknik Negeri Bali (PNB) memiliki pimpinan tertinggi yang disebut sebagai Direktur, dimana dalam menjalankan tugas operasionalnya, Direktur PNB memiliki empat Pembantu Direktur (Pudir), yaitu: Pembantu Direktur I mengemban tugas bidang Akademik, Pembantu Direktur II membidangi tugas bidang Administrasi Umum, Keuangan dan Kepegawain, Pembantu Direktur III mengemban tugas bidang Kemahasiswaan, dan Pembantu Direktur IV menjalankan tugas dalam bidang Kerjasama dan Hubungan Internasional (Evaluasi Diri PNB, 2017).

PNB memiliki Senat Akademik yang merupakan badan normatif yang berfungsi dalam penyusunan, monitoring, dan evaluasi penyelenggaran kegiatan akademik. PNB juga memiliki Dewan Pertimbangan yang beranggotakan berasal dari unsur pemerintah, internal PNB, asosiasi profesi, BUMN, industri (praktisi), alumni dan purna bakti PNB Adapun susunan keanggotaan Dewan Pertimbangan PNB adalah sebagai berikut (Evaluasi Diri PNB, 2017):

1. Gubernur Bali;
2. Bupati Badung;
3. Mantan Direktur PNB pada satu periode sebelumnya;
4. Pengusaha;
5. Ketua Asosiasi Profesi sesuai bidang jurusan;
6. Ketua Asosiasi BUMN;
7. 1 (satu) orang alumni; dan/atau
8. 1 (satu) orang purna bakti PNB.

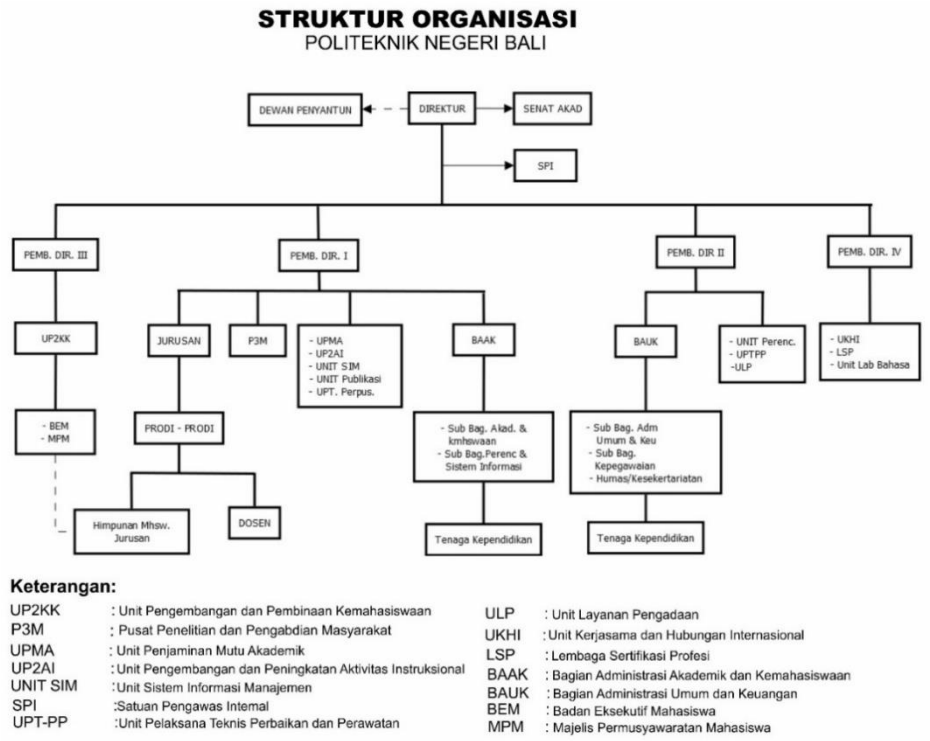
Pada pelayanan administrasi institusi, Politeknik Negeri Bali memiliki dua bagian dan empat sub bagian. Masing-masing dapat dirinci sebagai berikut (Evaluasi Diri PNB, 2017):

1. Bagian Administrasi Akademik dan Kemahasiswaan (BAAK), dengan dua sub bagian:
   a. Sub Bag. Akademik dan Kemahasiswaan
   b. Sub Bag. Perencanaan dan Sistem Informasi
2. Bagian Administrasi Umum, Keuangan, dan Kepegawaian (BAUK), terdiri dari dua sub bagian:
   a. Sub Bag. Keuangan dan Administrasi
   b. Sub Bag. Kepegawaian

Selain dua bagian yang dimiliki oleh Politeknik Negeri Bali, dalam mendukung tercapainya visi, misi, dan tujuan pada tataran operasional telah dibentuk pula unit, dan pusat. Unit dan pusat yang dibentuk dalam rangka menjamin efektifitas ketercapaian dari renstra PNB. Unit dan pusat yang dibentuk mengemban tugas sejalan dengan tugas dan fungsi PNB sebagai lembaga pendidikan tinggi, meliputi (Evaluasi Diri PNB, 2017):

1. Pusat Penelitian dan Pengabdian pada Masyarakat (P3M)
2. Unit Penjaminan Mutu Akademik (UPMA)
3. Unit Pengembangan dan Peningkatan Aktivitas Instruksional (UP2AI)
4. Unit Publikasi dan Penerbitan
5. Unit Perencanaan (UP)
6. Unit Sistem Informasi Manajemen (Unit SIM)
7. Unit Layanan Pengadaan (ULP)
8. Unit Pelaksana Teknis Perawatan dan Perbaikan (UPT-PP)
9. Lembaga Sertifikasi Profesi (LSP)
10. Unit Kerjasama, Pemberdayaan Aset dan Hubungan Internasional (UKPHI)
11. Satuan Pengawas Internal (SPI)
12. Unit Pelaksana Teknis Perpustakaan
13. Unit Pengembangan dan Pembinaan Kegiatan Kemahasiswaan (UP2KK)
14. Unit Bahasa

Secara struktur, format organisasi kelembagaan PNB dapat digambarkan seperti pada bagan struktur organisasi di Gambar 2.2 (Politeknik Negeri Bali, 2017d).



Gambar 2.2 Struktur Organisasi Politeknik Negeri Bali (PNB)

Pada tingkat Jurusan, operasional tata kelola jurusan dipimpin oleh Ketua Jurusan yang dibantu oleh Sekretaris Jurusan, Koordinator Praktik Kerja Lapangan (PKL), Ketua Program Studi (Kaprodi), Ketua Lab, Tim Penjamin Mutu Jurusan (TPMJ), dan Tim Pengembangan Jurusan yang berposisi sebagai pemberi masukan kepada Ketua Jurusan terkait dengan kebijakan strategis dalam pengembangan jurusan (Evaluasi Diri PNB, 2017).

2.1.1.2 Unit Sistem Informasi Manajemen Politeknik Negeri Bali

Unit Sistem Informasi Manajemen Politeknik Negeri Bali (PNB) merupakan unit yang menyusun perencanaan, pengelolaan dan pengembangan system informasi manajemen secara terpadu dan menyeluruh di lingkungan Politeknik Negeri Bali, dibawah kendali Pembantu Direktur I (Evaluasi Diri PNB, 2017). Di era keterbukaan informasi, peran sistem informasi menjadi kakas yang sangat strategis dalam upaya penyebaran informasi bagi pemangku kepentingan dan juga dalam kepentingan penyediaan data bagi pengambilan keputusan yang tepat. Jika melihat pada fungsi dari sistem informasi pada institusi pendidikan dan selaras dengan visi dari Politeknik Negeri Bali (PNB), maka visi pengembangan SI/TI Politeknik Negeri Bali dibawah naungan Unit Sistem Informasi Manajemen (SIM), adalah "Menjamin ketersediaan data dan informasi yang akurat dan akuntabel dalam mendukung mutu serta daya saing internasional PNB". Selanjutnya dari visi pengembangan SI/TI diturunkan kedalam beberapa misi sebagai berikut (Renstra SI/TI Unit SIM 2015-2019):

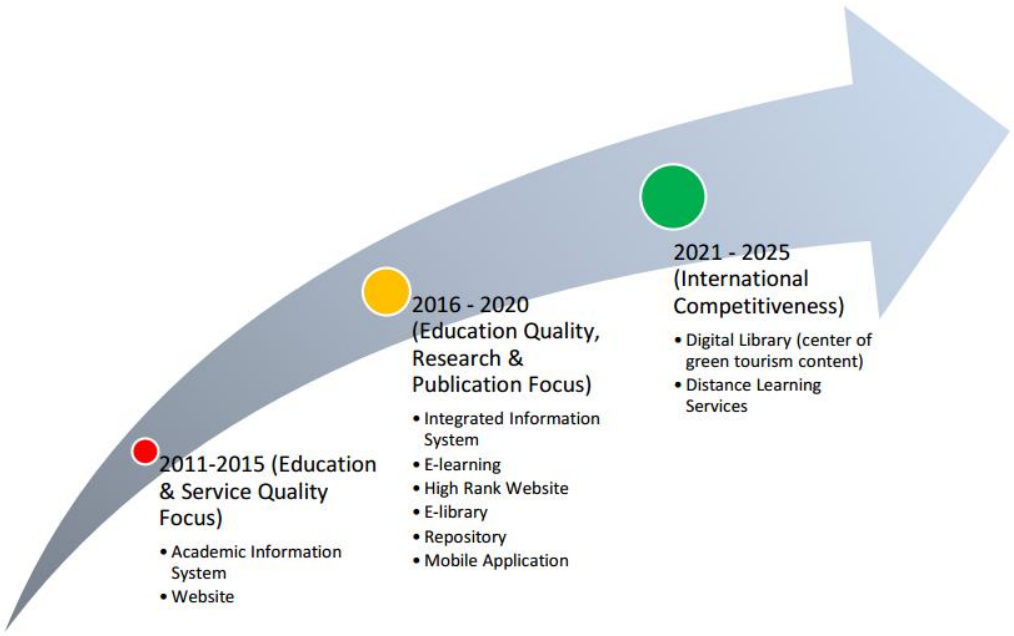
1. Mengembangkan sistem informasi institusi
2. Menyediakan teknologi informasi institusi
3. Menyediakan data dan informasi yang akurat dan akuntabel

Ada tiga sasaran utama dalam pengembangan dan penerapan SI/TI di Politeknik Negeri Bali (PNB), yaitu:

1. Peningkatan efisiensi kerja institusi dengan melakukan otomasi berbagai proses yang mengelola informasi.
2. Peningkatan efektifitas kinerja manajemen institusi dengan menyediakan informasi sesuai kebutuhan pengguna informasi serta dalam kepentingan pengambilan keputusan.

3. Peningkatan kemampuan daya saing atau meningkatkan keunggulan kompetitif Politeknik Negeri Bali (PNB) pada tridarma perguruan tinggi.

Pengembangan SI/TI dibuat selaras dengan arah pengembangan lembaga, yaitu periode 2011-2015 berupa penguatan mutu pendidikan dan penguatan mutu layanan yang mengacu pada pemenuhan Standar Nasional Pendidikan Tinggi (SNPT), periode Tahun 2016–2020 pengembangan diarahkan pada penguatan layanan pendidikan yang memiliki mutu sama dengan mutu pendidikan ASEAN, dan periode Tahun 2021–2025, menuju pada Internasionalisasi PNB sebagai lembaga pendidikan tinggi vokasi yang mampu bersaing secara internasional. Tahapan pengembangan SI/TI dapat dilihat pada Gambar 2.3



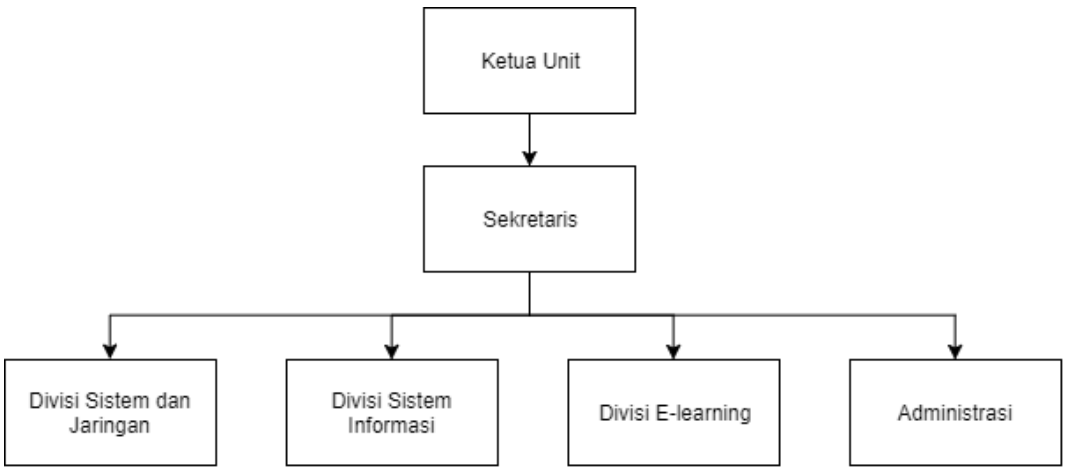
Gambar 2.3 Tahapan Pengembangan SI/TI tahun 2011-2025

Unit Sistem Informasi Manajemen (SIM): menyusun perencanaan, pengelolaan dan pengembangan system informasi manajemen secara terpadu dan menyeluruh di lingkungan Politeknik Negeri Bali, yang meliputi tugas-tugas :

a. Menyusun cetak biru (blue print) sistem informasi secara terpadu dan menyeluruh
b. Menyusun Perencanaan, Pengadaan, pengendalian dan pengembangan jaringan (hardware)

c. Mengembangkan perangkat lunak (software) pangkalan data Politeknik Negeri Bali
d. Mengendalikan Manajemen data dan informasi pangkalan data Politeknik Negeri Bali
e. Membantu mengembangkan aplikasi baru untuk pemenuhan kebutuhan data dan manajemen lembaga berbasis Informasi Teknologi (IT)
f. Mengelola Informasi dan data berbasis Website
g. Membantu mengolah data bidang akademik dan kemahasiswaan
h. Membantu penyelenggaraan pembelajaran berbasis IT

Adapun struktur organisasi Unit Sistem Informasi Manajemen (SIM) di Politeknik Negeri Bali yang telah diolah kembali dapat dilihat di Gambar 2.4.



Gambar 2.4 Struktur Organisasi Unit Sistem Informasi Manajemen (SIM)

2.1.1.3 Pengelolaan Teknologi Informasi Politeknik Negeri Bali

Demi mewujudkan visi perusahaan untuk menjadi lembaga pendidikan tinggi vokasi terdepan penghasil lulusan profesional berdaya saing internasional pada tahun 2025, PNB telah menerapkan Teknologi Informasi (TI) untuk mendukung kegiatan operasional dari semua unit yang ada di PNB. Penerapan TI merupakan salah satu langkah yang dilakukan PNB untuk meningkatkan mutu Pendidikan dan dapat memberikan layanan yang terbaik bagi civitas akademik PNB. Untuk lebih mengoptimalkan kinerja TI Politeknik Negeri Bali telah membuat *blueprint* yang bertujuan untuk meningkatkan Tata Kelola TI yang lebih baik (Good Governance) .

Sebagai salah satu contoh dari penerapan TI, Politeknik Negeri Bali telah menerapkan Sistem Informasi Terpadu (SION) dan Sistem Informasi Management Penelitian dan Pengabdian Masyarakat (SIMLITABMAS) Sistem Informasi Perencanaan dan Anggaran (SIPERA), Sistem Informasi Aset (SI-ASET), Sistem Informasi Kepegawaian (Simpeg), dan saat ini dalam pengembangan Sistem Informasi Akademik (SIMAK) (Politeknik Negeri Bali, 2017a) .

2.1.2 Penelitian Terdahulu

Mengacu pada latar belakang masalah yang telah dijelaskan pada bab sebelumnya, penelitian ini ingin melakukan penilaian risiko di Politeknik Negeri Bali khususnya di Unit Sistem Informasi Manajemen untuk mendapatkan profil risiko TI. Dalam pembuatan penelitian ini terdapat beberapa penelitian sebelumnya yang digunakan sebagai kajian dalam penyelesaian permasalahan yang ada. Ada 2 jenis penelitian yang dijadikan referensi dalam pembuatan penelitian ini. Kelima penelitian terdahulu dapat dilihat pada Tabel 2.1 dan Tabel 2.2.

Tabel 2.1 Penelitian terdahulu pertama

Penelitian Ke-1	
Judul Penelitian	Penyusunan Mekanisme Kerja Identifikasi Risiko TI pada Departemen Pengelolaan Sistem Informasi Bank Indonesia dengan Pengabungan *Best Practice*
Nama Peneliti	Edwina Fiqhe Anandita
Tahun Penelitian	2014
Latar belakang masalah yang diangkat	Bank Indonesia memiliki terlalu banyak profil risiko TI yang dihasilkan setiap tahunnnya. Sehingga Departemen Sistem Informasi Bank Indonesia mengalami kesulitan dalam memitigasi risiko
Hasil penelitian yang diperoleh	Rekomendasi mekanisme kerja identifikasi risiko yang *generic* yang mengacu pada proses bisnis Departemen Sistem Informasi Bank Indonesia menggunakan ISO 31000 dan COBIT 5 for Risk.

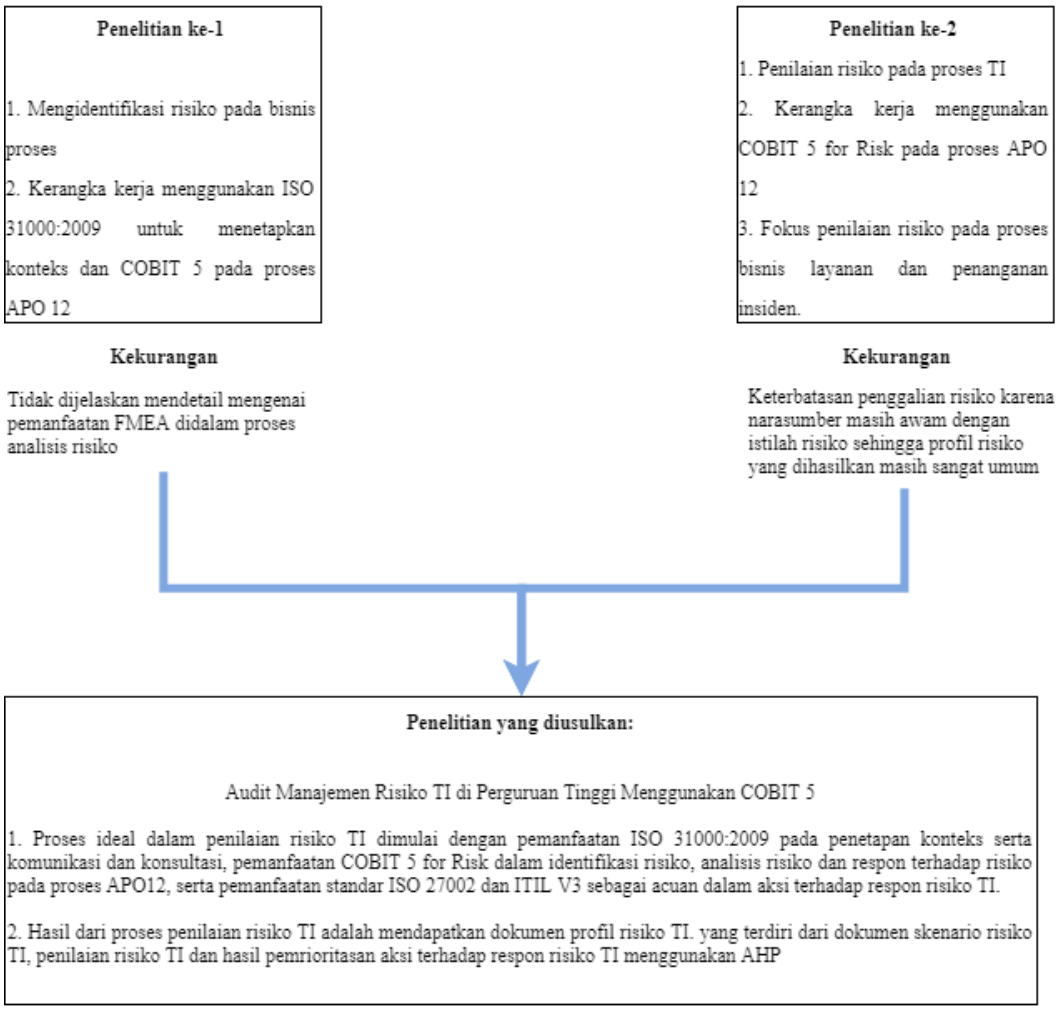
Penelitian Ke-1	
Kelebihan Penelitian	Berhasil merancang mekanisme identifikasi risiko yang *generic* yang dilihat melalui proses bisnis menggunakan ISO 31000 dan COBIT 5 for Risk
Kekurangan Penelitian	Pada penelitian ini menggunakan FMEA dalam melakukan analisis risikonya, namun tidak dijelaskan mengenai kenapa menggunakan FMEA didalam proses analisis risiko.
Hubungan penelitian ini dengan penelitian yang akan dilakukan	Pemanfaatan ISO 31000:2009 dalam proses penentuan konteks dalam pendefinisian risiko sebelum melakukan identifikasi risiko dan fase komunikasi dan konsultasi.

Tabel 2.2 Penelitian terdahulu kedua

Penelitian Ke-2	
Judul Penelitian	Penilaian Risiko Proses Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5 pada *Helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember.
Nama Peneliti	Chitra Utami Putri
Tahun Penelitian	2017
Latar belakang masalah yang diangkat	Belum pernah dilakukan identifikasi dan penilaian risiko tersendiri terkait pengelolaan layanan dan insiden di DPTSI ITS.
Hasil penelitian yang diperoleh	Mengetahui hasil identifikasi, penilaian, pemetaan dan mitigasi risiko terhadap proses TI yang terdapat pada unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI IPTS Surabaya berdasarkan pendekatan COBIT *for risk*

Penelitian Ke-2	
Kelebihan Penelitian	Peneliti secara detail menjabarkan proses aktivitas penilaian risiko mulai dari proses identifikasi hingga mitigasi risiko.
Kekurangan Penelitian	Keterbatasan penggalian risiko karena narasumber masih awam dengan istilah risiko sehingga profil risiko yang dihasilkan masih sangat *generic* atau umum
Hubungan penelitian ini dengan penelitian yang akan dilakukan	Pemanfaatan COBIT 5 *for Risk* dalam identifikasi, penilaian, pemetaan dan mitigasi risiko pada proses bisnis.

Berdasarkan keterkaitan dengan penelitian-penelitian sebelumnya yang dijabarkan diatas, sehingga kontribusi penelitian pada tesis ini adalah Audit Manajemen Risiko Teknologi Informasi pada Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5 khususnya pada Politeknik Negeri Bali. Harapannya hasil penilaian risiko dapat membantu pihak Unit Sistem Informasi Manajemen (SIM) Politeknik Negeri Bali dalam melakukan antisipasi dan pengelolaan risiko terkait proses TI. Berikut merupakan analisis gap dari kedua penelitian terdahulu tersebut yang ditunjukkan pada Gambar 2.5.



Gambar 2 5 Analisa kesenjangan terhadap penelitian sebelumnya

Mengacu pada Gambar 2.5, proses ideal dari Audit Manajemen Risiko Teknologi di Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5 adalah melakukan penilaian risiko TI yang dimulai dengan pemanfaatan ISO 31000:2009 pada fase penetapan konteks, dan fase komunikasi dan konsultasi. Pemanfaatan COBIT 5 *for Risk* dalam hal mengidentifikasi risiko, analisis risiko dan respon terhadap risiko pada proses APO12, serta pemanfaatan beberapa standar lainnya seperti ISO 27002, ITIL V3 sebagai acuan dalam aksi terhadap respon risiko TI yang telah didapatkan. Hasil dari proses penilaian risiko TI adalah berupa dokumen profil risiko TI. Dokumen profil risiko TI terdiri dari scenario risiko TI, hasil

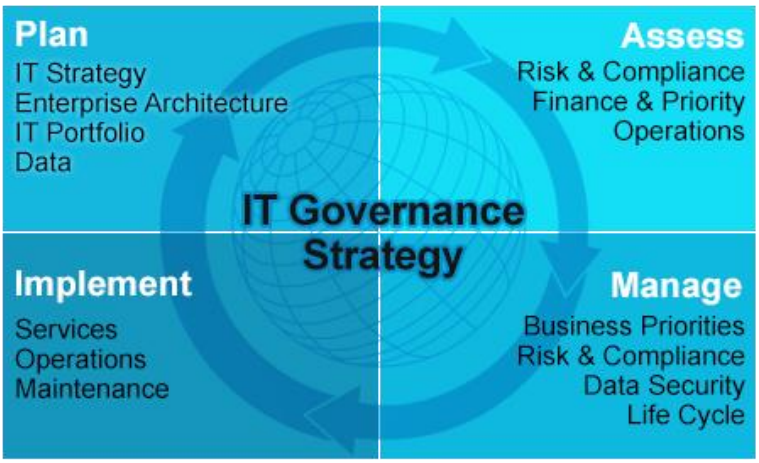
penilaian risiko TI dan hasil pemrioritasan aksi terhadap respon risiko TI menggunakan AHP.

2.2 Dasar Teori

Dasar teori menurut Buku Pedoman Penyusunan Tesis Program Pascasarjana ITS merupakan semua teori yang diambil atau dipilih yang melatarbelakangi permasalahan penelitian terkait di Politeknik Negeri Bali.

2.2.1 Tata Kelola TI dan Audit TI

Tata kelola TI berperan untuk memastikan pengukuran efektifitas dan efisiensi dari peningkatan proses bisnis melalui implementasi TI yang ada agar dapat menuju kepada tujuan bisnis sehingga tercapainya sebuah penambahan nilai dari perusahaan. Dalam penerapannya, tata kelola TI dalam sebuah perusahaan harus diikuti dengan proses kontrol dan monitoring yang baik.



Gambar 2.6 Strategi Tata Kelola Teknologi Informasi

Salah satu cara yang dapat dilakukan untuk mengukur tingkat keefektifan dan efisiensi dari tata kelola TI adalah dengan melakukan audit atau assessment terhadap tata kelola TI yang ada, dimana hubungan diantara keduanya dapat dilihat pada Gambar 2.6.

2.2.1.1 Pengertian Tata Kelola TI

Tata Kelola TI merupakan suatu cabang dari tata kelola perusahaan yang terfokus pada Sistem/Teknologi informasi serta manajemen Kinerja dan risikonya**.**

Tata kelola TI adalah struktur kebijakan atau prosedur dan kumpulan proses yang bertujuan untuk memastikan kesesuaian penerapan TI dengan dukungannya terhadap pencapaian tujuan institusi, dengan cara mengoptimalkan keuntungan dan kesempatan yang ditawarkan TI, mengendalikan penggunaan terhadap sumber daya TI dan mengelola risiko-risiko terkait TI

Tata kelola TI bukan bidang yang terpisah dari pengelolaan perusahan/organisasi, melainkan merupakan komponen pengelolaan perusahaan/organisasi secara keseluruhan, dengan tanggung jawab utama sebagai berikut:

1. Memastikan kepentingan *stakeholder diikutsertakan* dalam penyusunan strategi perusahaan.
2. Memberikan arahan kepada proses-proses yang menerap kan strategi perusahaan.
3. Memastikan proses-proses tersebut menghasilkan keluaran yang terukur.
4. Memastikan adanya informasi mengenai hasil yang diperoleh dan mengukurnya.
5. Memastikan keluaran yg dihasilkan sesuai dgn yg diharap

Implementasi tata kelola TI yang tidak efektif dan efisien dapat menimbulkan efek yang buruk terhadap perusahaan seperti kerugian bisnis, berkurangnya reputasi, melemahnya posisi di dalam kompetisi, dan masih banyak lagi. Namun sebaliknya jika tata kelola TI dapat diimplementasikan dengan efektif dan efisien di dalam sebuah perusahaan maka akan memberikan berbagai keuntungan-keuntungan antara lain (Kaban, 2009):

1. *The Wheel Exists*, penggunaan standar yang sudah ada dan *mature* akan sangat efisien. Perusahaan tidak perlu mengembangkan sendiri *framework* dengan mengandalkan pengalamannya sendiri yang tentunya sangat terbatas.
2. *Structured*, standar-standar yang baik menyediakan suatu *framework* yang sangat terstruktur, yang dapat dengan mudah dipahami dan diikuti oleh manajemen.
3. *Best Practices*, standar-standar tersebut telah dikembangkan dalam jangka waktu yang relatif lama dan melibatkan ratusan orang dan organisasi di

seluruh dunia. Pengalaman yang direfleksikan dalam model-model pengelolaan yang ada tidak dapat dibandingkan dengan suatu usaha dari satu perusahaan tertentu.

4. *Knowledge Sharing*, dengan mengikuti standar yang umum, manajemen akan dapat berbagi ide dan pengalaman antar organisasi melalui *user groups*, *website*, majalah, buku, dan media informasi lainnya.
5. *Auditable*, tanpa standar baku, akan sangat sulit bagi auditor, terutama auditor dari pihak ketiga untuk melakukan kontrol secara efektif. Dengan adanya standar, maka baik manajemen maupun auditor mempunyai dasar yang sama dalam melakukan pengelolaan TI dan pengukurannya

2.2.1.2 Cakupan Fokus Tata Kelola TI

Tata Kelola Teknologi Informasi memperkenalkan 5 (lima) area fokus yang harus dilihat dalam perspektif guna menyeimbangkan antara ekspektasi dan risiko. Adapun kelima domain dimaksud adalah sebagai berikut yang dapat dilihat pada Gambar 2.7 (Muthmainnah, 2015).

Gambar 2.7 Cakupan Area Tata Kelola Teknologi Informasi

1. Keselarasan Strategi (*Strategic Alignment*).

   "*IT Alignment is a journey not a destination*" – menggambarkan bahwa keselarasan strategi TI dengan strategi bisnis adalah sebuah proses untuk mencapai tujuan perusahaan. Dalam penerapan tata kelola TI dengan bisnis untuk masa sekarang dan masa yang akan daaing saja yang menjadi pokok

utama dalam *Stategic Alignment*, tetapi juga kemampuan untuk meningkatkan nilai bisnis yang dapat meningkatkan kinerja perusahaan.

2. Penciptaan Nilai (*Value Delivery*).

   Menurut ITGI (IT Governance Institute, 2006), Layanan TI sendiri tidak akan mampu memberikan manfaat secara langsung terhadap bisnis. Manfaat tersebut hanya bisa dihasilkan bila TI diimplementasikan bersama-sama dengan peningkatan dalam bisnis, bisnis proses, kompetensi dan prinsip kerja tiap individu dalam perusahaan, serta perubahan-perubahan yang dilakukan didalam perusahaan itu sendiri. Prinsip - prinsip dasar IT value adalah tepat waktu, sesuai anggaran dan dengan manfaat yang dimaksudkan. Oleh karenanya proses TI harus dirancang, digunakan dan dioperasikan dengan cara yang efisien dan efektif yang memenuhi tujuan dan harapan perusahaan yang ditentukan oleh business value driver yang dipengaruhi oleh faktor lingkungan.
3. Manajemen Sumber Daya (Resource Management).

   Pengelolaan sumber daya TI harus dilakukan secara tepat untuk kebutuhan bisnis. Sumber daya TI tersebut meliputi: perangkat lunak, perangkat keras, infrastruktur IT, peningkatan kualitas SDM dalam bidang TI dan hal-hal yang berkaitan dengan pengembangan dalam bidang teknologi.
4. Manajemen Risiko (*Risk Management*).

   Manajemen risiko menitikberatkan pada hal-hal yang berkenaan dengan pengendalian internal dan hubungan antara perusahaan dengan pelanggan, *stakeholder* dan *shareholder*. Segala kemungkinan risiko harus dapat diidentifikasikan sehingga dapat dilakukan langkah-langkah antisipasi untuk mengurangi dampak dari terjadinya risiko tersebut. Untuk melaksanakan pengelolaan terhadap risiko, dibutuhkan kesadaran anggota organisasi dalam memahami adanya risiko, kebutuhan organisasi, dan risiko-risiko signifikan yang dapat terjadi, serta menanamkan tanggung jawab dalam mengelola risiko yang ada di organisasi. Manajemen risiko pada teknologi informasi merupakan hal yang sangat penting. Risiko yang biasa dihadapi pada teknologi informasi antara lain serangan virus yang

dapat melumpuhkan kerja teknologi informasi, serangan pihak lain dengan tujuan untuk mengacaukan sistem maupun untuk mencuri data, kesalahan sistem, kerusakan sistem pendukung misalnya jaringan listrik putus, dan lain-lain. Semua risiko yang mungkin dihadapi tersebut harus diantisipasi sehingga ketika risiko tersebut terjadi tidak menyebabkan kerugian yang fatal.

5. Pengukuran Kinerja (*Performance Measurement*).

   Pengukuran kinerja akan menjadi tolok ukur keberhasilan penerapan tata kelola teknologi informasi. Hal ini dapat memberikan gambaran apakah hasil kinerja terhadap domain tata kelola TI sudah sesuai dengan tujuan masing-masing. Pada *accountability*, investasi teknologi informasi harus dapat dipertanggung jawabkan. Pertanggungjawaban ini berdasarkan suatu ukuran/ kriteria tertentu sehingga investasi tersebut dapat dipertanggungjawabkan. Kriteria tersebut dinilai berdasarkan kinerja yang dihasilkan oleh teknologi informasi terhadap proses bisnis dan tujuan organisasi secara keseluruhan. Penelusuran dan pengawasan implementasi dari strategi, pemenuhan proyek yang berjalan, penggunaan sumber daya, kinerja proses dan penyampaian layanan dengan menggunakan kerangka kerja seperti *Balanced Scorecard* yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan terukur dibandingkan dengan akuntansi konvensional.

2.2.1.3 Pengertian Audit TI

Secara umum Audit IT adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal. Audit IT lebih dikenal dengan istilah *EDP Auditing* (*Electronic Data Processing*), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. Salah satu penggunaan istilah tersebut adalah untuk menjelaskan proses penelahan dan evaluasi pengendalian-pengendalian internal dalam *EDP*. Jenis aktivitas ini disebut sebagai auditing melalui komputer. Penggunaan istilah lainnya adalah untuk menjelaskan pemanfaatan komputer oleh auditor untuk melaksanakan beberapa pekerjaan audit

yang tidak dapat dilakukan secara manual. Jenis aktivitas ini disebut audit dengan komputer.

Audit IT sendiri merupakan gabungan dari berbagai macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan *Behavioral Science*. Audit IT bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (*availability*), kerahasiaan (*confidentiality*), dan keutuhan (*integrity*) dari sistem informasi organisasi.

2.2.1.4 Jenis Audit TI

Dalam perkembang Audit IT yang semakin banyak digunakan audit IT di bagi menjadi 5 jenis audit diantaranya seperti berikut ini :

1. Sistem dan aplikasi.

   Audit yang berfungsi untuk memeriksa apakah sistem dan aplikasi sesuai dengan kebutuhan organisasi, berdayaguna, dan memiliki kontrol yang cukup baik untuk menjamin keabsahan, kehandalan, tepat waktu, dan keamanan pada input, proses, output pada semua tingkat kegiatan sistem.
2. Fasilitas pemrosesan informasi.

   Audit yang berfungsi untuk memeriksa apakah fasilitas pemrosesan terkendali untuk menjamin ketepatan waktu, ketelitian, dan pemrosesan aplikasi yang efisien dalam keadaan normal dan buruk
3. Pengembangan sistem.

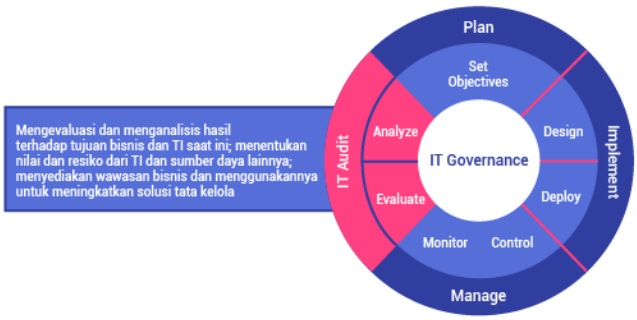
   Audit yang berfungsi untuk memeriksa apakah sistem yang dikembangkan mencakup kebutuhan obyektif organisasi.
4. Arsitektur perusahaan dan manajemen TI.

   Audit yang berfungsi untuk memeriksa apakah manajemen TI dapat mengembangkan struktur organisasi dan prosedur yang menjamin kontrol dan lingkungan yang berdaya guna untuk pemrosesan informasi.
5. *Client/Server*, telekomunikasi, intranet, dan ekstranet.

   Suatu audit yang berfungsi untuk memeriksa apakah kontrol-kontrol berfungsi pada *client, server,* dan jaringan yang menghubungkan *client* dan *server*.

2.2.1.5 Peranan Audit TI pada Tata Kelola TI

Secara global perkembangan TI saat ini sangatlah pesat yang membuat perusahaan menjadikan TI sebagai salah satu bagian penting dalam menjalankan kegiatan bisnis yang ada. Peran TI yang semakin vital dapat mempengaruhi seberapa jauh perusahaan telah mampu mencapai visi yang ada dan menjalankan misi dan tujuan strategisnya. Demi tercapainya kualitas yang baik dari implementasi TI, perusahaan perlu melakukan evaluasi terhadap pengelolaan TI agar tetap relevan terhadap perkembangan bisnis yang ada.



Gambar 2.8 Peranan Audit TI didalam Tata Kelola Teknologi Informasi

Gambar 2.8 memperlihatkan bahwa audit memiliki peran penting dalam pengimplementasian tata kelola TI pada perusahaan. Tidak dapat dipungkiri bahwa, saat ini, tingkat ketergantungan dunia usaha dan sektor usaha lainnya, termasuk badan-badan pemerintahan, terhadap teknologi informasi (TI) semakin lama semakin tinggi. Pemanfaatan TI di satu sisi dapat meningkatkan keunggulan kompetitif suatu organisasi, akan tetapi di sisi lain juga memungkinkan timbulnya risiko-risiko yang sebelumnya tidak pernah ada. Besarnya risiko yang mungkin muncul akibat penerapan TI di suatu perusahaan membuat audit TI sangat penting untuk dilakukan.

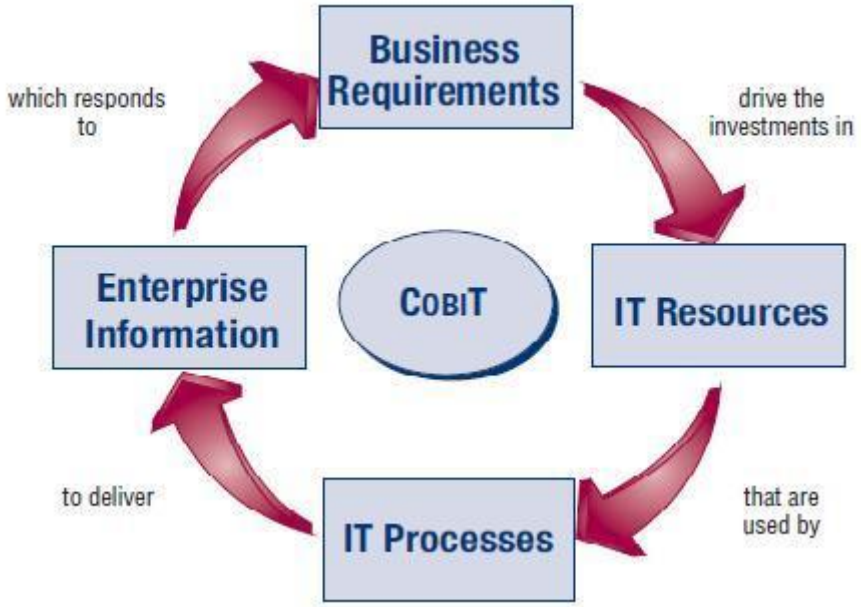
Ron Webber, Dekan Fakultas Teknologi Informasi, Monash University, dalam salah satu bukunya yaitu *Information Systems Control and Audit* (The Institute of Chartered Accountans of India, 2010) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Risiko kebocoran data.

4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

2.2.1.6 Korelasi Antara Audit TI dan COBIT

Audit tata kelola teknologi informasi (TI) merupakan sebuah proses yang memiliki dan melibatkan lingkup evaluasi yang luas dalam keseluruhan pengelolaan TI di dalam perusahaan. Dalam melakukan sebuah proses audit, auditor selaku pelaku proses membutuhkan sebuah *tool* atau alat bantu yang dapat digunakan sebagai alat ukur sebuah proses. Terdapat berbagai jenis *tool* atau alat bantu yang dapat digunakan, salah satunya adalah dengan menggunakan kerangka kerja atau *best practice* COBIT. COBIT merupakan sebuah panduan standar praktik dari manajemen teknologi informasi. COBIT memiliki peran yang penting dalam mengawali proses audit terutama pada daerah-daerah yang relevan dan memiliki risiko yang tinggi. Analisa objektivitas audit tersebut dapat dimulai dengan melakukan identifikasi terhadap *process goal* TI yang terkandung dalam beberapa domain yang ada. Auditor juga dapat menggunakan COBIT sebagai materi tambahan untuk menentukan prosedur dari proses audit yang akan dilakukan. Dalam melakukan pemeriksaan, COBIT berfungsi untuk mengetahui apakah setiap *process goal* TI yang dipilih telah disusun/ditetapkan/dijalankan. Selain itu COBIT juga dapat digunakan oleh auditor untuk mengetahui apakah kriteria yang diinginkan dari sebuah proses telah ditentukan dan mengetahui apakah proses yang ada telah mencakup aspek-aspek yang terkait (Suhardi & Baskoro, 2011).



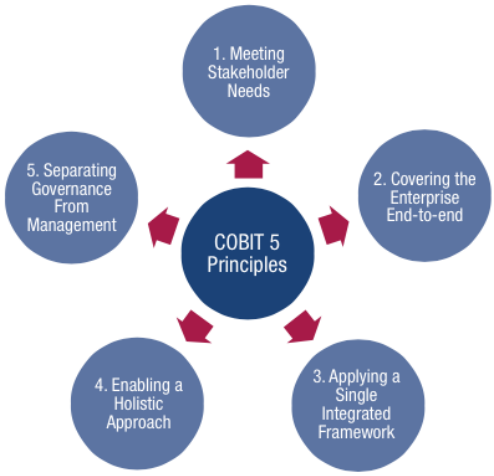
Gambar 2.9 Peranan COBIT didalam Audit TI

Berdasarkan perannya seperti yang diperlihatkan pada Gambar 2.9, COBIT pada dasarnya merupakan sebuah panduan ataupun *best practice* dari proses audit TI yang cukup mudah digunakan dan dapat disesuaikan dengan keadaan pengelolaan teknologi informasi masing-masing perusahaan. COBIT bukan hanya berfungsi sebagai petunjuk audit tetapi juga memiliki fungsi sebagai pengendali informasi dan petunjuk model kematangan/kapabilitas yang akan menentukan arah pengendalian bagi proses teknologi informasi perusahaan. Berdasarkan penjelasan tersebut dapat disimpulkan bahwa hubungan antara proses audit TI dengan COBIT sangatlah erat. COBIT dapat membantu proses audit TI dimulai dari menjadi acuan awal dalam menentukan lingkup pelaksanaan kegiatan hingga menjadi pelengkap bagi proses audit TI itu sendiri. Dengan kombinasi tersebut diharapkan nantinya dapat menghasilkan sebuah hasil evaluasi dan rekomendasi yang baik dan mutakhir untuk meningkatkan kualitas TI perusahaan.

2.2.2 Kerangka kerja COBIT 5

COBIT 5 (Control Objectives for Information & Related Technology) adalah suatu panduan standar praktek manajemen teknologi informasi dan sekumpulan dokumentasi *best practices* untuk tata kelola TI yang dapat membantu

auditor, manajemen, dan pengguna untuk menjembatani pemisah (*gap*) antara risiko bisnis, kebutuhan pengendalian, dan permasalahan-permasalahan teknis yang disusun oleh ISACA (Information Systems Audit and Control Association) dan ITGI (IT Governance Institute). COBIT 5 dibangun atas lima prinsip dasar yaitu dibahas secara terperinci, dan termasuk bentuk panduan yang luas pada *enabler* untuk tata kelola dan manajemen perusahaan teknologi informasi (TI). COBIT 5 menyediakan sebuah kerangka kerja yang komprehensif yang mampu membantu organisasi menciptakan nilai optimal dari TI dengan menjaga keseimbangan antara menyadari manfaat dan mengoptimalkan tingkat risiko dan penggunaan sumber daya. COBIT 5 membuat informasi dan teknologi yang saling berhubungan dapat dikelola secara holistik bagi keseluruhan perusahaan, mengambil seluruh tanggungjawab bisnis dan fungsional, memperhatikan kepentingan TI terkait *stakeholder* internal dan eksternal. Prinsip dan kemampuan COBIT 5 dapat diterapkan pada perusahaan berskala kecil – besar, baik yang swasta atau non-profit, juga pada sektor pelayanan publik.



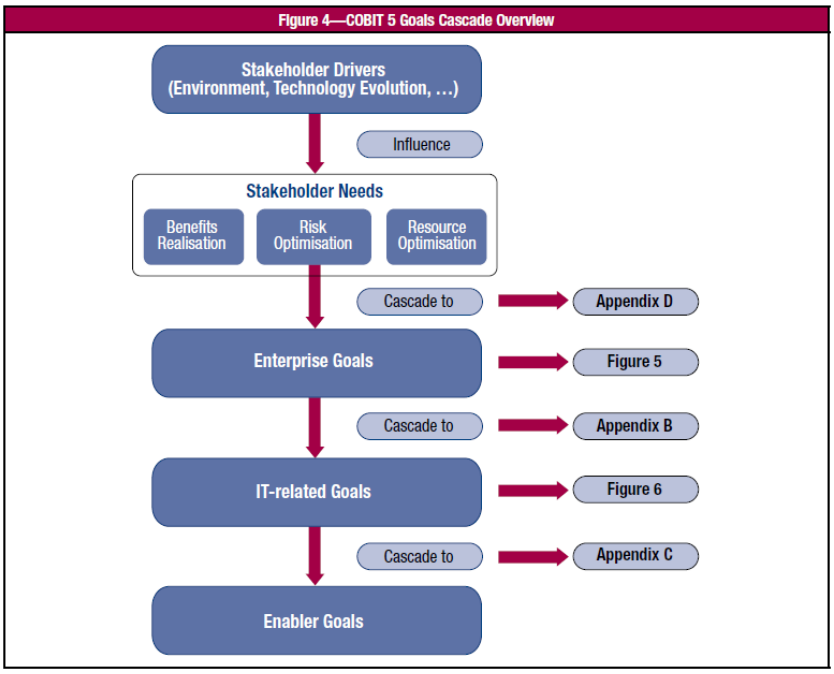
Gambar 2.10 Prinsip pada COBIT 5

Sesuai dengan Gambar 2.10. COBIT 5 mempunyai lima prinsip utama untuk tata kelola dan manajemen TI sebuah organisasi (ISACA, 2013b), antara lain:

1. **Prinsip 1**: Memenuhi Kebutuhan *stakeholder*

   Perusahaan memiliki banyak *stakeholder* dan memberikan nilai/keuntungan mempunyai arti yang berbeda dan kadang menimbulkan konflik antara satu sama lain. Untuk menciptakan nilai bagi *stakeholder* yang dimiliki

organisasi harus mempertahankan keseimbangan antara realisasi manfaat, optimalisasi risiko dan penggunaan sumber daya. COBIT 5 menerjemahkan kebutuhan *stakeholder* dalam tujuan yang spesifik dan praktis dalam konteks perusahaan, tujuan TI dan tujuan *enabler*, selain itu sistem tata kelola harus mempertimbangkan seluruh *stakeholder* ketika membuat keputusan mengenai penilaian manfaat, *resource* dan risiko. Dikarenakan setiap organisasi memiliki tujuan yang berbeda, perusahaan dapat menyesuaikan COBIT 5 sesuai dengan konteks perusahaan melalui *goal cascade* atau alur tujuan. Alur tujuan pada COBIT 5 berfungsi untuk mengetahui apakah tujuan-tujuan spesifik yang ada telah memenuhi kebutuhan *stakeholder* dan hal ini secara efektif mendukung keselarasan antara kebutuhan perusahaan dengan solusi dan layanan TI. Alur tujuan yang ada pada COBIT 5 dapat dilihat pada gambar 2.11.



Gambar 2.11 Alur tujuan COBIT 5 (Sumber: ISACA, 2012)

Gambar 2.11 menjelaskan bahwa setelah kebutuhan dari *stakeholder* yang ada diketahui, proses selanjutnya adalah memetakan kebutuhan *stakeholder* tersebut menjadi tujuan perusahaan. COBIT 5 mendefinisikan 17 tujuan umum perusahaan atau bisa disebut dengan *Enterprise Goal* seperti yang ditunjukkan pada Tabel 2.6. Tujuan perusahaan tersebut telah

dikembangkan menggunakan dimensi Balanced Scorecard (BSC) yang mempresentasikan sebuah daftar tujuan yang umum digunakan dimana sebuah perusahaan dapat mendefinisikan untuk dirinya sendiri.

Tabel 2.3 Enterprise Goal terhadap dimensi BSC.

BSC Dimension	*Enterpise Goal*
Financial	*1. stakeholder value of business investments*
	2. Portofolio of competitive product and services
	3. Manged business risk (safeguarding of assets)
	4. Compliance with external laws and regulation
	5. Financial transparency
Customer	*6. Customer-oriented service culture*
	7. Business service continuity and availabilty
	8. Business service continuity and availabilty
	9. Information-based strategic decision making
	10. Optimasation of service delivery costs
Internal	*11. Optimasation of business process functionality*
	12. Optimasation of business process costs
	13. Managed business change programmes
	14. Operational and staff productivity
	15. Compliance with internal policies
Learning and Growth	*16. Skilled and motivated people*
	17. Product and busniess innovation culture

Selanjutnya tujuan perusahaan tersebut diturunkan menjadi tujuan yang berhubungan dengan TI. Tidak jauh berbeda dengan tujuan perusahaan, tujuan TI disusun dengan dimensi-dimensi dalam *IT BSC* dimana COBIT 5 mendefinisikan 17 tujuan yang berhubungan dengan TI seperti yang ditunjukkan pada Tabel 2.7.

Tabel 2.4 Keterkaitan *IT Related Goal* dengan *IT BSC*

IT BSC Dimension		*Information and Related Technology Goal*
Financial	1	*Alignment of IT and business strategy*
	2	*IT compliance and support for business compliance with external laws and regulations*
		Commitment of executive management for making IT-related decisions
	4	*Managed IT-related business risk*
	5	*Realised benefits from IT-enabled investments and*

IT BSC Dimension		*Information and Related Technology Goal*
		services portfolio
	6	*Transparency of IT costs, benefits and risk*
Costumer	7	*Delivery of IT services in line with business requirement*
	8	*Adequate use of applications, information and technology*
		solutions
Internal	9	*IT agility*
	10	*Security of information, processing infrastructure and*
		applications
	11	*Optimisation of IT assets, resources and capabilities*
	12	*Enablement and support of business processes by*
		integrating applications and technology into business
		processes
	13	*Delivery of programmes delivering benefits, on time, on*
		budget, and meeting requirements and quality standards
	14	*Availability of reliable and useful information for decision making*
	15	*IT compliance with internal policies*
Learning and Growth	16	*Competent and motivated business and IT personnel*
	17	*Knowledge, expertise and initiatives for business*
		innovation

2. **Prinsip 2**: Meliputi *End-to-end* Perusahaan

   COBIT 5 mengintegrasikan tata kelola TI dari perusahaan menjadi sebuah tata kelola organisasi dimana:

   a. Mengakomodasi seluruh fungsi dan proses yang terdapat pada enterprise. COBIT 5 tidak hanya fokus pada ‘fungsi IT’, namun termasuk pada pemeliharaan informasi dan teknologi terkait sebagai aset layaknya aset-aset yang terdapat pada enterprise.

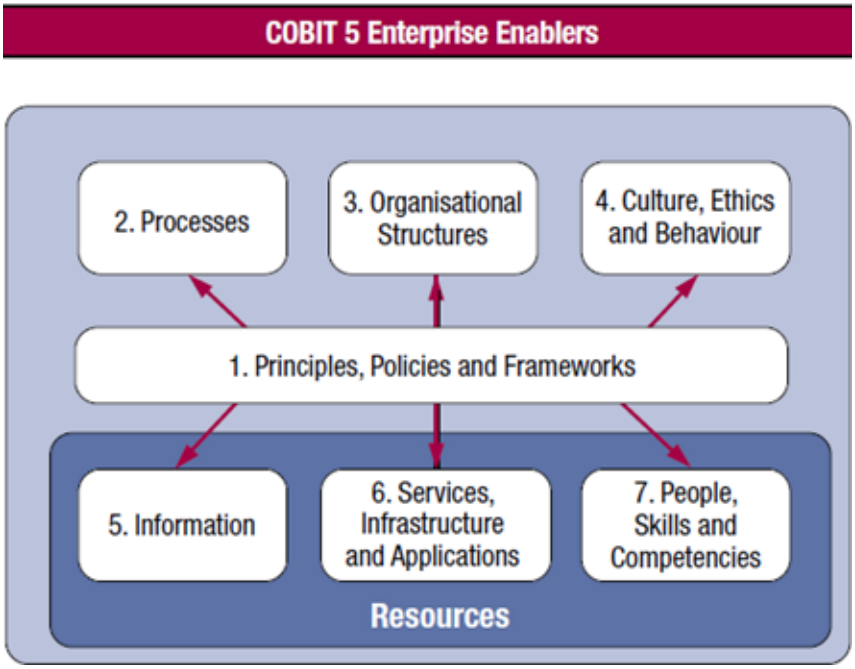
   b. Mengakomodasi seluruh *stakeholders*, fungsi dan proses yang relevan dengan keamanan informasi.

3. **Prinsip 3**: Menerapkan Integrasi Kerangka Kerja Tunggal.

   COBIT 5 dapat disesuaikan dengan standar dan *framework* lain, serta mengizinkan perusahaan untuk menggunakan standar dan *framework* lain sebagai lingkup manajemen kerangka kerja untuk *IT enterprise*.

4. **Prinsip 4**: Menggunakan Pendekatan yang Menyeluruh

   Pemerintahan dan manajemen perusahaan IT yang efektif dan efisien membutuhkan pendekatan secara holistik atau menyeluruh. COBIT 5 mendefinisikan kumpulan pemicu yang disebut *enabler* untuk mendukung implementasi pemerintahan yang komprehensif dan manajemen sistem perusahaan IT dan informasi. *Enablers* adalah faktor individual dan kolektif yang mempengaruhi sesuatu agar dapat berjalan atau bekerja. Kerangka kerja COBIT 5 mendefinisikan 7 kategori enablers yang dapat dilihat pada Gambar 2.12 berikut.



Gambar 2.12 *Enabler* COBIT 5 (Sumber: ISACA, 2012)

Ketujuh *enablers* yang digunakan pada COBIT 5 seperti yang dijelaskan pada Gambar 2.12 meliputi:

1. *Principles, Policies and Frameworks*
2. *Processes*
3. *Organisational Strucutres*
4. *Culture, Ethics and Behaviour*
5. *Information*

6. *Services, Infrastructure and Applications*
7. *People, Skills and Competencies*

5. **Prinsip 5**: Memisahkan Tata Kelola dengan Manajemen

   COBIT 5 membuat perbedaan yang jelas antara tata kelola dan manajemen. Kedua disiplin tersebut mencakup berbagai jenis kegiatan, membutuhkan struktur organisasi yang berbeda dan melayani tujuan yang berbeda. Perbedaan utama antara tata kelola dan manajemen pada COBIT 5 adalah:

   a. Tata kelola memastikan bahwa kebutuhan, kondisi dan pilihan *stakeholder* dievaluasi untuk menentukan keseimbangan berdasarkan tujuan perusahaan yang ingin dicapai. Selain itu tata kelola juga menetapkan arah melalui prioritas perusahaan, membuat keputusan, memantau kinerja dan kepatuhan terhadap arah dan tujuan yang disepakati.
   b. Manajemen melakukan perencanaan, membangun, menjalankan dan melakukan monitor yang sejalan dengan arah yang ditetapkan oleh tata kelola untuk mencapai tujuan perusahaan.

   Berlandaskan lima prinsip tersebut perusahaan dimungkinkan untuk membuat sebuah tata kelola dan kerangka kerja manajemen yang efektif dengan mengoptimalkan teknologi informasi dan investasi yang gunakan untuk kepentingan *stakeholder*

2.2.2.1 Model Referensi Proses COBIT 5

Pada COBIT 5 terdapat suatu model yang menggambarkan proses secara detail mengenai proses tata kelola dan manajemen. Model yang ada pada COBIT 5 tersebut merepresentasikan proses yang dapat ditemukan dalam perusahaan yang kaitanya dengan aktivitas TI. Model yang disediakan oleh COBIT 5 tersebut merupakan suatu model yang lengkap dan menyeluruh tapi bukan merupakan satu-satunya model proses yang dapat digunakan serta mudah dipahami oleh operasional TI dan manajer bisnis.

COBIT 5 membagi model referensi proses perusahaan yang ada menjadi dua bagian yaitu pada bagian tata kelola dan manajemen yang dapat dilihat pada penjelasan berikut (Diharja, 2013):

1. Tata kelola

   Tata kelola berfungsi untuk menjamin kebutuhan *stakeholder* dimana kondisi-kondisi dan pilihan yang ada selalu dievaluasi untuk menentukan tujuan perusahaan yang disepakati sesuai dengan prioritas dan pengambilan keputusan yang ada. Pada umumnya tata kelola yang ada secara menyeluruh merupakan tanggung jawab dari dewan direksi. Tata kelola yang lebih spesifik dapat didelegasikan kepada sebuah divisi khusus pada sebuah struktur organisasi yang kompleks. Model referensi yang menjadi bagian dari kontrol tata kelola adalah Evaluate, Direct and Monitoring (EDM).

2. Manajemen

   Manajemen memiliki fungsi untuk melakukan perencanaan, membangun, menjalankan dan melakukan pemantauan terhadap aktivitas yang ada dalam rangka penyelarasan arah tujuan perusahaan sesuai dengan penentuan dari badan tata kelola. Pada umumnya, yang bertanggung jawab untuk mengelola sebuah manajemen pada sebuah perusahan adalah manajemen eksekutif dibawah pimpinan CEO. Adapun model referensi yang tergabung di dalam control manajemen adalah sebagai berikut:

   a. Evaluate, Direct and Monitor (EDM)

      Proses untuk melakukan evaluasi, memerintah, dan mengawasi.

   b. Align, Plan and Organise (APO)

      Proses untuk melakukan penyelarasan, perencanaan, dan pengaturan.

   c. Build, Acquare and Implement (BAI)

      Proses untuk membangun, memperoleh dan mengimplementasikan.

   d. Deliver, Service and Support (DSS)

      Proses untuk mengirimkan, pelayanan, dan dukungan

   e. Monitor, Evaluate and Assess (MEA)

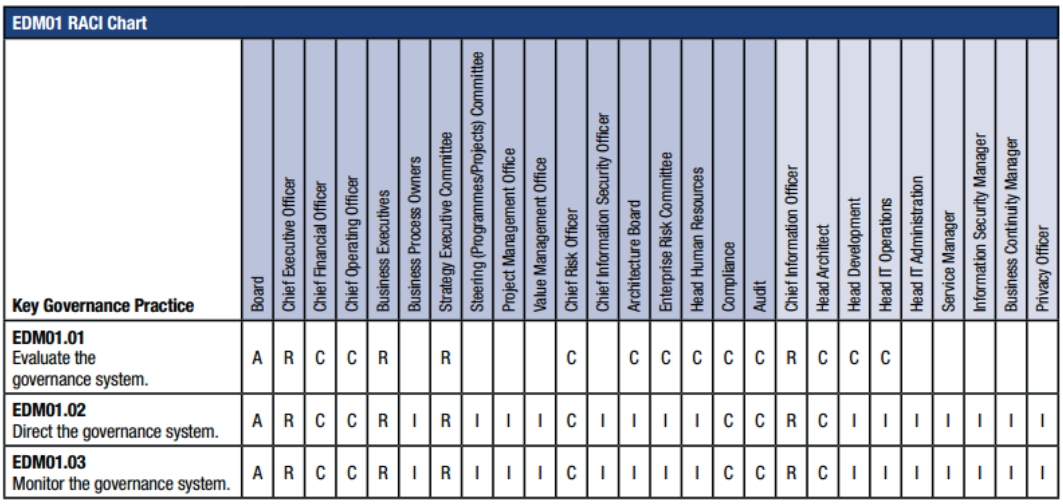
      Proses untuk mengawasi, evaluasi dan penilaian

2.2.2.2 RACI *Chart*

Framework COBIT 5 juga memiliki RACI *Chart* yang dapat digunakan dalam proses pemetaan pihak-pihak yang terkait dan bertanggung jawab dengan tepat dalam sebuah organisasi, hanya saja pada *framework* COBIT 5 pembahasan proses-proses dan RACI *Chart* secara eksplisit terdapat pada Buku COBIT 5: Enabling Proccesses. RACI *Chart* merupakan singkatan dari *Responsible, Accountable, Consulted* dan *Informed*. Dan tidak memiliki perbedaan seperti pada versi COBIT sebelumnya 4.1. Setiap *process goal* TI menerapkan RACI pada setiap aktivitas di dalamnya yang berfungsi untuk mendukung kesuksesan proses TI pada kelima *domain* yang ada. Adapun tujuan dari penerapan RACI adalah untuk memperjelas aktivitas sekaligus sebagai sarana untuk menentukan peran dari fungsi-fungsi lainnya terhadap suatu aktifitas tertentu. Berikut ini pembahasan dari RACI *Chart*, antara lain :

a. *Responsible*: Orang yang melakukan suatu kegiatan atau melakukan pekerjaan
b. *Accountable*: Orang yang akhirnya bertanggungjawab dan memiliki otoritas untuk memutuskan suatu perkara
c. *Consulted*: Orang yang diperlukan umpan atau sarannya dan berkontribusi akan kegiatan
d. *Informed*: Orang yang diperlukan tahu hasil dari suatu keputusan atau tindakan

RACI *chart* dapat membantu auditor untuk melakukan identifikasi terhadap orang-orang yang berkompeten untuk dilakukan proses wawancara. Terdapat 26 *role* atau peran pada COBIT 5.0 yang digunakan dalam RACI *chart* yang dapat dilihat pada Gambar 2.13. Semua *role* atau peran tersebut nantinya akan dipetakan sesuai dengan *role* atau peran yang ada pada perusahaan.



EDM01 RACI Chart																										
Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM01.01 Evaluate the governance system.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Direct the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Monitor the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

Gambar 2.13 Contoh RACI *role* pada COBIT 5

Pada COBIT 5 ada 26 *role* (Peran) yang digunakan RACI *chart*. Seluruh *role* tersebut kemudian disesuaikan dengan *role* yanga da pada organisasi yang akan dilakukan audit. Tabel 2.8 berikut ini menunjukan *role* yang ada pada COBIT serta penjelasan *role* dari masing-masing *role* (ISACA, 2013b).

Tabel 2.5 Penjelasan Peran (*role*) menurut COBIT 5

Role Pada COBIT 5.0	Penjelasan *Role*
Board	Kelompok eksekutif paling senior dan / atau direktur non-eksekutif perusahaan yang bertanggung jawab atas tata kelola perusahaan dan memiliki keseluruhan kontrol atas sumber dayanya
CEO	Petugas berpangkat tertinggi yang bertanggung jawab atas pengelolaan total perusahaan
CFO	Pejabat paling senior dari perusahaan yang bertanggung jawab atas semua aspek pengelolaan keuangan, termasuk risiko dan pengendalian keuangan
Chief Operating Officer (COO)	Pejabat paling senior dari perusahaan yang bertanggung jawab atas operasi perusahaan
CRO	Pejabat paling senior dari perusahaan yang bertanggung jawab atas semua aspek pengelolaan risiko di seluruh perusahaan. Fungsi petugas risiko TI dapat dibentuk untuk mengawasi risiko terkait TI.
CIO	Pejabat paling senior dari perusahaan yang bertanggung jawab untuk menyelaraskan strategi TI dan bisnis dan bertanggung jawab atas perencanaan, sumber daya dan pengelolaan penyampaian layanan dan solusi TI untuk mendukung tujuan perusahaan.

Role Pada COBIT 5.0	Penjelasan *Role*
Chief Information Security Officer (CISO)	Pejabat paling senior dari perusahaan yang bertanggung jawab atas keamanan informasi perusahaan dalam segala bentuknya
Business Executive	Seorang akuntan senior bertanggung jawab atas pengoperasian unit usaha atau anak perusahaan tertentu
Business Process Owner	Seorang individu bertanggung jawab atas kinerja sebuah proses dalam mewujudkan tujuannya, mendorong perbaikan proses dan menyetujui perubahan proses Strategi (*IT Executive*)
Strategy (IT Executive) Committee	Sekelompok eksekutif senior ditunjuk oleh dewan untuk memastikan bahwa dewan terlibat, dan terus menginformasikan, masalah dan keputusan utama yang berkaitan dengan TI. Komite bertanggung jawab untuk mengelola portofolio investasi TI, layanan TI dan aset TI, memastikan bahwa nilai diberikan dan risiko dikelola. Panitia biasanya diketuai oleh anggota dewan, bukan oleh CIO
(Project and Programme) Steering Committees	Sekelompok pemangku kepentingan dan ahli yang bertanggung jawab atas pembinaan program dan proyek, termasuk pengelolaan dan pemantauan rencana, alokasi sumber daya, penyampaian manfaat dan nilai, dan pengelolaan risiko program dan proyek.
Architecture Board	Sekelompok pemangku kepentingan dan pakar yang bertanggung jawab untuk panduan mengenai masalah dan keputusan terkait arsitektur perusahaan, dan untuk menetapkan kebijakan dan standar arsitektural
Enterprise Risk Committee	Kelompok eksekutif perusahaan yang bertanggung jawab atas kolaborasi dan konsensus tingkat perusahaan yang dibutuhkan untuk mendukung kegiatan dan keputusan manajemen risiko perusahaan. Sebuah dewan risiko TI dapat dibentuk untuk mempertimbangkan risiko TI secara lebih rinci dan menyarankan komite risiko perusahaan.
Head of HR	Pejabat paling senior dari perusahaan yang bertanggung jawab atas perencanaan dan kebijakan yang berkaitan dengan semua sumber daya manusia di perusahaan itu
Compliance	Fungsi dalam perusahaan yang bertanggung jawab atas panduan kepatuhan hukum, peraturan dan kontrak
Audit	Fungsi dalam perusahaan bertanggung jawab atas penyediaan audit internal
Head of Architecture	Seorang akuntan senior bertanggung jawab atas proses arsitektur enterprise

Role Pada COBIT 5.0	Penjelasan *Role*
Head of Development	Seorang akuntan senior bertanggung jawab atas proses pengembangan solusi terkait TI
Head of IT Operations	Seorang akuntan senior bertanggung jawab atas lingkungan dan infrastruktur operasional TI
Head of IT Administration	Seorang akuntan senior bertanggung jawab atas catatan terkait TI dan bertanggung jawab untuk mendukung masalah dan proyek administratif terkait TI
Programme and Project Management Office (PMO)	Fungsi yang bertanggung jawab untuk mendukung manajer program dan proyek, dan mengumpulkan, menilai dan melaporkan informasi tentang pelaksanaan program dan proyek penyusunnya
Value Management Office (VMO)	Fungsi yang bertanggung jawab untuk mendukung manajer program dan proyek, dan mengumpulkan, menilai dan melaporkan informasi tentang pelaksanaan program dan proyek penyusunnya
Service Manager	Individu yang mengelola pengembangan, pelaksanaan, evaluasi dan pengelolaan produk dan layanan baru dan yang ada untuk pelanggan (pengguna) atau kelompok pelanggan (pengguna) tertentu
Information Security Manager	Seseorang yang mengelola, merancang, mengawasi dan / atau menilai keamanan informasi perusahaan
Business Continuity Manager	Seseorang yang mengelola, merancang, mengawasi dan / atau menilai kemampuan kelangsungan bisnis perusahaan, untuk memastikan bahwa fungsi kritis perusahaan terus beroperasi setelah kejadian yang mengganggu
Privacy Officer	Seseorang yang bertanggung jawab untuk memantau risiko dan dampak bisnis undang-undang privasi dan untuk membimbing dan mengkoordinasikan pelaksanaan kebijakan dan kegiatan yang akan memastikan arahan privasi terpenuhi. Disebut juga petugas proteksi data.

Mengacu pada Tabel 2.8, kemudian disesuaikan masing-masing *role* tersebut dengan *role* yang ada pada Politeknik Negeri Bali. Untuk masing-masing *role* disini bisa saja ditempati oleh jabatan yang sama pada Politeknik Negeri Bali dikarenakan tidak seluruh organisasi memiliki *role* yang sama persis seperti pada COBIT 5, tetapi untuk tanggung jawaba ada yang memiliki tanggung jawab pada

bagian yang sama. Karena itu untuk pemetaan disini diperlukan hasild ari wawancara dengan pihak Politeknik Negeri Bali.

2.2.2.3 COBIT *Process Assessment Model*

Untuk mengidentifikasi kekuatan dan kelemahan TI, bagaimana kontribusi TI dalam mendukung pencapaian tujuan bisnis beserta risikonya dan solusi apa yang perlu direkomendasikan maka dibutuhkan audit TI dalam konteks *Process Maturity & Capability Assessment*. COBIT 5 menggunakan proses model *assessment* berdasarkan standar ISO/IEC 15504 untuk model penilaian dari proses dan dapat digunakan sebagai dasar untuk melakukan penilaian terhadap kemampuan setiap proses COBIT 5.0 proses penilaian akan berdasarkan tingkat kemampuan sebuah organisasi dalam melakukan proses-proses yang telah didefinisikan dalam model *assessment*. Tingkat kapabilitas dari sebuah proses ditentukan atas dasar pencapaian proses atribut tertentu menurut ISO/IEC 15504-2:2003 (ISACA, 2013a). Adapun penjelasan mengenai 6 tingkatan kapabilitas adalah sebagai berikut:

1. *Level* 0: *Incomplete Process*

   Organisasi pada tahap ini tidak melaksanakan proses proses TI yang seharusnya ada atau belum berhasil mencapai tujuan dari proses TI tersebut.
2. *Level* 1: *Performed Process*

   Organisasi pada tahap ini telah berhasil melaksanakan proses TI dan tujuan proses TI tersebut benar-benar tercapai
3. *Level* 2: *Managed Process*

   Organisasi pada tahap ini dalam melaksanakan proses TI dan mencapai tujuannya dilaksanakan secara terkelola dengan baik, sehingga ada penilaian lebih karena pelaksanaan dan pencapaiannya dilakukan dengan pengelolaan yang baik. Pengelolaan berupa proses perencanaan, evaluasi dan penyesuaian untuk ke arah yang lebih baik lagi.
4. *Level* 3: *Established Process*

   Organisasi pada tahap ini memiliki proses-proses TI yang sudah distandarkan dalam lingkup organisasi secara keseluruhan. Artinya sudah memiliki standar proses yang berlaku diseluruh lingkup organisasi tersebut.

5. *Level* 4: *Predictable Process*

   Organisasi pada tahap ini telah menjalankan proses TI dalam batasan-batasan yang sudah pasti, misalkan batasan waktu. Batasan ini dihasilkan dari pengukuran yang telah dilakukan pada saat pelaksanaan proses TI tersebut sebelumnya.

6. *Level* 5: *Optimizing Process*

   Pada tahap ini, organisasi telah melakukan inovasi-inovasi dan melakukan perbaikan yang berkelanjutan untuk meningkatkan kemampuannya.

2.2.3 Pengertian Risiko

Risiko menurut Kamus Besar Bahasa Indonesia (KBBI) adalah akibat yang kurang menyenangkan dari suatu perbuatan atau tindakan (KBBI, 2017). Menurut Preston B. Cline, risiko dapat juga didefinisikan sebagai interaksi manusia dengan ketidakpastian (Cline, 2004). ISO 31000 mendifiniskan risiko sebagai efek yang ditimbulkan dari sebuah ketidakpastian dalam pencapaian tujuan dalam organisasi maupun perusahaan. Risiko adalah suatu ukuran dari besarnya kemungkinan (frekuensi) dan konsekuensi (dampak) yang berpengaruh dalam suatu proyek. Terdapat dua komponen utama dari risiko, yaitu (Kerzner, 2006):

1. Peluang (kemungkinan) dari terjadinya kejadian
2. Dampak dari peristiwa yang terjadi

Secara konsep, risiko dari setiap kejadian didefinisikan sebagai fungsi dari kemungkinan terjadi dan dampak yang ditimbulkan.

$$Risiko = f(kemungkinan, dampak) \quad 2.1$$

Secara matematis dapat ditulis sebagai berikut:

$$Risiko = Frekuensi\ x\ Dampak \quad 2.2$$

Jika digambarkan kedalam sebuah fungsi akan terlihat seperti Gambar 2.14:

Gambar 2.14 Risiko dan Komponen yang membentuk
(Sumber: Kerzner, 2006 yang telah diolah kembali)

Dampak risiko terbagi menjadi beberapa tingkatan, yaitu (Kerzner, 2006):

1. Risiko Rendah.
   Dampak yang dihasilkan kecil dan tidak mempengaruhi dari *event* yang ada.
2. Risiko Menengah
   Dampak yang dihasilkan mulai terasa dan dapat mempengaruhi tujuan yang ada walaupun kurang signifikan.
3. Risiko Tinggi
   Dampak yang dihasilkan sangat besar dan memiliki pengaruh yang signifikan terhadap *event* yang ada.

2.2.3.1 Risiko Teknologi Informasi/ Sistem Informasi

Risiko Teknologi Informasi/Sistem Informasi (Risiko TI/SI) menurut Panduan TIK Nasional oleh Depkominfo adalah segala risiko pengelolaan TIK oleh institusi yang mencakup risiko proyek TI/SI, risiko atas informasi dan risiko atas keberlangsungan layanan TI/SI (Departemen Komunikasi dan Informatika Republik Indonesia, 2007). Contoh profil risiko TI dapat dilihat di Tabel 2.9

Tabel 2.6 Contoh Profil Risiko TI Bank ABC

Key Process	***Risk Issue***	***Control Design***	***Inherent Risk***		
			Likelihood	*Impact*	*Rating*
1	2	3	4	5	6
Uji Coba DRP	Kesiapan petugas *level* operasional saat terjadi disaster	1. Dilakukan simulasi DRP	Likely	Major	Very High
		2. Sosialisasi melalui program *awareness*			
		3. Dokumentasi prosedur lengkap			
Pengelolaan menu user pada aplikasi green screen	Kesalahan pemberian fitur menu pada *user*	1. Penerapan mekanisme *Dual Custody* untuk *level* OS dan aplikasi	Possible	High	Very High
		2. Verifikasi kesesuaian antara user privilege di sistem dengan reporting user ID administration			

(Sumber: Christiyono, 2011 di Samaptoaji, 2014)

2.2.4 Manajemen Risiko

Manajemen risiko adalah sebuah tindakan atau praktik dalam penanganan risiko. Mencakup perencanaan risiko, proses identifikasi dan analisis risiko, pengembangan strategi penanganan risiko, dan pemantauan risiko untuk

menentukan bagaimana risiko telah berubah bentuk (Kerzner, 2006). Berdasarkan ISO 31000:2009, manajemen risiko adalah aktivitas yang terorganisir untuk menjalankan dan mengawasi sebuah perusahaan atau organisasi dengan pendekatan risiko. Tujuan dari implementasi manajemen risiko dalam proyek atau program kerja adalah (International Organization for Standardization, 2009):

1. Kesuksesan terhadap proyek
2. Menurunkan risiko biaya dan menaikkan keuntungan bagi manajemen
3. Mempertahankan kestabilan pemasukan
4. Mengurangi dan melindungi kemungkinan kegagalan karena berbagai perubahan yang berpengaruh terhadap pembiayaan proyek
5. Meningkatkan skala bisnis perusahaan.

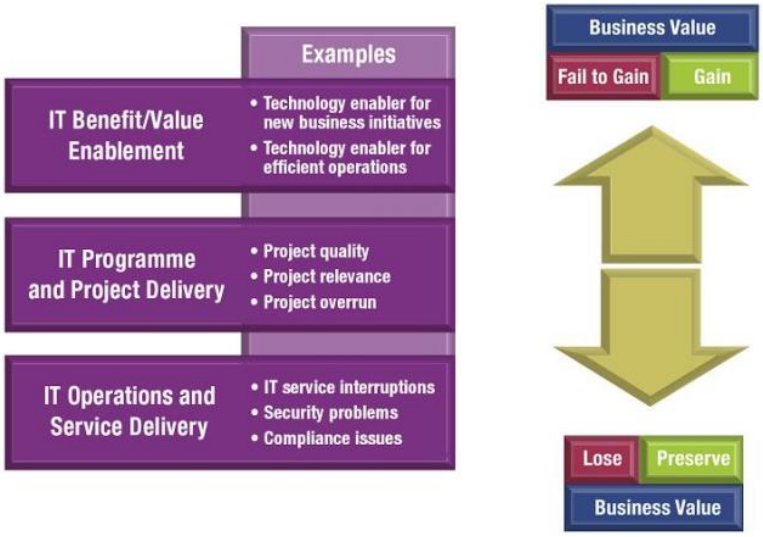
Sehingga, manajemen risiko dapat disimpulkan sebagai sebuah proses dimana risiko dapat dikelola pada organisasi atau perusahaan dengan tujuan untuk meminimalisir terjadinya risiko yang tidak diinginkan yang mampu menghambat proses bisnis dan tujuan dari organisasi atau perusahaan.

2.2.5 Kerangka Kerja Manajemen Risiko

Kesuksesan manajemen risiko bergantung pada efektifitas kerangka manajemen yang digunakan pada sebuah organsisasi. Kerangka kerja manajemen risiko memiliki tujuan, yaitu memastikan bahwa informasi mengenai risiko yang berasal dari proses manajemen risiko secara memadai dilaporkan dan digunakan sebagai dasar pengambilan keputusan serta kerangka kerja yang membantu pemenuhan akuntabilitas di semua tingkat organisasi yang relevan (Putri, 2017). Berikut merupakan kerangka kerja manajemen risiko yang umum digunakan dalam berbagai bidang:

2.2.5.1 COBIT 5 for Risk

COBIT 5 *for Risk* merupakan panduan manajemen risiko terkait TI yang ada didalam organisasi atau perusahaan. Risiko terkait TI menurut COBIT 5 *for Risk* dapat dikelompokkan menjadi tiga kategori, yaitu: *IT Benefit or Value Enablement*, *IT Programme and Project Delivery* dan *IT Operations and Service Delivery* (ISACA, 2013c).



Gambar 2.15 Kategori Risiko TI menurut COBIT 5 for Risk

(Sumber: COBIT 5 *For Risk*, ISACA, 2013)

Penjelasan lengkap mengenai katergori risiko TI yang mengacu pada Gambar 2.15 yaitu:

1. *IT Benefit or Value Enablement*

   Risiko TI yang berkaitan dengan kesempatan dalam menggunakan teknologi guna meningkatkan efisiensi atau efektifitas proses bisnis dan sebagai enabler untuk inisiatif bisnis baru.

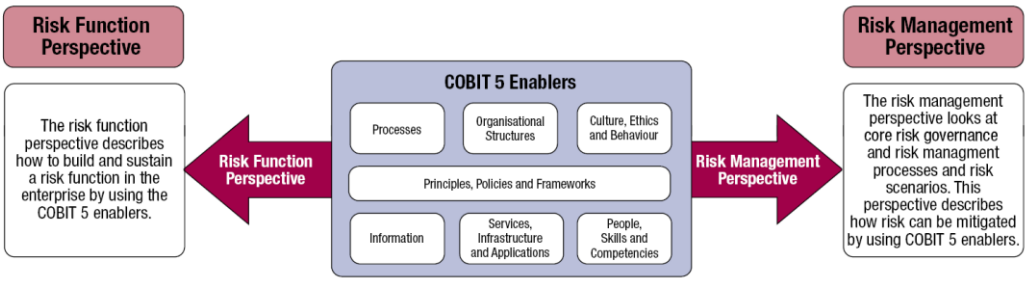
2. *IT Programme and Project Delivery*

   Risiko TI yang berkaitan dengan kontribusi TI dalam meningkatkan suatu bisnis atau membuat solusi bisnis baru. Biasanya dalam bentuk proyek dan menghasilkan program sebagai bagian dari portofolio perusahaan atau organisasi.

3. *IT Operation and Service Delivery*

   Risiko TI yang berkaitan dengan stabilitas operasional, perlindungan, ketersediaan dan pemulihan layanan TI dari semua aspek yang dapat membawa dampak buruk bagi nilai perusahaan atau organisasi.

COBIT 5 *for Risk* memiliki perspektif risiko TI yang dibagi menjadi dua, yaitu: *Risk Management Perspective* dan *Risk Function Perspective*.



Gambar 2.16 Dua Perspektif Risiko TI menurut COBIT 5 for Risk
(Sumber: COBIT 5 *for Risk*, ISACA, 2013)

Penjelasan mengenai dua perspektif risiko terkait TI yang mengacu pada Gambar 2.16, antara lain:

1. *Risk Function Perspective*

   Perspektif ini menjelaskan tentang tat acara membangun dan menjaga setiap fungsi risiko dalam perusahaan dengan berpedoman pada COBIT 5 Enabler. Contohnya:

   a. Proses, dalam hal ini proses apa yang dibutuhkan oleh suatu organisasi untuk menentukan dan menjaga fungsi risiko serta mengatur dan mengelola risiko
   b. Informasi, dalam hal ini informasi apa yang dibutuhkan oleh suatu organisasi untuk mengatur dan mengelola setiap risiko.
   c. Struktur Organisasi, dalam hal ini struktur organisasi seperti apa yang dibutuhkan oleh suatu organisasi untuk mengatur dan mengelola risiko secara efektif.
   d. Orang, skill dan kompetensi, dalam hal ini SDM seperti aoa atau SDM yang memiliki kemampuan seperti apa yang dibutuhkan oleh suatu orgnasisasi untuk mengendalikan dan mengoperasikan *risk function* agar lebih efektif.

2. *Risk Management Perspective*

   Perspektif ini menjelaskan tentang tat acara untuk mengurangi risiko dengan berpedoman pada COBIT 5 Enabler.

Gambar 2.17 Prinsip Manajemen Risiko

(Sumber: COBIT 5 *for Risk*, ISACA, 2013)

Mengacu pada Gambar 2.17, dapat diketahui bahwa terdapat tujuh prinsip dalam menerapkan manajemen risiko TI, antara lain:

1. Menghubungkan manajemen risiko TI dengan tujuan perusahaan
2. Menyelaraskan manajemen risiko TI dengan manajemen risiko organisasi atau perusahaan
3. Menyeimbangkan cost/benefit dari setiap risiko TI
4. Sarana untuk memperkenalkan organisasi dan membangun komunikasi terbuka
5. Menciptakan suasana yang baik dikalangan *top management*.
6. Berfungsi sebagai bagian dari aktifitas sehari-hari sebagai pendekatan yang konsisten

Terdapat dua proses TI untuk perspektif manajemen risiko menurut COBIT 5 *for Risk*, yaitu EDM03 (*Ensure Risk Optimization*) dan APO12 (*Manage Risk*). Penjelasan masing-masing proses TI, antara lain:

1. EDM03 (*Ensure Risk Optimisation*)

   Proses EDM03 bertujuan untuk memastikan apakah tingkat risiko dan besarnya toleransi yang dapat diterima oleh organisasi atau perusahaan telah dimengerti, diartikulasikan dan dikomunikasikan dengan baik, serta memastikan apakah

risiko-risiko yang terkait dengan TI telah diidentifikasi dan dikelola dengan baik. Proses EDM03 dibagi menjadi tiga, yaitu:

a. EDM03.01 (*Evaluate Risk Management*)

   EDM03.01 bertujuan untuk memeriksa dan menilai pengaruh risiko terhadap penggunaan TI di suatu organisasi pada masa kini dan masa yang akan datang. Disamping itu juga mempertimbangkan apakah batas toleransi terhadap risiko TI yang ditetapkan oleh organisasi sudah tepat dan dikelola dengan baik. Aktivitas dari EDM03.01, antara lain:

   i. Menentukan *level* penerapan manajemen risiko TI sehingga organisasi dapat memenuhi tujuannya.
   ii. Mengevaluasi dan menyetujui usulan tentang batas toleransi risiko TI terhadap risiko dan tingkat peluang yang dapat diterima oleh perusahaan atau organisasi.
   iii. Menyelaraskan antara strategi pengelolaan risiko TI dengan strategi pengelolaan risiko organisasi.
   iv. Mengevaluasi kembali faktor-faktor risiko TI dan memastikan bahwa organisasi telah membuat keputusan yang tepat terkait keputusan strategis organisasi.
   v. Menentukan metode atau cara penilaian risiko dan evaluasi risiko yang tepat.
   vi. Mengevaluasi dan memantau kegiatan manajemen risiko untuk memastikan keselarasan antara manajemen risiko dengan kapasitas perusahaan atau organisasi.

b. EDM03.02 (*Direct Risk Management*)

   EDM03.02 bertujuan untuk mengarahkan praktik penerapan manajemen risiko guna memastikan bahwa manajemen risiko TI yang telah diterapkan sudah benar-benar tepat serta memastikan bahwa risiko TI yang telah diidentifikasi tidak melebihi batas toleransi risiko. Aktivitas dari EDM03.02, antara lain:

   i. Mengenalkan budaya sadar risiko TI dan memberdayakan organisasi untuk secara proaktif mengidentifikasikan risiko TI, peluang dan potensi dampak terhadap proses bisnis.

ii. Mengintegrasikan antara strategi dan operasi risiko TI dengan strategi dan operasi risiko organisasi.

iii. Mengkomunikasikan setiap risiko dan rencana aksi yang dilakukan kepada semua lapisan organisasi.

iv. Menjalankan, mekanisme yang tepat untuk merespon setiap perkembangan risiko dengan cara melapor perkembangan risiko tersebut kepada pihak yang tepat dan disertai dengan dukungan dari prinsip yang telah disepakati.

v. Mengidentifikasi setiap risiko yang muncul, peluang timbulnya risiko dan dampak yang diakibatkan oleh risiko tersebut. Kemudian risiko tersebut dikelola sesuai dengan ketentuan dan prosesdur yang telah diterbitkan oleh pihak yang berwenang.

vi. Mengidentifikasi tujuan serta matriks pelaksanaan proses tata kelola dan manajemen untuk memantau dan menyetujui pendekatan, metode, teknik dan proses yang digunakan.

c. EDM03.03 (*Monitor Risk Management*)

EDM03.03 bertujuan untuk memantau apakah penerapan tata kelola dan manajemen risiko TI telah sesuai dengan tujuan utama, serta mengidentifikasi, melacak dan melaporkan penyimpangan atau masalah yang ditemukan untuk dilakukan perbaikan. Aktivitas dari EDM03.03, antara lain:

i. Memantau pengelolaan profil risiko organisasi apakah telah sesuai dengan *risk appetite* yang ditetapkan organisasi.

ii. Memantau penerapan proses tata kelola dan manajemen risiko, menganalisis faktor penyebab timbulnya suatu risiko dan merencanakan tindakan perbaikan untuk mengatasinya.

iii. Merekapitulasi ulasan dari *stakeholder* mengenai kunci untuk meraih tujuan dan kemajuan organisasi.

iv. Melaporkan segala permasalahan mengenai manajemen risiko kepada dewan atau komite eksekutif.

2. APO12 (*Manage Risk*)

Proses APO12 bertujuan untuk mengidentifikasi, menilai dan mengurangi risiko terkait dengan TI agar tidak melebihi batas toleransi yang telah ditentukan oleh manajemen eksekutif organisasi. Selain itu proses APO12 juga bertujuan untuk mengintegrasikan manajemen risiko TI dengan manajemen risiko perusahaan atau organisasi. Proses APO12 terbagi menjadi enam sub-proses, antara lain:

a. APO12.01 (*Collect Data*)

APO12.01 bertujuan untuk mengumpulkan data yang relevan untuk meningkatkan keefektifan dalam mengidentifikasi, menganalisis dan melaporkan risiko terkait TI. Aktivitas dari APO12.01, antara lain:

i. Membangun dan memelihara metoda yang tepat untuk mengumpulkan, mengklasifikasikan dan menganalisis data yang berhubungan dengan risiko TI, seperti definisi risiko, kategori risiko dan faktor risiko.

ii. Merekapitulasi data relevan yang berperan penting dalam proses pengelolaan risiko TI, baik yang berasal dari lingkungan internal maupun eksternal organisasi.

iii. Survey dan menganisisi usul data yang berkaitan dengan risiko TI yang berasal dari eksternal organisasi, meliputi riwayat kerugian akibat trend, rekan bisnis dan kesepakatan yang dibuat mengenai peristiwa yang umum

iv. Merekapitulasi data mengenai risk event, isu terkait, insiden, permasalahan dan investigasi yang mampu menimbulkan dampak pada *IT Benefit of Value Enablement*, *IT Programme and Project Delivery*, *IT Operational and Service Delivery*.

v. Mengidentifikasi dan mengelompokkan data yang telah dikelompokkan berdasarkan faktor umum yang terjadi di beberapa kasus.

vi. Menentukan kondisi seperti apa yang mungkin muncul saat terjadinya risiko, frekuensi kemungkinan munculnya kondisi tersebut dan dampak yang ditimbulkan oleh kondisi tersebut.

vii. Mengidentifikasi *risk issue* yang baru muncul akibat adanya event atau hasil analisis risiko periodic terkait risiko internal dan eksternal.

b. APO12.02 (*Analyze Risk*)

APO12.02 bertujuan untuk menganalisis dan mengembangkan informasi mengenai risiko TI serta memperhitungkan relevansinya dengan faktor risiko organisasi. Aktivitas dari APO12.02, antara lain:

i. Menentukan upaya dalam menganalisis risiko terkait faktor-faktor risiko dan kekritisan bisnis asset.

ii. Memperbarui scenario risiko secara terus-menerus dan teratur, menggabungkan scenario dengan jenis ancaman yang terjadi, melakukan kontrol risiko dan mendeteksi tindakan untuk merespon risiko.

iii. Memperkirakan frekuensi besarnya keuntungan dan kerugian yang berhubungan dengan scenario risiko TI, memperhitungkan faktor-faktor risiko, mengevaluasi pengendalian operasional dan memperkirakan nilai risiko residual.

iv. Membandingkan antara risiko residual dengan batas toleransi risiko yang dapat diterima oleh organisasi, serta mengidentifikasi risiko mana saja yang membutuhkan respon risiko

v. Melakukan analisis cost-benefit dari setiap pilihan respon risiko baik risk *Avoid*ance, risk reduction/mitigation, risk shared/*Transfer* maupun risk *Transfer*ance. Dari hasil analisis tersebut kemudian memberikan usulan respon yang paling optimal.

vi. Menentukan persyaratan untuk setiap proyek atau program yang akan menerapkan respon risiko yang sudah ditentukan serta mengidentifikasi kebutuhan dan harapan dari penerapan respon risiko tersebut.

vii. Memvalidasi hasil analisis risiko sebelum memutuskan untuk melakukan analisis risiko menggunakan kerangka kerja lain.

c. APO12.03 (*Maintain a Risk Profile*)

APO12.03 bertujuan untuk menjaga inventori atau atribut risiko seperti frekuensi kemungkinannya terjadi risiko, dampak akibat terjadinya risiko,

respon yang dilakukan untuk meminimalisir terjadinya risiko, sumber daya terkait dengan kegiatan pengendalian yang telah dilakukan sebelumnya. Aktivitas dari APO12.03, antara lain:

i. Menjaga inventori bisnis, termasuk personil pendukung, aplikasi, infrastruktur, fasilitas, catatan manual, vendor, supplier dana gen outsourcing, serta mendokumentasikan ketergantungan antara manajemen layanan TI dengan sumber daya infrasturktur TI.
ii. Menentukan infrastruktur layanan TI dan sumber daya TI yang berperan penting dalam mempertahankan jalannya proses bisnis.
iii. Mengelompokkan setiap skenario risiko berdasarkan kategori, lini bisnis atau area fungsional
iv. Mengumpulkan semua profil risiko secara teratur dan menggabungkannya menjadi kumpulan profil risiko.
v. Mendefinisikan seperangkat indikator berdasarkan dari profil risiko untuk mengidentifikasi risiko secara cepat dan memantaunya sesuai degan tren risiko saat ini.
vi. Mencatat semua informasi mengenai risiko TI yang telah terjadi, kemudian dimasukkan dalam profil risiko TI perusahaan atau organisasi.
vii. Mencatat semua informasi mengenai rencana yang digunakan untuk merespon risiko, kemudian dimasukkan kedalam profil risiko TI perusahaan.

d. APO12.04 (*Articulate Risk*)

APO12.04 bertujuan untuk mengkomunikasikan segala hal yang berhubungan dengan proses bisnis perusahaan, termasuk sumber daya pendukung, apikasi, infrastruktur, fasilitas, catatan manual, vendor, supplier dana get outsourcing, serta mendokumentasikan ketergantungan antara manajemen layanan TI dan sumber infrastruktur TI. Aktivitas dari APO12.04, antara lain:

i. Melaporkan hasil analisis risiko kepada semua pemangku kepentingan, termasuk frekuensi peluang, besarnya dampak dan

manfaat yang diperoleh guna mendukung keputusan yang harus diambil oleh perusahaan dan menyeimbangkan *risk-return*.

ii. Memberikan pemahaman kepada para pemangku kepentingan mengenai scenario risiko terburuk yang mungkin terjadi, uji kelayakan pada objek yang rentan terhadap risiko dan pertimbangan hukumnya.

iii. Membuat laporan berupa profil risiko untuk semua pemangku kepentingan guna meningkatkan efektivitas penerapan manajemen risiko serta mengontrol kesenjangan, inkonsistensi, redudansi dan dampak terhadap profil risiko itu sendiri.

iv. Meninjau dan memetakan hasil penilaian objektif yang dilakukan oleh pihak ketiga, audit internal maupun tinjauan jaminan kualitas ke dalam profil risiko. Dari hasil tinjauan tersebut dapat digunakan untuk menentukan kebutuhan analisis risiko tambahan.

e. APO12.05 (*Define a Risk Management Action Portfolio*)

APO12.05 bertujuan untuk mengelola peluang dalam mengurangi risiko sehingga sesuai dengan *Transferable level* dan menghasilkan portofolio. Aktivitas dari APO12.05, antara lain:

i. Menjalankan kegiatan pengendalian untuk mengelola setiap risiko agar sesuai dengan *Risk Appetite* dan *Risk Tolerance*. Kemudian mengelompokkan risiko tersebut kedalam laporan risiko TI yang spesifik.

ii. Memastikan apakah setiap entitas organisasi telah memonitor risiko dan mengelola risiko tersebut agar sesuai dengan batas toleransi individu dan portofolio.

iii. Membuat proposal dari setiap proyek yang dirancang untuk mengurangi risiko, meningkatkan peluang strategis, menghitung besarnya biaya dan manfaat, dan hal-hal lain yang mampu menimbulkan efek pada profil risiko.

f. APO12.06 (*Respond to Risk*)

APO12.06 bertujuan untuk merespon risiko secara tepat waktu dan membatasi besarnya kerugian yang ditimbulkan akibat risiko TI. Aktivitas dari APO12.06, antara lain:

i. Menyiapkan, menguji dan mendokumentasikan rencana untuk merespon suatu risiko yang dapat menyebabkan insiden operasional atau dampak bisnis yang serius.

ii. Menerapkan rencana respon risiko yang tepat untuk meminimalisisr dampak ketika terjadinya suatu risiko.

iii. Memeriksa riwayat kerugian dan kesempatan yang hilang serta penyebab dari peristiwa risiko terdahulu.

2.2.5.2 ISO 31000:2009

The International Organization for Standardization (ISO) 31000 merupakan sebuah standar internasional tentang manajemen risiko yang dibuat dengan tujuan memberikan prinsip dan panduan secara umum untuk penerapan manajemen risiko di organisasi atau perusahaan. Secara garis besar, manajemen risiko dalam ISO 31000 terbagi menjadi tiga bagian, yaitu prinsip, kerangka kerja dan proses.

Proses manajemen risiko menurut ISO/IEC 31000:2009 mengacu pada Gambar 2.18 secara umum terdapat pada klausa 5, yaitu:

1. *Establishing the Context*

   Proses ini menetapkan beberapa konteks untuk melakukan *risk assessment*, antara lain konteks internal organisasi, konteks eksternal yang mempengaruhi organisasi tersebut, konteks manajemen risiko yang memfokuskan pada penanganan risiko yang diidentifikasi, dan kriteria risiko sebagai parameter yang disepakati oleh suatu organisasi.

2. *Risk Identification*

   Proses dimana mengidentifikasi risiko-risiko yang terdapat di sekitar lingkungan suatu organisasi, mulai dari kategori risiko, penyebab risiko, kriteria tingkat keparahan risiko probabilitas terjadinya risiko hingga dampak yang disebabkan oleh risiko-risiko tersebut.

3. *Risk Analysis*

Proses menganalisis lebih lanjut penyebab, dampak dan konsekuensi yang ditimbulkan oleh risiko yang telah diidentifikasi.

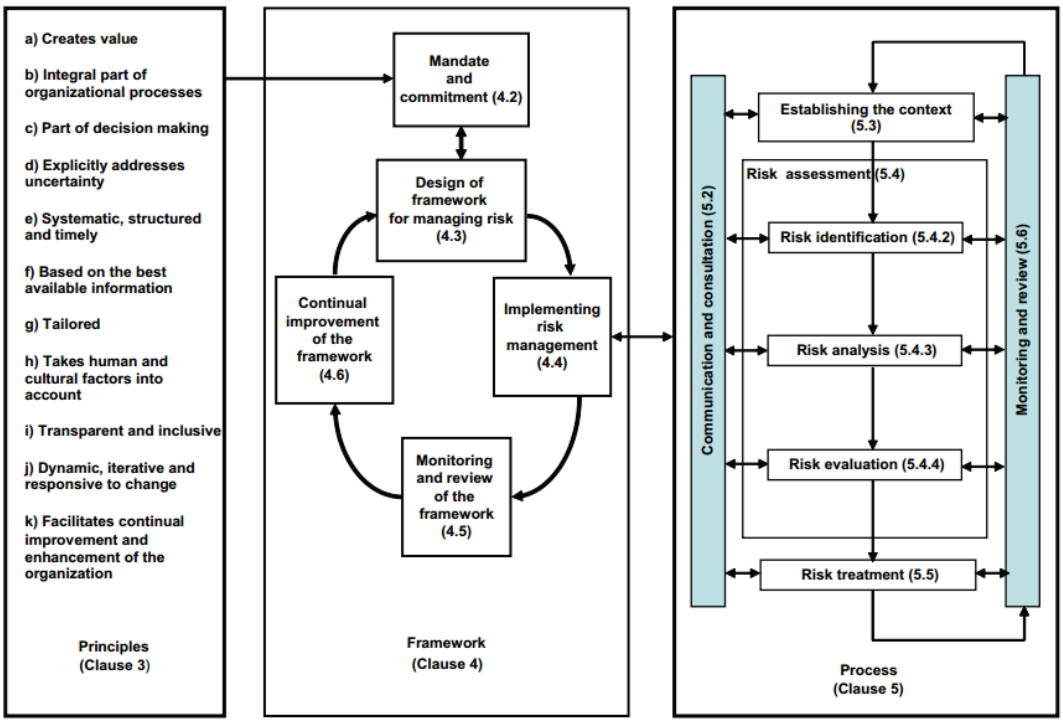
4. *Risk Evaluation*

   Proses membandingkan hasil analisis risiko dengan kriteria risiko untuk menentukan bagaimana penanganan risiko yang akan diterapkan.

5. *Risk Treatment*

   Merupakan strategi untuk melakukan mitigasi risiko yang terbagi menjadi beberapa pilihan, yaitu:

   a. *Risk Avoidance* (Menghindari risiko)
   b. *Risk Reduction* (Mitigasi risiko)
   c. *Risk Sharing* (*Transfer* risiko kepada pihak ketiga)
   d. *Risk Transferance* (Menerima risiko)



Gambar 2.18 Prinsip, kerangka kerja dan proses manajemen risiko

(Sumber: ISO 31000, 2009)

2.2.6. Metode Penilaian Risiko berdasarkan COBIT 5 for Risk

Penilaian risiko berdasarkan kerangka kerja COBIT 5 *for Risk*, perlu mengidentifikasi risiko terkait informasi yang harus ditentukan seperti tipe risiko,

kategori risiko, faktor risiko, skenario risiko, kontrol risiko, proses COBIT 5 yang terkait, serta frekuensi dan dampak (*magnitude*) dari masing-masing risiko (Putri, 2017)

2.2.6.1 Tipe Risiko

Risiko yang sudah diidentifikasi dapat dikategorisasikan berdasarkan tipe dari risiko tersebut. Tipe risiko dibagi menjadi tiga kategori (ISACA, 2013c), yaitu sebagai berikut:

1. *IT benefit / value enablement risk*, dimana risiko yang diidentifikasi masuk ke dalam kategori manfaat atau nilai risiko TI, yaitu apabila risiko terkait dengan (kehilangan) kesempatan untuk meanfaatkan TI dalam meningkatkan efisiensi atau efektivitas proses bisnis atau sebagai enabler untuk inisiatif bisnis baru. Contohnya adalah teknologi yang digunakan dalam inisiatif bisnis baru dan teknologi yang digunakan untuk mengefisiensikan proses operasional.
2. *IT programme and project delivery risk*, dimana risiko yang diidentifikasi masuk ke dalam kategori program dan proyek risiko TI, yaitu apabila risiko terkait dengan kontribusi TI untuk membuatkan atau meningkatkan solusi bisnis, biasanya dalam bentuk proyek dan program. Contohnya adalah kualitas proyek, relevansi proyek dan kelebihan waktu proyek dari yang ditentukan.
3. *IT operations and service delivery risk*, dimana risiko yang diidentifikasi masuk ke dalam kategori operasional dan layanan risiko TI, yaitu apabila risiko terkait dengan stabilitas operasional, ketersediaan, perlindungan dan pemulihan layanan TI, dimana risiko dapat membawa kerugian atau pengurangan nilai perusahaan. Contohnya adalah gangguan pada layanan TI, masalah keamanan dan isu-isu terkait.

Kemudian untuk memudahkan pembagian tingkat kiritikalisasi risiko, tipe risiko dikategorisasikan dalam dua hal (ISACA, 2013c):

1. Primer atau biasa dilambangkan dengan huruf ‘P’ untuk tipe skenario risiko yang menunjukkan primer atau menunjukkan tingkat yang lebih tinggi.
2. Sekunder atau biasa dilambangkan dengan huruf ‘S’ untuk tipe skenario risiko menunjukkan sekunder atau menunjukkan tipe yang lebih rendah.

2.2.6.2 Kategori Risiko

Mengacu kepada kerangka kerja COBIT 5 for Risks, terdapat dua puluh kategori risiko TI untuk setiap risiko yang diidentifikasi, berikut merupakan beberapa kategori risiko menurut COBIT 5 *for Risk* yang disajikan pada Tabel 2.10 (ISACA, 2013c).

Tabel 2.7 Kategori risiko menurut COBIT 5 For Risk

No	Kategori	Pengertian
1	*Portfolio establishment and maintenance*	Pengadaan dan pemeliharaan portofolio
2	*Programme/ projects life cycle management*	Manajemen siklus hidup program atau proyek
3	*IT investment decision making*	Investasi pengambilan keputusan TI
4	*IT expertise and skills*	Ketrampilan dan kemampuan TI

(Sumber: COBIT 5 *for Risk*, ISACA, 2013)

2.2.6.3 Faktor Risiko

Faktor risiko adalah kondisi yang mempengaruhi frekuensi dan/atau dampak bisnis dari skenario risiko. Faktor risiko dapat dapat diklasifikasikan ke dalam dua kategori utama, yaitu (ISACA, 2013c):

1. ***Internal Contextual Factors***, dimana faktor ini diberlakukan untuk risiko yang berada dibawah kendali perusahaan, meskipun organisasi tidak selalu mudah untuk berubah
2. ***External contextual factors***, dimana faktor ini diberlakukan untuk risiko yang berada diluar kendali perusahaan

2.2.6.4 Skenario Risiko

Skenario risiko TI adalah deskripsi dari suatu peristiwa yang berhubungan dengan TI yang dapat menyebabkan dampak bisnis, ketika risiko terjadi dan perkiraan apabila risiko terjadi. Pembuatan skenario risiko berdasarkan dua jenis, yaitu skenario positif dan skenario negative. COBIT 5 *For Risk* menyediakan 111

skenario risiko yang umum atau generik untuk membantu perusahaan atau organisasi dalam menentukan risiko (ISACA, 2013c)

2.2.6.5 Pemetaan risiko dengan Proses COBIT 5

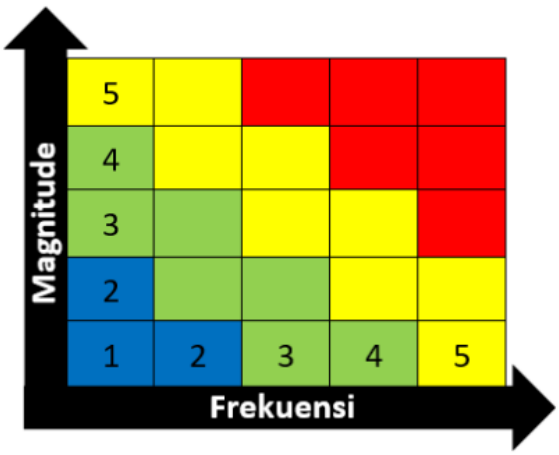
Risiko yang sudah diidentifikasi dan diberikan kontrol risiko dapat dipetakan dengan proses yang ada pada COBIT 5 *Enabling Process* sesuai keterkaitan tipe, faktor dan scenario risiko tersebut (ISACA, 2013c).

2.2.6.6 Penilaian Risiko berdasarkan Frekuensi dan Dampak Risiko

Berdasarkan acuan standar COBIT 5 *for Risk*, penilaian risiko dibagi berdasarkan dua aspek, yaitu aspek frekuensi dan *magnitude* (dampak). Untuk aspek frekuensi, peringkat dan parameternya dapat disesuaikan dengan konteks organisasi (ISACA, 2013c).

2.2.6.7 *level* Penilaian Risiko

Melalui penilaian risiko berdasarkan frekuensi dan dampak (*magnitude*) risiko TI, didapatkan prioritas risiko berdasarkan *level* penilaian risiko melalui pemetaan pada suatu peta risiko yang dibagi berdasarkan empat wilayah warna. Berikut penggambaran peta risiko ditampilkan pada Gambar 2.19 (ISACA, 2013c).



Gambar 2.19 Peta Frekuensi dan *Magnitude* Risiko
(Sumber: COBIT 5 *for Risk*, ISACA, 2013)

Pemetaan frekuensi dan *magnitude* berdasarkan empat wilayah warna kemudian diklasifikasikan berdasarkan *level* prioritas kegagalan yang memerlukan

penanganan lanjut. Berikut pemetaan *level* prioritas risiko ditampilkan pada Tabel 2.11 (ISACA, 2013c)

Tabel 2.8 *level* prioritas risiko

Pemetaan Warna	Level Prioritas
Merah	Very High
Kuning	High
Hijau	Medium
Biru	Low

(Sumber: COBIT 5 *for Risk*, ISACA, 2013)

2.2.6.8 Respon Mitigasi Risiko

Sebelum menentukan respon mitigasi risiko, awalnya adalah menentukan *Risk Appetite*, *Risk Tolerance* dan *Risk Capacity* yang terdapat di suatu perusahaan atau organisasi. *Risk Appetite* merupakan jumlah risiko dalam berbagai aspek yang dapat diterima oleh organisasi atau perusahaan dalam mengejar visinya. *Risk Tolerance* adalah tingkat variasi yang dapat diterima oleh manajemen dengan membiarkan adanya risiko tertentu karena mengejar suatu tujuan. *Risk Capacity* merupakan kerugian kumulatif yang dapat ditoleransi perusahaan tanpa mempertaruhkan kelangsungan hidupnya (ISACA, 2013c). *Risk Appetite*, *Risk Tolerance* dan *Risk Capacity* ditentukan oleh manajemen perusahaan atau organisasi.

Terdapat beberapa metode yang umum dalam mengekspresikan Risk Appetite menurut Risk and Insurance Management Society di tahun 2012 didalam publikasinya yang berjudul *Exploring Risk Appetite and Tolerance* (Risk and Insurance Management Society, 2012), yaitu :

1. Menentukan batasan pada frekuensi dan dampak dari risiko
2. Ukuran modal atau berdasarkan neraca keuangan
3. Ukuran untung dan rugi (tingkatan toleransi dari kerugian tahunan)
4. Batasan untuk masing-masing dampak pada indikator-indikator kunci yang dipengaruhi oleh risiko

Manajemen risiko adalah proses proaktif dimana dilakukan pengelolaan dan antisipasi risiko sebelum mereka terjadi. Risiko terbagi menjadi positif dan negatif. Risiko ngeatif dapat membahayakan tujuan proyek dan risiko positif dapat memberikan dampak positif terhadap proyek.

Tabel 2.9 Mitigasi Risiko Positif dan Negatif

Respon Risiko Negatif	Strategi Umum	Respon Risiko Positif
Avoid	*Eliminate uncertainty*	*Exploit*
Transfer	*Allocate ownership*	*Share*
Mitigate	*Modify exposure*	*Enhance*
Transfer	*Include in baseline*	*Ignore*

(Sumber: COBIT 5 *for Risk*, ISACA, 2013)

Jika untuk merespon risiko negatif menggunakan strategi *Avoid*, *Transfer*, *Mitigate* (*Treat*) dan *Transfer*, maka respon untuk risiko positif dibedakan menjadi *exploit*, *share*, *ehance* and *ignore*. Strategi respon risiko yang dapat dilihat pada Tabel 2.12 (ISACA, 2013c).

2.2.7 Kerangka Kerja Pendukung COBIT 5 for Risk

COBIT 5 *for Risk* sama seperti COBIT 5 yaitu secara harafiah merupakan sebuah "*umbrella approach*" dalam aktivitas terkait manajemen risiko (ISACA, 2013c). Ini memungkinkan jika COBIT 5 *for Risk* digunakan bersamaan dengan standar atau kerangka kerja lainnya terkait manajemen risiko.

2.2.7.1 ISO/IEC 27002:2013

ISO/IEC 27002:2013 kode praktis untuk kontrol keamanan informasi merupakan sebuah pedoman dan prinsip umum untuk memulai, melaksanakan, memelihara dan meningkatkan manajemen keamanan informasi didalam suatu sistem (BSI Standards Publication, 2013). ISO/IEC 27002:2013 mengandung praktik terbaik dalam pengendalian dan kontrol di bidang keamanan informasi (Andriyanto, Sihwi, & Anggrainingsih, 2015), mencakup:

1. Kebijakan keamanan informasi (klausal 5)
2. Organisasi keamanan informasi (klausal 6)
3. Keamanan sumber daya manusia (klausal 7)

4. Manajemen aset (klausal 8)
5. Akses kontrol (klausal 9)
6. Kriptografi (klausal 10)
7. Keamanan fisik dan lingkungan (klausal 11)
8. Keamanan operasi (klausal 12)
9. Keamanan komunikasi (klausal 13)
10. Akuisisi, pengembangan dan pemeliharaan sistem informasi (klausal 14)
11. Hubungan dengan *Supplier* (klausal 15)
12. Manajemen insiden keamanan informasi (klausal 16)
13. Aspek keamanan informasi dalam manajemen keberlangsungan bisnis (klausal 17)
14. Syarat pemenuhan (klausal 18)

Kegunaan ISO/IEC 27002:2013 dalam penelitian ini adalah sebagai acuan dalam melakukan aksi terhadap respon risiko TI.

2.2.7.2 ITIL V3: 2011

Information Technology Infrastructure Library (ITIL) merupakan suatu rangkaian konsep yang menekankan pada pengelolaan siklus hidup layanan yang disediakan oleh teknologi informasi atau ITSM (OGC, 2007). ITIL V3:2011 memiliki 5 domain yang diterbitkan kedalam lima buku berbeda, antara lain:

1. *Service Strategy*

   Panduan terhadap implementasi layanan TI dalam sudut pandang ITSM sebagai sebuah aset stratejik yang dimiliki oleh suatu perusahaan (OGC, 2011d).
2. *Service Design*

   Panduan terhadap implementasi layanan TI yang mana harus di desain terlebih dahulu berdasarkan tujuan bisnis menurut sudut pandang pelanggan. *Service Design* dapat digunakan untuk merancang layanan TI baru atau berdasarkan perubahan proses bisnis (OGC, 2011b).

3. *Service Transition*

   Panduan untuk memberikan gambaran bagaimana manajemen perubahan terhadap sebuah layanan TI yang sudah dirancang pada *Service Design* dan sudah sesuai dengan strategi bisnis pada *Service Strategy* dapat diimplementasikan secara efektif pada *Service Operation* (OGC, 2011e).

4. *Service Operation*

   Panduan untuk mengelola layanan TI secara efisien dan efektif serta menjamin tingkat kinerja yang telah disepakati antara pengguna dan pelanggan untuk mengelola aplikasi, teknologi dan infrastruktur yang mendukung penyampaian sebuah layanan (OGC, 2011c).

5. *Continual Service Improvement*

   Panduan penting dalam penyusunan serta memelihara kualitas layanan TI dari proses desain, transisi dan pengoperasiannya (OGC, 2011a).

Kegunaan ITIL V3: 2011 dalam penelitian ini adalah sebagai acuan dalam melakukan aksi terhadap respon risiko TI.

2.2.8 *Analytical Hierarchy Process* (AHP)

Analytical Hierarchy Process (AHP) merupakan salah satu metode *Multi-Criteria Decision Making* (MCDM) yang dirancang oleh Thomas L. Saaty. AHP merupakan pendekatan yang popular dalam hal pengambilan keputusan yang melibatkan data kualitatif (Saaty, 2008). Tahapan-tahapan dalam menggunakan metode AHP sebagai berikut:

1. Menentukan tujuan yang akan dicari dari berbagai macam kriteria yang telah ditetapkan.
2. Menyusun kriteria dan tujuan kedalam model struktur hirarki sehingga permasalahan yang kompleks dapat dilihat dari sisi yang lebih detail.
3. Melakukan perhitungan nilai prioritas pada setiap elemen kriteria pada setiap hirarki. Membuat matriks perbandingan berpasangan (*pair-wised matrix*), sehingga menghasilkan matriks perbandingan berpasangan antara seluruh elemen pada hirarki yang sama. Matriks perbandingan berpasangan ditunjukkan pada persamaan 2.3.

$$A = a_{ij} = \begin{pmatrix} 1 & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ \frac{1}{a_{1n}} & \cdots & 1 \end{pmatrix} \quad 2.3$$

4. Melakukan uji konsistensi terhadap perbandingan antara elemen yang ditempatkan pada tingkat hirarki untuk digunakan dalam pertimbangan pada perhitungan akhir.

Tabel 2.10 Intensitas Kepentingan Perankingan Akhir

Intensitas Kepentingan	Keterangan
1	Kedua elemen sama penting
3	Elemen yang satu sedikit lebih penting dari elemen lainnya
5	Elemen yang satu lebih penting dari elemen lainnya
7	Satu elemen jelas lebih penting dari elemen lainnya
9	Satu elemen mutlak lebih penting dari elemen lainnya
2,4,6,8	Nilai rata-rata tengah dua nilai pertimbangan yang berdekatan
Kebalikan	Nilai kebalikan $A_{ij} = \frac{1}{A_{ij}}$ dimana A adalah matriks perbandingan berpasangan antar elemen, baik kriteria, sub kriteria ataupun alternative tujuan.

5. Berdasarkan pertimbangan terhadap nilai dari matriks perbandingan berpasangan dilakukan sistensis untuk memperoleh keseluruhan prioritas. Proses sistesis dengan menjumlahkan nilai-nilai pada setiap kolom matriks, kemudian membagi setiap nilai dari kolom dengan total kolom yang bersangkutan untuk memperoleh normalisasi matriks, ditunjukkan pada persamaan 2.4.

$$Nilai\ elemen\ baru = \frac{Nilai\ setiap\ elemen\ matriks\ awal}{jumlah\ kolom\ lama} \quad 2.4$$

6. Pembobotan dilakukan dengan cara menjumlahkan nilai-nilai dari setiap baris dan membaginya dengan jumlah kriteria, ditunjukkan pada persamaan 2.5.

$$Bobot\ Prioritas = \frac{Jumlah\ baris}{Jumlah\ kriteria} \quad 2.5$$

7. Menghitung konsistensi untuk mengetahui seberapa baik konsistensi yang ada. Menghitung konsistensi dilakukan dengan mengalikan nilai pada kolom pertama dengan prioritas relatif elemen pertama, nilai kolom kedua dengan priritas relatif elemen kedua dan seterusnya, kemudian tiap baris dijumlahkan untuk mendapatkan nilai λ_{max}
8. Menghitung nilai *Consistency Index* (CI) menggunakan persamaan 2.6 berikut:

$$CI = \frac{(\lambda_{max} - n)}{(n-1)} \quad 2.6$$

Keterangan:

n merupakan banyaknya kriteria yang kita gunakan.

9. Menghitung *Consistency Ratio* (CR) dengan menggunakan persamaan 2.7 berikut:

$$CR = \frac{CI}{RI} \quad 2.7$$

Keterangan:

RI merupakan *Randomness Index* yang diperoleh dari tabel berikut ini

Tabel 2.11 *Randomess Index*

N	1	2	3	4	5	6	7	8	9	10
RI	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,51

(Sumber: Saaty & Tran, 2007)

Kegunaan AHP dalam penelitian ini adalah sebagai alat untuk memprioritaskan aksi terhadap respon suatu risiko TI.

2.2.9 *Weighted Geometric Mean Method*

Weighted Geometric Mean Method (WGMM) diperkenalkan oleh Aczel di tahun 1983 (Aczél & Saaty, 1983). *WGMM* merupakan metode yang digunakan untuk mencari nilai rata-rata dari masing-masing bobot penilaian pakar (Stirn & Groselj, 2010). Menurut Xu di tahun 2000, terdapat dua asumsi dalam menyimpulkan nilai rata-rata dari masing-masing pakar (Xu, 2000),antara lain:

1. *Geometric Mean*, asumsi jika masing-masing pakar memiliki bobot yang sama dalam membangun opini.

$$A_1 = \begin{bmatrix} A_{1_{a,a}} & A_{1_{a,b}} & A_{1_{a,c}} \\ A_{1_{b,a}} & A_{1_{b,b}} & A_{1_{b,c}} \\ A_{1_{c,a}} & A_{1_{c,b}} & A_{1_{c,c}} \end{bmatrix} \quad 2.8$$

$$A_2 = \begin{bmatrix} A_{2_{a,a}} & A_{2_{a,b}} & A_{2_{a,c}} \\ A_{2_{b,a}} & A_{2_{b,b}} & A_{2_{b,c}} \\ A_{2_{c,a}} & A_{2_{c,b}} & A_{3_{c,c}} \end{bmatrix} \quad 2.9$$

$$A_3 = \begin{bmatrix} A_{3_{a,a}} & A_{3_{a,b}} & A_{3_{a,c}} \\ A_{3_{b,a}} & A_{3_{b,b}} & A_{3_{b,c}} \\ A_{3_{c,a}} & A_{3_{c,b}} & A_{3_{c,c}} \end{bmatrix} \quad 2.10$$

Maka, *Geometric Mean* nya dapat dicari dengan menggunakan rumus:

$$\bar{A} = \begin{bmatrix} \sqrt[3]{A_{1_{a,a}} * A_{2_{a,a}} * A_{3_{a,a}}} & \cdots & \sqrt[3]{A_{1_{a,c}} * A_{2_{a,c}} * A_{3_{a,c}}} \\ \vdots & \ddots & \vdots \\ \sqrt[3]{A_{1_{c,a}} * A_{2_{c,,a}} * A_{3_{c,a}}} & \cdots & \sqrt[3]{A_{1_{c,c}} * A_{2_{c,c}} * A_{3_{c,c}}} \end{bmatrix} \quad 2.11$$

Setalah mendapatkan nilai dari $\bar{A}$, kemudian di normalisasi dan dicari bobotnya menggunakan langkah-langkah pada AHP.

2. *Weighted Mean*, asumsi jika masing-masing pakar memiliki bobot yang tidak sama (senioritas atau faktor lainnya), asumsi bobot pakar A_1=3/6, A_2=1/6, A_3=2/6.

$$A_1 = \begin{bmatrix} A_{1_{a,a}} & A_{1_{a,b}} & A_{1_{a,c}} \\ A_{1_{b,a}} & A_{1_{b,b}} & A_{1_{b,c}} \\ A_{1_{c,a}} & A_{1_{c,b}} & A_{1_{c,c}} \end{bmatrix} \quad 2.12$$

$$A_2 = \begin{bmatrix} A_{2_{a,a}} & A_{2_{a,b}} & A_{2_{a,c}} \\ A_{2_{b,a}} & A_{2_{b,b}} & A_{2_{b,c}} \\ A_{1_{c,a}} & A_{2_{c,b}} & A_{3_{c,c}} \end{bmatrix} \quad 2.13$$

$$A_3 = \begin{bmatrix} A_{3_{a,a}} & A_{3_{a,b}} & A_{3_{a,c}} \\ A_{3_{b,a}} & A_{3_{b,b}} & A_{3_{b,c}} \\ A_{3_{c,a}} & A_{3_{c,b}} & A_{3_{c,c}} \end{bmatrix} \quad 2.14$$

Maka, *Weighted Mean* nya dapat dicari dengan menggunakan rumus:

$$\bar{A} = \begin{bmatrix} \sqrt[6]{A_{1_{a,a}}{}^3} * \sqrt[6]{A_{2_{a,a}}} * \sqrt[6]{A_{3_{a,a}}{}^3} & \cdots & \sqrt[6]{A_{1_{a,c}}{}^3} * \sqrt[6]{A_{2_{a,c}}} * \sqrt[6]{A_{3_{a,c}}{}^3} \\ \vdots & \ddots & \vdots \\ \sqrt[6]{A_{1_{c,a}}{}^3} * \sqrt[6]{A_{2_{c,a}}} * \sqrt[6]{A_{3_{c,a}}{}^3} & \cdots & \sqrt[6]{A_{1_{c,c}}{}^3} * \sqrt[6]{A_{2_{c,c}}} * \sqrt[6]{A_{3_{c,c}}{}^3} \end{bmatrix} \quad 2.15$$

Setalah mendapatkan nilai dari $\bar{A}$, kemudian di normalisasi dan dicari bobotnya menggunakan langkah-langkah pada AHP.

Untuk memastikan asumsi mana yang akan digunakan didalam penelitian, maka harus dilakukan observasi di Politeknik Negeri Bali.

BAB III
METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai tahapan pelaksanaan penelitian dan penulisan laporan penelitian dengan judul "Audit Manajemen Risiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5". Terdiri dari tahapan penelitian, detail penjelasan terkait tahapan penelitian dan jadwal rencana kegiatan penelitian.

3.1 Tahapan Penelitian

Penelitian mengenai audit tata kelola teknologi informasi berbasis risiko ini akan dilakukan kedalam beberapa tahapan, dapat dilihat pada Gambar 3.1.

Penjelasan singkat diagram alir penelitian pada Gambar 3.1, sebagai berikut:

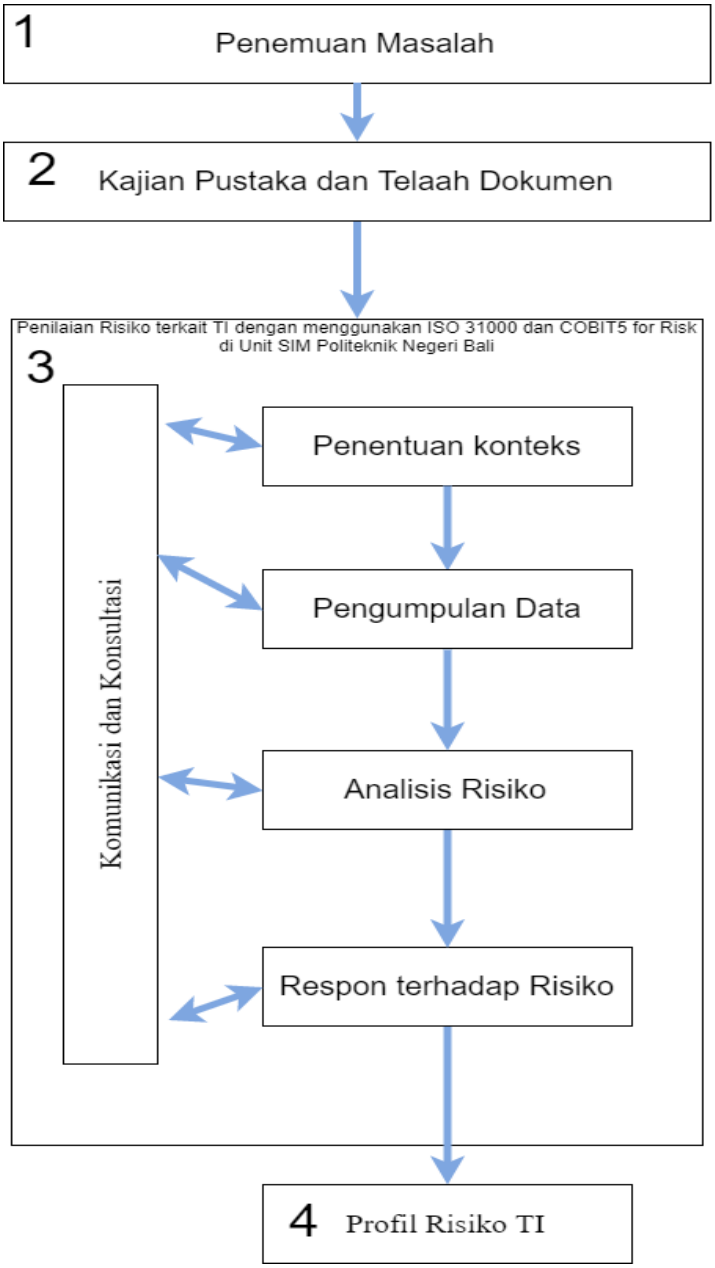
1. Penemuan masalah

   Penemuan masalah terkait manajemen risiko TI di Unit Sistem Informasi Manajemen Politeknik Negeri Bali
2. Kajian pustaka dan telaah dokumen

   Mencari dan mengkaji beberapa penelitian terdahulu serta menelaah dokumen Politeknik Negeri Bali terkait dengan penelitian ini.
3. Penilaian risiko terkait TI dengan ISO 31000 dan COBIT 5 *for Risk*

   Proses penilaian risiko dibagai menjadi beberapa tahapan, yaitu: penentuan konteks, komunikasi dan konsultasi, pengumpulan data, analisis risiko dan respon terhadap risiko.
4. Profil risiko TI

   Profil risiko TI merupakan hasil dari penilaian risiko yang sudah dilakukan di tahapan sebelumnya.



Gambar 3.1 Tahapan Penelitian

3.2 Penemuan masalah

Tahapan pertama adalah mendapatkan permasalah terkait manajemen risiko TI di Politeknik Negeri Bali yang menjadi latar belakang permasalahan penelitian ini dilaksanakan.

3.3 Kajian Pustaka dan Telaah Dokumen

Pada tahapan ini dilakukan pencarian dan pengkajian beberapa tesis, skripsi dan jurnal yang digunakan dalam penelitian terkait permasalahan manajemen risiko

TI di Unit Sistem Informasi Manajemen Politeknik Negeri Bali. Serta pemahaman atas pedoman yang dimiliki oleh Politeknik Negeri Bali khususnya di Unit Sistem Informasi Manajemen saat ini, pemahaman proses bisnis dan *Standard Operational Procedure* terkait. Pada proses ini dilakukan wawancara dan kajian atas dokumen terkait. Informasi yang didapat merupakan satu hal yang penting yang akan menentukan proses kajian selanjutnya. Adapun beberapa pendekatan yang dilakukan sebagai berikut:

a. Kajian dokumen

   Kajian dokumen memiliki tujuan untuk memahami keadaan TI di Politeknik Negeri Bali yang tertuang dalam dokumen Borang Politeknik Negeri Bali, Rencana Strategis SI/TI Unit SIM Politeknik Negeri Bali, Standar Operasional Prosedur Unit SIM Politeknik Negeri Bali dan Evaluasi diri Politeknik Negeri Bali.

b. Wawancara

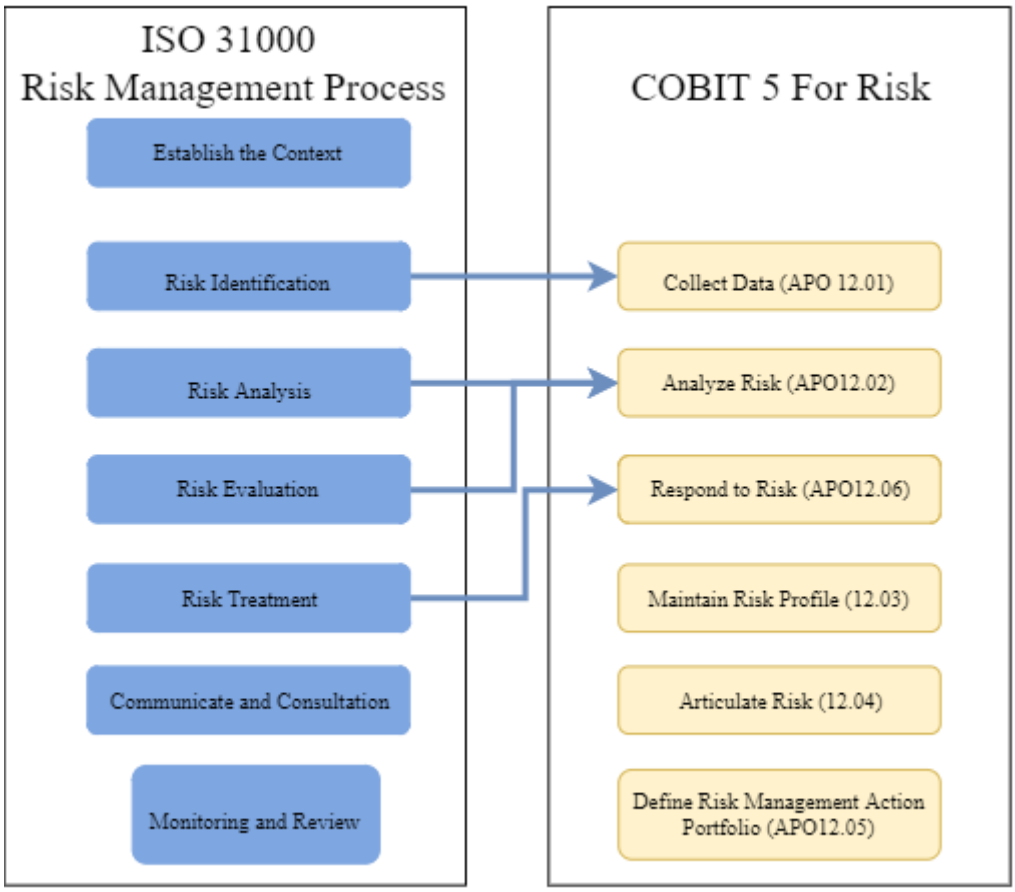
   Wawancara bertujuan untuk mendapatkan latar belakang masalah dan pemahaman terkait risiko proses bisnis yang dihadapi.

c. Observasi

   Observasi dilakukan pada area Unit SIM Politeknik Negeri Bali dan ruang server utama Unit SIM Politeknik Negeri Bali.

3.4 Penilaian risiko terkait TI dengan ISO 31000 dan COBIT 5 for Risk

Acuan yang digunakan dalam aktifitas penilaian risiko adalah ISO 31000 dan COBIT 5 *for Risk.* Proses penggabungan kedua *framework* dimulai dari mencari titik temu dari kedua *framework.* Gambar 3.2 merupakan titik temu antara ISO 31000:2009 dan COBIT 5 for Risk.



Gambar 3.2 Titik temu antara ISO 31000 dan COBIT 5 For Risk

Mengacu pada Gambar 3.2, proses manajemen risiko menurut ISO 31000 dibagi menjadi 7 (tujuh) tahapan (International Organization for Standardization, 2009), antara lain:

1. *Establish the Context*
2. *Risk Identification*
3. *Risk Analysis*
4. *Risk Evaluation*
5. *Risk Treatment*
6. *Comunication and Consultation*
7. *Monitoring and Review.*

Mengacu pada Gambar 3.2, proses manajemen risiko berdasarkan COBIT 5 *for Risk* menggunakan proses APO12. Proses APO12 dibagi menjadi 6

management practice, yang diurut berdasarkan proses pengerjaannya (ISACA, 2013c), yaitu:

1. *Collect Data* (APO12.01),
2. *Analyze Risk* (APO12.02),
3. *Respond to Risk* (APO12.06)
4. *Maintain Risk Profile* (12.03)
5. *Articulate Risk* (APO12.04)
6. *Define Risk Management Action Portfolio* (APO12.05)

Proses pencarian titik temu berdasarkan aktifitas-aktifitas kunci yang terdapat dari masing-masing kerangka kerja. Tabel 3.1 sampai Tabel 3.3 merupakan menjelaskan teknis dari titik temu kedua kerangka kerja.

Tabel 3.1 Teknis titik temu amtara kedua kerangka kerja (1)

Kerangka Kerja	**ISO 31000:2009**	**COBIT 5 for Risk**
Fase	Risk Identification	Collect Data
Aktifitas kunci	• mengkategorikan risiko, • mengidentifikasi penyebab terjadinya risiko, • kriteria tingkat keparahan risiko, • probabilitas terjadinya risiko • mengidentifikasi area yang akan terkena dampak dari sebuah risiko	• Mengumpulkan data yang relevan dengan apa yang akan di identifikasi risikonya • Menganalisis risiko TI yang berasal dari eksternal organisasi • Melakukan pengelompokan kategori skenario risiko yang mampu menimbulkan dampak pada *IT Benefit of Value Enablement, IT Programme and Project*

Kerangka Kerja	ISO 31000:2009	COBIT 5 for Risk
		Delivery, IT Operational and Service Delivery • Mengidentifikasi dan mengelompokkan risiko berdasarkan kategori risiko. COBIT menyediakan 20 kategori risiko terkait TI. • Menentukan frekuensi kemungkinan munculnya risiko dan dampaknya

(Sumber: ISO 31000:2009 dan COBIT 5 For Risk)

Berdasarkan Tabel 3.1, karena aktifitas kunci yang terdapat pada COBIT 5 pada *management practice* APO12.01 *Collect Data* lebih luas cakupannya dari fase *Risk Identification* oleh ISO 31000 dan meng-*cover* semua aktifitas yang terdapat pada fase *Risk Identification* oleh ISO 31000, maka aktifitas ideal yang digunakan adalah menggunakan APO12.01 *Collect Data* yang melakukan pengumpulan data hingga membuat skenario risiko.

Tabel 3.2 Titik temu antara kedua kerangka kerja (2)

Kerangka Kerja	ISO 31000:2009	COBIT 5 *for Risk*
Fase	Risk Analysis	*Analyze Risk*
Aktifitas kunci	• Menganalisis penyebab dari sebuah scenario risiko • Menganalisis dampak dari sebuah risiko	• menganalisis risiko terkait faktor-faktor risiko dan kekritisan aset yang menunjang bisnis

Kerangka Kerja	ISO 31000:2009	COBIT 5 *for Risk*
	• Menganalisis tingkat frekuensi kejadian dari sebuah risiko • Memetakan risiko kedalam Risk Map • Menganalisis efektifitas dan efisiensi kontrol yang sudah ada sebelumnya	• Memperkirakan frekuensi besarnya keuntungan dan kerugian yang berhubungan dengan scenario risiko TI • Memperhitungkan faktor risiko, mengevaluasi pengendalian operasional dan memperkirakan nilai residu dari risiko • Membandingkan antara risiko residual dengan *Risk Appetite* dan *Risk Tolerance* yang dapat diterima oleh organisasi, serta mengidentifikasi risiko mana saja yang membutuhkan respon risiko • Melakukan analisis cost-benefit dari setiap pilihan respon risiko baik *Avoid*, *Mitigate*, *Transfer*, maupun *Transfer*. • Memberikan usulan respon yang paling optimal berdasarkan hasil cost-benefit dari tiap respon risiko
Fase	Risk Evaluation	
Aktifitas kunci	• Membantu dalam membuat keputusan terkait hasil analisis risiko, risiko yang memerlukan pengendalian dan prioritas implementasi dari sebuah pengendalian	

Kerangka Kerja	ISO 31000:2009	COBIT 5 *for Risk*
		• Memvalidasi hasil analisis risiko sebelum memutuskan melakukan analisis risiko menggunakan kerangka kerja lain

(Sumber: ISO 31000:2009 dan COBIT 5 For Risk)

Berdasarkan Tabel 3.2, karena aktifitas kunci yang terdapat pada COBIT 5 pada *management practice* APO12.02 *Analyze Risk* lebih luas cakupannya dari fase *Risk Analysis* oleh ISO 31000 dan meng-*cover* semua aktifitas yang terdapat pada fase *Risk Evaluation* oleh ISO 31000 , maka aktifitas ideal yang digunakan adalah menggunakan APO12.02 *Analyze Risk* yang melakukan analisis risiko dari dampak, frekuensi terjadinya sebuah risiko, membuat *Risk Map* untuk memetakan risiko awal, hingga membuat *Risk Map* untuk memetakan Risiko Residu yang didapat dari kontrol yang telah ada yang telah disesuaikan dengan *Risk Appetite*, *Risk Tolerance* dan *Risk Capacity* dari Politeknik Negeri Bali khususnya di Unit Sistem Informasi Manajemen.

Tabel 3.3 Titik temu antara kedua kerangka kerja (3)

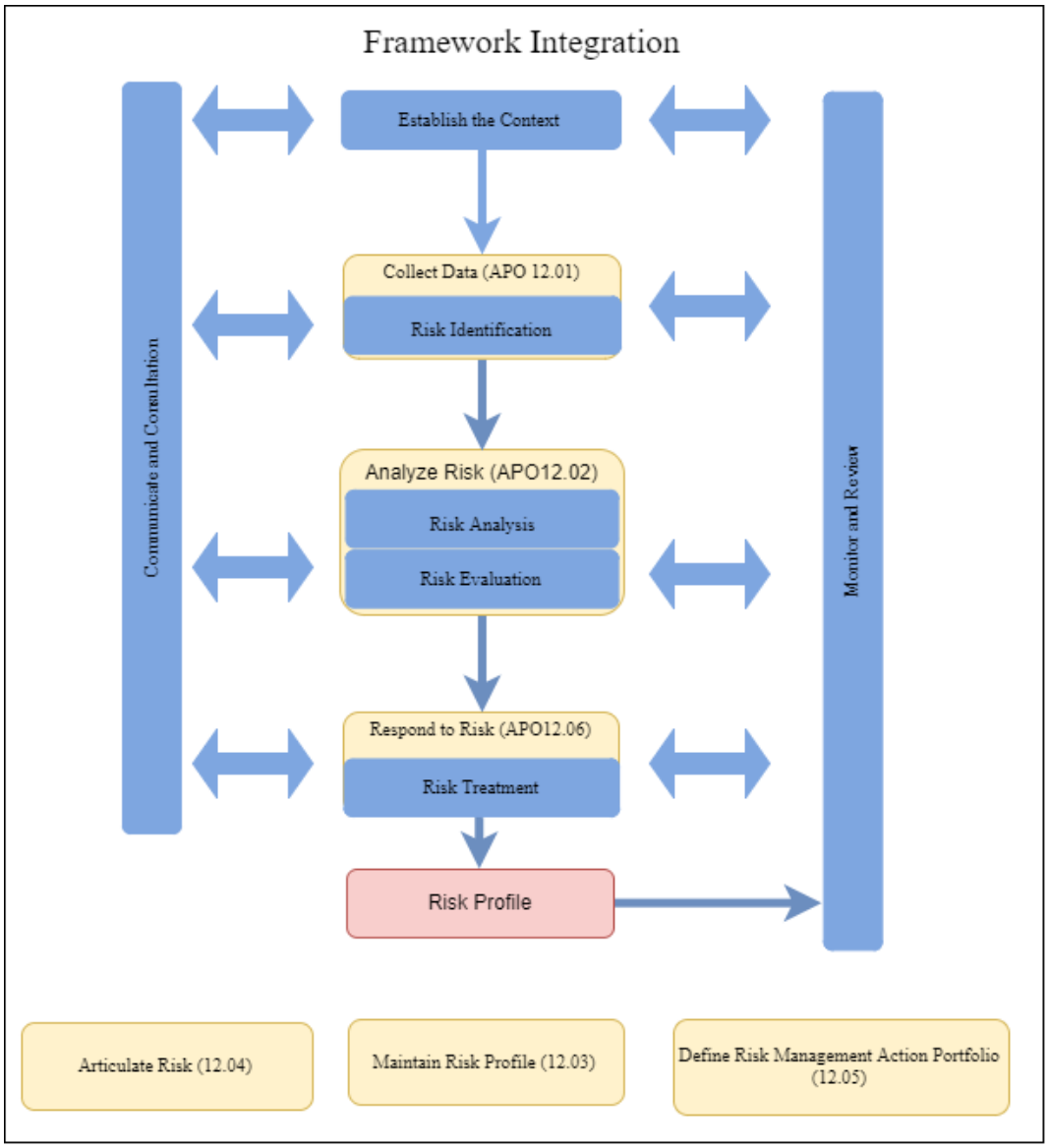
Kerangka Kerja	ISO 31000:2009	COBIT 5 for Risk
Fase	Risk Treatment	Respond to Risk
Aktifitas kunci	• Melakukan perawatan/pengobatan pada risiko yang memiliki respon yang cenderung negative, seperti "mitigasi, eliminasi,	• Menyiapkan, menguji dan mendokumentasikan rencana untuk merespon suatu risiko yang dapat menyebabkan insiden operasional atau dampak bisnis yang serius.

Kerangka Kerja	ISO 31000:2009	COBIT 5 for Risk
	mengurangi dan menghindari risiko”	• Memeriksa riwayat kerugian dan kesempatan yang hilang serta penyebab dari peristiwa risiko terdahulu. • Menerapkan rencana respon risiko yang tepat untuk meminimalisisr dampak ketika terjadinya suatu risiko

Berdasarkan Tabel 3.3, karena aktifitas kunci yang terdapat pada COBIT 5 pada *management practice* APO12.06 *Respond to Risk* lebih luas cakupannya dari fase *Risk Treatment* oleh ISO 31000 dan meng-*cover* semua aktifitas yang terdapat pada fase *Risk Treatment* oleh ISO 31000, maka aktifitas ideal yang digunakan adalah menggunakan APO12.06 *Respond to Risk* yang dimulai dari melakukan aktifitas penyiapan rencana respon terhadap risiko, sampai menerapkan rencana respon terhadap risiko.

Merujuk pada Gambar 3.2, fase *Establishing the Context*, *Communication and Consultation*, dan *Monitoring and Review* di ISO 31000 tidak memiliki titik temu dengan beberapa *management practice* di proses TI APO12 *Manage Risk* menurut COBIT 5. Begitu juga sebaliknya, APO12.04 *Articulate Risk*, APO12.03 *Maintain Risk Profile* dan APO12.05 *Define Risk Management Action Portfolio* tidak memiliki titik temu dengan fase manajemen risiko menurut ISO 31000. *Management practice* APO12.04 *Articulate Risk*, mengandung unsur kata *articulate*, jika di terjemahkan kedalam Bahasa Indonesia menjadi komunikasi. APO12.04 memiliki makna yang sama dengan fase *Communication and Consultation* di ISO 31000, namun secara aktifitas berbeda. dimana aktifitas APO12.04 jika merujuk pada aktifitas nomor 3 pada buku COBIT 5: *Enabling*

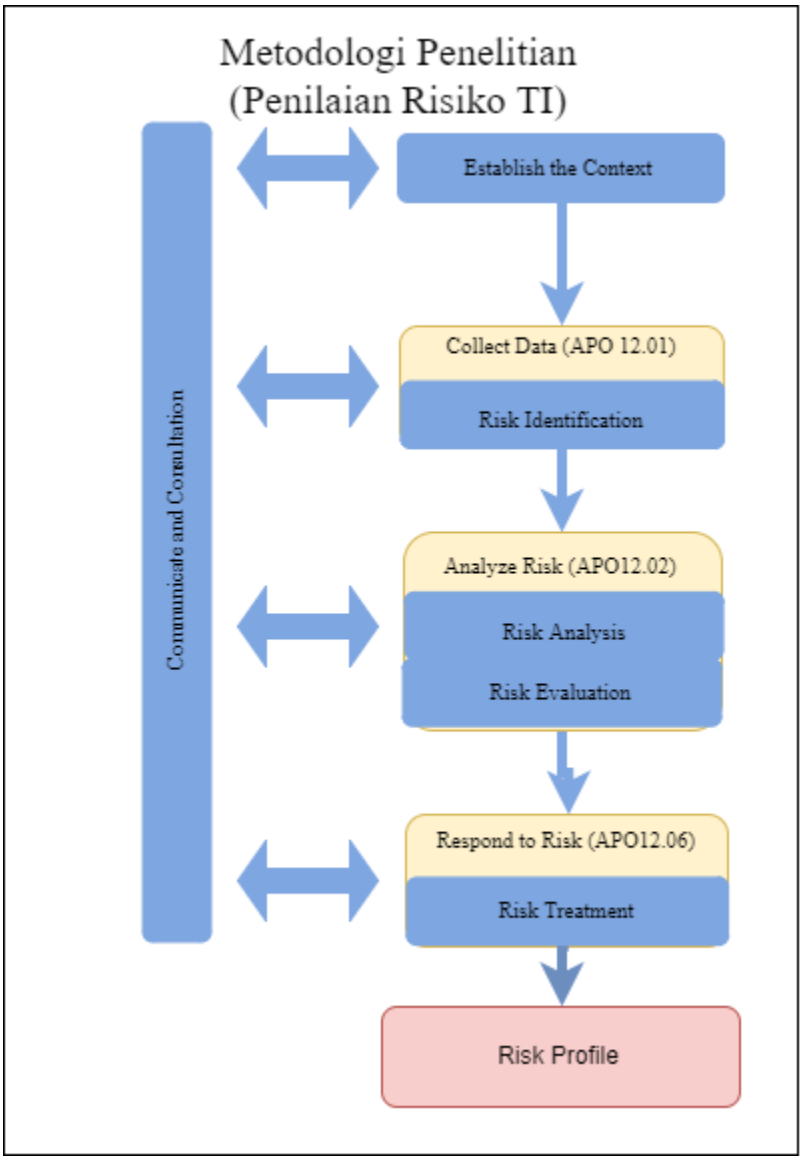
Process, memiliki makna "melaporkan profil risiko TI…" (ISACA, 2012). Sehingga peneliti tidak mengaitkan APO12.04 *Articulate Risk* dengan fase *Communication and Consultation*.



Gambar 3.3 Hasil integrasi dari ISO 31000 dan COBIT 5 for Risk

Mengacu pada Gambar 3.3, karena batasan dalam penelitian ini hanya sampai penilaian risiko untuk mendapatkan profil risiko TI, maka hasil integrasi dirampingkan sesuai dengan kebutuhan. Dimana tidak diperlukan fase Monitoring dan Review karena fase tersebut baru bisa dilakukan pada saat profil risiko sudah diperoleh. Gambar 3.4 merupakan hasil perampingan dari integrasi antara ISO

31000 dan COBIT 5 *for Risk* sekaligus menjadi acuan metode penelitian dalam penilaian risiko TI di Politeknik Negeri Bali, khususnya di Unit Sistem Informasi Manajemen.



Gambar 3.4 Perampingan hasil integrasi dari ISO 31000 dan COBIT 5 for Risk

Mengacu pada Gambar 3.4, proses penilaian risiko memiliki *output* berupa profil risiko TI. Penjelasan detil mengenai profil risiko TI dapat dilihat di Subbab 3.5.

3.4.1 Tahapan Menentukan Konteks (ISO 31000:2009)

Tahapan menentukan konteks mengacu pada ISO 31000:2009 karena Unit SIM Politeknik Negeri Bali belum memiliki ketentuan konteks untuk mendefinisikan risiko termasuk klasifikasi risikonya. Tahapan ini tidak terdapat pada COBIT 5 APO12 (Anandita, 2014), untuk itu perlu adanya kegiatan untuk menentukan konteks dan batasan terkait definisi risiko. Tujuan dari didirikannya Unit SIM Politeknik Negeri Bali adalah menjamin ketersedian data dan informasi yang akurat dan akuntabel dalam mendukung mutu serta daya saing internasional Politeknik Negeri Bali. Usaha ini dapat berjalan dengan baik apabila didukung dengan operasional yang baik. Dalam penerapan strategi tersebut tentu akan terjadi risiko yang mencakup kegiatan bisnis Unit SIM Politeknik Negeri Bali. Hal yang dijadikan acuan penentuan risiko strategis di Unit SIM Politeknik Negeri Bali adalah proses bisnis utama yang ada di dokumen Standar Operasional Prosedur Unit SIM Politeknik Negeri Bali. Alasan menggunakan proses bisnis digunakan sebagai acuan konteks risiko adalah keterbatasan dokumen yang dapat diteliti dan diberikan oleh Pihak Politeknik Negeri Bali. Penilaian risiko pada proses bisnis sebelumnya telah dilakukan oleh Edwina Fiqhe Anandita di Tahun 2014 (Anandita, 2014) dan Chitra Utami Putri di Tahun 2017 (Putri, 2017).

3.4.2 Tahapan Komunikasi dan Konsultasi (ISO 31000:2009)

Tahapan Komunikasi dan Konsultasi mengacu pada ISO 31000:2009 digunakan untuk menentukan alur komunikasi yang digunakan apabila terjadi gangguan pada divisi bisnis dan mempermudah Unit SIM Politeknik Negeri Bali dalam menumbuhkan budaya sadar risiko untuk seluruh Unit SIM Politeknik Negeri Bali sendiri (Anandita, 2014). Serta mengkomunikasikan segala hal yang berkaitan dengan tiap fase didalam proses penilaian risiko TI agar dokumen profil risiko yang akan dibuat menjadi lebih lengkap dan sesuai dengan keadaan saat ini di Politeknik Negeri Bali, khususnya di Unit Sistem Informasi Manajemen.

3.4.3 Mengumpulkan data (APO 12.01)

Aktifitas yang dilakukan pada tahapan ini adalah mengumpulkan data terkait proses bisnis Unit SIM Politeknik Negeri Bali, melakukan identifikasi risiko pada proses bisnis terkait serta melakukan wawancara terkait risiko-risiko yang

telah terjadi atau mungkin akan terjadi. Output dari fase Mengumpulkan data adalah skenario risiko terkait TI.

3.4.3.1 Data terkait proses bisnis Unit SIM

Data yang dikaji dalam identifikasi risiko adalah yang mencakup proses bisnis Unit SIM Poilteknik Negeri Bali, antara lain:

1. Pengembangan *software* (terdiri dari perencanaan, pengembangan dan operasional)
2. Pengembangan Jaringan/*Hardware* (terdiri pengembangan dan pemeliharaan)
3. Pengendalian Data dan Informasi
4. Pengelolaan Website Politeknik (update konten web, pembuatan email PNB, pembuatan web baru)
5. Penanganan *Disaster Recovery* (server lokal dan server cloud)
6. Pengelolaan *E-learning*
7. Data terkait lainnya yang mendukung berjalannya proses bisnis.

3.4.3.2 Identifikasi Risiko

Lampiran proses bisnis yang terdapat di Unit Sistem Informasi Manajemen Politeknik Negeri Bali dapat dilihat pada Lampiran 1. Proses identifikasi risiko ditentukan dari setiap proses yang dapat dikategorikan sebagai risiko terkait TI, antara lain:

a) Merancang Sistem Software

Terdapat sekurang-kurangnya sepuluh risiko dalam tahapan perancangan sistem software, yang sebagian merupakan risiko yang terdapat di dalam dokumen spesifikasi kebutuhan perangkat lunak yang merujuk pada penelitian yang dilakukan oleh Alzashly di tahun 2014 (Alshazly, Elfatatry, & Abougabal, 2014), antara lain: spesifikasi kebutuhan tidak sesuai dengan keinginan pemohon, informasi yang ditulis di dokumen kebutuhan memiliki makna yang multi tafsir.

b) Pembuatan Program

Terdapat sekurang-kurangnya delapan risiko dalam tahapan pembuatan program, antara lain: Kurangnya *programmer* yang terlatih, *Gold Plating*, dll.

c) Uji coba *Software*

Terdapat tiga risiko dalam tahapan uji coba *software*, antara lain: terdapat beberapa kebutuhan yang tidak dapat di implementasikan, dll.

d) Training/sosialisasi sistem

Risiko dalam tahapan sosialisasi sistem adalah pengguna akhir tidak dapat menggunakan aplikasi dengan baik

e) Implementasi sistem

Risiko dalam tahapan implementasi sistem adalah implementasinya sembarangan karena ingin working version lebih cepat (tidak efisiennya desain)

Aktifitas identifikasi risiko memiliki output berupa skenario risiko TI. Tabel 3.4 merupakan contoh lampiran scenario risiko pada Proses Bisnis Pemeliharaan Jaringan/ Hardware.

Tabel 3.4 Skenario risiko Proses Bisnis Pemeliharaan Jaringan

Ref	Kategori Skenario Risiko	Proses bisnis	Skenario Risiko
			Negative Scenario
SOP02-1001	IT Expertise and Skills	SOP02 Pemeliharaan Jaringan/ Hardware	Teknisi salah dalam melakukan identifikasi permasalahan terkait permintaan pemeliharaan jaringan/hadware

3.4.4 Analisis risiko (APO 12.02)

Aktifitas yang dilakukan pada tahapan ini adalah pengisian form analsisis risiko yang terdiri dari skenario risiko yang digolongkan sesuai dengan proses

bisnis yang ada di Unit SIM Politeknik Negeri Bali yang dapat dilihat pada Tabel 3.4, penentuan nilai terhadap dampak yang akan terjadi kepada Politeknik Negeri Bali pada area Finansial, Strategis, Produktifitas, Reputasi. Area dampak pada penelitian ini diperkuat dengan penelitian sebelumnya oleh Samaptoaji (2014) Jakaria (2013) mengenai area dampak yang menggunakan OCTAVE Allegro pada Universitas X.

Setelah mengisi lembar evaluasi penilaian risiko, langkah selanjutnya adalah menilai tingkat *Impact* dan *Frequency* dari risiko yang diadopsi dari COBIT 5 *for Risk*. Panduan tingkatan *Impcat* menggunakan referensi dari COBIT 5 *for Risk* dapat dilihat pada Lampiran 8 sampai Lampiran 11. Mengacu pada Lampiran 8-11, tingkat dampak (*I*) dari area dampak yang dihasilkan merupakan rata-rata nilai dari total nilai dari jumlah area yang terkena dampak dibagi dengan jumlah area yang ada. Rumus rata-rata tingkat dampak (*I*) dapat dilihat pada rumus (1).

$$Tingkat\ Impact = \frac{\sum nilai\ area\ dampak}{\sum area\ dampak} \qquad 3.1$$

Contoh:

Contoh Nilai Dampak (*I*) berdasarkan area dampak dapat dilihat pada Tabel 3.5.

Tabel 3.5 Contoh penilaian *Impact* berdasarkan Area Dampak

Risk Issue	Kriteria Dampak				I
	Finansial	Strategis	Produktivitas	Reputasi	
Teknisi salah dalam melakukan identifikasi permasalahan pada proses pemeliharaan jaringan/ hardware	2	1	3	2	$= \frac{2+1+3+2}{4}$ =1,75

(Sumber: Peneliti, 2017)

Mengacu pada Tabel 3.5, didapat tingkat *Impact* dari *risk issue* "Teknisi salah dalam melakukan identifikasi permasalahan pada proses pemeliharaan jaringan/*hardware* " sebesar 1,75. Didapat dengan menggunakan rumus (1).

Tabel 3.6 Panduan tingkat *Frequency* menggunakan acuan COBIT 5 for Risk

Efek	Ranking	Kriteria
Sangat Jarang	1	Frekuensi terjadinya risiko terjadi diantara 0,01 < N ≤ 0,1 dalam satu tahun.
Jarang	2	Frekuensi terjadinya riisko lebih dari 0,1 < N ≤ 1 dalam satu tahun
Kadang-kadang	3	Frekuensi terjadinya risiko terjadi lebih dari 1 < N ≤ 10 kali dalam satu tahun
Sering	4	Frekuensi terjadinya risiko terjadi lebih dari 10 < N ≤ 100 kali dalam satu tahun
Sangat Sering	5	Frekuensi terjadinya risiko terjadi lebih dari 100 kali dalam satu tahun

(Sumber: Putri, 2017 yang akan diolah kembali)

Mengacu pada Tabel 3.2, *Frequency* merupakan seberapa sering risiko itu terjadi dapat dinilai dengan skala 1-4 menggunakan acuan COBIT 5 *for Risk*.

Setelah menghitung nilai dampak dan probabilitas yang terdapat pada sebuah risiko, kemudian aktifitas yang akan dilakukan selanjutnya adalah pembuatan *Risk Map* atau peta risiko yang berukuran *grid* 5x5 (sesuai dengan acuan COBIT 5 *for Risk*).

3.4.5 Respon terhadap Risiko TI (APO 12.06)

Terdapat dua aktifitas yang dilakukan pada tahapan ini, yaitu pemilihan opsi respon terhadap risiko dan pemrioritasan respon terhadap risiko.

3.4.5.1 Pemilihan Opsi Respon Terhadap Risiko

Setelah melakukan analisis risiko dan memperoleh peta risiko (*Risk Map*), respon terhadap risiko disesuaikan dengan *Risk Appetite* yang dimiliki oleh Politeknik Negeri Bali. *Risk Appetite* dapat dikatakan tinggi, apabila sebagian besar risiko diterima (*Transfer*). Sebaliknya *Risk Appetite* dikatakan rendah, apabila hanya sebagian kecil risiko yang dapat diterima oleh Politeknik Negeri Bali. Terdapat empat pilihan respon terhadap risiko menurut COBIT 5 *for Risk*, yaitu: terima risiko (*Transfer*), mitigasi risiko (*Mitigate*), limpahkan risiko ke pihak lain (*Transfer*), hindari risiko (*Avoid*). Masing-masing risiko harus dibuat keempat opsi responnya dengan mencantumkan parameter seperti efisiensi dan efektifitas dari sebuah respon yang mengacu pada COBIT 5 *for Risk*.

3.4.5.2 Pemrioritasan Respon Terhadap Risiko

Pemrioritasan respon terhadap risiko dilakukan untuk memudahkan para manajemen di Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen dalam merencanakan aksi dalam merespon sebuah risiko. Pemrioritasan respon terhadap risiko dilakukan dengan menggunakan *Analytical Hierarchy Process* (AHP), tujuannya adalah memprioritaskan respon terbaik dari sebuah risiko. Kriterianya didapat dari beberapa jurnal, antara lain:

1. Durasi Proyek (DUP)

   Total waktu yang diperlukan dari awal mulai perencanaan hingga aksi terhadap respon risiko telah dilaksanakan (Oztaysi, 2014)

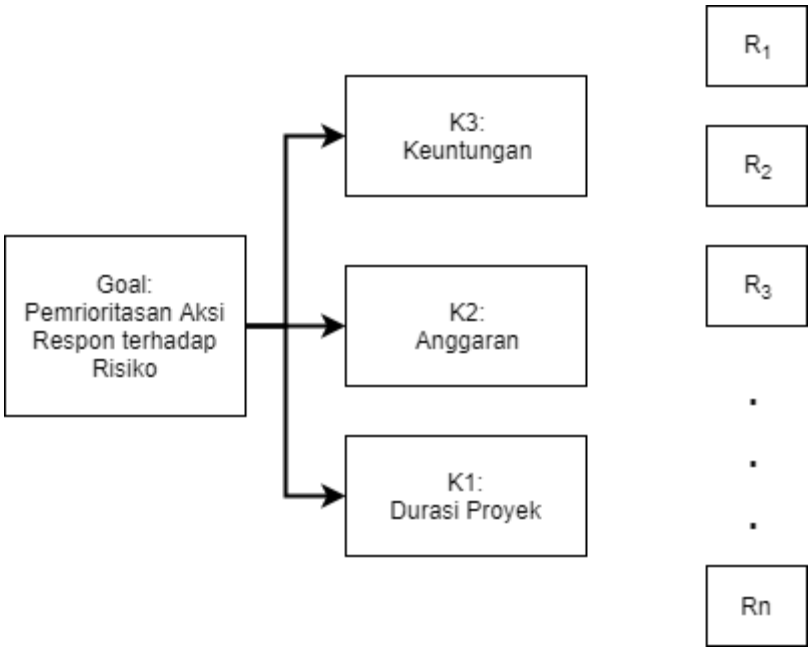
2. Anggaran (ANG)

   Total biaya yang dikeluarkan untuk menutupi biaya implementasi dan biaya pendukung lainnya (Oztaysi, 2014)

3. Keuntungan (KEU)

   Keuntungan yang diperoleh oleh pihak Politeknik Negeri Bali, khususnya Unit Sistem Informasi Manajemen dalam hal peningkatan produktivitas (Karasakal & Aker, 2017).

Gambar 3.5 merupakan bentuk hirarki dari pemrioritasan aksi respon terhadap risiko.



Gambar 3.5 Hirarki dari pemrioritasan aksi respon terhadap risiko

Sedangkan alternatifnya adalah aksi terhadap respon risiko sesuai dengan respon risiko yang ditentukan oleh pihak manajemen Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen yang disimbolkan dengan R_n.

3.5 Profil Risiko TI

Profil risiko TI didapat dari hasil penilaian terhadap risiko yang ada di Politeknik Negeri Bali, khususnya di Unit Sistem Informasi Manajemen. Profil risiko TI berbentuk dokumen, yang terdiri dari:

1. Risk register, yang terdiri dari rangkuman data, deskripsi risiko (skenario risiko) dan hasil analisis risiko yang dibagi menjadi 7 buah sesuai dengan ruang lingkup proses bisnis yang dilakukan penilaian risikonya.
2. Perencanaan aksi terhadap risiko
3. Kejadian yang menyebabkan kerugian dalam bentuk material maupun non-material (dulu dan sekarang)
4. Faktor risiko
5. Temuan berdasarkan hasil penilaian independen (Audit)

(Halaman ini sengaja dikosongkan)

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menjelaskan mengenai hasil penelitian dan pembahasan penelitian dengan judul "Audit Manajemen Risiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5". Terdiri dari tahapan pengumpulan data, hasil peta risiko Unit SIM, hasil frekuensi dan dampak risiko di Unit SIM, profil risiko TI di Unit SIM, hasil audit di Unit SIM, hasil kuesioner AHP dan hasil pemrioritasan respon terhadap risiko TI.

4.1 Tahapan Pengumpulan Data

Metode pengumpulan data yang digunakan pada penelitian ini, antara lain: *focus group discussion*, wawancara dan penyebaran kuesioner. Hasil dokumentasi pengumpulan data dapat dilihat pada Gambar 4.1 sampai Gambar 4.2.

1. *Focus Group Discussion* dilakukan bersama dengan Pembantu Direktur I, Ketua Unit SIM, Sekretaris Unit SIM, Ketua Divisi Sistem dan Jaringan, dan Ketua Divisi *e-learning.*

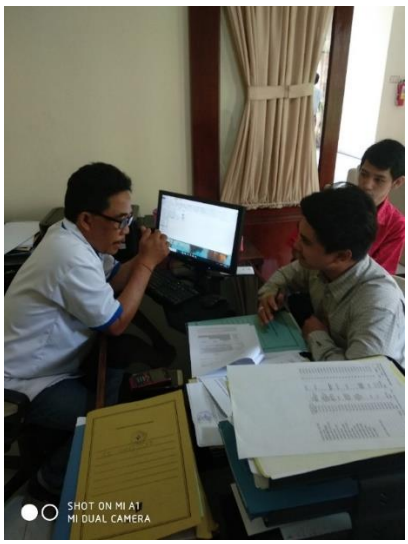
Gambar 4.1 Hasil Dokumentasi *focus group discussion* di Politeknik Negeri Bali

Focus Group Discussion digunakan untuk mendapatkan:

a. Pernyataan area dampak (sektor finansial, strategis, reputasi, hukum) terhadap risiko yang ada di Unit Sistem Informasi Manajemen Politeknik Negeri Bali;

b. Pernyataan ambang batas frekuensi risiko yang ada di Unit Sistem Informasi Manajemen Politeknik Negeri Bali;
c. Penentuan peta risiko (*Risk Map*) yang ada di Unit Sistem Informasi Manajemen Politeknik Negeri Bali.
d. Penentuan kapan target waktu rencana mitigasi risiko dapat dilaksanakan

2. Wawancara ditujukan kepada Ketua Unit SIM dan masing-masing ketua divisi yang membawahi proses bisnis yang ada di Unit SIM Politeknik Negeri Bali.



(a) (b)

Gambar 4 2 (a) Hasil Dokumentasi wawancara dengan Ketua Unit SIM, (b) Ketua Divisi *E-learning* dan Ketua Divisi Sistem dan Jaringan

Wawancara digunakan untuk mendapatkan:

a. Pernyataan kontrol yang ada saat ini pada skenario risiko yang terdapat pada masing-masing proses bisnis operasional Unit SIM Politeknik Negeri Bali.
b. Pernyataan bahwa kriteria AHP yang diusulkan kepada Unit SIM Politeknik Negeri Bali benar-benar dibutuhkan. Pernyataan kriteria AHP ditujukan kepada Ketua Unit SIM Politeknik Negeri Bali.

3. Kuesioner digunakan untuk mendapatkan:
   a. Nilai dari pembobotan kriteria AHP untuk respon aksi terhadap risiko oleh masing-masing responden penelitian. Responden penelitian dalam penilaian bobot kriteria AHP dapat dilihat pada Tabel 4.3.

b. Nilai dari pemrioritasan respon aksi terhadap risiko dimana bobotnya telah diolah terlebih dahulu dengan menggunakan AHP. Responden yang terlobat dalam pengisian pemrioritasan respon aksi terhadap risiko dapat dilihat pada Tabel 4.3.

4.1.1 Karakteristik responden

Responden penelitian ditentukan berdasarkan pemetaan RACI *Chart* yang ada di dalam COBIT 5 yang kemudian disesuaikan dengan jabatan yang ada di Politeknik Negeri Bali. Karena penelitian ini berfokus pada manajemen risiko TI, maka proses TI yang terpilih adalah APO 12 *Manage Risk*. *Key Management Practice* yang dipilih adalah APO12.06 *Respond to Risk*. APO 12.06 *Respond to Risk* dipilih untuk kepentingan kuesioner. Kuesioner yang dimaksud adalah kuesioner yang dibuat untuk mengetahui tingkat kepentingan setiap kriteria guna mendapatkan bobot untuk prioritas respon terhadap risiko terkait Teknologi Informasi (TI) menggunakan *Analytical Hierarchy Process* (AHP). Hasil pemetaan RACI *Chart* Menggunakan Kerangka Kerja COBIT 5 dapat dilihat pada Tabel 4.1.

Tabel 4.1 Hasil pemetaan RACI Chart Menggunakan Kerangka Kerja COBIT 5

APO 12 *Manage Risk*												
Key Management Practice	*Business Process Owner*	*Project Management Officer*	*Chief Risk Officer*	*Chief Information Security Officer*	*Head Architecht*	*Head Development*	*Head IT Operation*	*Head IT Administration*	*Service Manager*	*Information Security Manager*	*Business Continuity Manager*	*Privacy Officer*
APO12.06 *Respond to Risk*	R	R	R	R	R	R	R	R	R	R	R	R

(Sumber: ISACA, 2012. COBIT 5 – *Enabling Process*)

Berdasarkan hasil pemetaan RACI *Chart* Menggunakan Kerangka Kerja COBIT 5 pada Tabel 4.1, peran yang terpilih adalah yang msemiliki label *R*

(Responsible). Peran yang memiliki label *R/Responsible* terpilih karena ia yang memiliki tanggung jawab penuh terkait kegiatan yang sedang dikerjakan. Tabel 4.2 menunjukkan hasil pemetaan peran di Politeknik Negeri Bali dengan RACI *Chart* COBIT 5.

Tabel 4.2 Hasil pemetaan peran di Politeknik Negeri Bali dengan RACI Chart COBIT 5

Business Process Owner	Sekretaris Unit Sistem Information Manajemen (SIM)
Project Management Officer	-
Chief Risk Officer	Pembantu Direktur I
Chief Information Security Officer	Ketua Unit Sistem Information Manajemen (SIM)
Head Architecht	Ketua Unit Sistem Information Manajemen (SIM)
Head Development	Ketua Unit Sistem Information Manajemen (SIM)
Head IT Operation	Ketua Unit Sistem Information Manajemen (SIM)
Head IT Administration	Ketua Unit Sistem Information Manajemen (SIM)
Service Manager	3 ketua Divisi dari Unit SIM
Information Security Manager	Ketua Pejabat Pengelolaa Informasi dan Dokumentasi (PPID)
Business Continuity Manager	Ketua Unit Sistem Information Manajemen (SIM)
Privacy Officer	Ketua Pejabat Pengelola Informasi dan Dokumentasi (PPID)

(Sumber: Peneliti, 2017)

Mengacu pada hasil pemetaan peran Menggunakan Kerangka Kerja COBIT 5 yang telah disesuaikan dengan kondisi di Politeknik Negeri Bali (Tabel 4.1 dan Tabel 4.2), kuesioner ini ditujukan kepada 7 responden, antara lain: Pembantu Direktur I, Ketua Unit Sistem Informasi Manajemen (SIM), Sekretaris Unit SIM, Ketua Divisi Sistem dan Jaringan Unit SIM, Ketua Divisi Sistem Informasi Unit SIM, Ketua Divisi *E-learning* Unit SIM dan Ketua Pejabat Pengelola Informasi dan Dokumentasi (PPID). Tabel 4.3 menunjukkan nama responden yang menduduki jabatan di Politeknik Negeri Bali.

Tabel 4.3 Responden penelitian

Jabatan	Nama
Pembantu Direktur 1, Ketua PPID*	I Putu Mertha Astawa, S.E., M.M.
Ketua Unit SIM	I Ketut Suja, S.E., M.Si.

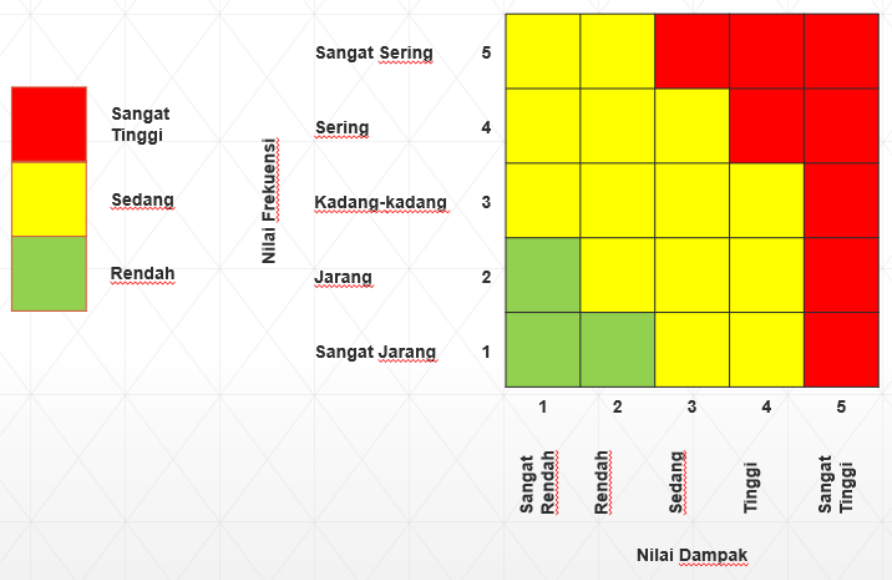
Jabatan	Nama
Sekretaris Unit SIM, Ketua Divisi Sistem Informasi Unit SIM*	Kadek Cahya Dewi, S.T., M.Cs.
Ketua Divisi Sistem dan Jaringan	Ketut Ngurah Semadi, S.Kom.
Ketua Divisi *E-learning* Unit SIM	Putu Indah Ciptayani, S.Kom., M.Cs

Responden Penelitian yang merujuk pada Tabel 4.3 yaitu, Ketua Divisi Sistem Informasi Unit SIM tidak bisa hadir pada saat penelitian berlangsung di Politeknik Negeri Bali dikarenakan ada kesibukan yang tidak bisa beliau tinggalkan. Oleh sebab itu, maka langsung diwakilkan oleh Sekretaris Unit SIM. Ketua Pejabat Pengelola Informasi dan Dokumentasi (PPID) dijabat oleh Pembantu Direktur 1 Politeknik Negeri Bali yang ditetapkan melalui Keputusan Direktur Politeknik Negeri Bali. Jadi jumlah responden hanya 5 orang.

4.2 Peta Risiko Unit SIM Politeknik Negeri Bali

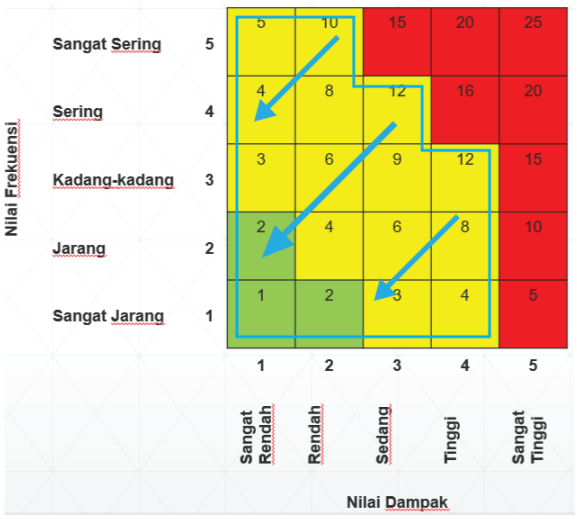
Berdasarkan hasil *focus group discussion* dengan Ketua Unit SIM, Pembantu Direktur I Politeknik Negeri Bali Sekretaris Unit SIM, Ketua Divisi Sistem dan Jaringan, Ketua Divisi Sistem Informasi dan Ketua Divisi E-learning, didapat peta risiko yang dapat dilihat pada Gambar 4.3.

Mengacu pada Gambar 4.3, petinggi Unit Sistem Informasi Manajemen sepakat untuk menerima risiko jika frekuensi terjadinya risiko dalam rentang jarang terjadi namun dampak yang ditimbulkan sangat rendah atau dampak yang ditimbulkan rendah namun frekuensi terjadinya risiko sangat jarang terjadi. Para Petinggi Unit Sistem Informasi Manajemen sepakat jika terdapat risiko yang memiliki frekuensi kejadian yang sangat jarang terjadi namun dampaknya sampai dapat mengganggu eksistensi puncak manajemen Unit Sistem Informasi Manajemen, maka risiko tersebut harus dihindari. Risiko yang harus dihindari juga jika memiliki frekuensi kejadian yang sangat sering dan dampak yang tinggi.



Gambar 4.3 Peta Risiko Unit SIM Politeknik Negeri Bali

Mengacu pada Gambar 4.4, *risk appetite* Unit Sistem Informasi Manajemen cenderung rendah. Ini menandakan Unit Sistem Informasi Manajemen memiliki selera risiko yang rendah. Unit Sistem Informasi Manajemen memiliki selera risiko yang rendah karena eksistensi Unit Sistem Insformasi Manajemen sendiri merupakan salah satu unit yang melayani Politeknik Negeri Bali, sehingga tidak mengejar keuntungan namun lebih condong memberikan pelayanan terbaik. Ini dibuktikan dengan *Risk Tolerance* Unit Sistem Informasi Manajemen yang sangat besar.



Gambar 4.4 Risk Appetitte dan *Risk Tolerance* Unit SIM

4.3 Hasil Parameter Frekuensi dan Dampak Risiko

Setiap perusahaan atau organisasi memiliki parameter frekuensi dan dampak risiko yang berbeda-beda, bergantung dari perusahaan atau organisasi dalam menangani risiko. Berdasarkan hasil *Focus Group Discussion*, dimana peneliti bertindak sebagai moderator–perwakilan manajemen Unit SIM menentukan ambang bawah-atas frekuensi risiko di Unit SIM Politeknik Negeri Bali. Tabel 4.4 menunjukkan parameter frekuensi risiko Unit SIM dapat dilihat dibawah ini.

Tabel 4.4 Parameter Frekuensi risiko di Unit SIM

Efek	Ranking	Justifikasi
Sangat Jarang	1	Kejadian tidak lebih dari 2 kali per tahun; atau kejadian rata-rata tidak lebih dari 1 kali setiap enam bulan
Jarang	2	Kejadian lebih dari 2 kali per tahun; atau kejadian rata-rata tidak lebih dari 2 kali setiap enam bulan
Kadang-kadang	3	Kejadian tidak lebih dari 5 kali per tahun; atau kejadian rata-rata tidak lebih dari 1 kali tiga bulan
Sering	4	Kejadian lebih dari 5 kali per tahun; atau kejadian rata-rata tidak lebih dari 1 kali setiap bulan
Sangat Sering	5	Kejadian lebih dari 10 kali per tahun; atau kejadian rata-rata lebih dari 1 kali setiap bulan.

(Sumber: COBIT 5 for Risk; yang telah disesuaikan dengan kondisi di PNB)

Berdasarkan hasil *Focus Group Discussion* yang dilakukan bersama manajemen Unit SIM, Unit SIM belum memiliki dana tersendiri untuk mengelola manajemen risiko. Sehingga tidak memiliki patokan berapa total kerugian/pengeluaran yang masih dalam toleransi Unit SIM. Namun, Unit SIM memiliki anggaran tersendiri setiap tahunnya untuk pengeluaran dalam mengelola infrastuktur TI yang ada di Politeknik Negeri Bali yakni berjumlah Rp.96.000.000,-

. Sehingga peneliti dan perwakilan manajemen Unit SIM sepakat untuk mencantumkan dana pengelolaan infrastruktur TI sebagai dampak parameter finansial di Unit SIM yang dapat dilihat pada Tabel 4.5.

Tabel 4.5 Parameter dampak finansial di Unit SIM

Efek	Tingkat Dampak	Justifikasi
		Finansial
Sangat Rendah	1	Kerugian dan/atau adanya pengeluaran biaya sampai dengan maksimal sebesar Rp.24.000.000,-
Rendah	2	Kerugian dan/atau adanya pengeluaran biaya antara Rp.24.000.001,- hingga Rp.48.000.000,-
Sedang	3	Kerugian dan/atau adanya pengeluaran biaya antara Rp.48.000.001,- hingga Rp.72.000.000,-
Tinggi	4	Kerugian dan/atau adanya pengeluaran biaya antara Rp.72.000.001 hingga Rp.96.000.000,-
Sangat Tinggi	5	Kerugian dan/atau adanya pengeluaran biaya lebih dari Rp.96.000.000,-

(Sumber: COBIT 5 for Risk; yang telah disesuaikan dengan kondisi di PNB)

Berdasarkan *Focus Group Discussion*, Manajemen Unit SIM menentukan parameter dampak hukum seperti yang tercantum pada Tabel 4.6. Manajemen Unit SIM menyatakan bahwa parameter dampak hukum yang hanya dapat diterima oleh Unit SIM hanya sampai peringatan dari individu (atasan) atau dari manajemen pusat Politeknik Negeri Bali itu sendiri. Selebihnya, Unit SIM harus melakukan mitigasi, *Transfer* atau menghindari risiko agar tidak sampai melebihi batas kemampuan Unit SIM itu sendiri.

Tabel 4.6 Parameter dampak Hukum di Unit SIM

Efek	Tingkat Dampak	Justifikasi Hukum
Sangat Rendah	1	Terdapat permasalahan hukum (misal pelanggaran) namun belum menjadi tuntutan hukum

Efek	Tingkat Dampak	Justifikasi Hukum
Rendah	2	Adanya surat peringatan dari individu/instansi dengan dampak relatif kecil
Sedang	3	Tuntutan hukum yang berdampak pada kinerja /peforma Unit Sistem Informasi Manajemen
Tinggi	4	Tuntutan hukum yang mengancam eksistensi dan manajemen puncak Unit Sistem Informasi Manajemen
Sangat Tinggi	5	Tuntutan hukum terhadap keseluruhan Unit Sistem Informasi Manajemen sehingga dapat menyebabkan Unit SIM berhenti beroperasi

(Sumber: COBIT 5 for Risk; yang telah disesuaikan dengan kondisi di PNB)

Berdasarkan *Focus Group Discussion*, Manajemen Unit SIM menentukan parameter dampak reputasi seperti yang tercantum pada Tabel 4.7. Manajemen Unit SIM menyatakan bahwa parameter dampak reputasi yang hanya dapat diterima oleh Unit SIM hanya sampai pemberitahuan negative (*gossip*) yang dapat menurunkan kepercayaan sebagian kecil pemangku kepentingan di Unit SIM itu sendiri. Selebihnya, Unit SIM harus melakukan mitigasi, *Transfer* atau menghindari risiko agar tidak sampai melebihi batas kemampuan Unit SIM itu sendiri.

Tabel 4.7 Parameter dampak Reputasi di Unit SIM

Efek	Tingkat Dampak	Justifikasi Reputasi
Sangat Rendah	1	Terdapat pemberitahuan negatif namun tidak mengakibatkan penurunan kepercayaan stakeholder
Rendah	2	Terdapat pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian kecil stakeholder

Efek	Tingkat Dampak	Justifikasi Reputasi
Sedang	3	Terdapat pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar stakeholder
Tinggi	4	Terdapat pemberitahuan negatif yang dapat menghilangkan kepercayaan stakeholder
Sangat Tinggi	5	Terdapat pemberitahuan negatif di media massa terkait Politeknik Negeri Bali

(Sumber: COBIT 5 for Risk; yang telah disesuaikan dengan kondisi di PNB)

Berdasarkan *Focus Group Discussion*, Manajemen Unit SIM menentukan parameter dampak operasional seperti yang tercantum pada Tabel 4.8. Manajemen Unit SIM menyatakan bahwa parameter dampak operasional yang hanya dapat diterima oleh Unit SIM hanya sampai penundaan proses bisnis kerja antara setengah sampai dengan maksimal 1 hari kerja. Selebihnya, Unit SIM harus melakukan mitigasi, *Transfer* risiko agar tidak sampai melebihi batas kemampuan Unit SIM itu sendiri. Jika ada sebuah risiko yang berpotensi membuat lumpuh proses bisnis lebih dari satu minggu (5 hari kerja di Politeknik Negeri Bali), maka Unit SIM harus menghindarinya.

Tabel 4 8 Parameter Dampak Operasional di Unit SIM

Efek	Tingkat Dampak	Justifikasi Operasional
Sangat Rendah	1	Penundaan proses bisnis maksimal sampai dengan setengah hari kerja
Rendah	2	Penundaan proses bisnis antara setengah hari sampai dengan maksimal 1 hari kerja
Sedang	3	Penundaan proses bisnis antara 1 hari sampai dengan maksimal 3 hari kerja

Efek	Tingkat Dampak	Justifikasi Operasional
Tinggi	4	Penundaan proses bisnis antara 3 hari sampai dengan maksimal 5 hari kerja
Sangat Tinggi	5	Penundaan proses bisnis sampai dengan lebih dari 5 hari kerja

(Sumber: COBIT 5 for Risk; yang telah disesuaikan dengan kondisi di PNB)

4.4 Penilaian risiko TI di Unit SIM Politeknik Negeri Bali

Terdapat dua pendekatan dalam penilaian risiko di Unit SIM Politeknik Negeri Bali, yaitu pendekatan *top-down* dan *bottom-up*. Perbedaan antara risiko *top-down* dan *bottom up* tergantung pada siapa yang menjadi pemilik risikonya. Risiko *top-down* merupakan potret risiko secara garis besar yang ada di Unit SIM. Risiko *top-down* di Unit SIM merupakan tugas utama yang harus diselesaikan oleh pihak top manajemen Unit SIM dan top manajemen Politeknik Negeri Bali. Sedangkan risiko *bottom-up* dimiliki oleh *staff* operasional yang berada di Unit SIM. Risiko *Bottom-up* sifatnya lebih taktis – spesifik ke tugas masing-masing *staff* atau dimana proses bisnis mereka terlibat. Kedua penilaian risiko ini harus dikolaborasikan agar mendapatkan profil risiko yang komprehensif.

4.4.1 Penilaian risiko *Top-down* Unit SIM Politeknik Negeri Bali

1. **Risiko Kelangsungan Bisnis**
    a. Unit Sistem Informasi Manajemen harus selalu tanggap untuk menghadapi dan mengatasi risiko yang sifatnya dari alam, yang dapat berdampak pada lumpuhnya/penundaan/terhentinya proses bisnis seperti gempa bumi ataupun kebakaran. Risiko ini memang memiliki kemungkinan yang sangat jarang, namun dampak yang dihasilkan sangat tinggi. Solusinya adalah dengan merancang *Business Continuity Plan* yang efektif (bukan hanya *backup* data saja) – tapi juga perencanaan dimana lokasi cadangan ditempatkan, apa saja permintaan layanan yang dapat dijalankan (Sesuai SOP) pada saat terjadinya kasus seperti kebakaran atau gempa bumi.

b. Unit Sistem Informasi Manajemen memiliki *Standard Operating Procedure* yang kurang detail. Solusinya adalah Unit Sistem Informasi Manajemen harus memisahkan proses bisnisnya menjadi dua kelompok *Standard Operating Procedure* (*procurement* dan *non-procurement*) untuk proses bisnis pengembangan software, pengembangan jaringan/ hardware dan pemeliharaan jaringan/hardware. *Non-procurement* untuk project dibawah Rp.50.000.000,- dan *Procurement* untuk project diatas Rp.50.000.000,-. Pengelompokan ini bermaksud untuk memudahkan bagian operasional untuk melaksanakan tugas nya, pihak internal dalam melakukan kontrol kesesuaian dan pihak eksternal dalam melakukan audit.

c. Unit Sistem Informasi Manajemen tidak memiliki manajemen waktu pelaksanaan terkait setiap berjalannya proses bisnis. Solusinya dengan cara menambahkan berapa lama waktu yang dibutuhkan (manajemen waktu pelaksanaan) untuk menyelesaikan satu *Standard Operating Procedure* untuk setiap proses bisnisnya.

2. Risiko Aset dan Teknologi Informasi

a. Dalam perkembangan teknologi yang semakin maju, dimana berbagai informasi dapat diakses melalui internet, keamanan data Unit Sistem Informasi Manajemen merupakan sesuatu yang wajib disorot. Risiko akannya penempatan aset yang tidak sesuai dengan standar ISO 27001 seperti panel listrik yang tidak memiliki kunci pengaman rentan mengalami sabotase dari internal dan eksteral Politeknik Negeri Bali, kondisi ruang server yang kurang baik rentan mengalami permasalahan baik dari oknum yang tidak bertanggung jawab maupun alam. Risiko ini memiliki kemungkinan yang kadang-kadang terjadi, namun dampak yang dihasilkan tinggi bahkan bisa sangat tinggi dan dapat berimbas pada reputasi Unit Sistem Informasi Manajemen sendiri. Solusinya adalah dengan memindahkan panel listrik ke lokasi yang memiliki keamanan yang lebih tinggi, mengganti gagang pintu manual yang terdapat di titik-titik penting didalam gedung Unit Sistem Informasi Manajemen dengan *fingerprint sensor* dan merehab plafon di ruang

server diganti dengan plafon anti api serta menutup manhole pada plafon di ruang server.

b. Pelayanan yang belum sepenuhnya menggunakan bantuan Teknologi Informasi. Banyak form permintaan yang belum terisi, permintaan masih dilakukan via telepon langsung menuju staff ataupun petinggi Unit Sistem Informasi, merupakan salah satu potret garis besar kurang baiknya pelayanan yang diberikan oleh Unit Sistem Informasi Manajemen. Dampaknya adalah beban kerja yang semakin meningkat dan tidak berjalannya proses bisnis sesuai dengan SOP yang telah ditentukan. Solusinya adalah dengan mendesain dan mengembangkan sistem pelayanan terintegrasi antara permintaan pengembangan software, permintaan pengembangan jaringan/*hardware*, permintaan pemeliharaan jaringan/*hardware*.yang mengacu pada ITIL V3 2011.

3. Risiko Sumber Daya Manusia

a. Keberlangsungan perkembangan Unit Sistem Informasi Manajemen tidak terlepas dari kualitas sumber daya manusia yang dimilikinya. Risiko akan pergantian kursi kepemimpinan karena masa akhir jabatan ataupun karena unsur politik internal, mundurnya karyawan karena surat keputusan tugas tidak diperpanjang, kompetensi sumber daya manusia dan alokasi sumber daya manusia yang minim adalah potret secara garis besar risiko sumber daya manusia di Unit Sistem Informasi Manajemen. Solusinya adalah dengan menambah alokasi sumber daya manusia sehingga dapat meringankan beban kerja di Unit Sistem Informasi Manajemen.

b. Kurangnya *Transfer knowledge* yang menyebabkan banyak beban kerja yang hanya bertumpu pada beberapa staff saja di Unit Sistem Informasi Manajemen (Contohnya: melakukan *backup server* lokal maupun *cloud*). Solusinya adalah dengan cara membuat panduan secara detail terkait cara pelaksanaan yang bersifat teknis (baik itu *backup server*, maupun saat melaksanakan proses pemeliharaan jaringan)

4. **Risiko Reputasi**

   Risiko reputasi Unit Sistem Informasi Manajemen meliputi keluhan pelayanan terkait sistem informasi, website maupun infrastruktur jaringan internet di Politeknik Negeri Bali. Solusinya adalah dengan melakukan evaluasi dengan cara survey menggunakan kuisioner terkait bagaimana peforma Unit Sistem Informasi selama satu tahun menangani pelayanan dan menyertakan opini yang sekiranya dapat dijadikan masukan untuk perbaikan Unit Sistem Informasi Manajemen ditahun berikutnya.

5. **Risiko Hukum dan Regulasi**

   Saat menjalankan operasionalnya, Unit Sistem Informasi Manajemen menghadapi berbagai jenis peraturan hukum dan perubahan regulasi yang terkait serta aturan yang dibuat dalam perjanjian dengan pihak ketiga dengan Unit Sistem Informasi Manajemen seperti *Service level Agreement* dengan pihak penyedia server *cloud* terkait *downtime* dan *uptime* yang diberikan. Jika tidak sesuai dengan SLA, Unit Sistem Informasi Manajemen dapat melakukan protes dan menuntut kompensasi.

4.4.2 Penilaian risiko *Bottom-up* Unit SIM Politeknik Negeri Bali

Penilaian risiko *Bottom-up* dilihat dari proses bisnis yang ada di Unit Sistem Informasi Manajemen Politeknik Negeri Bali. Unit Sistem Informasi Manajemen sendiri memiliki tujuh buah proses bisnis yang telah memiliki *Standard Operating Procedure* - nya masing-masing.

4.4.2.1 Penilaian risiko pada Pengembangan *Software*

Salah satu tugas dibentuknya Unit Sistem Informasi Manejemn adalah membantu Politeknik Negeri Bali dalam mengembangkan perangkat lunak atau sistem informasinya. Gambar proses bisnis pengembangan *software* di Unit Sistem Informasi Manajemen dapat dilihat pada Lampiran 1. Tabel 4.9 merupakan proses kerja dari pengembangan *software* di Unit Sistem Informasi Manajemen.

Tabel 4.9 Alur Proses kerja Pengembangan Software

Fase	Alur Proses	Aset TI
1	Pengisian Form pengembangan *software* dari pemohon (Semua Fungsi)	**1. Sumber Daya Manusia** • Pemohon • *Team Leader/ Project Manager* • *Analyst* • *Database Adiminstrator (DBA)* • *Programmer* • *Helpdesk* Unit SIM • Fungsi Verifikator (Ketua Unit SIM) • *Quality Assurance* • *Trainer* • *End User* **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-03 tentang Pengembangan Software **3. Teknologi** • **Sistem informasi berbasis web (PHP)** • ***Notebook*** • **Perangkat *Server*** • **Perangkat *Server***
2	Penerimaan permintaan/ Analisis Kebutuhan *software* oleh Unit SIM	
3	Pengajuan usulan pengembangan sistem oleh Divisi Sistem dan Informasi Unit SIM	
4	Perancangan Sistem *software* oleh Divisi Sistem dan Informasi	
5	Pembuatan Program oleh Divisi Sistem dan Informasi	
6	Uji coba *software* oleh Divisi Sistem dan Informasi	
7	Pelatihan/ Sosialisasi *software* oleh Divisi Sistem dan Informasi	
8	Implementasi sistem oleh pengguna akhir	
9	Evaluasi sistem oleh Divisi Sistem dan Informasi	
10	Pengarsipan	

Mengacu pada Tabel 4.9, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses pengembangan *software* di Unit Sistem

Informasi Manajemen, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Dimana Sumber Daya Manusia yang terlibat dalam aktivitas pengembangan *software* adalah pemohon, team leader, *analyst*, database administrator, programmer, *Helpdesk* Unit SIM, Fungsi *Verifikator*, *Quality Assurance*, *Trainer*, dan *End User*. Sedangkan proses yang terlibat adalah SOP-USIM-03 tentang Pengembangan *software*. Teknologi yang terlibat adalah Notebook yang digunakan untuk pengembangan *software* maupun *server* yang digunakan untuk menampung database dari *software* yang akan dikembangkan. Merujuk pada Tabel 4.9, Perangkat *Server* tidak dijabarkan secara detail terkait sistem operasi ataupun processornya karena server yang digunakan untuk menampung database dari *software* yang akan dikembangkan akan dipilih sendiri oleh DBA nya.

Hasil identifikasi risiko menunjukkan terdapat sekurang-kurangnya 36 risiko yang berhasil di identifikasi yang tersebar pada masing-masing fase didalam proses bisnis pengembangan *software*. Tabel 4.10 menunjukkan 3 *sample* dari total sekurang-kurangnya 36 risiko yang dapat diidentifikasi pada proses bisnis pengembangan *software.*

Unit SIM memang belum memiliki dokumen profil risiko, namun secara tak tertulis banyak dari skenario risiko telah memiliki kontrol terhadap risikonya. Merujuk pada Tabel 4.10, peneliti merancang *template* identifikasi risiko yang mengacu pada skenario risiko ideal dari COBIT 5 *for Risk* yang dibagi menjadi 7 bagian, yaitu: skenario risiko, kategori risiko, aktor, tipe ancaman, event, aset/ sumber daya, timing. Peneliti menambahkan dua kolom yaitu: kolom penyebab dan kontrol saat ini. Mengacu pada COBIT 5 *for Risk*, risiko yang diidentifikasi adalah risiko saat ini (*current risk*) – yang berarti segala risiko yang telah memiliki kontrol.

Tabel 4.10 Hasil identifikasi *current risk* pada proses bisnis pengembangan *software*

ID Risiko	Skenario Risiko	Kategori Risiko	Aktor	Tipe Ancaman	Event	Aset/Sumber daya	Timing	Penyebab	Kontrol yang ada saat ini
R0303-20	Dokumen SRS yang dibuat tidak sesuai dengan keinginan aplikasi yang diminta oleh pemohon. Sehingga belum dapat masuk kedalam tahap pengembangan aplikasi	*IT Expertise and Skills*	Internal - *Analyst*	*Failure*	*Ineffective Design*	*Information*	Fase ke 6 – Saat proses merancang sistem *software*	Kurangnya pengalaman *analyst* dalam membuat dokumen SRS	Analyst yang ditunjuk untuk membuat blueprint (SRS) merupakan dosen-dosen pilihan yang tergabung dalam tim percepatan pembangunan PNB
R0303-28	Aplikasi memiliki kualitas keamanan yang rendah *(dapat dengan mudah diserang menggunakan sql injection, deface)*	*Software*	Internal – *Programmer*	*Malicious*	*Destruction*	*Applications*	Tahap ke 8 – Saat proses uji coba *software*	Pemrograman yang kurang baik, masih memiliki *bug*	Tidak ada
R0303-35	Aplikasi yang telah memasuki tahap implemntasi belum pernah dilakukan evaluasi terhadap dampak dari penggunaan aplikasi dari sisi pengguna	*IT Expertise and Skills*	Internal – *Quality Assurance*	*External Requirement*	*Rules and Regulations*	*Applications*	Tahap ke 11 – Saat proses evaluasi sistem	Dana yang diperlukan untuk evaluasi *software* belum dianggarkan	Tidak ada

Merujuk pada Tabel 4.10, skenario pertama adalah risiko yang memiliki ID Risiko R0303-20, yang artinya adalah risiko nomor 20 pada SOP No 03 – merujuk pada dokumen *Standard Operational Procedure* Pengembangan *software* (SOP-USIM-03) Unit Sistem Informasi Manajemen Politeknik Negeri Bali. *Timing* pada kolom ke 8 adalah pada saat apa sebuah risiko dapat terjadi. Pada skenario pertama, risiko dapat terjadi pada saat proses merancang sistem *software*. Penyebabnya adalah kurangnya pengalaman seorang *analyst* dalam membuat dokumen *software Requirement Spesification*. Aktor / pelaku yang menyebabkan skenario risiko ini berjalan ialah seorang *analyst* itu sendiri. Risiko ini termasuk dalam kategori *IT Expertise and Skills* (keahlian dan keterampilan pada TI). Masuk kedalam *event* (peristiwa) desain yang kurang efektif dan aset yang berdampak pada risiko adalah informasi. Kontrol yang ada saat proses identifikasi risiko berlangsung adalah *analyst* yang ditunjuk untuk membuat blueprint (SRS) merupakan dosen-dosen pilihan yang tergabung dalam tim percepatan pembangunan PNB. Skenario kedua adalah risiko yang memiliki ID Risiko 0303-28. Skenario risikonya berbunyi "Aplikasi memiliki kualitas keamanan yang rendah (dapat dengan mudah diserang menggunakan sql injection, deface)". Risiko ini dapat terjadi pada saat proses uji coba *software* sedang berlangsung. Aktor dari skenario risiko ini adalah programmer. Penyebab dari risiko ini adalah kualitas pemrograman yang kurang baik karena masih banyak *bug* (celah) untuk terinfeksi malware. Skenario risiko ini belum memiliki kontrol sama sekali. Skenario ketiga adalah risiko yang memiliki ID Risiko 0303-35. Skenario risikonya berbunyi "Aplikasi yang telah memasuki tahap implementasi belum pernah dilakukan evaluasi terhadap dampak dari penggunaan aplikasi dari sisi pengguna". Risiko ini dapat terjadi pada saat proses evaluasi sistem sedang berlangsung. Aktor dari skenario risiko ini adalah seorang *quality assurance*. Penyebab dari risiko ini adalah dana yang diperlukan untuk evaluasi *software* belum dianggarkan. Skenario risiko ini belum memiliki kontrol sama sekali.

Tabel 4.10 berhubungan dengan Tabel 4.11 dan Tabel 4.12. Merujuk pada Tabel 4.11, risiko dengan ID Risiko R0303-20 memiliki frekuensi/ kemungkinan terjadinya kadang-kadang. Kadang-kadang memiliki nilai '3' dengan penjelasan bahwa kejadian tidak lebih dari 5 kali per tahun. Risiko R0303-20 memiliki 3 dampak, yaitu dampak pada aspek finansial, operasional dan reputasi. Pada aspek finansial, Risiko R0303-20 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya kurang dari Rp.1.000.000,- (kalkulasi secara kasar dengan menimbang beberapa faktor seperti harga kertas untuk membuat dokumen SRS, waktu yang dihabiskan dalam membuat dokumen SRS, kompetensi yang dimiliki oleh seorang *Analyst*, biaya transportasi) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah sangat rendah '1'. Pada aspek operasional, risiko R0303-20 kemungkinan dapat menyebabkan penundaan proses bisnis sampai maksimal 1 hari kerja (menimbang pegawai di Unit SIM kecuali administrator adalah tenaga pengajar di Politeknik Negeri Bali sehingga kesibukan dapat menjadi sebuah alasan). Maka dari itu, dampak yang dihasilkan adalah rendah '2'. Risiko R0303-20 tidak memiliki dampak pada aspek hukum. Karena risiko R0303-20 masih didalam proses pengembangan *software* – dalam kasus ini masih didalam internal Unit SIM – dan tidak ada catatan hukum apapun yang mengikat. Pada aspek reputasi, risiko R0303-20 kemungkinan dapat menyebabkan pemberitahuan atau isu negatif dari internal Unit SIM ataupun eksternal (masih dalam ruang lingkup internal Politeknik Negeri Bali) yang dapat menurunkan kepercayaan sebagian kecil pemangku kepentingan di Unit SIM itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan rendah '2'. Total nilai risiko R0303-20 adalah 5,25. Sebagai pemilik risiko, *analyst* melakukan mitigasi risiko terhadap R0303-20 dengan cara memperbaiki dokumen SRS yang dibuat sesuai dengan keinginan aplikasi yang diminta oleh pemohon sesuai dengan acuan ISO 27002:2013 tentang tanggung jawab manajemen (*Management Responsibilities*)

Masih merujuk pada Tabel 4.11, risiko dengan ID Risiko R0303-28 memiliki frekuensi/ kemungkinan terjadinya sangat jarang. Sangat jarang memiliki nilai ‘1’ dengan penjelasan bahwa kejadian tidak lebih dari 2 kali per tahun. Risiko R0303-28 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0303-28 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya kurang dari Rp.500.000,- (kalkulasi secara kasar dengan menimbang beberapa faktor seperti waktu yang dihabiskan dalam mencari *bug*, kompetensi yang dimiliki oleh seorang *programmer*, biaya transportasi, biaya konsumsi) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah sangat rendah ‘1’. Pada aspek operasional, risiko R0303-28 kemungkinan dapat menyebabkan penundaan proses bisnis antara 1 sampai maksimal 3 hari kerja (menimbang pegawai di Unit SIM kecuali administrator adalah tenaga pengajar di Politeknik Negeri Bali dan tingkat kesulitan dari penemuan *bug* itu tersendiri). Dapat disimpulkan bahwa aspek operasional dampak yang dihasilkan adalah sedang ‘3’. Risiko R0303-28 memiliki dampak pada aspek hukum dengan nilai rendah ‘2’. Karena risiko R0303-28 masih didalam proses uji coba *software* – dalam kasus ini masih didalam internal Unit SIM – dan jika lolos uji tes namun masih memiliki bug kemungkinan terjadi adanya pelanggaran yang dilakukan namun belum menjadi sebuah tuntutan hukum. Pada aspek reputasi, risiko R0303-28 kemungkinan dapat menyebabkan pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar *stakeholder* (masih dalam ruang lingkup internal Politeknik Negeri Bali) yang dapat menurunkan kepercayaan pemangku kepentingan di Unit SIM itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sedang ‘3’. Total nilai risiko R0303-28 adalah 2,25. Sebagai pemilik risiko, Project Manager melakukan mitigasi risiko ini dengan cara bekerja sama dengan pihak ketiga dalam hal pengembangan aplikasi sehingga jika ada celah pada aplikasi dapat menyerahkannya ke pihak ketiga. Sesuai dengan ISO 27002:2013 tentang Control of operational *software.*

Risiko dengan ID Risiko R0303-35 memiliki frekuensi/ kemungkinan sering terjadi. Sering memiliki nilai ‘2’ dengan penjelasan bahwa kejadian tidak lebih dari 2 kali tiap enam bulan. Risiko R0303-35 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0303-35 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya kurang dari Rp.1.000.000,- (kalkulasi secara kasar dengan menimbang beberapa faktor seperti waktu yang dihabiskan dalam membuat kuesioner, kompetensi yang dimiliki oleh seorang *quality assurance*, biaya transportasi, biaya konsumsi, waktu yang digunakan untuk menyebarkan kuesioner kepuasan) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah sangat rendah ‘1’. Risiko pada operasional bernilai rendah ‘2’, karena dapat menghambat berjalannya proses bisnis sampai dengan waktu 1 hari (membuat kuesioner terkait kualitas sistem informasi di Politeknik Negeri Bali). Risiko R0303-35 memiliki dampak pada aspek hukum dengan nilai sangat rendah ‘1’. Karena risiko R0303-35 sudah memasuki tahapan proses evauasi. Pada aspek reputasi, risiko R0303-35 kemungkinan dapat menyebabkan pemberitahuan atau isu negatif dari internal Unit SIM ataupun eksternal (masih dalam ruang lingkup internal Politeknik Negeri Bali) namun tidak dapat menurunkan kepercayaan pada pemangku kepentingan di Unit SIM itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan rendah ‘1’. Total nilai risiko R0303-35 adalah 2,5. Sebagai pemilik risiko, *Quality Assurance* di Divisi Sistem Informasi Unit SIM akan melakukan mitigasi pada risiko 0303-35 dengan cara bekerja sama dengan ketua SIM dalam merancang ketetapan untuk wajibnya dilakukan evaluasi terhadap dampak dari penggunaan aplikasi dari sisi pengguna. Sesuai dengan standar ISO 25040:2011 tentang *Systems and software Quality Requirements and Evaluation*

Merujuk pada Tabel 4.12, *analyst* merespons risiko R0303-20 dengan melakukan mitigasi dengan cara harus memperbaiki SRS agar sesuai dengan keinginan pengguna. Respon terhadap aksi risiko ternyata sudah dilakukan oleh *analyst* ybs. Project Manager merespons risiko R0303-28 dengan

melakukan *Transfer*, karena beberapa dari sistem utama dibuat dari pihak ketiga – hasil dari *e-procurement* – sehingga jika maish terdapat *bug* atau kesalahan lainnya masih dapat di *maintenance* oleh pihak ketiga. Justifikasi respon risiko ini mengacu pada ISO/IEC 27002:2013. Respon terhadap aksi risiko ternyata sudah dilakukan oleh Project Manager ybs. *Quality Assurance* di Divisi Sistem Informasi merespons risiko R0303-35 dengan melakukan mitigasi bersama dengan ketua SIM dalam merancang ketetapan untuk wajibnya dilakukan evaluasi sistem informasi di lingkungan Politeknik Negeri Bali. Justifikasi respon risiko ini mengacu pada ISO/IEC 25040:2011 tentang proses evaluasi perangkat lunak. Respon terhadap aksi ini akan di rencanakan sebelum akan diimplementasikan.

Tabel 4.11 Hasil analisis risiko pada proses bisnis pengembangan *software*

ID Risiko	Residual Risk	Frekuensi	Dampak				Rata-rata dampak	Nilai risiko	*Risk Map*
			Finansial	Operasional	Hukum	Reputasi			
R0303-20	Belum terlihat	3	1	2	0	2	1,75	5,25	Medium
R0303-28	Masih terdapat bug di aplikasi	1	1	3	2	3	2,25	2,25	Medium
R0303-35	Tidak adanya ketentuan untuk evaluasi sistem	2	1	2	1	1	1,25	2,5	Medium

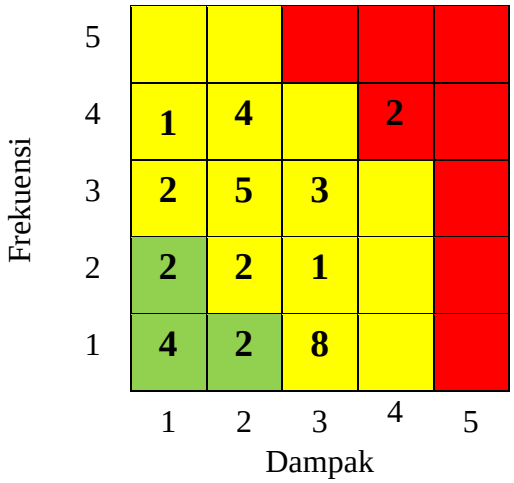
Tabel 4.12 Hasil respon terhadap risiko pada proses bisnis pengembangan *software*

ID Risiko	Respon Risiko	Pemilik Risiko	Justifikasi	Standar justifikasi respon risiko	Rencana Aksi	
					Sudah	Rencana
R0303-20	*Mitigate*	Analyst	Analyst harus memperbaiki dokumen SRS yang dibuat sesuai dengan keinginan aplikasi yang diminta oleh pemohon	ISO/IEC 27002:2013 – Clause 7 Human resource security Subclause 7.2 During employment 7.2.1 Management responsibilities	✓	
R0303-28	Share	Project Manager	Divisi sistem informasi bekerja sama dengan pihak ketiga dalam hal pengembangan aplikasi sehingga jika ada celah pada aplikasi dapat menyerahkannya ke pihak ketiga	ISO/IEC 27002:2013 – Clause 12 Operations security Subclause 12.5 Control of operational software 12.5.1 Installation of *software* on operational systems	✓	
R0303-35	*Mitigate*	Quality Assurance	Divisi sistem informasi bekerja sama dengan ketua SIM dalam merancang ketetapan untuk wajibnya dilakukan evaluasi terhadap dampak dari penggunaan aplikasi dari sisi pengguna.	ISO 25040:2011 Systems and *software* engineering < Systems and *software* Quality Requirements and Evaluation (SQuaRE) < Evaluation process		✓

Mengacu pada Tabel 4.12, jumlah risiko yang terdapat pada proses pengembangan *software* berjumlah 36 risiko yang tersebar di 3 kategori, rendah (hijau), sedang (kuning), tinggi (merah). Setelah melalui tahapan analisis risiko, terdapat 8 risiko yang berada pada kategori rendah. Divisi Sistem Informasi tidak perlu melakukan sesuatu untuk merespons risiko karena masih didalam kategori *risk appetite* nya. Terdapat 26 risiko yang berada dikategori sedang, divisi sistem informasi memiliki kebijakan untuk melakukan mitigasi atau *Transfer* risikonsya. Berdasarkan hasil respon terhadap risiko, terdapat 17 respon terhadap risiko yang telah diterapkan oleh Divisi Sistem Informasi Manajemen dan 9 respon yang belum diterapkan.

Terdapat 2 risiko yang berada dikategori tinggi, risiko ini harus dihindari oleh Divisi Sistem Informasi jika tidak menginginkan sesuatu yang tidak diinginkan terjadi. Berdasarkan hasil respon terhadap risiko, belum ada satupun respon terhadap risiko yang sudah diimplementasikan.

Tabel 4.13 Peta risiko proses pengembangan *software*



4.4.2.2 Penilaian risiko pada Pengembangan Jaringan/*Hardware*

Salah satu tugas dibentuknya Unit Sistem Informasi Manejemn adalah membantu Politeknik Negeri Bali dalam mengembangkan infrastruktur jaringan internet atau perangkat keras lainnya. Gambar proses bisnis pengembangan jaringan/*hardware* di Unit Sistem Informasi Manajemen

dapat dilihat pada Lampiran 2. Tabel 4.14 merupakan alur proses kerja dari pengembangan jaringan dan hardware di Unit Sistem Informasi Manajemen.

Tabel 4.14 Alur proses kerja Pengembangan Jaringan dan Hardware

Fase	Alur Proses	Aset TI
1	Penerimaan permintaan instalasi jaringan oleh Teknisi Divisi Sistem dan Jaringan	**1. Sumber Daya Manusia** • Pemohon • Teknisi Divisi Sistem dan Jaringan • Fungsi Verifikator (Ketua Unit) • Pejabat Unit Pengadaan • Pembantu Direktur III Politeknik Negeri Bali **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-02 tentang Pengembangan Jaringan dan Hardware **3. Teknologi** • **Backbone Fiber Optic** • **Topologi Star** • **Kabel UTP Cat 6** • **Kabel UTP Cat 5** • **Switch** • **Router** • **Access Point**
2	Survey lokasi dilakukan oleh Teknisi Divisi Sistem dan Jaringan	
3	Analisis kebutuhan material oleh Teknisi Divisi Sistem dan Jaringan	
4a	Unit SIM mengajukan proposal pembelian alat kepada Pembantu Direktur III jika stok tidak ada	
4a.a	Jika proposal disetujui, maka Unit SIM melakukan pembelian alat jika nominal dibawah Rp.50.000.000. Jika diatas Rp.50.000.000 maka akan masuk ke Unit Pengadaan untuk dilelang	
4.a.b	Jika proposal tidak disetujui, maka Unit SIM akan menginformasikan ke Unit/Jurusan dengan menerbitkan surat pemberitahuan.	
4b	Jika stok masih ada, maka teknisi Divisi Sistem dan Jaringan dapat langsung melakukan pemasangan	
5a.a	Teknisi Divisi Sistem dan Jaringan melakukan pemasangan jaringan	

Fase	Alur Proses	Aset TI
6	Uji coba jaringan dilakukan oleh Teknisi Divisi Sistem dan Jaringan	• **Perangkat Server**
7	Pengecekan ulang dilakukan oleh Ketua Unit SIM	
8	Teknisi Divisi Sistem dan Jaringan melaporkan bahwa jaringan siap dipakai kepada pemohon	
9	Pengarsipan	

Mengacu pada Tabel 4.14, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses pengembangan jaringan/*hardware* di Unit Sistem Informasi Manajemen, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Dimana Sumber Daya Manusia yang terlibat dalam aktivitas pengembangan jaringan/*hardware* adalah pemohon, teknisi divisi sistem dan jaringan, fungsi verifikator (Ketua Unit SIM), Pejabat Unit Pengadaan dan Pembantu Direktur III. Sedangkan proses yang terlibat adalah SOP-USIM-03 tentang Pengembangan Jaringan dan *Hardware*. Teknologi yang terlibat adalah Fiber *Optic*, UTP Cat 6, UTP Cat 5, Router, *Access Point*, dan perangkat server. Fiber Optic menjadi *backbone* infrastruktur jaringan di PNB. *Backbone* ini menyebar dengan topologi star ke area yang menjadi pusat bagi gedung-gedung lain yang berdekatan. Pusat dari sebaran koneksi tersebut terhubung kedalam *manageable switch* yang selanjutnya dinamakan *node* oleh pihak Politeknik Negeri Bali. Terdapat 6 node yang dihubungkan dengan fiber *optic* yang memiliki *core* sejumlah 12 buah dan 4 *node* terhubung dengan fiber optik yang memiliki *core* sejumlah 24 buah. Node-node tersebut menjadi pusat sebaran koneksi jaringan ke gedung-gedung terdekat dengan memanfaatkan kabel UTP Cat 6. Sedangkan koneksi didalam gedung memanfaatkan kabel UTP Cat 5.

Hasil identifikasi risiko menunjukkan terdapat sekurang-kurangnya 31 risiko yang terdapat pada proses bisnis pengembangan jaringan/*hardware*.

Merujuk pada Tabel 4.15, skenario pertama adalah risiko yang memiliki ID Risiko R0202-16, yang artinya adalah risiko nomor 16 pada SOP No 02 – merujuk pada dokumen *Standard Operational Procedure* Pengembangan Jaringan/*Hardware* (SOP-USIM-02) dan '2' merupakan kode pengembangan jaringan/*hardware* Unit Sistem Informasi Manajemen Politeknik Negeri Bali. *Timing* pada kolom ke 8 adalah pada saat apa sebuah risiko dapat terjadi. Pada skenario pertama, risiko dapat terjadi pada saat proses pembelian alat. Penyebabnya adalah tidak ada metode pengambilan keputusan untuk pemrioritasan *supplier*. Aktor / pelaku yang menyebabkan skenario risiko ini berjalan ialah pejabat pengadaan. Risiko ini termasuk dalam kategori *Suppliers*. Termasuk dalam *event* (peristiwa) Rules and Regulation (aturan dan regulasi) dan aset yang berdampak pada risiko adalah *people and skills*. Kontrol yang ada saat ini terkait skenario pertama adalah Proses pemilihan supplier tidak menggunakan metode pengambilan keputusan. semuanya diserahkan kepada proses *e-procurement*. Skenario kedua adalah risiko yang memiliki ID Risiko 0202-26. Skenario risikonya berbunyi "Saat pemasangan jaringan/hardware, teknisi tidak mengindahkan prosedur keselamatan dan keamanan kerja, sehingga dapat mencelakai diri sendiri maupun orang lain". Risiko ini dapat terjadi pada saat proses pemasangan jaringan sedang berlangsung. Aktor dari skenario risiko ini adalah Teknisi. Penyebab dari risiko ini adalah tidak adanya pengaman standar yang dapat digunakan oleh teknisi yang sedang melakukan pemasangan jaringan/*hardware*. Kontrol yang ada saat ini terkait skenario kedua adalah selama ini Teknisi menggunakan pakaian kasual kerja saat melakukan pemasangan jaringan/hardware. Skenario ketiga adalah risiko yang memiliki ID Risiko 0202-26. Skenario risikonya berbunyi "Teknisi yang ditunjuk oleh Divisi Sistem dan Jaringan tidak memiliki pengetahuan yang cukup untuk dapat melakukan uji coba terhadap jaringan/hardware yang telah terpasang". Risiko ini dapat terjadi pada saat proses uji coba instalasi jaringan sedang berlangsung. Aktor dari skenario risiko ini adalah Teknisi Divisi Sistem dan Jaringan. Penyebab dari risiko ini adalah kurangnya pengetahuan yang dimiliki oleh teknisi divisi sistem dan jaringan. Kontrol yang ada saat ini

untuk skenario ketiga adalah Teknisi dipandu oleh salah satu pegawai senior sekaligus dosen di Politeknik Negeri Bali.

Tabel 4.14 berhubungan dengan Tabel 4.15 dan Tabel 4.16. Merujuk pada Tabel 4.15, risiko dengan ID Risiko R0202-16 memiliki frekuensi/ kemungkinan jarang terjadi. Jarang memiliki nilai '2' dengan penjelasan bahwa kejadian tidak lebih dari 2 kali enam bulan. Risiko R0202-16 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0202-16 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya berkisar Rp.50.000.000 – Rp 60.000.000 (kalkulasi secara kasar dengan kerugian e-procurement dalam memilih supplier yang bermasalah atau barang yang diberikan tidak bagus, supplier tidak profesional) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah sedang '3'. Pada aspek operasional, risiko R0202-16 kemungkinan dapat menyebabkan penundaan proses bisnis sampai maksimal satu hari kerja. Maka dari itu, dampak yang dihasilkan adalah rendah '2'. Pada aspek hukum, risiko R0202-16 kemungkinan dapat menyebabkan adanya surat peringatan dari individu/instansi dengan dampak relatif kecil. Maka, dampak yang dihasilkan pada aspek hukum adalah tinggi '2'. Pada aspek reputasi, risiko R0202-16 kemungkinan dapat menyebabkan Terdapat pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian kecil stakeholder. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sangat rendah '1'. Total nilai risiko R0202-16 adalah 4. Pemilik Proses Bisnis akan melakukan mitigasi pada risiko R0202-16 dengan cara mengawasi jalannya proses lelang melalui LPSE sesuai dengan ISO 27002:2013 terkait *Supplier relationships*.

Masih merujuk pada Tabel 4.15, risiko dengan ID Risiko R0202-26 memiliki frekuensi/ kemungkinan jarang terjadi. Jarang memiliki nilai '2' dengan penjelasan bahwa kejadian tidak lebih dari 2 kali tiap enam bulan. Risiko R0202-26 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0202-26 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya mencapai

Rp.40.000.000,- (kalkulasi secara kasar dengan biaya rumah sakit akibat kecelakaan kerja saat melakukan pengembangan jaringan/*hardware* yang bergantung pada tingkat keseriusan cedera yang dialami) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah rendah '2'. Pada aspek operasional, risiko R0202-26 kemungkinan dapat menyebabkan penundaan proses bisnis sampai maksimal 1 hari kerja. Maka dari itu, dampak yang dihasilkan adalah rendah '2'. Pada aspek hukum, risiko R0202-26 kemungkinan dapat menyebabkan Tuntutan hukum yang berdampak pada kinerja /peforma Unit Sistem Informasi Manajemen. Maka, dampak yang dihasilkan pada aspek hukum adalah sedang '3'. Pada aspek reputasi, risiko R0202-26 kemungkinan dapat menyebabkan pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar stakeholder. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sedang '3'. Total nilai risiko R0202-26 adalah 5. Sebagai pemilik risiko, perwakilan manajemen Unit SIM diharapkan menggalakkan prosedur keselamatan kerja dengan mengedukasi divisinya agar selalu mengutamakan keselamatan dalam bekerja sesuai dengan OHSAS 18002:2008 (Kesehatan dan Keselamatan Kerja)

Risiko dengan ID Risiko R0202-27 memiliki frekuensi/ kemungkinan terjadinya jarang. Jarang memiliki nilai '2' dengan penjelasan bahwa kejadian tidak lebih dari 2 kali enam bulan. Risiko R0202-27 memiliki 3 dampak, yaitu dampak pada aspek operasional, hukum dan reputasi. Pada aspek operasional, risiko R0202-27 kemungkinan dapat menyebabkan penundaan proses bisnis 3 hari sampai maksimal 5 hari kerja. Maka dari itu, dampak yang dihasilkan adalah sedang '3'. Pada aspek hukum risiko R0202-27, kemungkinan dapat menyebabkan tuntutan hukum yang berdampak pada kinerja /peforma Unit Sistem Informasi Manajemen. Sehingga dampak yang dihasilkan adalah sedang '3' Pada aspek reputasi, risiko R0202-27 kemungkinan dapat menyebabkan Terdapat pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar *stakeholder*. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan rendah '2,5'. Total nilai risiko R0202-27 adalah 5.

Sebagai pemilik risiko, Teknisi Divisi Jaringan/ Hardware harus membawa panduan cara melakukan uji coba terhadap jaringan/hardware yang telah terpasang. Sesuai dengan standar ISO 27002:2013 tentang *Human Resource Security*.

Mengacu pada Tabel 4.16, jumlah risiko yang terdapat pada proses pengembangan jaringan/hardware berjumlah 31 risiko yang tersebar di 3 kategori, rendah (hijau), sedang (kuning), tinggi (merah). Setelah melalui tahapan analisis risiko, terdapat 13 risiko yang berada pada kategori rendah. Divisi Sistem dan Jaringan tidak perlu melakukan sesuatu untuk merespons risiko karena masih didalam kategori *risk appetite* nya. Terdapat 16 risiko yang berada dikategori sedang. Divisi Sistem dan Jaringan memiliki kebijakan untuk melakukan mitigasi atau *Transfer* risikonya. Terdapat 3 respon aksi yang sudah diterapkan oleh Divisi Sistem dan Jaringan, 13 respon aksi masih dalam rencana untuk diimplementasikan. Terdapat 2 risiko yang berada dikategori tinggi, risiko ini harus dihindari oleh Divisi Sistem dan Jaringan jika tidak menginginkan sesuatu yang tidak diinginkan terjadi. 1 respon risiko sudah diimplementasikan oleh Divisi Sistem dan Jaringan.

Tabel 4.15 Hasil identifikasi *current risk* pada proses bisnis pengembangan jaringan/*hardware*

ID Risiko	Skenario Risiko	Kategori Risiko	Aktor	Tipe Ancaman	*Event*	Aset/ Sumber daya	*Timing*	Penyebab	Kontrol yang ada saat ini
R0202-16	Tidak melakukan pemrioritasan pada *supplier* dalam konteks meyediakan keamanan berkelanjutan, efisiensi, dan efektifitas distribusi layanan	*Suppliers*	Internal – Pejabat Pengadaan	*External Requirement*	*Rules and Regulation*	*People and Skills*	Tahap ke 9 – Pembelian Alat	Tidak ada metode pengambilan keputusan untuk pemrioritasan supplier	Proses pemilihan supplier tidak menggunakan metode pengambilan keputusan. semuanya diserahkan kepada proses e-procurement
R0202-24	Saat pemasangan jaringan/*hardware*, teknisi tidak mengindahkan prosedur keselamatan dan keamanan kerja, sehingga dapat mencelakai diri sendiri maupun orang lain	*Regulatory Compliance*	Internal – Teknisi Divisi Sistem dan Jaringan	*External Requirement*	*Rules and Regulation*	*People and Skills*	Tahap ke 10 – Melakukan Pemasangan	Tidak adanya pengaman standar yang dapat digunakan oleh teknisi yang sedang melakukan pemasangan jaringan/hardware	Teknisi menggunakan pakaian kasual kerja saat melakukan pemasangan jaringan/hardware.
R0202-26	Teknisi yang ditunjuk oleh Divisi Sistem dan Jaringan tidak memiliki pengetahuan yang cukup untuk dapat melakukan uji coba terhadap jaringan/hardware yang telah terpasang	*IT Expertise and Skills*	Internal – Teknisi Divisi Sistem dan Jaringan	*Failure*	*Ineffective Execution*	*People and Skills*	Tahap ke 11 – Uji Coba Instalasi Jaringan	Kurangnya pengetahuan yang dimiliki oleh teknisi divisi sistem dan jaringan	Teknisi dipandu oleh salah satu pegawai senior sekaligus dosen di Politeknik Negeri Bali

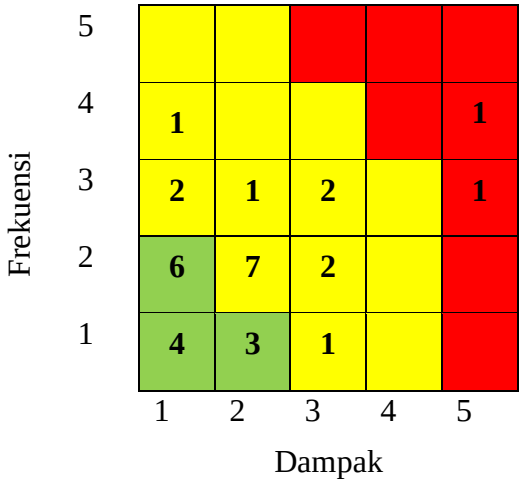
Tabel 4.16 Hasil analisis risiko pada proses bisnis pengembangan jaringan/*hardware*

ID Risiko	Residual Risk	Frekuensi	Dampak				Rata-rata dampak	Nilai risiko	Risk Map
			Finansial	Operasional	Hukum	Reputasi			
R0202-16	Belum terlihat	2	3	2	2	1	2	4	Medium
R0202-24	Risiko terkait jatuh dari tangga atau tertimpa sesuatu tanpa proteksi di kepala	2	2	2	3	3	2,5	5	Medium
R0202-26	Belum terlihat	2	0	3	3	3	2,25	4,5	Medium

Tabel 4.17 Hasil respon terhadap risiko pada proses bisnis pengembangan jaringan/*hardware*

ID Risiko	Respon Risiko	Pemilik Risiko	Justifikasi	Standar justifikasi respon risiko	Rencana Aksi	
					Sudah	Rencana
R0202-16	*Mitigate*	Pemilik Proses Bisnis	Divisi mengawasi jalannya proses lelang melalui LPSE	ISO/IEC 27002:2013 Clause 15 – Supplier relationships Subclause 15.2 Supplier service delivery management 15.2.1 Monitoring and review of supplier services	✓	
R0202-24	*Avoid*	Perwakilan Manajemen	Unit SIM diharapkan menggalakkan prosedur keselamatan kerja dengan mengedukasi divisinya agar selalu mengutamakan keselamatan dalam bekerja	OHSAS 18002:2008 Clause 4 OH&S management system requirements		✓
R0202-26	*Transfer*	Teknisi Jaringan/ Hardware	Membawa panduan cara melakukan uji coba terhadap jaringan/hardware yang telah terpasang	ISO/IEC 27002:2013 Clause 7 – Human resource security Subclause 7.2 During employment 7.2.2 Information security awareness, education and training		✓

Tabel 4.18 Peta risiko proses bisnis pengembangan jaringan/*hardware*



4.4.2.3 Penilaian risiko pada Pemeliharaan Jaringan/*Hardware*

Salah satu tugas dibentuknya Unit Sistem Informasi Manejemn adalah membantu Politeknik Negeri Bali dalam memelihara jaringan/*hardware*. Gambar proses bisnis pengembangan *software* di Unit Sistem Informasi Manajemen dapat dilihat pada Lampiran 2. Tabel 4.19 merupakan alur proses kerja dari pemeliharaan jaringan dan hardware di Unit Sistem Informasi Manajemen.

Tabel 4.19 Alur proses kerja Pemeliharaan Jaringan/Hardware

Fase	Alur Proses	Aset TI
1	Penerimaan laporan kerusakan oleh Helpdesk Unit SIM	**1. Sumber Daya Manusia** • Pemohon • Teknisi Divisi Sistem dan Jaringan • Fungsi Verifikator (Ketua Unit SIM) • Third Party (Telkom, rekanan Unit SIM)
2	Teknisi Divisi Jaringan dan Server melakukan identifikasi jenis kerusakan	
3a	Jika kerusakan berhubungan dengan provider, teknisi kemudian menghubungi provider	

Fase	Alur Proses	Aset TI
3b	Jika kerusakan diketahui, maka Teknisi Divisi Sistem dan Jaringan segera melakukan perbaikan	**2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-02 tentang Pemeliharaan Jaringan dan Hardware **3. Teknologi** • ***WiFi*** • ***Backbone Fiber Optic*** • ***Topologi Star*** • **Kabel UTP Cat 6** • **Kabel UTP Cat 5** • ***Switch*** • ***Router*** • ***Access Point*** • **Perangkat *Server***
3c	Jika kerusakan tidak diketahui, maka Teknisi Divisi Sistem dan Jaringan menghubungi Ketua SIM.	
4a	Helpdesk Unit SIM menerima informasi dari provider	
4b.a	Jika sudah selesai diperbaiki, maka Teknisi Divisi Sistem dan Jaringan membuat laporan hasil perbaikan	
4b.b	Jika belum selesai diperbaiki, maka akan dilakukan trial dan error dalam melakukan perbaikan sampai berhasil	
4c	Ketua Unit SIM melakukan analisis kerusakan.	
5a	Unit SIM menginformasikan ke Unit/Jurusan melalui surat pemberitahuan, kasus ditunda	
5c.a	Jika masalah telah ditemukan, kemudian Teknisi Divisi Sistem dan Jaringan melakukan perbaikan	
5c.b	Jika belum ada pemecahan masalah, maka Unit SIM akan	

Fase	Alur Proses	Aset TI
	menginformasikan kepada Unit/Jurusan, kasus ditunda	
6c.a dan 5b	Setelah selesai diperbaiki, Teknisi Divisi Sistem dan Jaringan kemudian membuat laporan hasil perbaikan	
7	Pengarsipan	

Mengacu pada Tabel 4.19, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses pemeliharaan jaringan/*hardware* di Unit Sistem Informasi Manajemen, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Dimana Sumber Daya Manusia yang terlibat dalam aktivitas pemeliharaan jaringan/*hardware* adalah pemohon, teknisi divisi sistem dan jaringan, fungsi verifikator (Ketua Unit SIM), dan Third Party (Telkom sebagai penyedia fiber optic maupun rekanan Politeknik Negeri Bali yang telah melakukan pengembangan infrastruktur jaringan melalui *e-procurement*). Sedangkan proses yang terlibat adalah SOP-USIM-03 tentang Pengembangan Jaringan dan Hardware. Teknologi yang terlibat adalah WiFi, Fiber *Optic*, UTP Cat 6, UTP Cat 5, Router, *Access Point*, dan perangkat server. Fiber *Optic* menjadi backbone infrastruktur jaringan di PNB. Backbone ini menyebar dengan topologi star ke area yang menjadi pusat bagi gedung-gedung lain yang berdekatan. Pusat dari sebaran koneksi tersebut terhubung kedalam manageable switch yang selanjutnya dinamakan node oleh pihak Politeknik Negeri Bali. Terdapat 6 *node* yang dihubungkan dengan fiber *optic* yang memiliki *core* sejumlah 12 buah dan 4 *node* terhubung dengan fiber optik yang memiliki core sejumlah 24 buah. *Node-node* tersebut menjadi pusat sebaran koneksi jaringan ke gedung-gedung terdekat dengan memanfaatkan kabel UTP Cat 6. Sedangkan koneksi didalam gedung memanfaatkan kabel UTP Cat 5.

Hasil identifikasi risiko menunjukkan terdapat sekurang-kurangnya 20 risiko yang terdapat pada proses bisnis pemeliharaan jaringan/*hardware*. Merujuk pada Tabel 4.20, skenario pertama adalah risiko yang memiliki ID Risiko R0201-04, yang artinya adalah risiko nomor 4 pada SOP No 02 – merujuk pada dokumen *Standard Operational Procedure* Pengembangan Jaringan/*Hardware* (SOP-USIM-02) dan '1' merujuk pada pemeliharaan jaringan/*hardware*. Unit Sistem Informasi Manajemen Politeknik Negeri Bali. *Timing* pada kolom ke 8 adalah pada saat apa sebuah risiko dapat terjadi. Pada skenario pertama, risiko dapat terjadi pada saat proses menerima laporan kerusakan jaringan/*hardware*. Penyebabnya adalah administrator lupa atau sedang disibukkan dengan kegiatan lain. Aktor / pelaku yang menyebabkan skenario risiko ini berjalan ialah seorang administrator yang mengurus permasalahan terkait jaringan. Risiko ini termasuk dalam kategori *Staff operation (human error)*. Termasuk dalam *event* (peristiwa) *Rules and Regulations* (Peraturan dan regulasi) dan aset yang berdampak pada risiko adalah *People and Skills* (orang dan kemampuannya). Kontrol yang ada saat ini adalah Administrator segera menangani permintaan insiden terkait jaringan/hardware yang masuk. Skenario kedua adalah risiko yang memiliki ID Risiko 0201-06. Skenario risikonya berbunyi "Teknisi yang ditunjuk oleh Divisi Sistem dan Jaringan melakukan kesalahan dalam mengidentifikasi masalah yang dialami oleh pelapor karena data dan informasi yang ada tidak lengkap". Risiko ini dapat terjadi pada saat proses mengidentifikasi jenis kerusakan sedang berlangsung. Aktor dari skenario risiko ini adalah teknisi. Penyebab dari risiko ini adalah teknisi yang ditunjuk tidak memiliki kemampuan dibidang TI. Kontrol yang ada saat ini adalah Jika ada laporan yang tidak spesifik (misal permasahalan terkait WiFi) maka yang dilakukan adalah *trial* dan *error*. Skenario ketiga adalah risiko yang memiliki ID Risiko 0201-11. Skenario risikonya berbunyi "Teknisi melakukan kesalahan dalam eksekusi penanganan insiden terkait jaringan/hardware sehingga menimbulkan permasalahan baru". Risiko ini dapat terjadi pada saat proses meakukan perbaikan jaringan/*hardware* sedang berlangsung. Aktor dari skenario risiko ini adalah teknisi. Penyebab dari risiko ini adalah kurangnya

pengalaman teknisi dibidang TI khususnya pemeliharaan jaringan/hardware. Tidak ada kontrol untuk saat ini karena yang selama ini dilakukan hanya *trial* dan *error*.

Tabel 4.20 berhubungan dengan Tabel 4.21 dan Tabel 4.22. Merujuk pada Tabel 4.21, risiko dengan ID Risiko R0401-04 memiliki frekuensi/ kemungkinan terjadinya sering terjadi. Sering memiliki nilai '4' dengan penjelasan bahwa kejadian tidak lebih dari 1 kali setiap bulan. Risiko R0401-04 memiliki 2 dampak, yaitu dampak pada aspek operasional dan reputasi. Pada aspek operasional, risiko R0401-04 kemungkinan dapat menyebabkan penundaan proses bisnis sampai maksimal satu hari kerja. Maka dari itu, dampak yang dihasilkan adalah rendah '2'. Pada aspek reputasi, risiko R0401-04 kemungkinan dapat menyebabkan pemberitahuan atau isu negatif dari internal Unit SIM ataupun eksternal (masih dalam ruang lingkup internal Politeknik Negeri Bali) namun tidak dapat menurunkan kepercayaan pemangku kepentingan di Unit SIM itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sangat rendah '1'. Total nilai risiko R0401-04 adalah 3. Sebagai pemilik risiko, *Helpdesk* harus langsung menangani permintaan yang masuk dengan cepat dan konsisten. Sesuai dengan standar ISO 27002:2013 tentang *Management Responsibilities*.

Masih merujuk pada Tabel 4.18, risiko dengan ID Risiko R0401-06 memiliki frekuensi/ kemungkinan terjadinya sangat jarang. Sangat jarang memiliki nilai '1' dengan penjelasan bahwa kejadian tidak lebih dari 2 kali per tahun. Risiko R0401-06 memiliki 2 dampak, yaitu dampak pada aspek operasional dan reputasi. Pada aspek operasional, risiko R0401-04 kemungkinan dapat menyebabkan penundaan proses bisnis sampai maksimal setengah hari kerja. Maka dari itu, dampak yang dihasilkan adalah sangat rendah '1'. Pada aspek reputasi, risiko R0401-06 kemungkinan dapat menyebabkan pemberitahuan atau isu negatif dari internal Unit SIM ataupun eksternal (masih dalam ruang lingkup internal Politeknik Negeri Bali) yang dapat menurunkan kepercayaan sebagian kecil pemangku kepentingan di Unit SIM itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang

dihasilkan rendah ‘1’. Total nilai risiko R0401-06 adalah 0,75. Sebagai pemilik risiko, Teknisi Divisi Sistem Informasi Unit SIM menerima risiko R0401-06 karena masih dalam kategori *risk appetite* nya.

Risiko dengan ID Risiko R0401-11 memiliki frekuensi/ kemungkinan sangat jarang terjadi. Sangat jarang memiliki nilai ‘1’ dengan penjelasan bahwa kejadian tidak lebih dari 2 kali per tahun. Risiko R0401-12 memiliki 3 dampak, yaitu dampak pada aspek operasional, hukum dan reputasi. Risiko R0401-11 memiliki dampak pada aspek operasional dengan nilai rendah ‘2’ yang dapat menyebabkan penundaan proses bisnis dari 1 hari hingga maksimal 3 hari kerja. Pada aspek hukum, risiko R0401 kemungkinan dapat menyebabkan tuntutan hukum yang berdampak pada kinerja /peforma Unit Sistem Informasi Manajemen. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sedang ‘3’. Pada aspek reputasi, risiko R0401-11 kemungkinan dapat menyebabkan terdapat pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar *stakeholder*. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sedang ‘3’. Total nilai risiko R0303-35 adalah 2. Sebagai pemilik risiko, Teknisi Divisi Sistem Informasi Unit SIM menerima risiko R0401-11 karena masih dalam kategori *risk appetite* nya.

Mengacu pada Tabel 4.20, jumlah risiko yang terdapat pada proses pengembangan jaringan/hardware berjumlah 20 risiko yang tersebar di 2 kategori, rendah (hijau) dan sedang (kuning). Setelah melalui tahapan analisis risiko, terdapat 10 risiko yang berada pada kategori rendah. Divisi Sistem dan Jaringan tidak perlu melakukan sesuatu untuk merespons risiko karena masih didalam kategori *risk appetite* nya. Terdapat 10 risiko yang berada dikategori sedang, Divisi Sistem dan Jaringan memiliki kebijakan untuk melakukan mitigasi atau *Transfer* risikonya. Terdapat 2 respon aksi yang telah di implementasikan oleh Divisi Sistem dan Jaringan, 8 sisanya belum.

Tabel 4.20 Hasil identifikasi *current risk* pada proses bisnis pemeliharaan jaringan/*hardware*

ID Risiko	Skenario Risiko	Kategori Risiko	Aktor	Tipe Ancaman	Event	Aset/Sumber daya	Timing	Penyebab	Kontrol yang ada saat ini
R0201-04	Administrator tidak segera menangani permintaan dan insiden yang masuk, sehingga pengelolaannya menjadi terhambat	*Staff operation (human error)*	Internal – Administrator	*Accidental*	Rules and Regulations	*People and Skills*	Menerima Laporan kerusakan jaringan/hardware	Administrator lupa atau sedang disibukkan dengan kegiatan lain	Administrator segera menangani permintaan insiden terkait jaringan/hardware yang masuk
R0201-06	Teknisi yang ditunjuk oleh Divisi Sistem dan Jaringan melakukan kesalahan dalam mengidentifikasi masalah yang dialami oleh pelapor karena data dan informasi yang ada tidak lengkap	*IT Expertise and Skills*	Internal - Teknisi	*Failure*	*Ineffective Executions*	*People and Skills*	Mengidentifikasi Jenis Kerusakan	Teknisi yang ditunjuk tidak memiliki kemampuan dibidang TI	Jika ada laporan yang tidak spesifik (misal permasahalan terkait WiFi) maka yang dilakukan adalah trial dan error
R0201-11	Teknisi melakukan kesalahan dalam eksekusi penanganan insiden terkait jaringan/hardware sehingga menimbulkan permasalahan baru	*IT Expertise and Skills*	Internal - Teknisi	*Failure*	Ineffective Executions	People and Skills	Lakukan perbaikan	Kurangnya pengalaman teknisi dibidang TI khususnya pemeliharaan jaringan/hardware	Tidak ada (selama ini hanya trial dan error)

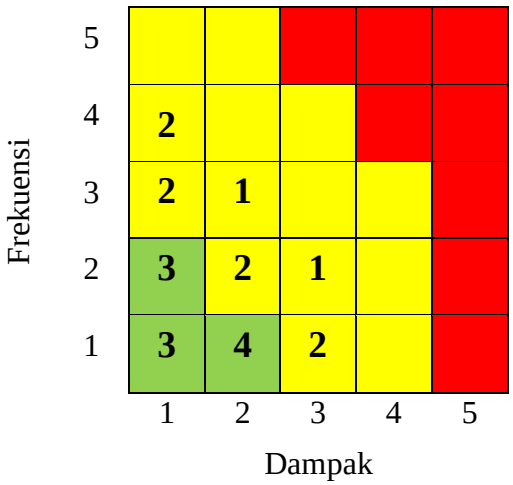
Tabel 4.21 Hasil analisis risiko pada proses bisnis pemeliharaan jaringan/*hardware*

ID Risiko	Residual Risk	Frekuensi	Dampak				Rata-rata dampak	Nilai risiko	Risk Map
			Finansial	Operasional	Hukum	Reputasi			
R0201-04	Belum terlihat	4	0	2	0	1	0,75	3	Medium
R0201-06	Belum terlihat	1	0	1	1	1	0,75	0,75	Rendah
R0201-11	Belum terlihat	1	0	2	3	3	2	2	Rendah

Tabel 4.22 Hasil respon terhadap risiko pada proses bisnis pemeliharaan jaringan/*hardware*

ID Risiko	Respon Risiko	Pemilik Risiko	Justifikasi	Standar justifikasi respon risiko	Rencana Aksi	
					Sudah	Rencana
R0201-04	*Mitigate*	Helpdesk	Help desk harus langsung menangani permintaan yang masuk dengan cepat.	ISO/IEC 27002:2013 – Clause 7 Human resource security Subclause 7.2 During employment 7.2.1 Management responsibilities		✓
R0201-06	*Transfer*	Teknisi Jaringan/ Hardware	Divisi sistem dan jaringan menerima risiko yang dialami karena masih dalam *risk appetite* nya	-		
R0201-12	*Transfer*	Teknisi Jaringan/ Hardware	Divisi sistem dan jaringan menerima risiko yang dialami karena masih dalam *risk appetite* nya	-		

Tabel 4.23 Peta risiko proses pemeliharaan jaringan/*hardware*



4.4.2.4 Penilaian risiko pada Pengendalian Data dan Informasi

Salah satu tugas dibentuknya Unit Sistem Informasi Manejemn adalah membantu Politeknik Negeri Bali dalam mengendalikan data dan informasi. Gambar proses bisnis pengendalian data dan informasi di Unit Sistem Informasi Manajemen dapat dilihat pada Lampiran 3. Proses pengendalian data dan informasi sedikit unik karena terdiri dari tiga proses yang berbeda, antara lain: penanganan penerimaan mahasiswa baru, penanganan mahasiswa tahun ajaran baru, dan prosedur permintaan data. Masing-masing alur proses akan dijabarkan pada Tabel 4.24 sampai 4.26.

Tabel 4.24 Alur proses Penanganan Penerimaan Mahasiswa Baru

Fase	Alur Proses	Aset TI
1	Helpdesk Unit SIM menerima data calon mahasiswa berupa berita acara	**1. Sumber Daya Manusia** • Helpdesk Unit SIM **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-04 tentang Pengendalian Data dan
2	Helpdesk Unit SIM melakukan input data calon mahasiswa menggunakan program SION	

Fase	Alur Proses	Aset TI
3	Helpdesk Unit SIM menginformasikan kepada bagian penerimaan mahasiswa berupa berita acara	Informasi (Prosedur Penanganan Penerimaan Mahasiswa Baru) **3. Teknologi** • Aplikasi SION (Sistem Informasi Akademik Online Politeknik Negeri Bali) • **Server:** o CPU: Intel Xeon o Memory: 16 GB o Harddisk: 1tb x 4 o OS: Centos 7 x64 o Web server: Apache o Database: MySQL o Aplikasi: Sistem informasi Akademik Online
4	Unit SIM menerima data yang lulus seleksi dalam bentuk berita acara	
5	Helpdesk Unit SIM melakukan pendaftaran kembali menggunakan program SION	
6	Helpdesk Unit SIM melakukan pembagian kelas menggunakan program SION	
7	Helpdesk Unit SIM membuat KRS Mahasiswa Baru menggunakan program SION	
8	Unit SIM melakukan pembuatan absensi kelas yang ditujukan kepada akademik dan jurusan dalam bentuk berita acara	
9	Pengarsipan	

Mengacu pada Tabel 4.24, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses penanganan penerimaan mahasiswa baru di Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi.

Sumber Daya Manusia yang terlibat adalah Helpdesk Unit SIM sebagai tukang input data pada proses penerimaan mahasiswa baru, sebagai sarana untuk tempat keluhan jika terjadi permasalahan terkait proses penanganan mahasiswa baru. Sedangkan proses yang terlibat adalah SOP-USIM-04 tentang Pengendalian Data dan Informasi yang khusus menangani penerimaan mahasiswa baru. Teknologi yang terlibat didalam proses penanganan penerimaan mahasiswa baru adalah Aplikasi Sistem Informasi Akedemik Online Terintegrasi (SION) Politeknik Negeri Bali dan Server yang digunakan untuk menampung data dari SION.

Tabel 4.25 Alur proses penanganan mahasiswa tahun ajaran baru

Fase	Alur Proses	Aset TI

1	Helpdesk Unit SIM melakukan *update* status mahasiswa (Seperti Data Yudisium) kemudian akan diteruskan kedalam bentuk berita acara	**1. Sumber Daya Manusia**
		• Helpdesk Unit SIM
		• Administrator Jurusan
		2. Proses
		• Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-04 tentang Pengendalian Data dan Informasi (Prosedur Penanganan Mahasiswa Tahun Ajaran Baru)
		3. Teknologi
		• Aplikasi SION (Sistem Informasi Akademik Online Politeknik Negeri Bali)
		• **Server:**
		  ○ CPU: Intel Xeon
		  ○ Memory: 16 GB
		  ○ Harddisk: 1tb x 4

2	Helpdesk Unit SIM melakukan *update* status mahasiswa (Contoh: Data Yudisium) yang kemudian akan diteruskan kedalam bentuk berita acara	
3	Helpdesk Unit SIM membuat KRS dan Penjurusan pembuatan absensi perkuliahan didalam program SION	
4	Helpdesk Unit SIM melakukan input absensi	

Fase	Alur Proses	Aset TI
	perkuliahan dan nilai ujian didalam program SION	○ OS: Centos 7 x64 ○ Web server: Apache ○ Database: MySQL ○ Aplikasi: Sistem informasi Akademik Online
5a	Jika tidak terjadi kesalahan dalam input nilai, maka Jurusan dapat melakukan proses rapor mahasiswa dan transkrip menggunakan Program SION	
5b	Jika terjadi kesalahan dalam input nilai, maka Helpdesk Unit SIM menerima permintaan koreksi dari jurusan berupa berita acara dari jurusan	
6b	Helpdesk Unit SIM kemudian mengupdate data nilai mahasiswa berupa berita acara yang kemudian jurusan akan memproses rapor mahasiswa dan transkrip nya menggunakan SION	
7	Pengarsipan	

Mengacu pada Tabel 4.25, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses penanganan mahasiswa tahun ajaran baru di Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Sumber Daya Manusia yang terlibat adalah *Helpdesk* Unit SIM dan Administrator Jurusan. Administrator Jurusan bertugas untuk memproses rapor mahasiswa dan transkrip akademik dari mahasiswa. Helpdesk Unit SIM sebagai tukang input dan *update* data pada proses penanganan tahun ajar baru,

serta sebagai sarana untuk tempat keluhan jika terjadi permasalahan terkait proses penanganan mahasiswa pada tahun ajaran baru. Sedangkan proses yang terlibat adalah SOP-USIM-04 tentang Pengendalian Data dan Informasi yang khusus menangani permasalahan terkait tahun ajar baru. Teknologi yang terlibat didalam proses penanganan penerimaan mahasiswa baru adalah Aplikasi Sistem Informasi Akedemik Online Terintegrasi (SION) Politeknik Negeri Bali dan Server yang digunakan untuk menampung data dari SION.

Tabel 4.26 Alur proses Permintaan Data

Fase	Alur Proses	Aset TI
1	Pemohon melakukan pengisian form permintaan data	**1. Sumber Daya Manusia** • Helpdesk Unit SIM • Pemohon **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-04 tentang Pengendalian Data dan Informasi (Prosedur Permintaan Data) **3. Teknologi** • Aplikasi SION (Sistem Informasi Akademik Online Politeknik Negeri Bali) • Aplikasi lainnya
2	Helpdesk Unit SIM melakukan proses pencarian data melalui program/aplikasi	
3a	Jika data yang dicari sudah sesuai dengan keinginan pemohon, maka Helpdesk Unit SIM akan menyerahkan data dan kemudian akan membuat laporan pengerjaan data	
3b	Jika data yang dicari tidak sesuai, maka Helpdesk Unit SIM melakukan pencarian data kembali sampai sesuai	
4	Pengarsipan	

Mengacu pada Tabel 4.26, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses permintaan data di Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Sumber Daya Manusia yang terlibat adalah Pemohon dan Helpdesk Unit SIM. Helpdesk bertindak

sebagai tukang cari data pada proses pencarian data dan membuat laporan laporan pengerjaan data. Sedangkan proses yang terlibat adalah SOP-USIM-04 tentang Pengendalian Data dan Informasi yang khusus menangani pencarian data. Teknologi yang terlibat didalam proses pencarian data adalah Sistem Informasi Akedemik Online Terintegrasi (SION), dan Sistem informasi lainnya seperti Sistem Informasi Evaluasi Dosen dan Pegawai dll.

Hasil identifikasi risiko menunjukkan terdapat sekurang-kurangnya 33 risiko yang terdapat pada proses bisnis pengendalian data dan informasi. Merujuk pada Tabel 4.27, skenario pertama adalah risiko yang memiliki ID Risiko R0401-06, yang artinya adalah risiko nomor 6 pada SOP No 04 – merujuk pada dokumen *Standard Operational Procedure* Pengendalian Data dan Informasi (SOP-USIM-04) dan angka '1' merujuk pada penanganan mahasiswa tahun ajaran baru di Politeknik Negeri Bali. Unit Sistem Informasi Manajemen Politeknik Negeri Bali. *Timing* pada kolom ke 8 adalah pada saat apa sebuah risiko dapat terjadi. Pada skenario pertama, risiko dapat terjadi pada saat proses Input Data Calon Mahasiswa. Penyebabnya adalah terdapat *bug* pada *script* aplikasi. Aktor / pelaku yang menyebabkan skenario risiko ini berjalan ialah pihak internal ataupun eksternal Politeknik Negeri Bali. Risiko ini termasuk dalam kategori *Malware*. Termasuk dalam *event* (peristiwa) *Destruction* (perusakan) dan aset yang berdampak pada risiko adalah infrastruktur TI. Kontrol yang ada saat ini adalah Sistem di Politeknik Negeri Bali memiliki proteksi aplikasi yang sudah baik dari SQL injection karena telah dilakukan percobaan inputan langsung oleh peneliti. Skenario kedua adalah risiko yang memiliki ID Risiko 0402-05, yang artinya adalah risiko nomor 5 pada SOP No 04 dan angka '2' merujuk pada penanganan mahasiswa tahun ajaran baru di Politeknik Negeri Bali. Skenario risikonya berbunyi "Administrator salah dalam proses input absensi perkuliahan dan nilai ujian sehingga dapat membuat mahasiswa protes dengan hasil yang didapatkan". Risiko ini dapat terjadi pada saat proses input absensi perkuliahan dan nilai ujian sedang berlangsung. Aktor dari skenario risiko ini adalah administrator. Penyebab dari risiko ini adalah keteledoran

administrator dalam proses input absensi perkuliahan dan nilai ujian. Skenario ketiga adalah risiko yang memiliki ID Risiko 0403-35. Kontrol saat ini adalah dengan mengubah kembali proses input. Skenario risikonya berbunyi "PC tidak terinstall anti virus. Sehingga PC dapat terserang virus melalui *flashdisk*/*hard disk* eksternal saat proses pemberian data/file oleh pemohon". Risiko ini dapat terjadi pada saat proses serah terima data sedang berlangsung. Aktor dari skenario risiko ini adalah pihak internal atau eksternal Politeknik Negeri Bali. Penyebab dari risiko ini adalah sebelum meng-copy data/file yang diberikan tidak terlebih dahulu di scan (*removable disk*). Kontrol yang ada saat ini adalah *Personal Computer (PC)* yang digunakan oleh administrator/ *helpdesk* telah dilengkapi auto scan terhadap *removable disk*.

Tabel 4.27 berhubungan dengan Tabel 4.28 dan Tabel 4.29. Merujuk pada Tabel 4.28, risiko dengan ID Risiko R0401-06 memiliki frekuensi/ kemungkinan terjadinya kadang-kadang. Kadang-kadang memiliki nilai '3' dengan penjelasan bahwa kejadian tidak lebih dari 5 kali per tahun. Risiko R0401-06 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0401-06 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya kurang dari Rp.5.000.000,- (kalkulasi secara kasar dengan menimbang waktu yang dihabiskan dalam mengembalikan aplikasi kembali seperti semula, memperbaiki bug yang terdapat pada aplikasi, kompetensi yang dimiliki oleh orang yang bertugas untuk keamanan informasi) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah sangat rendah '1'. Pada aspek operasional, risiko R0401-06 kemungkinan dapat menyebabkan penundaan proses bisnis sampai lebih dari 1 hari kerja. Maka dari itu, dampak yang dihasilkan adalah sangat tinggi '2'. Pada aspek hukum, risiko R0401-06 kemungkinan dapat menyebabkan tuntutan hukum yang berdampak pada kinerja /peforma Unit Sistem Informasi Manajemen. Maka, dampak yang dihasilkan pada aspek hukum adalah sedang '3'. Pada aspek reputasi, risiko R0401-06 kemungkinan dapat menyebabkan pemberitahuan

negative yang dapat menurunkan kepercayaan sebagian besar stakeholder. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sedang ‘3’. Total nilai risiko R0401-06 adalah 5. Sebagai pemilik risiko, Admin Sistem bertanggung jawab untuk mengembalikan sistem ke keadaan semula dengan menghilangkan seluruh script malicious yang diinputkan. Sesuai dengan ISO 27002:2013 *Controls Againts Malware*.

Masih merujuk pada Tabel 4.22, risiko dengan ID Risiko R0402-05 memiliki frekuensi/ kemungkinan terjadinya jarang. Jarang memiliki nilai ‘2’ dengan penjelasan bahwa kejadian lebih dari 2 kali per tahun namun tidak lebih dari dua kali setiap enam bulan. Risiko R0402-05 memiliki 3 dampak, yaitu dampak pada aspek operasional, hukum dan reputasi. Pada aspek operasional, risiko R0402-05 kemungkinan dapat menyebabkan penundaan proses bisnis sampai dengan satu hari kerja. Dapat disimpulkan bahwa aspek operasional dampak yang dihasilkan adalah sangat rendah ‘2’. Risiko R0402-05 memiliki dampak yang mungkin menyebabkanadanya surat peringatan dari individu/instansi dengan dampak relatif kecil. Nilai dampak hukum adalah rendah ‘2’. Pada aspek reputasi, risiko R0402-05 kemungkinan dapat menyebabkan pemberitahuan atau isu negatif dari internal Unit SIM ataupun eksternal (masih dalam ruang lingkup internal Politeknik Negeri Bali) yang dapat menurunkan kepercayaansebagian kecil pemangku kepentingan di Unit SIM itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sedang ‘3’. Total nilai risiko R0402-05 adalah 3,5. Sebagai pemilik risiko, Helpdesk/Admin SION wajib menginputkan kembali dengan benar absensi dan nilai mahasiswa yang sebelumnya salah. Sesuai dengan ISO 27002:2013 *Management Responsibilities*

Risiko dengan ID Risiko R0403-05 memiliki frekuensi/ kemungkinan jarang terjadi. Jarang memiliki nilai ‘1’ dengan penjelasan bahwa kejadian tidak lebih dari 2 kali per tahun namun. Risiko R0403-05 memiliki 2 dampak, yaitu dampak pada aspek operasional dan reputasi. Risiko R0403-05 memiliki dampak pada aspek operasional dengan nilai sangat rendah ‘1’ yang dapat menyebabkan penundaan proses bisnis maksimal setengah hari. Pada

aspek reputasi, risiko R0403-05 kemungkinan dapat menyebabkan pemberitahuan negatif namun tidak mengakibatkan penurunan kepercayaan stakeholder. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan rendah '1'. Total nilai risiko R0403-05 adalah 1. Sebagai pemilik risko, Helpdesk Divisi Sistem Informasi Unit SIM akan melakukan mitigasi pada risiko R0403-05 karena tidak dalam kategori *risk appetite* nya namun masih dalam *Risk Tolerance* nya.

Mengacu pada Tabel 4.30, jumlah risiko yang terdapat pada proses pengendalian data dan informasi berjumlah 33 risiko yang tersebar di 3 kategori, rendah (hijau), sedang (kuning), tinggi (merah). Setelah melalui tahapan analisis risiko, terdapat 11 risiko yang berada pada kategori rendah. Divisi Sistem dan Jaringan tidak perlu melakukan sesuatu untuk merespons risiko karena masih didalam kategori *risk appetite* nya. Terdapat 21 risiko yang berada dikategori sedang, Divisi Sistem dan Jaringan memiliki kebijakan untuk melakukan mitigasi atau *Transfer* risikonya. Terdapat 12 respon aksi yang telah diimplementasikan oleh Divisi Sistem dan Jaringan dan 9 respon aksi masih dalam tahap rencana untuk diimplementasikan. Terdapat 1 risiko yang berada dikategori tinggi, risiko ini harus dihindari oleh Divisi Sistem dan Jaringan jika tidak menginginkan sesuatu yang tidak diinginkan terjadi. Respon aksi masih dalam tahap perencanaan.

Tabel 4.27 Hasil identifikasi *current risk* pada proses bisnis pengendalian data dan informasi

ID Risiko	Skenario Risiko	Kategori Risiko	Aktor	Tipe Ancaman	*Event*	Aset/Sumber daya	*Timing*	Penyebab	Kontrol yang ada saat ini
R0401-06	Hacker memasukkan script malicious sebagai inputan akun/bypass login (SQL Injection)	*Malware*	Internal, Eksternal – Civitas PNB, Masyarakat	*Malicious*	Destruction	IT Infrastructure	Input Data Calon Mahasiswa	Terdapat *bug* pada *script* aplikasi	Sistem di Politeknik Negeri Bali memiliki proteksi aplikasi yang sudah baik dari SQL injection
R0402-05	Administrator salah dalam proses input absensi perkuliahan dan nilai ujian sehingga dapat membuat mahasiswa protes dengan hasil yang didapatkan	*Staff Operation (Human Error)*	Internal – Administrator	*Failure*	Ineffective Execution	Information	Input Absensi Perkuliahan dan Nilai Ujian	Keteledoran administrator dalam proses input absensi perkuliahan dan nilai ujian	Mengedit kembali proses input
R0403-05	PC tidak terinstall anti virus. Sehingga PC dapat terserang virus melalui flashdisk/harddisk eksternal saat proses pemberian data/file oleh pemohon	*Infrastructure Destruction*	Internal, Eksternal – Civitas PNB, Masyarakat	*Malicious*	Destruction	IT Infrastructure	Serah terima Data	Sebelum meng-*copy* data/file yang diberikan tidak terlebih dahulu di scan (*removable disk*)	PC di Administrator telah dilengkapi auto scan terhadap removable disk

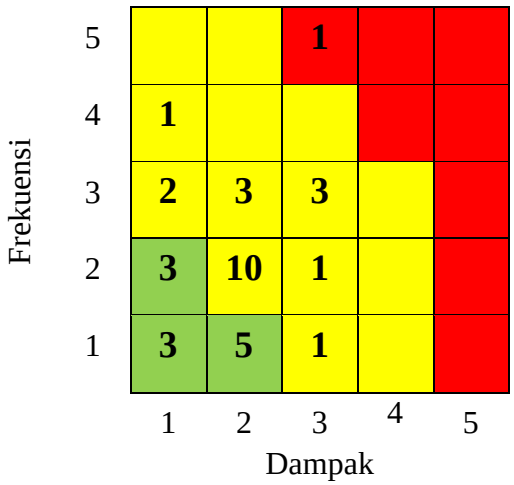
Tabel 4.28 Hasil analisis risiko pada proses bisnis pengendalian data dan informasi

ID Risiko	Residual Risk	Frekuensi	Dampak				Rata-rata dampak	Nilai risiko	Risk Map
			Finansial	Operasional	Hukum	Reputasi			
R0401-06	Terdapat beberapa bug yang terlewat oleh pihak ketiga pengembang software	3	1	2	3	3	2,25	6,75	Medium
R0402-05	Belum terlihat	2	0	2	2	3	1,75	3,5	Medium
R0403-05	Belum terlihat	1	0	1	0	1	0,5	0,5	Rendah

Tabel 4.29 Hasil respon terhadap risiko pada proses bisnis pengendalian data dan informasi

ID Risiko	Respon Risiko	Pemilik Risiko	Justifikasi	Standar justifikasi respon risiko	Respon Aksi	
					Sudah	Rencana
R0401-06	*Mitigate*	Admin Sistem	Mengembalikan sistem ke keadaan semula dengan menghilangkan seluruh script malicious yang diinputkan.	ISO/IEC 27002:2013 – Clause 12 Operations security Subclause 12.2 Protection from malware 12.2.1 Controls against malware		✓
R0402-05	*Mitigate*	Helpdesk/ Admin SION	Menginputkan kembali dengan benar absensi dan nilai mahasiswa yang sebelumnya salah.	ISO/IEC 27002:2013 – Clause 7 Human resource security Subclause 7.2 During employment 7.2.1 Management Responsibilities	✓	
R0403-05	*Transfer*	Helpdesk	Divisi sistem informasi menerima risiko yang dialami karena masih dalam *risk appetite* nya			

Tabel 4.30 Peta risiko proses pengendalian data dan informasi



4.4.2.5 Penilaian risiko pada Pengelolaan *Website* Politeknik

Salah satu tujuan dibentuknya Unit Sistem Informasi Manejemn adalah membantu Politeknik Negeri Bali dalam mengelola *website* politeknik. Gambar proses bisnis pengembangan *software* di Unit Sistem Informasi Manajemen dapat dilihat pada Lampiran 4. Proses pengelolaan website politeknik sedikit unik karena terdiri dari tiga proses yang berbeda, antara lain: *update* web content, pembuatan email baru, pembuatan web baru. Alur proses pada masing-masing prosedur dapat dilihat pada Tabel 4.31 sampai 4.33.

Tabel 4.31 Alur proses *update* Web Content

Fase	Alur Proses	Aset TI
1	Pemohon melakukan pengisian form pengelolaan website	**1. Sumber Daya Manusia** • Helpdesk Unit SIM • Pemohon **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-05
2	Helpdesk Unit SIM menerima data dari pemohon yang dapat berupa data file atau informasi	
3	Helpdesk Unit SIM melakukan proses update. Setelah proses *update* selesai, Helpdesk	

Fase	Alur Proses	Aset TI
	membuat berita acara *update* web content	tentang Pengelolaan Website Politeknik (Prosedur Permintaan Data) **3. Teknologi** • **Website utama Politeknik Negeri Bali** www.pnb.ac.id • **Perangkat Server** o Processor: Intel Xeon o RAM: 16 gb o Harddisk: 1 tb x 4 o OS: Centos 7 , 64 bit o Web Server: Apache o Database: MySQL
4a	Jika data yang telah di *update* sudah sesuai dengan keinginan pemohon, maka Helpdesk Unit SIM akan mem-publish informasi pada website nya	
4b	Jika data yang telah di *update* belum sesuai dengan keinginan pemohon, maka Helpdesk Unit SIM akan melakukan proses *update* kembali sampai sesuai dengan keinginan pemohon	
5	Pengarsipan	

Mengacu pada Tabel 4.31, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses permintaan data di Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Sumber Daya Manusia yang terlibat adalah Pemohon dan Helpdesk Unit SIM. Helpdesk bertindak sebagai tukang cari data pada proses pencarian data dan membuat laporan laporan pengerjaan data. Sedangkan proses yang terlibat adalah SOP-USIM-04 tentang Pengendalian Data dan Informasi yang khusus menangani pencarian data. Teknologi yang terlibat didalam proses pencarian data adalah Sistem Informasi Akedemik Online Terintegrasi (SION), dan Sistem informasi lainnya seperti Sistem Informasi Evaluasi Dosen dan Pegawai dll.

Tabel 4.32 Alur proses pembuatan email Politeknik Negeri Baru

Fase	Alur Proses	Aset TI
1	Pemohon melakukan pengisian form pengajuan pembuatan email Politeknik Negeri Bali	**1. Sumber Daya Manusia** • Divisi Sistem dan Jaringan • Pemohon **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-05 tentang Pengelolaan Website Politeknik (Pembuatan Email PNB) **3. Teknologi** • Google Apps for Education •
2	Divisi Sistem dan Jaringan menerima form pengajuan pembuatan email Politeknik Negeri Bali	
3	Divisi Sistem dan Jaringan membuat email dan kemudian membuat berita acara pembuatan email	
4	Divisi Sistem dan Jaringan menginformasikan nama email ke pemohon	
5	Pengarsipan	

Mengacu pada Tabel 4.32, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses permintaan data di Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Sumber Daya Manusia yang terlibat adalah Pemohon dan *Helpdesk* Unit SIM. Helpdesk bertindak sebagai tukang cari data pada proses pencarian data dan membuat laporan laporan pengerjaan data. Sedangkan proses yang terlibat adalah SOP-USIM-04 tentang Pengendalian Data dan Informasi yang khusus menangani pencarian data. Teknologi yang terlibat didalam proses pencarian data adalah Sistem Informasi Akedemik Online Terintegrasi (SION), dan Sistem informasi lainnya seperti Sistem Informasi Evaluasi Dosen dan Pegawai dll.

Tabel 4.33 Alur proses pembuatan web baru

Fase	Alur Proses	Aset TI
1	Pemohon melakukan pengisian form pembuatan website	**1. Sumber Daya Manusia** • Pemohon • Analyst • DBA • Trainer **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-05 tentang Pengelolaan Website Politeknik (Pembuatan web baru) **3. Teknologi** • **Server** • **Notebook**
2	Analyst mengidentifikasi kebutuhan konten dari website kemudian membuat laporan identifikasi kebutuhan website	
3	DBA kemudian memberikan nama sub domain pada website yang telah dibuat	
4	DBA menyiapkan tempat dan nama di server	
5	Programmer melakukan proses pembuatan website	
6	Trainer melakukan sosialisasi konten kepada pemohon dan membuat berita acara sosialisasi konten	
7a	Jika konten pada web sudah sesuai dengan keinginan pemohon, maka Unit SIM dapat melakukan *update* informasi dan maintenance web	
7b	Jika konten pada web belum sesuai dengan keinginan pemohon, maka website akan dirombak kembali untuk menyesuaikan dengan keinginan pemohon	
8	Pengarsipan	

Mengacu pada Tabel 4.33, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses permintaan data di Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Sumber Daya Manusia yang terlibat adalah Pemohon dan Helpdesk Unit SIM. Helpdesk bertindak sebagai tukang cari data pada proses pencarian data dan membuat laporan laporan pengerjaan data. Sedangkan proses yang terlibat adalah SOP-USIM-04 tentang Pengendalian Data dan Informasi yang khusus menangani pencarian data. Teknologi yang terlibat didalam proses pencarian data adalah Sistem Informasi Akedemik Online Terintegrasi (SION), dan Sistem informasi lainnya seperti Sistem Informasi Evaluasi Dosen dan Pegawai dll.

Hasil identifikasi risiko menunjukkan terdapat sekurang-kurangnya 29 risiko yang terdapat pada proses pengelolaan *website* politeknik. Merujuk pada Tabel 4.34, skenario pertama adalah risiko yang memiliki ID Risiko R0501-07, yang artinya adalah risiko nomor 7 pada SOP No 05 – merujuk pada dokumen *Standard Operational Procedure* Pengelolaan *Website* Politeknik (SOP-USIM-05) dan angka '1' merujuk pada *update* konten website di seluruh Politeknik Negeri Bali. *Timing* pada kolom ke 8 adalah pada saat apa sebuah risiko dapat terjadi. Pada skenario pertama, risiko dapat terjadi pada saat proses *update* web. Penyebabnya adalah keteledoran admin website yang memiliki satu *password* untuk semua aplikasi. Aktor / pelaku yang menyebabkan skenario risiko ini berjalan ialah admin aplikasi itu sendiri. Risiko ini termasuk dalam kategori *Staff Operation (Human Error).* Termasuk dalam *event* (peristiwa) pencurian, perusakan atau pengungkapan informasi dan aset yang berdampak pada risiko adalah infrastruktur TI dan informasi. Skenario ini belum memiliki kontrol yang ada. Skenario kedua adalah risiko yang memiliki ID Risiko 0502-02, yang artinya adalah risiko nomor 2 pada SOP No 05 dan angka '2' merujuk pada pembuatan email baru untuk seluruh pegawai Politeknik Negeri Bali. Skenario risikonya berbunyi "Divisi Sistem Informasi menghilangkan form pengelolaan website yang berisi permohonan pembuatan email, sehingga proses input data penerimaan

siswa baru tidak dapat dilakukan". Risiko ini dapat terjadi pada saat proses menerima form pengajuan pembuatan email baru. Aktor dari skenario risiko ini adalah admin aplikasi. Penyebab dari risiko ini adalah kesibukan yang dimiliki oleh jajaran divisi sistem informasi dalam melakukan respon terhadap permohonan pembuatan email. Skenario ini belum memiliki kontrol yang ada. Skenario ketiga adalah risiko yang memiliki ID Risiko 0503-03, yang artinya adalah risiko nomor 3 pada SOP No 05 dan angka '3' merujuk pada pengembangan website baru untuk Politeknik Negeri Bali. Skenario risikonya berbunyi "Usulan pengembangan website tidak memiliki keuntungan sama sekali.". Risiko ini dapat terjadi pada saat proses identifikasi kebutuhan web content sedang berlangsung. Aktor dari skenario risiko ini adalah salah satu anggota divisi sistem informasi. Penyebab dari risiko ini adalah usulan pengembangan *software* dibuat secara tergesa-gesa. Kontrol saat ini adalah setiap ada usulan pengembangan website akan dirapatkan dengan Ketua Unit SIM.

Tabel 4.34 berhubungan dengan Tabel 4.35 dan Tabel 4.36. Merujuk pada Tabel 4.35, risiko dengan ID Risiko R0501-07 memiliki frekuensi/ kemungkinan terjadinya kadang-kadang. Kadang-kadang memiliki nilai '3' dengan penjelasan bahwa kejadian tidak lebih dari 5 kali per tahun. Risiko R0501-07 memiliki 3 dampak, yaitu dampak pada aspek operasional, hukum dan reputasi. Pada aspek operasional, risiko R0501-07 kemungkinan dapat menyebabkan penundaan proses bisnis sampai setengah hari kerja (menimbang merubah password memerlukan waktu yang sangat singkat karena terdapat fitur *forget password*). Maka dari itu, dampak yang dihasilkan adalah rendah '1'. Pada aspek hukum, risiko R0501-07 kemungkinan dapat menyebabkan adanya permasalahan hukum (misal pelanggaran) namun belum menjadi tuntutan hukum. Maka dari itu, dampak yang dihasilkan adalah sangat rendah '1'. Pada aspek reputasi, risiko R0501-07 kemungkinan dapat menyebabkan terjadinya pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar *stakeholder* di Unit Sistem Informasi Manajemen itu sendiri. Sehingga dapat disimpulkan tingkat

dampak yang dihasilkan sangat rendah ‘1’. Total nilai risiko R0501-07 adalah 2,25. Sebagai pemilik risiko, Admin aplikasi wajib membuat password yang berbeda di masing-masing websitenya. Sesuai dengan standar ISO 27002:2013 tentang *Password management systems*.

Masih merujuk pada Tabel 4.35, risiko dengan ID Risiko R0502-02 memiliki frekuensi/ kemungkinan terjadinya jarang. Jarang memiliki nilai ‘2’ dengan penjelasan bahwa kejadian tidak lebih dari 2 kali per enam bulan. Risiko R0502-02 memiliki 2 dampak, yaitu dampak pada aspek operasional dan reputasi. Pada aspek operasional, risiko R0502-02 kemungkinan dapat menyebabkan penundaan proses bisnis maksimal sampai setengah hari kerja (menimbang admin aplikasi dapat menanyakan kembali isian pada form pembuatan email baru). Dapat disimpulkan bahwa aspek operasional dampak yang dihasilkan adalah sedang ‘1’. Pada aspek reputasi, risiko R0502-02 kemungkinan dapat menyebabkan adanya pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian kecil *stakeholder* di Unit Sistem Informasi Manajemen itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan rendah ‘2’. Total nilai risiko R0502-02 adalah 1,5. Sebagai pemilik risiko, Admin aplikasi menerima risiko R0502-02 karena masih didalam dalam kategori *risk appetite* nya.

Risiko dengan ID Risiko R0503-03 memiliki frekuensi/ kemungkinan kadang-kadang terjadi. Kadang-kadang memiliki nilai ‘3’ dengan penjelasan bahwa kejadian lebih dari 5 kali per tahun. Risiko R0503-03 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0503-03 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya kurang dari Rp.1.000.000,- (kalkulasi secara kasar dengan menimbang beberapa faktor seperti waktu yang dihabiskan dalam membuat dokumen usulan pengembangan website, kompetensi yang dimiliki oleh seorang *project manager*, biaya transportasi dan biaya konsumsi) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah sangat rendah ‘1’. Pada aspek Operasional, risiko R0503-03 kemungkinan dapat menyebabkan penundaan berjalannya proses

bisnis sampai maksimum 3 hari kerja. Sehingga tingkat dampak yang dihasilkan bernilai sedang ‘3’. Pada aspek hukum, risiko R0503-03 memiliki kemungkinan adanya surat peringatan dari individu/instansi dengan dampak relatif kecil. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan rendah ‘2’. Pada aspek reputasi, risiko R0503-03 kemungkinan dapat menyebabkan adanya Terdapat pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar stakeholder. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sedang ‘3’. Total nilai risiko R0503-03 adalah 6,75. Sebagai pemilik risiko, Project Manager harus memperbaiki proposal usulan pengembangan website, agar proposal tersebut memiliki benefit yang akan didapat. Sesuai dengan standar ISO 27002:2013 tentang *Transferable use of assets.*

Mengacu pada Tabel 4.37, jumlah risiko yang terdapat pada proses pengelolaan *website* politeknik berjumlah 28 risiko yang tersebar di 2 kategori, rendah (hijau) dan sedang (kuning). Setelah melalui tahapan analisis risiko, terdapat 13 risiko yang berada pada kategori rendah. Divisi Sistem Informasi tidak perlu melakukan sesuatu untuk merespons risiko karena masih didalam kategori *risk appetite* nya. Terdapat 15 risiko yang berada dikategori sedang, Divisi Sistem Informasi memiliki kebijakan untuk melakukan mitigasi atau *Transfer* risikonya. Terdapat 10 respon aksi telah diimplementasikan di Divisi Sistem Informasi dan 5 respon aksi masih dalam tahap perencanaan.

Tabel 4.34 Hasil identifikasi *current risk* pada proses bisnis pengelolaan *website* politeknik

ID Risiko	Skenario Risiko	Kategori Risiko	Aktor	Tipe Ancaman	*Event*	Aset/Sumber daya	*Timing*	Penyebab	Kontrol yang ada saat ini
R0501-07	Teknisi Divisi Sistem Informasi hanya memiliki satu password untuk semua website dan aplikasi, sehingga jika password tersebar, dengan mudah seorang hacker mengambil/ mengubah data dan informasi	*Staff Operation (Human Error)*	Internal – Admin Aplikasi	*Malicious*	Theft, Destruction, Disclosure	IT Infrastructure, Information	Proses *update* content web	Keteledoran Admin Sistem yang memiliki satu password untuk semua aplikasi	Tidak ada
R0502-02	Divisi Sistem Informasi lambat dalam melakukan respon terhadap permohonan pembuatan email web	*Staff Operation (Human Error)*	Internal – Admin Aplikasi	*Failure*	Ineffective Execution	Information	Menerima Form Pengajuan pembuatan email	Kesibukan yang dimiliki oleh jajaran divisi sistem informasi dalam melakukan respon terhadap permohonan pembuatan email	Tidak ada
R0503-03	Usulan pengembangan website tidak memiliki benefit sama sekali.	*Project Life Cycle Management*	Internal – Divisi Sistem Informasi	External Requirement	*Ineffective Design*	People and Skills	Identifikasi Kebutuhan Web Content	Usulan pengembangan *software* dibuat secara tergesa-gesa	Setia pada usulan pengembangan website akan dirapatkan dengan Ketua Unit SIM

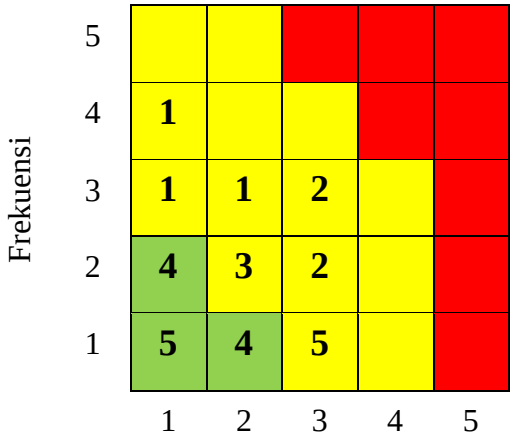
Tabel 4.35 Hasil analisis risiko pada proses bisnis pengelolaan *website* politeknik

ID Risiko	Residual Risk	Frekuensi	Dampak				Rata-rata dampak	Nilai risiko	Risk Map
			Finansial	Operasional	Hukum	Reputasi			
R0501-07	Admin sistem memiliki satu password untuk seluruh aplikasi sistem informasi	3	0	1	1	1	0,75	2,25	Medium
R0502-02	Kesibukan yang dimiliki oleh salah satu personel divisi sistem informasi dalam melakukan respon terhadap pemohonan pembuatan email	2	0	1	0	2	0,75	1,5	Rendah
R0503-03	Belum terlihat	3	1	3	2	3	2,25	6,75	Medium

Tabel 4.36 Hasil respon terhadap risiko pada proses bisnis pengelolaan *website* politeknik

ID Risiko	Respon Risiko	Pemilik Risiko	Justifikasi	Standar justifikasi respon risiko	Respon Aksi	
					Sudah	Belum
R0501-07	*Mitigate*	Admin aplikasi	Membuat password yang berbeda dimasing-masing websitenya	ISO/IEC 27002:2013 – *Clause 9 Access control* *Subclause 9.4 System and application access control* *9.4.3 Password management system*	✓	
R0502-02	*Transfer*	Admin aplikasi	Divisi sistem informasi menerima risiko yang dialami karena masih didalam *risk appetite* nya	-		
R0503-03	*Transfer*	Project Manager	Divisi sistem informasi memperbaiki proposal usulan pengembangan website, agar proposal tersebut memiliki *benefit* yang akan didapat.	ISO/IEC 27002:2013 *Clause 8 – Asset management* *Subclause 8.1 Responsibility of assets* *8.1.3 Transferable use of assets*	✓	

Tabel 4.37 Peta risiko proses pengelolaan *website* politeknik



4.4.2.6 Penilaian risiko pada Penanganan *Disaster Recovery*

Salah satu tugas dibentuknya Unit Sistem Informasi Manejemn adalah membantu Politeknik Negeri Bali dalam melakukan *backup* data baik pada server lokal maupun server *cloud.* Terdapat dua prosedur dalam melakukan penanganan *Disaster Recovery* mengacu pada *Standard Operating Procedure* di Unit SIM, antara lain: penanganan *backup* mingguan pada server lokal dan penanganan *backup* mingguan pada server *cloud.* Gambar proses bisnis Penanganan *Disaster Recovery* di Unit Sistem Informasi Manajemen dapat dilihat pada Lampiran 5. Sedangkan alur proses penanganan *backup* mingguan baik, pada server lokal maupun *cloud* dapat dilihat pada Tabel 4.38 dan Tabel 4.39

Tabel 4.38 Penanganan *backup* mingguan dan bulanan pada server lokal

Fase	Alur Proses	Aset TI
1	Penyediaan server cadangan	**1. Sumber Daya Manusia** • Teknisi Divisi Sstem dan Jaringan **2. Proses**
2	Jika data program hilang atau rusak maka copy file dari *backup* tanpa mematikan sistem	
2a	Jika data program tidak hilang atau rusak, dan jika database	

Fase	Alur Proses	Aset TI
	hilang/rusak maka langkah-langkahnya adalah : 1. Matikan sistem 2. Restore database 3. Hidupkan sistem	• Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-06 tentang Penanganan *Disaster Recovery* (Backup data pada server lokal) **3. Teknologi** • **Software imager cloneZilla** • **Server Utama:** ○ CPU: Intel Xeon ○ Memory: 16 GB ○ Harddisk: 1tb x 4 ○ OS: Centos 7 x64 ○ Web server: Apache ○ Database: MySQL ○ Aplikasi: Sistem informasi Akademik Online • **Server Utama 2:** ○ CPU: Intel Xeon ○ Memory: 4 GB ○ Harddisk: 500 GB ○ OS: Windows Server 2003 std ○ Web server: Apache ○ Database: Oracle ○ Aplikasi: Sistem Informasi Manajemen • **Server Utama 3:**
3	Jika database tidak hilang/rusak dan server tidak dapat dari internal, maka langkah-langkahnya adalah: 1. Ping server 2. Pantau jarak jauh 3. Akses fisik server 4. Cek peralatan yang rusak/putus	
3a	Jika server diterima oleh internal namun sistem tidak dapat diakses, maka langkah penanganannya adalah restart layanan dasar sistem	
4	Jika sistem dapat diakses namun sistem tidak merespon semua proses, maka langkah penanganannya adalah reset paksa dengan tekan tombol reset atau putuskan aliran listrik	
4a	Jika sistem merespon semua proses namun sistem operasi rusak, maka langkah penanganannya adalah mengalihkan sistem ke server	

Fase	Alur Proses	Aset TI
	backup atau restore sistem operasi dari clone (backup bulanan)	○ CPU: Intel Xeon ○ Memory: 4 GB ○ Harddisk: 500 GB ○ OS: Windows Server 2008 Std. ○ Database: MySQL ○ Webserver : Apache ○ Aplikasi: CAT-UKG, PLTI • **Server Feeder Dikti** ○ CPU: Intel Core i5 ○ Memory: 8GB ○ Harddisk: 1 TB ○ OS: Windows 10 ○ Webserver: Apache ○ Database: MySQL • **Server DNS Lokal** ○ CPU: Intel Xeon ○ Memory: 4 GB ○ Harddisk: 500 GB ○ OS: Linux • **Server Backup** ○ CPU: Intel Xeon ○ Memory: 4GB ○ Harddisk: 500 GB
5	Jika sistem operasi tidak rusak namun hardware rusak maka langkah penanganannya adalah: 1. Mengalihkan sistem ke server backup 2. Restore *backup* data terakhir	

Mengacu pada Tabel 4.38, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses penanganan penerimaan mahasiswa baru di Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Sumber Daya Manusia yang terlibat adalah Teknisi Divisi Sistem dan

Jaringan yang ditugaskan untuk melakukan *backup* server mingguan di server lokal Unit SIM. Sedangkan proses yang terlibat adalah SOP-USIM-06 tentang penanganan *Disaster Recovery* yang khusus menangani *backup* server lokal. Teknologi yang terlibat didalam proses *backup* server lokal adalah 3 server utama untuk menampung aplikasi yang terdapat di Politeknik Negeri Bali, 1 Server untuk *Feeder* Dikti, 1 DNS Server lokal dan 1 Server *backup* serta aplikasi untuk *backup* dengan cloneZilla.

Tabel 4.39 Penanganan *backup* mingguan pada server cloud

Fase	Alur Proses	Aset TI
1	Backup virtual machine bulanan	**1. Sumber Daya Manusia** • Teknisi Divisi Sistem dan Jaringan • Telkom **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi Manajemen SOP-USIM-06 tentang Penanganan Distaster Recovery (Prosedur *backup* data mingguan kedalam harddisk eksternal pada server cloud) **3. Teknologi** • **Server *cloud* 1:** o Dibagi menjadi 4 Virtual Machine yang terdiri dari 1 Compute Unit. OS yang digunakan adalah Centos 6.7 (64-bit) Website, Sistem Informasi Akademik dikelompokkan menurut
2	Jika sistem *cloud* tidak dapat diakses, maka langkah penanganannya adalah sebagai berikut: 1. Periksa apakah sistem *cloud* berjalan/tidak; 2. Jika server *cloud* masih berjalan tetapi tidak dapat diakses dari internet, maka koordinasi dengan penyedia layanan cloud; 3. Jika server *cloud* tidak berjalan, maka lakukan restart terhadap virtual machine; 4. Jika restart tidak dapat dilakukan, maka	

Fase	Alur Proses	Aset TI
	nonaktifkan virtual machine dan menjalankan virtual machine *backup* atau minta pihak penyedia layanan *cloud* untuk membuat ulang virtual machine dan melakukan restore	kategorinya masing-masing kemudian di tampung pada virtual machine yang terpisah. • **Server *cloud* 2:** ○ CPU: 4 Compute Unit ○ RAM: 4 GB ○ HDD: 500 GB ○ OS: Ubuntu 16.04.2 LTS (64 bit) ○ Aplikasi yang ditampung: Sistem informasi perpustakaan dan sistem informasi penelitian dan pengembangan masyarakat (Simlitabmas)
2a	Jika sistem *cloud* dapat diakses namun sistem operasi tidak dapat diakses, maka langkah penanganannya adalah restore data langsung ke sistem yang sedang berjalan atau install ulang kemudian lakukan restore data pada sistem baru	

Mengacu pada Tabel 4.39, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses penanganan penerimaan mahasiswa baru di Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Sumber Daya Manusia yang terlibat adalah Teknisi Divisi Sistem dan Jaringan yang ditugaskan untuk melakukan *backup* mingguan pada server *cloud* dan Pihak Telkom sebagai penyedia layanan *cloud.* Sedangkan proses yang terlibat adalah SOP-USIM-06 tentang penanganan *Disaster Recovery* khusus menangani yang khusus menangani *backup* mingguan server *cloud.* Teknologi yang terlibat didalam proses *backup* mingguan server *cloud* adalah 2 server *cloud.* 1 server *cloud* yang terdapat dibagi menjadi 4 Vitual Machine

yang masing-masing memiliki 1 compute unit. Sedangkan server *cloud* lainnya masih utuh memiliki 4 Compute unit.

Hasil identifikasi risiko menunjukkan terdapat sekurang-kurangnya 20 risiko yang terdapat pada proses bisnis Penanganan *Disaster Recovery*. Merujuk pada Tabel 4.40, skenario pertama adalah risiko yang memiliki ID Risiko R0601-01, yang artinya adalah risiko nomor 01 pada SOP No 06 – merujuk pada dokumen *Standard Operational Procedure* Penanganan *Disaster Recovery* (SOP-USIM-06) Unit Sistem Informasi Manajemen Politeknik Negeri Bali. *Timing* pada kolom ke 8 adalah pada saat apa sebuah risiko dapat terjadi. Pada skenario pertama, risiko dapat terjadi di semua fase di proses *backup* server lokal mingguan. Skenario risikonya berbunyi "Terjadinya gap antara keahlian yang dimiliki oleh Teknisi Divisi Sistem dan Jaringan dengan teknologi yang digunakan pada proses *backup* mingguan pada server lokal". Penyebabnya adalah kurangnya pengetahuan yang dimiliki oleh teknisi divisi sistem dan jaringan terkait permasalahan *backup* server lokal mingguan. Aktor / pelaku yang menyebabkan skenario risiko ini berjalan adalah teknisi divisi jaringan/*hardware*. Risiko ini termasuk dalam kategori *IT Expertise and Skills* (keahlian dan keterampilan pada TI). Termasuk dalam *event* (peristiwa) eksekusi yang kurang efektif. Kontrol yang ada saat ini adalah teknisi sudah memiliki kemampuan yang sesuai dengan tugasnya. Skenario kedua adalah risiko yang memiliki ID Risiko 0601-05. Skenario risikonya berbunyi "Sistem Operasi yang digunakan pada server lokal telah berumur dan telah diberhentikan dukungannya oleh pihak penyedia sistem operasi". Risiko ini dapat terjadi pada saat berlangsungnya proses *backup* lokal berlangsung. Aktor dari skenario risiko ini adalah sistem operasi pada server. Penyebab dari risiko ini adalah Microsoft telah memberhentikan support pada Microsoft Server 2003 Rev II sejak tahun 2015. Namun salah satu sistem operasi pada Server masih menggunakan Microsoft Server 2003. Belum ada kontrol yang ada untuk skenario ini. Skenario ketiga adalah risiko yang memiliki ID Risiko 0601-15. Skenario risikonya berbunyi "Penempatan lokasi baik fisik server maupun alat

penunjang seperti power panel ditempatkan pada tempat yang kurang sesuai". Risiko ini dapat terjadi pada saat diluar fase *backup* mingguan berlangsung. Aktor dari skenario risiko ini adalah internal/ eksternal civitas Politeknik Negeri Bali. Penyebab dari risiko ini adalah penempatan lokasi server atau sarana penunjang yang tidak direncanakan sehingga terjadi kejadian yang dilakukan oleh oknum-oknum tertentu. Belum ada kontrol untuk skenario ini.

Tabel 4.40 berhubungan dengan Tabel 4.41 dan Tabel 4.42. Merujuk pada Tabel 4.41, risiko dengan ID Risiko R0601-01 memiliki frekuensi/ kemungkinan terjadinya sangat jarang. Sangat jarang memiliki nilai '1' dengan penjelasan bahwa kejadian tidak lebih dari 2 kali per tahun. Risiko R0601-01 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0601-01 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya kurang dari Rp.4.000.000,- (kalkulasi secara kasar dengan menimbang pendapatan yang dimiliki oleh Teknisi Divisi Jaringan/Server) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah sangat rendah '1'. Pada aspek operasional, risiko R0601-01 kemungkinan dapat menyebabkan penundaan proses bisnis sampai maksimal 3 hari kerja (menimbang pegawai di Unit SIM kecuali administrator adalah tenaga pengajar di Politeknik Negeri Bali sehingga kesibukan dapat menjadi sebuah alasan). Maka dari itu, dampak yang dihasilkan adalah sedang '3'. Risiko R0601-01 pada aspek hukum kemungkinan dapat menyebabkan Terdapat permasalahan hukum (misal pelanggaran) namun belum menjadi tuntutan hukum. Sehingga dapat yang ditimpulkan dapat beriniali kecil '1'. Pada aspek reputasi, risiko R0601-01 kemungkinan dapat menyebabkan pemberitahuan atau isu negatif dari internal Unit SIM ataupun eksternal (masih dalam ruang lingkup internal Politeknik Negeri Bali) yang dapat menurunkan kepercayaan sebagian kecil pemangku kepentingan di Unit SIM itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan rendah '1,75'. Total nilai risiko R0601-01 adalah 1,75. Sebagai pemilik risiko, Admin Server menerima risiko R0601-01 karena masih dalam kategori *risk appetite* nya.

Masih merujuk pada Tabel 4.41, risiko dengan ID Risiko R0601-05 memiliki frekuensi/ kemungkinan terjadinya kadang-kadang. Kadang memiliki nilai ‘3’ dengan penjelasan bahwa kejadian tidak lebih dari 5 kali per tahun. Risiko R0601-05 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0601-05 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya kurang dari Rp.15.000.000,- (kalkulasi secara kasar dengan menimbang beberapa faktor seperti membeli sistem operasi baru untuk server sejumlah server yang dimiliki oleh Unit Sistem Informasi Manajemen) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah sangat rendah ‘1’. Pada aspek operasional, risiko R0601-05 kemungkinan dapat menyebabkan penundaan proses bisnis sampai lebih dari 5 hari kerja. Dapat disimpulkan bahwa aspek operasional dampak yang dihasilkan adalah sedang ‘5’. Risiko R0601-05 memiliki dampak pada aspek hukum dengan nilai sedang ‘3’, yaitu tuntutan hukum yang berdampak pada kinerja /peforma Unit Sistem Informasi Manajemen. Pada aspek reputasi, risiko R0601-05 kemungkinan dapat menyebabkan pemberitahuan atau isu negatif dari internal Unit SIM ataupun eksternal (masih dalam ruang lingkup internal Politeknik Negeri Bali) yang dapat menurunkan kepercayaan pemangku kepentingan di Unit SIM itu sendiri. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan tinggi ‘4’. Total nilai risiko R0601-05 adalah 9. Sebagai pemilik risiko, Admini server wajib mengganti sistem operasi pada server lokal dengan sistem operasi yang baru. Sesuai dengan standar ISO 27002:2013 tentang *Control of Operational software.*

Risiko dengan ID Risiko R0601-15 memiliki frekuensi/ kemungkinan sering terjadi. Sering memiliki nilai ‘4’ dengan penjelasan bahwa kejadian tidak lebih dari 5 kali per tahun. Risiko R0601-15 memiliki 4 dampak, yaitu dampak pada aspek finansial, operasional, hukum dan reputasi. Pada aspek finansial, Risiko R0601-15 kemungkinan dapat menyebabkan kerugian atau pengeluaran biaya kurang lebih Rp.90.000.000,- (kalkulasi secara kasar dengan menimbang beberapa faktor seperti konsletnya power panel,

permasalahan arus listrik pada server, malungsinya server yang dapat menyebabkan kerusakan fisik pada server) sehingga dapat disimpulkan bahwa pada aspek finansial, dampak yang dihasilkan adalah tinggi ‘4’. Risiko R0601-15 memiliki dampak operasional yang kemungkinan dapat menyebabkan terhentinya proses bisnis selama satu hari. Risiko R0601-15 memiliki dampak pada aspek hukum dengan nilai sedang ‘3’. Tuntutan hukum yang berdampak pada kinerja /peforma Unit Sistem Informasi Manajemen. Pada aspek reputasi, risiko R0601-15 kemungkinan dapat menyebabkan adanya pemberitahuan negatif yang dapat menghilangkan kepercayaan stakeholder. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan tinggi ‘4’. Total nilai risiko R0601-15 adalah 13. Sebagai pemilik risiko, Perwakilan Manajemen Unit Sistem Informasi Manajemen wajib memindahkan power panel yang berada di luar gedung Unit SIM ke tempat yang lebih aman. Sesuai dengan standar ISO 27002:2013 tentang *Physical Security Perimeter*

Mengacu pada Tabel 4.43, jumlah risiko yang terdapat pada proses penanganan *Disaster Recovery* berjumlah 20 risiko yang tersebar di 3 kategori, rendah (hijau), sedang (kuning), tinggi (merah). Setelah melalui tahapan analisis risiko, terdapat 8 risiko yang berada pada kategori rendah. Divisi Sistem Informasi tidak perlu melakukan sesuatu untuk merespons risiko karena masih didalam kategori *risk appetite* nya. Terdapat 7 risiko yang berada dikategori sedang, Divisi Sistem Informasi memiliki kebijakan untuk melakukan mitigasi atau *Transfer* risikonya. Terdapat 2 respon aksi telah diimplementasikan oleh Divisi Sistem dan Jaringan untuk risiko kategori sedang. Terdapat 5 risiko yang berada dikategori tinggi, risiko ini harus dihindari oleh Divisi Sistem Informasi jika tidak menginginkan sesuatu yang tidak diinginkan terjadi. Belum ada respon aksi untuk risiko kategori tinggi yang diimplementasikan sama sekali.

Tabel 4.40 Hasil identifikasi *current risk* pada proses bisnis penanganan *disaster recovery*

ID Risiko	Skenario Risiko	Kategori Risiko	Aktor	Tipe Ancaman	*Event*	Aset/Sumber daya	*Timing*	Penyebab	Kontrol yang ada saat ini
R0601-01	Terjadinya gap antara keahlian yang dimiliki oleh Teknisi Divisi Sistem dan Jaringan dengan teknologi yang digunakan pada proses *backup* mingguan pada server lokal	*IT Expertise and Skills*	Internal – *Teknisi Divisi Sistem dan Jaringan*	*Failure*	*Ineffective Executions*	*People and Skills*	Semua fase di proses *backup* server lokal mingguan	Kurangnya pengetahuan yang dimiliki oleh teknisi divisi sistem dan jaringan terkait permasalahan *backup* server lokal mingguan	Teknisi sudah memiliki kemampuan yang sesuai dengan tugasnya
R0601-05	Sistem Operasi yang digunakan pada server lokal telah berumur dan telah diberhentikan dukungannya oleh pihak penyedia sistem operasi	*Software*	Internal – *Sistem operasi pada server*	*Failure*	*Ineffective Design*	*Applications*	Sistem operasi pada salah satu server	Microsoft telah memberhentikan support pada Microsoft Server 2003 Rev II sejak tahun 2015. Namun salah satu sistem operasi pada Server masih menggunakan Microsoft Server 2003	-
R0601-15	Penempatan lokasi baik fisik server maupun alat penunjang seperti power panel ditempatkan pada tempat yang kurang sesuai	*Architechture*	Internal/ Eksternal Civitas PNB	*Failure*	*Destruction*	*Physical Infrastructure*	Diluar fase *backup* mingguan server	Penempatan lokasi server atau sarana penunjang yang tidak direncanakan sehingga terjadi kejadian yang dilakukan oleh oknum-oknum tertentu	

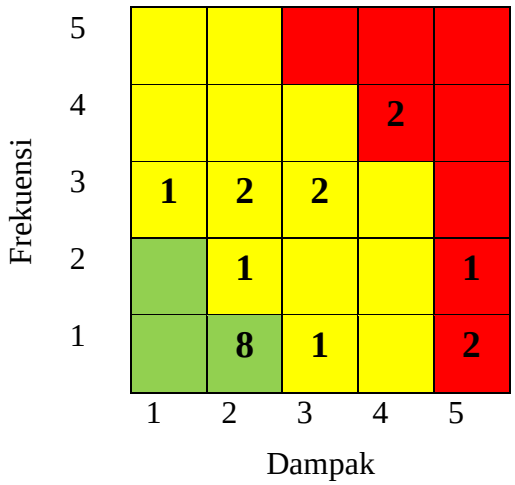
Tabel 4.41 Hasil analisis risiko pada proses bisnis penanganan *disaster recovery*

ID Risiko	Residual Risk	Frekuensi	Dampak				Rata-rata dampak	Nilai risiko	Risk Map
			Finansial	Operasional	Hukum	Reputasi			
R0601-01	Belum terlihat	1	1	3	1	2	1,75	1,75	Rendah
R0601-05	Tidak ada penanganan lebih lanjut mengenai salah satu sistem operasi pada Server masih menggunakan Microsoft Server 2003, padahal Microsoft telah memberhentikan support pada Microsoft Server 2003 Rev II sejak tahun 2014.	3	1	5	3	3	3	9	Medium
R0601-15	Tidak ada penanganan lebih lanjut mengenai ada beberapa kejadian yang dilakukan oleh oknum-oknum tertentu karena penempatan lokasi server atau sarana penenujang yang tidak direncanakan sebelumnya	4	4	2	3	4	3,25	13	High

Tabel 4.42 Hasil respon terhadap risiko pada proses bisnis penanganan *diaster recovery*

ID Risiko	Respon Risiko	Pemilik Risiko	Justifikasi	Standar justifikasi respon risiko	Respon Aksi	
					Sudah	Rencana
R0601-01	*Accept*	Admin *Server*	Divisi sistem informasi menerima risiko yang dialami karena masih didalam *risk appetite* nya			
R0601-05	*Mitigate*	Admin *Server*	Mengganti sistem operasi pada *server* lokal dengan sistem operasi yang baru	ISO/IEC 27002:2013 – *Clause 12 Operations security Subclause 12.5 Control of operational software 12.5.1 Installation of software on operational systems*		✓
R0601-15	*Avoid*	Perwakilan Manajemen	Memindahkan power panel yang berada di luar gedung Unit SIM ke tempat yang lebih aman	ISO/IEC 27002:2013 – *Clause 11 Physical and Environmental Security Subclause 11.1 Secure Areas 11.1.1 Physical security perimeter*		✓

Tabel 4.43 Peta risiko proses *disaster recovery*



4.4.2.7 Penilaian risiko pada Pengelolaan *E-learning*

Tujuan terakhir dibentuknya Unit Sistem Informasi Manejemn adalah membantu Politeknik Negeri Bali dalam mengelola pembelajaran digital (*e-learning*). Gambar proses bisnis pengelolaan *E-learning* di Unit Sistem Informasi Manajemen dapat dilihat pada Lampiran 6. Sedangkan alur proses pengelolaan *E-learning* dapat dilihat pada Tabel 4.44.

Tabel 4.44 Alur proses pengelolaan *E-learning* di Unit SIM

Fase	Alur Proses	Aset TI
1	Administrator Prodi melakukan konfirmasi kurikulum	**1. Sumber Daya Manusia** • Administrator di masing-masing Prodi • Pengelola E-learning • Dosen • Mahasiswa **2. Proses** • Standar Operasional Prosedur Unit Sistem Informasi
2	Administrator Prodi melakukan konfirmasi mata kuliah dan kelas per dosen	
3	Pengelola *E-learning* melakukan *update* mata kuliah	
4	Menempatkan dosen pada mata kuliah tertentu pada program e-learning	

Fase	Alur Proses	Aset TI
5	Dosen melakukan *update* buku ajar digital pada aplikasi e-learning	Manajemen SOP-USIM-07 tentang Pengelolaan E-learning **3. Teknologi** • **Notebook/PC** • **Sistem informasi *E-learning* berbasis Modular Object-Oriented Dynamic Learning Environment (Moodle)** • **Server Cloud** o VMware o CPU: 1 Compute Unit o RAM: 2GB o HDD: 120 GB o OS: Centos 6.7 64 bit
6	Administrator Prodi melakukan pengumpulan buku ajar digital	
7	Pengelola *E-learning* melakukan upload buku ajar digital melalui aplikasi e-learning	
8	(Opsional) Dosen melakukan *update* materi pembelajaran jika ada yang kurang atau penambahan materi baru	
9	Mahasiswa mendownload buku ajar digital	

Mengacu pada Tabel 4.44, terdapat 3 Aset Teknologi Informasi yang terlibat dalam berjalannya proses pengelolaan *E-learning* Politeknik Negeri Bali, yaitu: Sumber Daya Manusia, Proses dan Teknologi. Sumber Daya Manusia yang terlibat adalah Administrator di masing-masing prodi, pengelola e-learning, dosen dan mahasiswa. Administrator bertindak sebagai konfirmator terkait mata kuliah dan kurikulum yang terdapat di prodinya masing-masing dan pengumpulan buku ajar digital. Pengelola *E-learning* bertindak sebagai updater data mata kuliah dan menempatkan dosen di berbagai mata kuliah yang tersedia. Sedangkan proses yang terlibat adalah SOP-USIM-07 tentang Pengelolaan *e-learning.* Teknologi yang terlibat didalam proses pengelolaan *E-learning* adalah Notebook/PC, Sistem *E-learning* dan Server untuk tempat database *E-learning* ditempatkan.

Hasil identifikasi risiko menunjukkan terdapat sekurang-kurangnya 13 risiko yang terdapat pada proses bisnis pengelolaan *e-learning.* Merujuk pada Tabel 4.45, skenario pertama adalah risiko yang memiliki ID Risiko R0701-07, yang artinya adalah risiko nomor 7 pada SOP No 07 – merujuk pada dokumen *Standard Operational Procedure* Pengelolaan *E-learning* (SOP-USIM-07) Unit Sistem Informasi Manajemen Politeknik Negeri Bali. *Timing* pada kolom ke 8 adalah pada saat apa sebuah risiko dapat terjadi. Pada skenario pertama, risiko dapat terjadi pada saat proses *update* mata kuliah per prodi. Penyebabnya adalah Admin *E-learning* kurang teliti atau teledor dalam proses *update* mata kuliah per prodi. Aktor / pelaku yang menyebabkan skenario risiko ini berjalan ialah admin *E-learning* itu sendiri. Risiko ini termasuk dalam kategori *Staff Operation (Human Error)* (ketidak sengajaan atau keteledoran). Termasuk dalam *event* (peristiwa) eksekusi yang tidak efektif dan aset yang berdampak pada risiko adalah *people and skills*. Tidak ada kontrol saat ini karena selama ini Admin *E-learning* hanya mengupdate mata kuliah sesuai yang diberikan oleh Admin Prodi. Skenario kedua adalah risiko yang memiliki ID Risiko R0701-09. Skenario risikonya berbunyi "Dosen salah dalam proses *update* buku ajar digital sehingga dapat menimbulkan kebingungan dalam tahapan berikutnya". Risiko ini dapat terjadi pada saat proses *update* buku ajar digital sedang berlangsung. Aktor dari skenario risiko ini adalah dosen yang meng-inputkan buku ajar digital. Penyebab dari risiko ini adalah dosen kurang teliti atau teledor dalam proses *update* buku ajar digital. Belum ada kontrol untuk skenario ini. Skenario ketiga adalah risiko yang memiliki ID Risiko 0701-13. Skenario risikonya berbunyi "Mahasiswa tidak mengerti cara mengunduh buku ajar, sehingga mahasiswa tidak bisa merasakan manfaat adanya *e-learning*". Risiko ini dapat terjadi pada saat proses mengunduh buku ajar digital sedang berlangsung. Aktor dari skenario risiko ini adalah mahasiswa yang sedang mengakses *e-learning.* Penyebab dari risiko ini adalah kurangnya informasi mengenai tata acara mengunduh buku ajar. Kontrol yang ada saat ini adalah mahasiswa bertanya pada temannya yang fasih menggunakan *e-learning.*

Tabel 4.45 berhubungan dengan Tabel 4.46 dan Tabel 4.47. Merujuk pada Tabel 4.46, risiko dengan ID Risiko R0701-07 memiliki frekuensi/ kemungkinan terjadinya jarang. Jarang memiliki nilai '2' dengan penjelasan bahwa kejadian tidak lebih dari 2 kali tiap enam bulan. Risiko R0701-07 memiliki 3 dampak, yaitu dampak pada aspek operasional, hukum dan reputasi. Pada aspek operasional, risiko R0701-07 kemungkinan dapat menyebabkan penundaan proses bisnis sampai maksimal setengah hari kerja (menimbang admin *E-learning* dapat melakukan *update* kembali mata kuliah pada aplikasi e-learning). Maka dari itu, dampak yang dihasilkan adalah sangat rendah '1'. Pada aspek hukum, Risiko R0701-07 kemungkinan dapat terjadinya permasalahan hukum (misal pelanggaran) namun belum menjadi tuntutan hukum. Sehingga dampak yang dihasilkan adalah sangat kecil '1'. Pada aspek reputasi, Risiko R0701-07 kemungkinan dapat menyebabkan adamya pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar stakeholder. sehingga dapat disimpulkan bahwa pada aspek reputasi, dampak yang dihasilkan adalah sedang '3'. Risiko R0701-07 tidak memiliki dampak pada aspek finansial. Karena risiko R0701-07 murni pada saat proses pengelolaan *E-learning* sedang berlangsung, tidak ada biaya ataupun kontrak yang dapat menjadi permasalahan hukum. Total nilai risiko R0701-07 adalah 2,5. Sebagai pemilik risiko, Admin *E-learning* wajib mengecek kembali mata kuliah per prodi yang telah di *update* sebelum di submit kedalam aplikasi *e-learning.* Sesuai dengan standar ISO 27002:2013 tentang *Operational procedures and responsibilities*.

Masih merujuk pada Tabel 4.46, risiko dengan ID Risiko R0701-09 memiliki frekuensi/ kemungkinan terjadinya jarang. Jarang memiliki nilai '2' dengan penjelasan bahwa kejadian jarang tidak dari 2 kali tia enam bulan. Risiko R0701-09 memiliki 3 dampak, yaitu dampak pada aspek operasional, hukum dan reputasi. Pada aspek operasional, risiko R0701-09 kemungkinan dapat menyebabkan penundaan proses bisnis sampai maksimal setengah hari kerja (menimbang admin *E-learning* dapat melakukan *update* kembali mata kuliah pada aplikasi e-learning). Maka dari itu, dampak yang dihasilkan

adalah sangat rendah ‘1’. Pada aspek hukum, Risiko R0701-09 kemungkinan dapat terjadinya permasalahan hukum (misal pelanggaran) namun belum menjadi tuntutan hukum. Sehingga dampak yang dihasilkan adalah sangat kecil ‘1’. Pada aspek reputasi, Risiko R0701-09 kemungkinan dapat menyebabkan adamya pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar stakeholder. sehingga dapat disimpulkan bahwa pada aspek reputasi, dampak yang dihasilkan adalah sedang ‘3’. Risiko R0701-09 tidak memiliki dampak pada aspek finansial. Karena risiko R0701-09 murni pada saat proses pengelolaan *E-learning* sedang berlangsung, tidak ada biaya ataupun kontrak yang dapat menjadi permasalahan hukum. Total nilai risiko R0701-09 adalah 2,5. Sebagai pemilik risiko, Dosen Pengguna *E-learning* wajib mengecek kembali proses *update* buku ajar digital yang telah di *update* sebelum di submit kedalam aplikasi *e-learning.* Sesuai dengan standar ISO 27002:2013 tentang *Operational procedures and responsibilities*.

Risiko dengan ID Risiko R0701-13 memiliki frekuensi/ kemungkinan kadang-kadang. Kadang-kadang memiliki nilai ‘3’ dengan penjelasan bahwa kejadian tidak lebih dari 5 kali per tahun. Risiko R0701-13 memiliki 2 dampak, yaitu dampak pada aspek operasional dan reputasi. Pada aspek operasional kemungkinan penundaan proses bisnis maksimal sampai dengan setengah hari kerja. Sehingga dampak yang diasilkan bernilai sangat rendah ‘1’. Pada aspek reputasi, risiko R0701-13 kemungkinan dapat menyebabkan adanya pemberitahuan negatif yang dapat menurunkan kepercayaan sebagian besar *stakeholder*. Sehingga dapat disimpulkan tingkat dampak yang dihasilkan sedang ‘3’. Total nilai risiko R0701-13 adalah 3. Sebagai pemilik risiko, Admin *E-learning* wajib menyediakan informasi pada Aplikasi *E-learning* tentang tata cara mengunduh buku ajar. Sesuai dengan standar ISO 27002:2013 tentang *Management Responsibilities*.

Tabel 4.45 Hasil identifikasi *current risk* pada proses bisnis pengelolaan *e-learning*

ID Risiko	Skenario Risiko	Kategori Risiko	Aktor	Tipe Ancaman	*Event*	Aset/ Sumber daya	*Timing*	Penyebab	Kontrol yang ada saat ini
R0701-07	Admin *E-learning* salah dalam proses *update* mata kuliah per prodi sehingga dapat menimbulkan kebingungan dalam tahapan berikutnya	Staff Operation (Human Error)	Admin – E-learning	*Accidental*	Ineffective Execution	People and Skills	Update Mata Kuliah per Prodi	Admin *E-learning* kurang teliti atau teledor dalam proses *update* mata kuliah per prodi	Tidak ada (selama ini Admin *E-learning* hanya mengupdate mata kuliah sesuai yang diberikan oleh Admin Prodi)
R0701-09	Dosen salah dalam proses *update* buku ajar digital sehingga dapat menimbulkan kebingungan dalam tahapan berikutnya	Staff Operation (Human Error)	Internal – Dosen Politeknik Negeri Bali	*Accidental*	Ineffective Execution	People and Skills	Update Buku Ajar Digital	Dosen kurang teliti atau teledor dalam proses *update* buku ajar digital	Tidak ada
R0701-13	Mahasiswa tidak mengerti cara mengunduh buku ajar, sehingga mahasiswa tidak bisa merasakan manfaat adanya e-learning	Staff Operation (Human Error)	Internal - Mahasiswa	*Accidental*	Ineffective Execution	People and Skills	Download Buku Ajar Digital	Kurangnya informasi mengenai tata acara mengunduh buku ajar	Bertanya pada teman yang fasih menggunakan e-learning

Tabel 4.46 Hasil analisis risiko pada proses bisnis pengelolaan *e-learning*

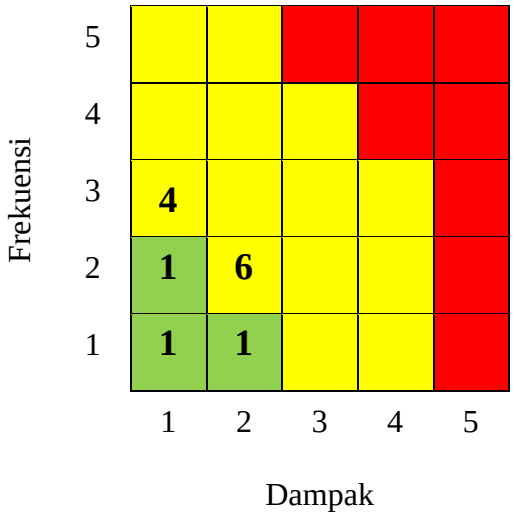
ID Risiko	Residual Risk	Frekuensi	Dampak				Rata-rata dampak	Nilai risiko	Risk Map
			Finansial	Operasional	Hukum	Reputasi			
R0701-07	Kesalahan *update* mata kuliah oleh Admin E-learning	2	0	1	1	3	1,25	2,5	Medium
R0701-09	Belum adanya penanganan khusus mengenai kondisi dimana dosen kurang teliti atau teledor dalam proses *update* buku ajar digital	2	0	1	1	3	1,25	2,5	Medium
R0701-13	Belum terlihat	3	0	1	0	3	1	3	Medium

Tabel 4.47 Hasil respon terhadap risiko pada proses bisnis pengelolaan *E-learning*

ID Risiko	Respon Risiko	Pemilik Risiko	Justifikasi	Standar justifikasi respon risiko	Respon Aksi	
					Sudah	Rencana
R0701-07	*Mitigate*	Admin E-learning	Mengecek kembali mata kuliah per prodi yang telah di *update* sebelum di submit kedalam aplikasi e-learning	ISO/IEC 27002:2013 – *Clause 12 Operations security.* *Subclause 12.1 Operational procedures and responsibilities.* *12.1.1 Documented operating procedures*		✓
R0701-09	*Mitigate*	Dosen Pengguna E-learning	Mengecek kembali proses *update* buku ajar digital yang telah di *update* sebelum di submit kedalam aplikasi e-learning	ISO/IEC 27002:2013 – *Clause 12 Operations security* *Subclause 12.1 Operational procedures and responsibilities* *12.1.1 Documented operating procedures*		✓
R0701-13	*Transfer*	Admin E-learning	Menyediakan informasi pada Aplikasi *E-learning* tentang tata cara mengunduh buku ajar	ISO/IEC 27002:2013 – *Clause 7 Human resource security* *Subclause 7.2 During employment* *7.2.1 Management Responsibilities*		✓

Mengacu pada Tabel 4.48, jumlah risiko yang terdapat pada proses pengelolaan *E-learning* berjumlah 13 risiko yang tersebar di 2 kategori, rendah (hijau) dan sedang (kuning). Setelah melalui tahapan analisis risiko, terdapat 3 risiko yang berada pada kategori rendah. Divisi *E-learning* tidak perlu melakukan sesuatu untuk merespons risiko karena masih didalam kategori *risk appetite* nya. Terdapat 10 risiko yang berada dikategori sedang, Divisi *E-learning* memiliki kebijakan untuk melakukan mitigasi atau *Transfer* risikonya. Terdapat 2 respon aksi yang telah diimplemtasikan pada risiko dalam kategori sedang. Sehingga masih terdapat 8 respon aksi yang masih dalam tahap perencanaan.

Tabel 4.48 Peta risiko proses pengelolaan e-learning



Berdasarkan hasil penilaian risiko dan pemilihan respon terhadap risiko, terdapat 66 risiko yang masih didalam *risk appetite* Unit Sistem Informasi Manajemen, 105 risiko pada risiko kategori sedang. 48 risiko telah memiliki respon aksi dan 57 risiko masih dalam proses perencanaan untuk diimplementasikan. Terdapat total 10 risiko dalam kategori tinggi, dimana 1 risiko telah terimplementasi respon risikonya, sehingga 9 risiko lagi perlu di prioritaskan untuk usulan urutan pengerjaannya. 57 risiko untuk kategori sedang dan 9 risiko untuk kategori tinggi ini selanjutnya akan dilakukan pemrioritasan guna mendapatkan usulan urutan pengerjaan sesuai dengan pembobotan kriteria menggunakan AHP.

Setelah melakukan penilaian risiko, langkah selanjutnya adalah mengelompokkan risiko yang memiliki kategori tinggi (merah) dan risiko yang memiliki kategori sedang (kuning). Risiko dengan kategori tinggi memiliki prioritas pertama untuk ditindaklanjuti, sedangkan risiko dengan kategori sedang memiliki prioritas kedua untuk ditindaklanjuti. Masing-masing kategori risiko akan diprioritaskan dengan menggunakan *Analytical Hierarchy Process* yang akan dibahas pada sub bab 4.8.

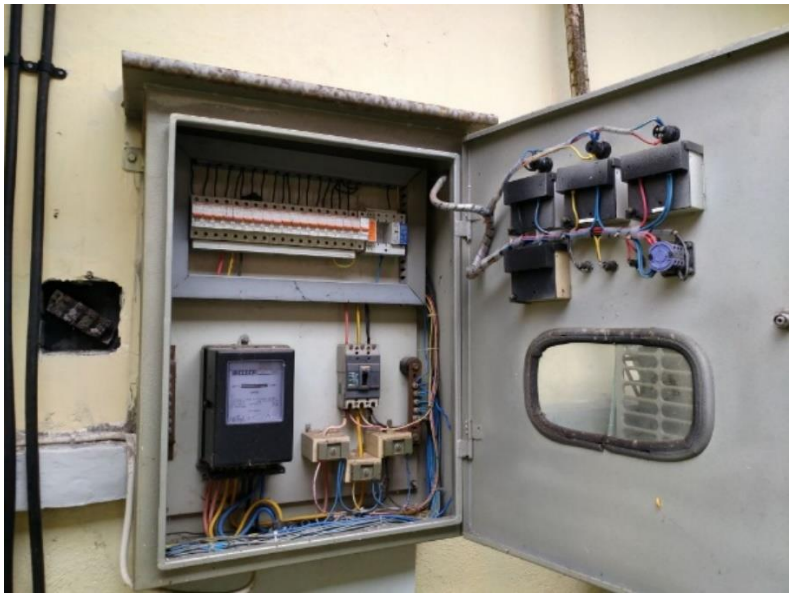
Tabel 4.49 Kriteria pemrioritasan risiko

Nilai risiko	Target Waktu Penanganan	Prioritas
Tinggi	Kurun waktu maksimal sampai 1 tahun anggaran baru.	1 (Tinggi)
Sedang	Kurun waktu maksimal sampai 2 tahun anggaran baru.	2 (Sedang)

(Sumber: berdasarkan hasil *Focus Group Discussion* dengan para petinggi Unit Sistem Informasi Manajemen)

4.5 Hasil Audit di Unit SIM Politeknik Negeri Bali

Mengacu pada COBIT 5 *for Risk*, profil risiko yang komprehensif mencantumkan hasil audit dihasilkan oleh pihak eksternal. Pada kesempatan kali ini, karena Unit Sistem Informasi Manajemen belum pernah melakukan audit yang dilakukan oleh pihak eksternal, maka peneliti bertindak juga sebagai auditor eksternal untuk membantu Unit Sistem Informasi Manajemen dalam merancang profil risiko yang lengkap. Cakupan audit yang dilakukan adalah pengecekan situs ruangan server Politeknik Negeri Bali yang bertempat di Unit Sistem Informasi Manajemen dan kesesuaian jalannya operasional Unit Sistem Informasi dengan standar yang telah dibuat sebelumnya.

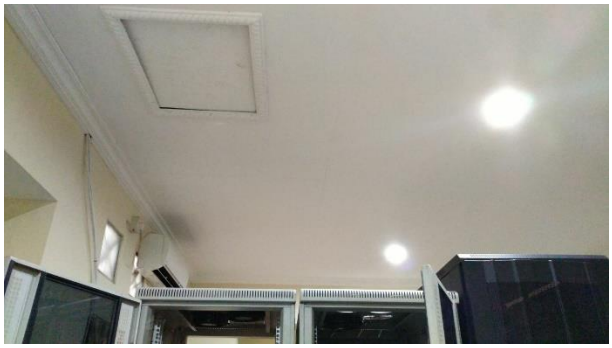


Gambar 4.5 Hasil audit di Unit SIM (1)

Mengacu pada Gambar 4.7, *Power panel* utama yang menjadi sumber daya kelistrikan *server* Politeknik Negeri Bali berada diluar bangunan Unit Sistem Informasi Manajemen. *Power panel* tidak dalam keadaan terkunci karena rumah kunci sudah berkarat dan kunci ya hilang. Berdasarkan wawancara dengan salah satu pegawai di Unit Sistem Informasi, setiap libur semester selalu ada oknum yang tidak bertanggung jawab yang iseng untuk mematikan *power panel*. Sehingga jika server mati – jika baterai di UPS sudah tidak cukup untuk menghidupkan *server* – maka salah satu pegawai Unit Sistem Informasi Manajemen harus pergi ke Politeknik Negeri Bali hanya untuk menghidupkan *power panel* dan mengidupkan kembali *server*.

Gambar 4.6 Hasil Audit di Unit SIM (2)

Mengacu pada Gambar 4.8, *Air Conditioner (AC)* di ruang server berada tepat diatas router Politeknik Negeri Bali. Penempatan router hanya berjarak kurang lebih 10 cm dari tembok. Risiko *AC* bocor merembes ke tembok atau menetes tepat di router akan berdampak pada matinya atau terjadi arus pendek pada router sehingga dapat menyebabkan lumpuhnya operasional Unit Sistem Informasi Manajemen, secara luasnya Politeknik Negeri Bali.



Gambar 4.7 Hasil Audit di Unit SIM (3)

Mengacu pada Gambar 4.9, terdapat *manhole* yang tepat berada diatas rak server Unit Sistem Informasi Manajemen. Risiko perusakan fisik server atau pencurian data langsung dari server sangat mungkin dapat terjadi karena jarak ketinggian antara *manhole* ke rak *server* lebih rendah dari tinggi orang dewasa.

Hasil audit lainnya adalah per tanggal 31 Januari (tanggal dimana penelitian selesai dilakukan di Unit Sistem Informasi Manajemen) ada beberapa operasional

Unit Sistem Informasi Manajemen yang tidak sesuai dengan standar yang tercantum pada dokumen *Standard Operasional Procedure* Unit Sistem Informasi Manajemen, sehingga banyak risiko yang tidak memiliki kontrol yang ada, terutama risiko yang sangat bergantung pada SOP Unit Sistem Informasi Manajemen. Sehingga Unit Sistem Informasi Manajemen kurang lebih memiliki 90 lebih risiko yang harus di mitigasi/ *Transfer* dan kurang lebih 7 risiko yang harus dihindari.

4.6 Hasil Kuesioner Pembobotan Kriteria untuk Respon Risiko

Berdasarkan hasil pemetaan responden menggunakan RACI *Chart* yang terdapat pada Tabel 4.1 dan penyesuaian dengan personil yang ada di Politeknik Negeri Bali, didapat sejumlah 7 responden (Tabel 4.2). Namun, karena adanya rangkap jabatan (Pembantu Direktur 1 merangkap sebagai Ketua PPID dan Sekretaris SIM merangkap sebagai Ketua Divisi Sistem Informasi), maka responden yang dijadikan pakar dalam pengisian kuesioner AHP hanya berjumlah 5 orang (Tabel 4.3). Metode yang digunakan dalam pengisian kuesioner AHP adalah kualitatif (memberikan langsung kuesioner kepada pakar dan kemudian diisi oleh masing-masing pakar, dimana peneliti hanya menjawab pertanyaan jika pakar kurang mengerti). Contoh lampiran kuesioner AHP dapat dilihat pada Lampiran 7.

4.6.1 Hasil kuesioner dengan pakar Ketua Unit SIM

Berdasarkan hasil kuesioner AHP dengan pakar Ketua Unit SIM pada Tabel 4.8. Pakar lebih mementingkan keuntungan (efektivitas) daripada kriteria lainnya (Keuntungan 3 kali lebih penting dari Anggaran dan Durasi Proyek). Pakar memiliki asumsi bahwa setiap proyek yang akan direncanakan akan ditimbang terlebih dahulu keuntungannya, jika memiliki banyak keuntungan dalam hal efektivitas (bukan profit karena PNB merupakan instansi non-profit). Kemudian setelah itu anggaran dan durasi proyek mengikuti. Durasi proyek dan anggaran memiliki bobot yang sama pentingnya dikarenakan durasi proyek dan anggaran akan selalu mengikuti jika proposal proyek yang memiliki keuntungan terkait efisiensi ini tembus.

Tabel 4.50 Hasil kuesioner pembobotan kriteria AHP dengan pakar Ketua Unit SIM

Pembobotan Kriteria			
Kriteria	Durasi Proyek	Anggaran	Keuntungan (Efektivitas)
Durasi Proyek	1	1,00	0,333333333
Anggaran	1	1	0,33
Keuntungan (Efektivitas)	3	3	1
Total	5	5	1,666666667

4.6.2 Hasil kuesioner dengan pakar Pembantu Direktur I

Berdasarkan hasil kuesioner AHP dengan pakar Pembantu Direktur I pada Tabel 4.11. Pakar lebih mementingkan keuntungan (efektivitas) daripada kriteria lainnya (Keuntungan 3 kali lebih penting dari Durasi Proyek dan 7 kali lebih penting dari Anggaran). Pakar memiliki asumsi bahwa setiap proyek yang akan direncanakan akan ditimbang terlebih dahulu keuntungannya, jika memiliki banyak keuntungan dalam hal efektivitas. Kemudian pakar melihat durasi atau lama waktu pengerjaan, kemudian anggaran untuk proyek akan menyesuaikan. Kriteria anggaran memiliki nilai yang paling kecil disebabkan anggaran untuk sebuah proyek akan selalu ada untuk tiap tahun kedepannya.

Tabel 4.51 Hasil kuesioner pembobotan kriteria AHP dengan pakar Pembantu Direktur I

Pembobotan Kriteria			
Kriteria	Durasi Proyek	Anggaran	Keuntungan (Efektivitas)
Durasi Proyek	1	5,00	0,33
Anggaran	0,2	1	0,14
Keuntungan (Efektivitas)	3	7	1
Total	4,2	13	1,476190476

4.6.3 Hasil kuesioner dengan pakar Sekretaris Unit SIM

Berdasarkan hasil kuesioner AHP dengan pakar Sekretaris Unit SIM pada Tabel 4.14. Pakar lebih mementingkan Anggaran daripada kriteria lainnya (Anggaran 3 kali lebih penting dari Durasi Proyek dan 3 kali lebih penting dari Keuntungan). Pakar memiliki asumsi bahwa setiap proyek yang akan direncanakan akan di cek terlebih dahulu anggarannya. Jika anggaran tersedia, baru proposal perencanaan proyek dapat dibuat. Kriteria Durasi Proyek dengan Keuntungan memiliki nilai kepentingan yang sama karena lama waktu pengerjaan proyek dan keuntungan baru dapat dibuat setelah anggaran tersedia.

Tabel 4.52 Hasil kuesioner pembobotan kriteria AHP dengan pakar Sekretaris Unit SIM

Pembobotan Kriteria			
Kriteria	Durasi Proyek	Anggaran	Keuntungan (Efektivitas)
Durasi Proyek	1	0,33	1,00
Anggaran	3	1	3,00
Keuntungan (Efektivitas)	1	0,333333333	1
Total	5	1,666666667	5

4.6.4 Hasil kuesioner dengan pakar Kadiv Sistem dan Jaringan

Berdasarkan hasil kuesioner AHP dengan pakar Kepala Divisi Sistem dan Jaringan pada Tabel 4.17. Pakar lebih mementingkan keuntungan (efektivitas) daripada kriteria lainnya (Keuntungan 5 kali lebih penting dari Durasi Proyek dan 2 kali lebih penting dari Anggaran). Pakar memiliki asumsi bahwa setiap proyek yang akan direncanakan akan ditimbang terlebih dahulu keuntungannya, jika memiliki banyak keuntungan dalam hal efektivitas. Kemudian pakar melihat anggaran yang tersedia, memungkinkan atau tidak, yang terakhir adalah durasi proyek atau lama waktu pengerjaannya.

Tabel 4.53 Hasil kuesioner pembobotan kriteria AHP dengan pakar Kepala Divisi Sistem dan Jaringan

Pembobotan Kriteria			
Kriteria	Durasi Proyek	Anggaran	Keuntungan (Efektivitas)
Durasi Proyek	1	0,33	0,20
Anggaran	3	1	0,50
Keuntungan (Efektivitas)	5	2	1
Total	9	3,333333333	1,7

4.6.5 Hasil kuesioner dengan pakar Kadiv *E-learning*

Berdasarkan hasil kuesioner AHP dengan pakar Kepala Divisi *E-learning* pada Tabel 4.20. Pakar lebih mementingkan keuntungan (efektivitas) daripada kriteria lainnya (Keuntungan 7 kali lebih penting dari Durasi Proyek dan 3 kali lebih penting dari Anggaran). Pakar memiliki asumsi bahwa setiap proyek yang akan direncanakan akan ditimbang terlebih dahulu keuntungannya, jika memiliki banyak keuntungan dalam hal efektivitas. Kemudian pakar melihat anggaran yang tersedia, memungkinkan atau tidak, yang terakhir adalah durasi proyek atau lama waktu pengerjaannya.

Tabel 4.54 Hasil kuesioner pembobotan kriteria AHP dengan pakar Kepala Divisi *E-learning*

Pembobotan Kriteria			
Kriteria	Durasi Proyek	Anggaran	Keuntungan (Efektivitas)
Durasi Proyek	1	0,20	0,14
Anggaran	5	1	0,33
Keuntungan (Efektivitas)	7	3	1
Total	13	4,2	1,476190476

4.7 Rata-rata penilaian pakar menggunakan *Geometric Mean Method*

Pakar yang menjadi responden berjumlah 5 orang, oleh karena itu penilaian kusisoner AHP harus dilakukan rata-rata untuk mendapatkan satu penilaian yang komprehensif, salah satunya dengan menggunakan *Weighted Geometric Mean Method*. Berdasarkan observasi yang dilakukan di Politeknik Negeri Bali, dengan menimbang faktor budaya, jabatan, *expertise* dan kebiasaan dalam memutuskan hal yang sifatnya lebih ke arah teknologi informasi, pakar-pakar dapat disimpulkan memiliki bobot yang sama. Maka dari itu dapat disimpulkan bahwa rata-rata penilaian pakar menggunakan metode *Geometric Mean*.

$$E_1 = \begin{bmatrix} 1 & 1 & \frac{1}{3} \\ 1 & 1 & \frac{1}{3} \\ 3 & 0 & 1 \end{bmatrix}, E_2 = \begin{bmatrix} 1 & 1 & \frac{1}{3} \\ 1 & 1 & \frac{1}{3} \\ 3 & 0 & 1 \end{bmatrix}, E_3 = \begin{bmatrix} 1 & 1 & \frac{1}{3} \\ 1 & 1 & \frac{1}{3} \\ 3 & 0 & 1 \end{bmatrix},$$

$$E_4 = \begin{bmatrix} 1 & 1 & 1/3 \\ 1 & 1 & \frac{1}{3} \\ 3 & 0 & 1 \end{bmatrix}, E_5 = \begin{bmatrix} 1 & 1 & 1/3 \\ 1 & 1 & \frac{1}{3} \\ 3 & 0 & 1 \end{bmatrix} \quad (4.1)$$

$$\bar{E} = \begin{bmatrix} \sqrt[5]{E_{1_{1,1}} * E_{2_{1,1}} * \dots * E_{5_{1,1}}} & \cdots & \sqrt[5]{E_{1_{3,1}} * E_{2_{3,1}} * \dots * E_{5_{3,1}}} \\ \vdots & \ddots & \vdots \\ \sqrt[5]{E_{1_{1,3}} * E_{2_{1,3}} * \dots * E_{5_{1,3}}} & \cdots & \sqrt[5]{E_{1_{3,3}} * E_{2_{3,3}} * \dots * E_{5_{3,3}}} \end{bmatrix} \quad (4.2)$$

Keterangan:

$E_{1,2,\dots,5} = Pakar$

$\bar{E} = Geometric\ Mean\ dari\ tiap - tiap\ pakar$

Mengacu psada rumus 4.1, $E_{1,2,\dots,5}$ merupakan penilaian masing-masing pakar yang sudah dibuat dalam bentuk matriks sederhana. E_1 merupakan penilaian dari Ketua Unit SIM, E_2 merupakan penilaian dari Pembantu Direktur I, E_3 merupakan penilaian dari Sekretaris Unit SIM, E_4 merupakan penilaian dari

Ketua Divisi Sistem dan Jaringan dan E_5 merupakan penilaian dari Ketua Divisi *e-learning.*

Rata-rata penilaian setiap pakar menggunakan metode *Geometric Mean* yang dapat dilihat pada rumus 4.2. Matriks yang dihasilkan adalah matriks ber-ordo 3x3. Nilai pada baris 1 kolom 1 dari rata-rata menggunakan Geometric Mean didapat dari akar pangkat lima (karena jumlah pakar adalah 5) dari hasil perkalian penilaian pakar pertama pada baris 1 kolom 1 sampai penilaian pakar kelima pada baris 1 kolom 1. Untuk kolom 2 baris 2 sampai kolom 5 baris 5 menggunakan cara yang sama. Hasil kalkulasi pembobotan kriteria AHP kelima pakar dapat dilihat pada Tabel 4.23.

Tabel 4.55 Hasil kalkulasi pembobotan kriteria AHP kelima pakar menggunakan *WGMM*

Pembobotan Kriteria			
GM Kriteria	GM1	GM2	GM3
GM1	1,00	0,64	0,32
GM2	1,55	1,00	0,47
GM3	3,16	2,11	1,00
Total	5,71166388	3,75617978	1,790006775

Mengacu pada hasil kalkulasi pembobotan kriteria AHP kelima pakar menggunakan *Geometric Mean* pada Tabel 4.23, setelah melakukan normalisasi dengan menggunakan tahapan yang sama seperti AHP didapat hasil bahwa bobot keuntungan yang paling tinggi diantara bobot kriteria lainnya. Tabel 4.24 merupakan bobot hasil dari kelima pakar menggunakan *Geometric Mean*.

Tabel 4.56 Hasil pemrioritasan bobot pakar menggunakan *GMM*

Bobot GM1 (Durasi Proyek)	Bobot GM2 (Anggaran)	Bobot GM3 (Keuntungan)
17,45%	26,75%	55,80%

Berdasarkan hasil kalkulasi pembobotan kriteria AHP kelima pakar menggunakan *Geometric Mean*, Rasio konsistensi kseputusan (CR) bernilai 0,02%, yang bermakna rata-rata keputusan yang diambil oleh kelima pakar konsisten. Rata-rata keputusan yang diambil oleh kelima pakar konsisten karena nilai CR dibawah 10%. Tabel 4.25 menunjukkan persentase konsistensi rata-rata kelima pakar menggunakan *Geometric Mean*.

Tabel 4.57 Persentase konsistensi pembobotan pakar menggunakan *GMM*

Lambda Max	CI	CR	Konsisten?	Persentase
3,000183173	9,15867E-05	0,0001579	Konsisten	0,02%

Berdasarkan hasil dari pembobotan kriteria menggunakan Geometric Mean AHP, prosentase bobot terbesar merupakan keuntungan (55,80%). Keuntungan disini bermakna efisiensi. Semua proyek yang akan direalisasikan di Unit Sistem Informasi Manajemen harus memiliki keuntungan berupa efisiensi, sesuai dengan tujuan operasional Unit Sistem Informasi Manajemen yaitu Meningkatkan Efisiensi Operasional. Dituangkan didalam dokumen Rencana Strategis Sistem Informasi/Teknologi Informasi Unit SIM (Astawa et al., 2015).

4.8 Hasil usulan pemrioritasan respon terhadap risiko TI menggunakan AHP

Setelah mendapatkan bobot menggunakan *Geometric Mean Method*, langkah selanjutnya adalah memprioritaskan respon terhadap risiko TI. Pemrioritasan dilakukan dengan menyebarkan kuesioner kepada 7 pemangku jabatan atau 5 orang sesuai dengan responden yang telah ditentukan pada Tabel 4.3. Mengacu pada COBIT 5 *for Risk*, pemrioritasan respon terhadap risiko dibagi menjadi 2 kelompok, risiko yang berada pada kategori tinggi dan risiko dengan kategori sedang. Risiko dengan kategori tinggi memiliki prioritas terlebih dahulu.

Peneliti menggunakan beberapa sub kriteria yang berhubungan dengan kriteria yang digunakan pada kuisioner AHP. Guna menilai seberapa penting masing-masing respon risiko yang didapat dari beberapa sumber yang dapat dilihat pada Tabel 4.58.

Tabel 4.58 Kriteria penilaian untuk masing-masing respon risiko

Kriteria	Sub Kriteria	Sumber Referensi
Durasi	1. s/d 1 minggu pengerjaan	Hasil kesepakatan target waktu penanganan risiko (Tabel 4.49)
	2. s/d 1 bulan pengerjaan	
	3. s/d 6 bulan pengerjaan	
	4. s/d 1 tahun anggaran	
	5. s/d 2 tahun anggaran	
Anggaran	1. ≤ Rp.24.000.000,-	Hasil penetapan parameter dampak finansial (Tabel 4.5)
	2. ≤ Rp.48.000.000,-	
	3. ≤ 72.000.000,-	
	4. ≤ 96.000.000,-	
	5. ≥ Rp. 96.000.000,-	
Keuntungan	1. Membuka keran peluang pekerjaan baru di Unit Sistem Informasi Manajemen	(Karasakal & Aker, 2017)
	2. Output dari proyek memiliki dampak positif bagi kehidupan sosial mahasiswa/I di Politeknik Negeri Bali	
	3. Output dari proyek memiliki dampak positif bagi kehidupan sosial Pegawai dan Manajemen Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen	
	4. Output dari proyek memiliki dampak positif bagi lingkungan sekitar Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen	
	5. Proyek dapat menciptakan kolaborasi antara industri dengan pihak Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen	
	6. Mempercepat jalannya proses bisnis yang ada di Politeknik Negeri Bali	(Oztaysi, 2014)

Mengacu pada Tabel 4.58, sebuah respon risiko dianggap sangat prioritas, apabila memenuhi keenam sub kriteria dari kriteria Keuntungan. Memiliki nominal anggaran yang dikeluarkan lebih dari Rp.96.000.000,- dan durasi pengerjaannya sampai dengan 2 tahun anggaran. Asumsi, jika sebuah proyek memiliki total anggaran Rp.200.000.000,- dengan durasi pengerjaan 2 tahun dan memiliki poin-

poin keuntungan seperti di Tabel 4.58, tentunya proyek tersebut akan diprioritaskan utama, karena pengerjaan proyek tersebut harus dicicil sampai waktunya selesai. Total poin yang mungkin didapat untuk kriteria Keuntungan sebanyak 6 poin, Anggaran sebanyak 5 poin, dan Durasi sebanyak 5 poin.

4.8.1 Hasil usulan pemrioritasan respon pada risiko dengan kategori tinggi

Terdapat total 9 risiko yang termasuk dalam kategori "Tinggi". Menggunakan kriteria penilaian pada Tabel 4.58 untuk masing-masing respon terhadap risiko, Tabel 4.59 menampilkan hasil usulan kalkulasi pemrioritasan respon risiko dengan kategori tinggi.

Tabel 4.59 Hasil usulan kalkulasi pemrioritasan respon risiko kategori tinggi

Kode Respon Risiko	Kriteria AHP			Total Bobot
	17,45%	26,75%	55,80%	
	Durasi	Anggaran	Keuntungan	
R0202-18	2	2	3	2,558031836
R0303-10	2	2	3	2,558031836
R0303-13	3	2	5	3,848574311
R0401-10	1	2	3	2,383553033
R0601-03	4	5	6	5,383553033
R0601-04	4	4	4	4
R0601-12	4	4	4	4
R0601-14	4	4	4	4
R0601-15	4	4	4	4

Merujuk pada Tabel 4.59, Total Bobot untuk masing-masing respon terhadap risiko dihasilkan melalui kalkulasi sebagai berikut:

$$Total\ Bobot\ RA_n\ = \\ Nilai\ RA_n\ terhadap\ Durasi\ x\ Bobot\ Durasi + \\ Nilai\ RA_n\ terhadap\ Durasi\ x\ Bobot\ Durasi + \\ Nilai\ RA_n\ terhadap\ Durasi\ x\ Bobot\ Durasi \quad (4.3)$$

Contoh, respon risiko dengan kode R0202-18 memiliki Total Bobot 2,558. Didapat melalui hasil kalkulasi sebagai berikut:

$$Total\ Bobot\ RA_1 = 2x17{,}45\% + 2x26{,}75\% + 3x55{,}80\% = 2{,}558 \qquad 4.4$$

Setelah mendapatkan Total Bobot untuk masing-masing respon risiko, langkah selanjutnya adalah mengurut respon risiko berdasarkan Total Bobot yang paling tinggi ke rendah. Tabel 4.60 merupakan hasil pengurutan respon risiko dengan kategori tinggi. Didapat respon risiko dengan kode R0601-03 menempati nomor urut 1 dengan Total Bobot 5,384. Menempati nomor urut 2 sampai 9 bukan berarti respon risiko tidak dilaksanakan, respon risiko tetap dilaksanakan setelah respon risiko dengan kode R0601-03 dilaksanakan terlebih dahulu, dan sebelum respon risiko dengan kategori sedang dilaksanakan.

Tabel 4.60 Hasil pengurutan respon risiko kategori tinggi

Urutan	Kode Respon Risiko	Total Bobot
1	R0601-03	5,383553033
2	R0601-04	4
3	R0601-12	4
4	R0601-14	4
5	R0601-15	4
6	R0303-13	3,848574311
7	R0202-18	2,558031836
8	R0303-10	2,558031836
9	R0401-10	2,383553033

Kode respon risiko digunakan pada pembahasan hasil pemrioritasan respon terhadap risiko untuk mempermudah peneliti dalam membahas satu persatu tahapan yang dilaksanakan. Deskripsi respon risiko yang sebenarnya dapat dilihat pada Tabel 4.61.

Tabel 4.61 Deskripsi respon risiko kategori tinggi

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
R0601-03	Memiliki server *backup* yang spesifikasinya sesuai dengan server yang digunakan saat ini	Penanganan Disaster Recovery
R0601-04	Perancangan Water Hydrant didekat Gedung Unit SIM	Penanganan Disaster Recovery
R0601-12	Melakukan perbaikan di plafon ruang server dengan menggunakan plafon anti api, menutup manhole di ruang server	Penanganan Disaster Recovery
R0601-14	Mengganti gagang pintu akses ke ruang server dengan sensor fingerprint	Penanganan Disaster Recovery
R0601-15	Memindahkan power panel yang berada di luar gedung Unit SIM ke tempat yang lebih aman	Penanganan Disaster Recovery
R0303-13	Project Manager serta Ketua SIM harus memeriksa dan menganalisis terlebih dahulu dana yang tersedia beserta benefit yang ditawarkan oleh suatu proyek sebelum meloloskan proyek tersebut	Pengembangan Software
R0202-18	Melakukan pengecekkan kembali ke proposal pengadaan alat yang memiliki cost yang tidak sesuai dengan benefit yang diperoleh	Pengembangan Jaringan dan Hardware
R0303-10	Fungsi Verifikator harus memberikan arahan/briefing kepada para personelnya untuk membiasakan selalu mengecek kembali anggaran yang sudah disediakan satu tahunnya untuk pengembangan *software*.	Pengembangan Software
R0401-10	Membackup (Fotokopi) data pendaftaran mahasiswa ke tempat lain yang aman dan	Pengendalian Data dan Informasi

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
	memiliki kemungkinan untuk hilang yang kecil.	

4.8.2 Hasil usulan pemrioritasan respon pada risiko dengan kategori sedang

Terdapat total 57 respon risiko yang termasuk dalam kategori "Sedang". Menggunakan kriteria penilaian pada Tabel 4.58 untuk masing-masing respon terhadap risiko, Tabel 4.62 menampilkan 10 besar hasil kalkulasi usulan pemrioritasan respon risiko dengan kategori sedang. Hasil usulan kalkulasi keseluruhan pemrioritasan respon risiko dengan kategori sedang dapat dilihat pada Lampiran 8.A.

Tabel 4.62 Hasil kalkulasi pemrioritasan respon risiko kategori sedang

Kode Respon Risiko	Kriteria AHP			Total Bobot
	17,45%	26,75%	55,80%	
	Durasi	Anggaran	Keuntungan	
R0201-03	1	2	1	1,267489361
R0201-04	1	1	3	2,116063672
R0201-05	1	1	4	2,674095508
R0201-07	2	2	4	3,116063672
R0201-14	1	1	3	2,116063672
R0201-18	1	2	3	2,383553033
R0201-19	1	2	4	2,941584869
R0201-20	1	2	3	2,383553033
R0202-16	2	2	3	2,558031836
R0202-17	1	1	3	2,116063672

Merujuk pada Tabel 4.58, Total Bobot untuk masing-masing respon terhadap risiko dihasilkan melalui kalkulasi sebagai berikut:

$$Total\ Bobot\ RA_n\ = \\ Nilai\ RA_n\ terhadap\ Durasi\ x\ Bobot\ Durasi + \\ Nilai\ RA_n\ terhadap\ Durasi\ x\ Bobot\ Durasi + \\ Nilai\ RA_n\ terhadap\ Durasi\ x\ Bobot\ Durasi \quad 4.3$$

Contoh, respon risiko dengan kode R0201-03 memiliki Total Bobot 1,267. Didapat melalui hasil kalkulasi sebagai berikut:

$$Total\ Bobot\ RA_1 = 1x17{,}45\% + 2x26{,}75\% + 1x55{,}80\% = 1{,}267 \quad 4.4$$

Setelah mendapatkan *Total Bobot* untuk masing-masing respon risiko, langkah selanjutnya adalah mengurut respon risiko berdasarkan Total Bobot yang paling tinggi ke rendah. Tabel 4.62 merupakan hasil pengurutan respon risiko dengan kategori sedang. Hasil pengurutan respon risiko kategori sedang secara keseluruhan dapat dilihat pada Lampiran 8.B. Didapat respon risiko dengan kode R0503-09 menempati nomor urut 1 dengan Total Bobot 3,674. Menempati nomor urut 2 sampai 55 bukan berarti respon risiko tidak dilaksanakan, respon risiko tetap dilaksanakan setelah respon risiko dengan kode R0503-09 dilaksanakan terlebih dahulu, dan setelah respon risiko dengan kategori tinggi dilaksanakan.

Tabel 4.63 Hasil pengurutan respon risiko kategori sedang (10 besar)

Urutan	Kode Respon Risiko	Total Bobot
1	R0503-09	3,674095508
2	R0503-10	3,674095508
3	R0303-29	3,499616705
4	R0303-30	3,499616705
5	R0303-35	3,290542475
6	R0601-05	3,20907423
7	R0201-07	3,116063672
8	R0202-24	3,116063672
9	R0201-19	2,941584869
10	R0303-05	2,941584869

Kode respon risiko digunakan pada pembahasan hasil pemrioritasan respon terhadap risiko untuk mempermudah peneliti dalam membahas satu persatu tahapan yang dilaksanakan. Deskripsi respon risiko yang sebenarnya (10 besar) dapat dilihat pada Tabel 4.63. Deskripsi respon risiko yang lengkap dapat dilihat pada Lampiran 8.C.

Tabel 4.64 Deskripsi respon risiko kategori sedang (10 besar)

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
R0503-09	Programmer yang kurang paham dalam mengerti kemauan pemohon tersebut harus meminta bantuan kepada personel yang telah berpengalaman dalam memahami kemauan pemohon.	Pengelolaan Website Politeknik – Pembuatan Website Baru
R0503-10	Programmer dapat berdiskusi dengan divisi sistem informasi dalam pengembangan website, agar website yang dikembangkan tidak terlalu sulit secara teknis.	Pengelolaan Website Politeknik – Pembuatan Website Baru
R0303-29	Project Manager harus segera menyusun rencana untuk dilakukannya user *Transfer*ance test.	Pengembangan Software
R0303-30	Melakukan *Transfer*ance test dengan merilis versi beta agar dapat dilihat bug atau kelengkapannya terlebih dahulu sebelum dirilis versi finalnya	Pengembangan Software
R0303-35	Divisi sistem informasi bekerja sama dengan ketua SIM dalam merancang ketetapan untuk wajibnya dilakukan evaluasi terhadap dampak dari penggunaan aplikasi dari sisi pengguna	Pengembangan Software

R0601-05	Mengganti sistem operasi pada server lokal dengan sistem operasi yang baru	Penanganan Disaster Recovery
R0201-07	Unit SIM diharapkan menggalakkan prosedur keselamatan kerja dengan mengedukasi divisinya agar selalu mengutamakan keselamatan dalam bekerja	Pemeliharaan Jaringan/ Hardware
R0202-24	Menggalakkan prosedur keselamatan kerja dengan mengedukasi divisinya agar selalu mengutamakan keselamatan dalam bekerja	Pengembangan Jaringan/ Hardware
R0201-19	Unit help desk harus dapat mendistribusikan kembali surat pemberitahuan tersebut dengan baik ke pihak pelapor.	Pemeliharaan Jaringan/ Hardware
R0303-05	Divisi sistem informasi bekerja sama dengan ketua SIM dalam membuat usulan proposal pengembangan software	Pengembangan Software

BAB V
SIMPULAN DAN SARAN

Bab ini menjelaskan mengenai kesimpulan dan saran penelitian dengan judul "Audit Manajemen Risiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5".

5.1 Simpulan

Kesimpulan yang didapat menjawab rumusan masalah yang telah disebutkan pada BAB I Pendahuluan. Berdasarkan pembahasan yang dilakukan dari proses penetapan konteks manajemen risiko, identifikasi, penilaian, dan strategi dalam melakukan respon terhadap risiko, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Proses integrasi antara ISO 31000:2009 (Standar Manajemen Risiko secara umum) dengan APO 12 COBIT 5 *for Risk* dilakukan dengan cara melakukan pencocokan (*matching*). Didapat bahwa fase *Risk Identification* pada ISO 31000 memiliki kesamaan aktivitas dengan *Management Practice* APO12.01 *Collect Data* di COBIT 5 *for Risk.* Fase *Risk Analysis* dan *Risk Evaluation* pada ISO 31000 memiliki kesamaan aktivitas dengan *Management Practice* APO12.02 *Analyze the Risk* di COBIT 5 *for Risk.* Fase *Risk Treatment* pada ISO 31000 memiliki kesamaan aktivitas dengan *Management Practice* APO12.06 Respond to Risk. Namun ada fase di ISO 31000 yang tidak dimiliki oleh APO 12 COBIT 5 *for Risk*, yaitu fase *Establish the Context.* Sehingga kesimpulan yang didapat menjadikan proses integrasi antara ISO 31000, COBIT 5 *for Risk* menjadi metode penelitian untuk melakukan audit manajemen risiko teknologi informasi pada perguran tinggi Menggunakan Kerangka Kerja COBIT 5. Penelitian ini juga menggunakan alat bantu pengambilan keputusan AHP. AHP digunakan pada pemrioritasan respon terhadap aksi risiko. karena jika terdapat banyak risiko yang perlu respon didalam kategori yang sama

(Tinggi atau Medium), pemrioritasan dapat dilakukan dengan menggunakan AHP.

2. Proses penilaian risiko TI mengambil lokasi penelitian di Politeknik Negeri Bali khususnya di Unit Sistem Informasi Manajemen (Unit SIM). Berdasarkan wawancara awal dan telaah dokumen bisnis organisasi, Unit SIM belum pernah melakukan penilaian risiko. Cakupan penilaian risiko pada penelitian ini sesuai dengan fase penetapan konteks adalah pada proses bisnis yang terdapat di Unit Sistem Informasi Manajemen. Proses bisnis tersebut telah tertuang didalam masing-masing *Standard Operating Procedure*, antara lain: Pemeliharaan Jaringan dan *Hardware*, Pengembangan Jaringan dan *Hardware*, Pengembangan *Software*, Pengendalian Data dan Informasi, Pengembangan Website Politeknik, Penanganan *Disaster Recovery* dan Pengelolaan *e-learning.* Terdapat 181 *risk scenario* (skenario risiko) yang telah diidentifikasi didalam 7 proses bisnis di Unit Sistem Informasi Manajemen, antara lain: 20 skenario risiko pada proses pemeliharaan jaringan dan hardware, 31 skenario risiko pada proses pengembangan jaringan dan hardware, 36 skenario risiko pada proses pengembangan software, 33 skenario risiko pada proses pengendalian data dan informasi, 28 skenario risiko pada proses pengembangan website politeknik, 20 skenario risiko pada proses penanganan *Disaster Recovery* dan 13 skenario risiko pada proses pengelolaan *e-learning.*
3. Berdasarkan kompilasi hasil analisis risiko, didapat 66 risiko yang masih didalam *risk appetite* (risiko yang masih dapat diterima) dari Unit SIM. 105 risiko yang masuk kedalam batas toleransi risiko (harus dilakukan penanganan risiko) di Unit SIM dan 10 risiko yang diluar batas kapasitas risiko yang dimiliki oleh Unit SIM (sifatnya kritikal dan harus dihindari). Risiko yang paling tinggi ada 2, yaitu Risiko terkait tempat yang digunakan sebagai ruang server lokal memiliki keamanan yang kurang baik disebabkan oleh terbatasnya lahan yang dimiliki oleh Politeknik Negeri Bali dengan nilai risiko sebesar 13 (tinggi) dan Penempatan baik fisik server maupun alat penunjang seperti power panel yang ditempatkan pada tempat yang

kurang sesuai yang disebabkan oleh kurangnya perencanaan oleh Manajemen Politeknik Negeri Bali dengan nilai risiko sebesar 13 (tinggi). Selanjutnya, terdapat beberapa acuan yang digunakan untuk melakukan respon terhadap risiko, antara lain: ISO 27001 tentang Persyaratan kebutuhan dalam mengelola keamanan informasi, ISO 27002 tentang panduan organisasi dalam mempraktikkan standar keamanan informasi dan mengelola keamanan informasi sesuai dengan ISO 27001, OHSAS 18002 terkait panduan terkait sistem standar keamanan dan keselamatan kerja dan ISO 25040 terkait *Systems and software Quality Requirements and Evaluations*. Jumlah respon yang telah dilaksanakan pada risiko yang memiliki kategori tinggi dan sedang berturut-turut adalah 1 risiko dan 48 risiko. Sehingga masih terdapat 9 respon terhadap risiko untuk kategori tinggi dan 57 respon terhadap risiko untuk kategori sedang yang belum dilakukan/ masih direncanakan.

4. Pemrioritasan respon terhadap risiko TI dikelompokkan menjadi 2 kategori, yaitu kategori nilai risiko "Tinggi" dan "Sedang". Nilai risiko "*Tinggi*" memiliki prioritas yang didahulukan. Target waktu penanganan nya adalah sampai 1 tahun anggaran baru. Hasil yang didapat untuk kategori nilai risiko "*Tinggi*", Memiliki server *backup* yang spesifikasinya sesuai dengan server yang digunakan saat ini memiliki prioritas tertinggi dari 9 risiko yang memiliki kategori nilai risiko "*Tinggi*". Sedangkan nilai risiko "Sedang" memiliki target waktu penanganan sampai 2 tahun anggaran baru. *Programmer* yang kurang paham dalam mengerti kemauan pemohon tersebut harus meminta bantuan kepada personel yang telah berpengalaman dalam memahami kemauan pemohon memiliki prioritas tertinggi dari 57 respon risiko yang memiliki kategori risiko "*Sedang*". Kriteria yang digunakan pada AHP adalah Keuntungan (Efisiensi), Anggaran (Total Pengeluaran) dan Durasi (Lama waktu pengerjaan) dari sebuah respon risiko.
5. Sebuah profil risiko yang lengkap mengacu pada literatur COBIT 5 *for Risk* harus berisi *Risk Register* (rangkuman data, deskripsi risiko (skenario risiko) dan hasil analisis risiko), Perencanaan aksi terhadap risiko, Indikator

Dampak dan Frekuensi dari terjadinya sebuah risiko dan Hasil temuan yang dilakukan oleh pihak eksternal (Eksternal Audit). Secara komprehensif, profil risiko TI pada Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen dapat dilihat pada Lampiran 9.

5.2 Saran

Saran yang dapat digunakan oleh Politeknik Negeri Bali khususnya Unit Sistem Informasi Manajemen (Unit SIM) maupun peneliti selanjutnya yang tertarik pada tema manajemen risiko TI sebagai berikut:

1. Kerangka kerja gabungan dari ISO 31000 dan COBIT 5 *for Risk* dapat dipertimbangkan untuk digunakan bagi Unit Sistem Informasi Manajemen untuk melakukan pengelolaan risiko TI. Dengan tidak lupa menggunakan AHP sebagai salah satu cara pengambilan keputusan jika terdapat banyak risiko yang memiliki kategori nilai risiko yang sama. Kriteria yang digunakan adalah Keuntungan, Durasi dan Anggaran.
2. Penilaian risiko yang dilakukan baru sebatas pada operasional yang terdapat di Unit Sistem Informasi Manajemen. Peneliti menyadari bahwa kemampuan teknis yang dimiliki peneliti masih sangat rendah sehingga penelitian selanjutnya dapat menyempurnakan profil risiko TI di Politeknik Negeri Bali khususnya Unit SIM melalui penilaian risiko bawaan dari masing-masing aset TI terutama pada teknologi yang digunakan.

DAFTAR PUSTAKA

Aczél, J., & Saaty, T. L. (1983). Procedures for synthesizing ratio judgements. *Journal of Mathematical Psychology*, *27*(1), 93–102. https://doi.org/10.1016/0022-2496(83)90028-7

Adhitya, Y. (2016). *Audit Tata Kelola Teknologi Informasi Untuk Mengetahui Implementasi Prinsip GCG (Good Corporate Governance) Dalam Kaitannya Dengan Pengaturan dan Pemeliharaan Kerangka Tata Kelola serta Pengelolaan Solusi TI (Studi Kasus: PT. ANGKASA PURA I (PERSERO) Caba*. *MMT ITS*. Insitut Teknologi Sepuluh Nopember.

Aisha, L., Wardani, K., Ramadani, L., Industri, F. R., Operation, S., Transition, S., & Publik, S. (2016). Perancangan Tata Kelola Manajemen Layanan Teknologi Informasi Menggunakan ITIL V3 Domain Service Transition dan Service Operation di Pemerintahan Kota Bandung, *3*(2), 3272–3278.

Alshazly, A. A., Elfatatry, A. M., & Abougabal, M. S. (2014). Detecting defects in *software* requirements specification. *Alexandria Engineering Journal*, *53*(3), 513–527. https://doi.org/10.1016/j.aej.2014.06.001

Anandita, E. F. (2014). *Penyusunan Mekanisme Kerja Identifikasi Risiko TI pada Departemen Pengelolaan Sistem Informasi Bank Indonesia dengan Penggabungan Best Practice*.

Andriyanto, F., Sihwi, S. W., & Anggrainingsih, R. (2015). SISTEM PAKAR UNTUK RISK ASSESSMENT KEAMANAN SISTEM INFORMASI BERDASARKAN ISO 27002 DENGAN METODE FORWARD CHAINING, 1–10.

Astawa, P. M., Suja, I. K., Dewi, K. C., Sentana, I. W. B., Ciptayani, P. I., Suwintara, I. K., & Manuaba, I. B. P. (2015). *Rencana Strategis Sistem Informasi/ Teknologi Informasi*.

BSI Standards Publication. (2013). ISO/ IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls.

Calder, A., & Watkins, S. (2015). *IT Governance 6th edition: An International Guide to Data Security and ISO27001/27002* (6th ed.). KoganPage.

Cline, P. B. (2004). The Merging of *Risk Analysis* and Adventure Education. *Wilderness Risk Management*.

Departemen Komunikasi dan Informatika Republik Indonesia. (2007). *Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional*.

Diharja, A. A. (2013). Audit Tata Kelola Sistem Kepegawaian Dinas Tenaga Kerja dan Transmigrasi Provinsi Sumatera Selatan dengan Kerangka KerjaCOBIT Versi 5. *Thesis Universitas Bina Darma*, *Palembang*, *5*, 1–9. https://doi.org/Di Indonesia, rumah sakit sebagai salah satu bagian sistem pelayanan kesehatan secara garis besar memberikan pelayanan untuk masyarakat berupa pelayanan kesehatan

Edi Nugroho, L. (2009). *Penerapan Teknologi Informasi di Perguruan Tinggi*.

International Organization for Standardization. (2009). *ISO 31000 Risk Management-Principles and guidelines*.

ISACA. (2009). The Risk IT Framework.

ISACA. (2012). *COBIT 5: Enabling Processes*. Retrieved from www.isaca.org

ISACA. (2013a). *COBIT ® Process Assessment Model (PAM): Using COBIT ® 5*.

ISACA. (2013b). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Retrieved from www.isaca.org

ISACA. (2013c). *COBIT 5 for Risk*. ISACA.

IT Governance Institute. (2003). *Board Birefing on IT Governance* (2nd ed.). IT Governance Institute.

Jakaria, D. A., Dirgahayu, R. T., & Hendrik. (2013). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, *15 Juni*, 37–42.

Kaban, I. E. (2009). Tata kelola teknologi informasi - (IT GOVERNANCE). *CommIT*, *3*(C), 1–5.

Karasakal, E., & Aker, P. (2017). A multicriteria sorting approach based on data envelopment analysis for R&D project selection problem. *Omega*, *73*, 79–92. https://doi.org/10.1016/j.omega.2016.12.006

KBBI. (2017). Kata risiko atau resiko yg baku menurut Kamus Besar Bahasa Indonesia (KBBI) Online. Retrieved September 16, 2017, from

https://kbbi.web.id/risiko-atau-resiko

Kerzner, H. (2006). *Project management-A Systems Approach to Planning, Scheduling, and Controlling*. *Project Management* (8th ed.). John Wiley & Sons, Inc. https://doi.org/10.1108/eb006384

Muthmainnah. (2015). Model Perancangan Tata Kelola Teknologi Informasi (It Governance) Pada Proses Pengelolaan Data Di Universitas Malikussaleh Lhokseumawe. *Techsi*.

OGC. (2007). *The Official Introduction to the ITIL Service Lifecycle*. *The Stationery Office* (Vol. 69). https://doi.org/citeulike-article-id:2420971

OGC. (2011a). *ITIL - Continual Service Improvement*. https://doi.org/10.1007/978-0-387-77393-3_6

OGC. (2011b). *ITIL - Service Design*. *The Stationery Office*. https://doi.org/10.1007/978-0-387-77393-3

OGC. (2011c). *ITIL - Service Operation*. *The Stationery Office*. https://doi.org/10.1007/978-0-387-77393-3

OGC. (2011d). *ITIL - Service Strategy*.

OGC. (2011e). *ITIL Service Transition*. *The Stationery Office*. https://doi.org/10.1186/1472-6947-11-76

Oztaysi, B. (2014). A decision model for information technology selection using AHP integrated TOPSIS-Grey: The case of content management systems. *Knowledge-Based Systems*, *70*, 44–54. https://doi.org/10.1016/j.knosys.2014.02.010

Politeknik Negeri Bali. (2010). *Rencana Induk Pembangunan Politeknik Negeri Bali 2011-2025*.

Politeknik Negeri Bali. (2017a). *Borang - Akreditasi Institusi Politeknik Negeri Bali*.

Politeknik Negeri Bali. (2017b). Sejarah Politeknik Negeri Bali. Retrieved August 12, 2017, from http://pnb.ac.id/poltekbali/sejarah_pnb

Politeknik Negeri Bali. (2017c). Seputar Sistem Penerimaan Mahasiswa Baru Politeknik Negeri Bali. Retrieved August 12, 2017, from http://www.pnb.ac.id/berita/detail/61/seputar-sistem-penerimaan-mahasiswa-baru-politeknik-negeri-bali

Politeknik Negeri Bali. (2017d). Struktur Organisasi Politeknik Negeri Bali. Retrieved August 12, 2017, from http://pnb.ac.id/poltekbali/struktur_organisasi

Putri, C. U. (2017). *Penilaian Risiko Proses Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5 pada Helpdesk Subdirektorat Layanan Teknologi dan Sistem Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember*.

Risk and Insurance Management Society. (2012). Exploring Risk Appetite and Tolerance. *RIMS Executive Report*, (Apr), 12.

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1*(1), 83. https://doi.org/10.1504/IJSSCI.2008.017590

Saaty, T. L., & Tran, L. T. (2007). On the invalidity of fuzzifying numerical judgments in the Analytic Hierarchy Process. *Mathematical and Computer Modelling*, *46*(7–8), 962–975. https://doi.org/10.1016/j.mcm.2007.03.022

Samaptoaji, S. (2014). *Evalasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah (Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri)*. Universitas Indonesia.

Stirn, L. Z., & Groselj, P. (2010). Multiple Critera Methods with Focus on Analytic Hierarchy Process and Group Decision Making. *Croatian Operational Research Review (Crorr), Vol 1*, *1*, 2–11.

Suhardi, S. N., & Baskoro, F. (2011). EVALUASI KEMATANGAN PENGELOLAAN TEKNOLOGI INFORMASI PADA PT . MULTI GARMENJAYA SURABAYA. *Prosiding Seminar Nasional Manajemen Teknologi XIII*.

Suyatna, R. (2015). Penggunaan Aplikasi Sumber Terbuka Moodle dalam Diklat Berbasis Elektornik, 3–4.

The Institute of Chartered Accountans of India. (2010). *Information Systems Control and Audit*.

Xu, Z. (2000). On consistency of the weighted geometric mean complex judgment matric in AHP. *European Journal of Operational Research*, *126*, 126(3), 683–687.

BIODATA PENULIS

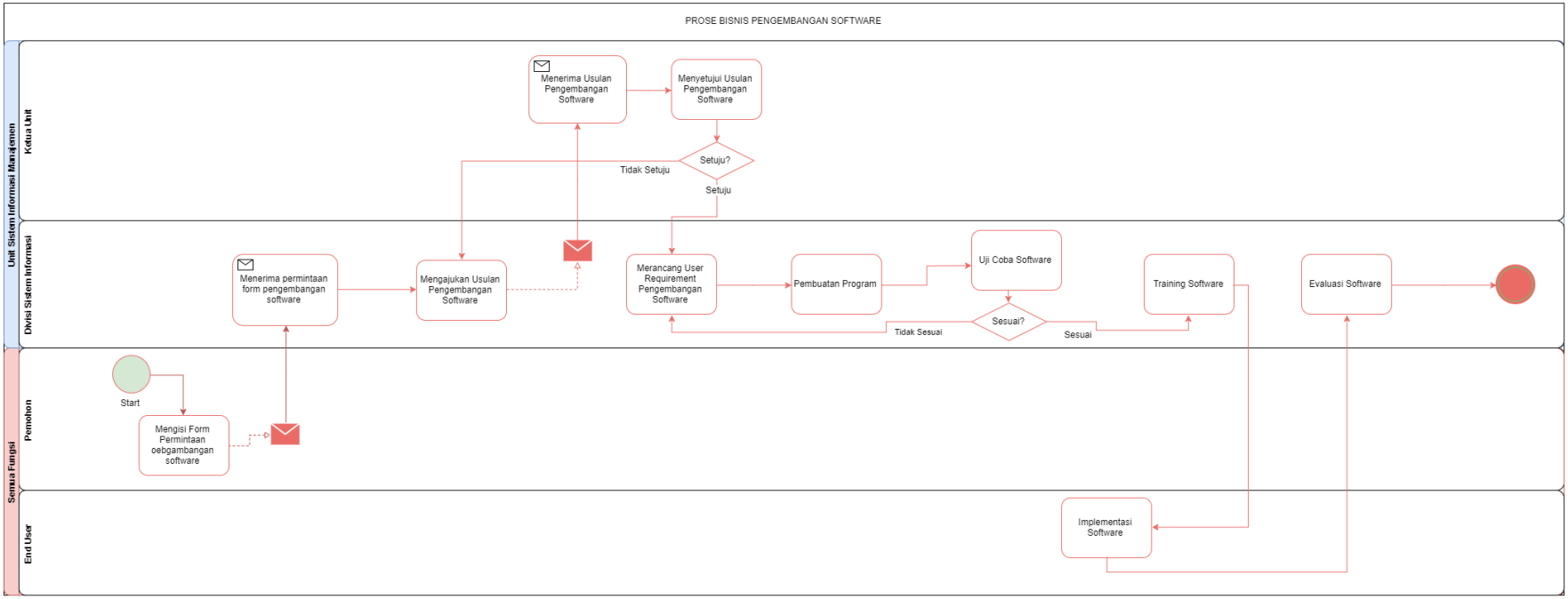
Penulis bernama lengkap Ida Bagus Gde Kresna Adi Jaya, yang biasa dipanggil Gusde. Dilahirkan di Kota Denpasar, 15 September 1993. Riwayat pendidikan penulis dimulai pada tahun 1999 di SD Saraswati 1 Denpasar dan lulus pada tahun 2005. Penulis melanjutkan pendidikan di SMP Negeri 4 Denpasar pada tahun 2005 dan lulus pada tahun 2008. Penulis melanjutkan jenjang pendidikan menengah atas di SMA Negeri 1 Denpasar di tahun 2008 dan lulus di tahun 2011. Tahun 2011, Penulis melanjutkan pendidikan bangku kuliah di Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Udayana. Penulis lulus di tahun 2015 dan memperoleh gelar *Sarjana Teknologi Informasi (S.TI)*. Tahun 2016, Penulis merantau ke Kota Surabaya untuk melanjutkan pendidikan magister di Magister Manajemen Teknologi, Konsentrasi Manajemen Teknologi Informasi, Institut Teknologi Sepuluh Nopember. Penulis terdaftar sebagai mahasiswa dengan NRP 09211650053009. Saat ini (21 Mei 2018), Penulis telah menyelesaikan Tesis dengan judul "Audit Manajemen Risiko Teknologi Informasi pada Perguran Tinggi Menggunakan Kerangka Kerja COBIT 5" sebagai salah satu syarat kelulusan guna memperoleh gelar *Magister Manajemen Teknologi (M.MT.)*

Penulis dapat dihubungi melalui e-mail : kresnaadijaya@gmail.com

(Halaman ini sengaja dikosongkan)

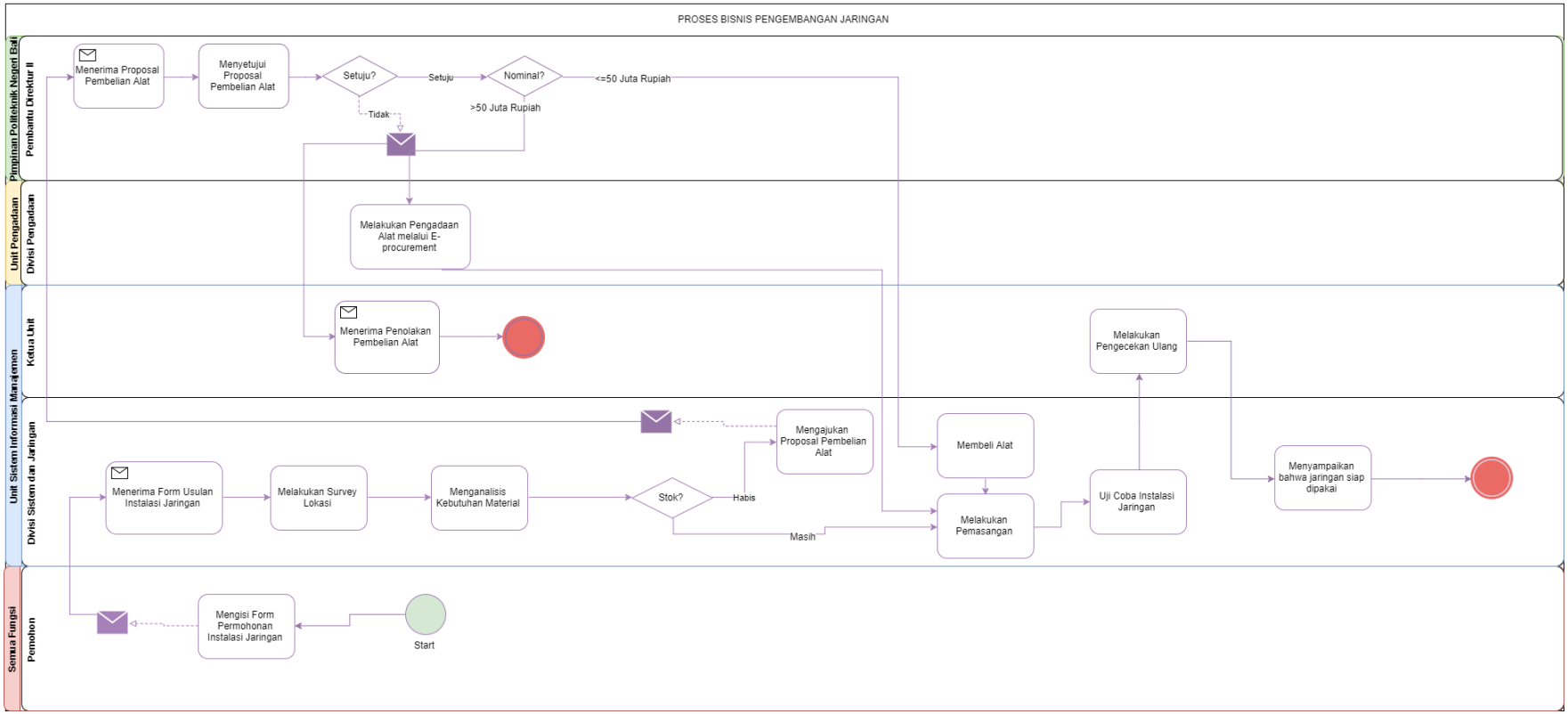
LAMPIRAN

Lampiran 1: Proses bisnis pengembangan Software

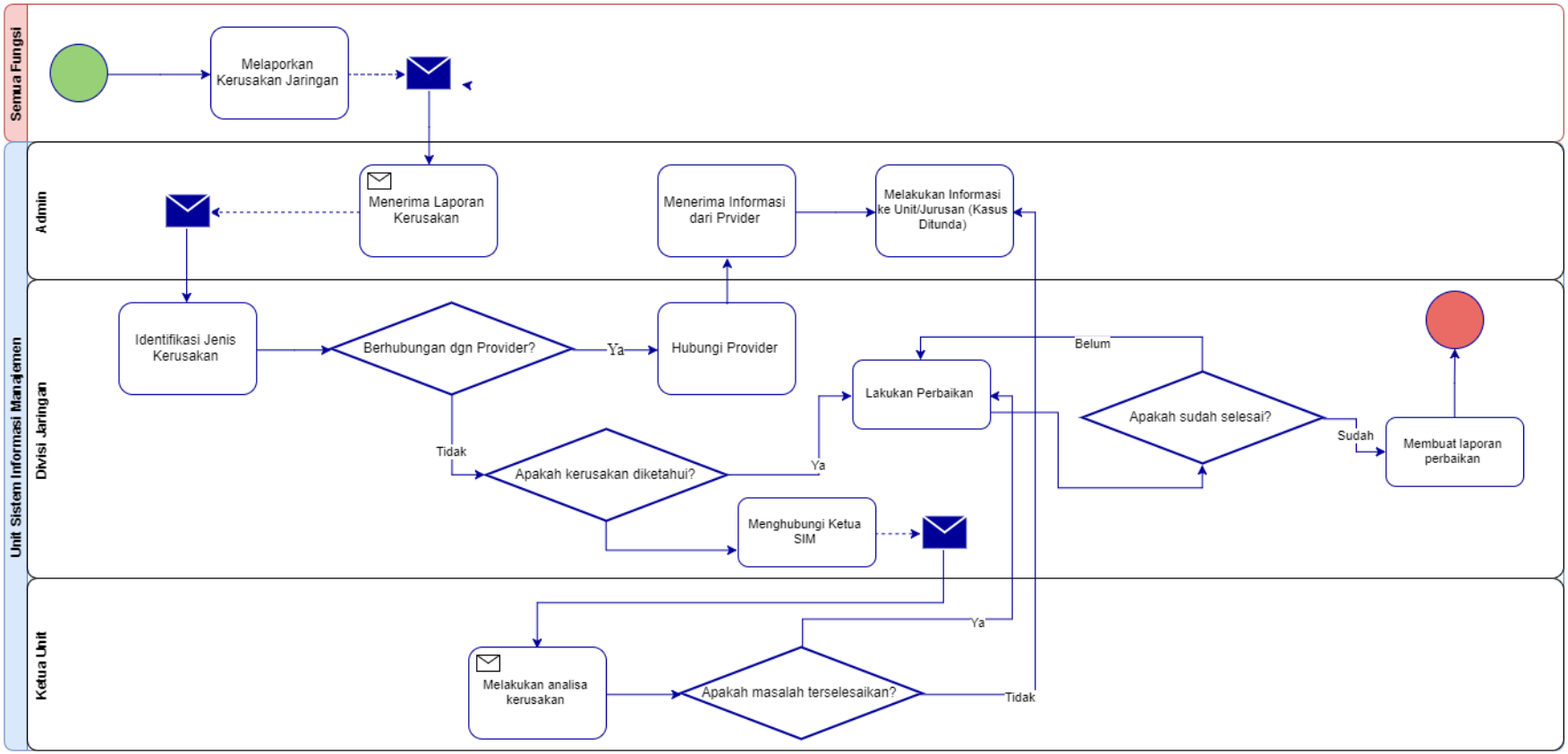


Proses Bisnis Pengembangan *software* di Unit SIM Politeknik Negeri Bali

Lampiran 2: Proses bisnis pengembangan Jaringan/Hardware

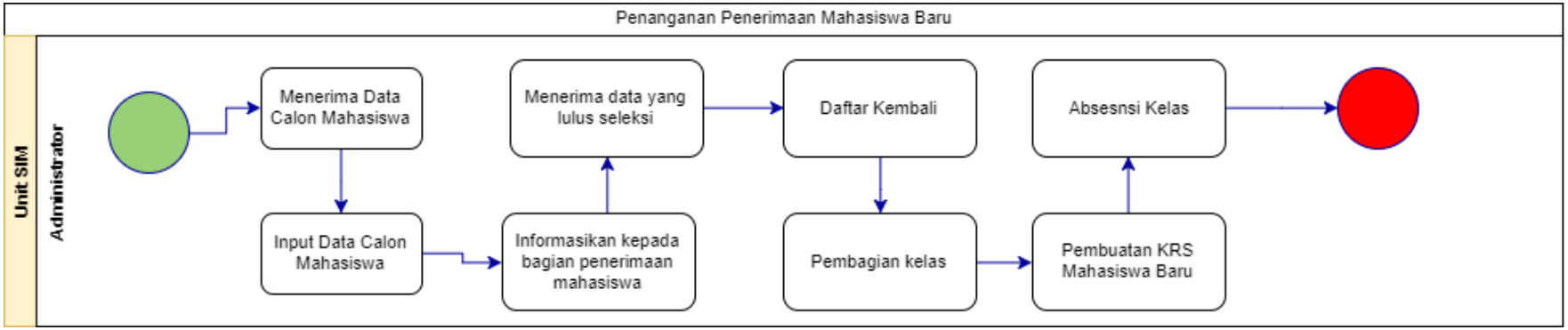


Proses bisnis pengembangan Jaringan/ Hardware di Unit SIM Politeknik Negeri Bali

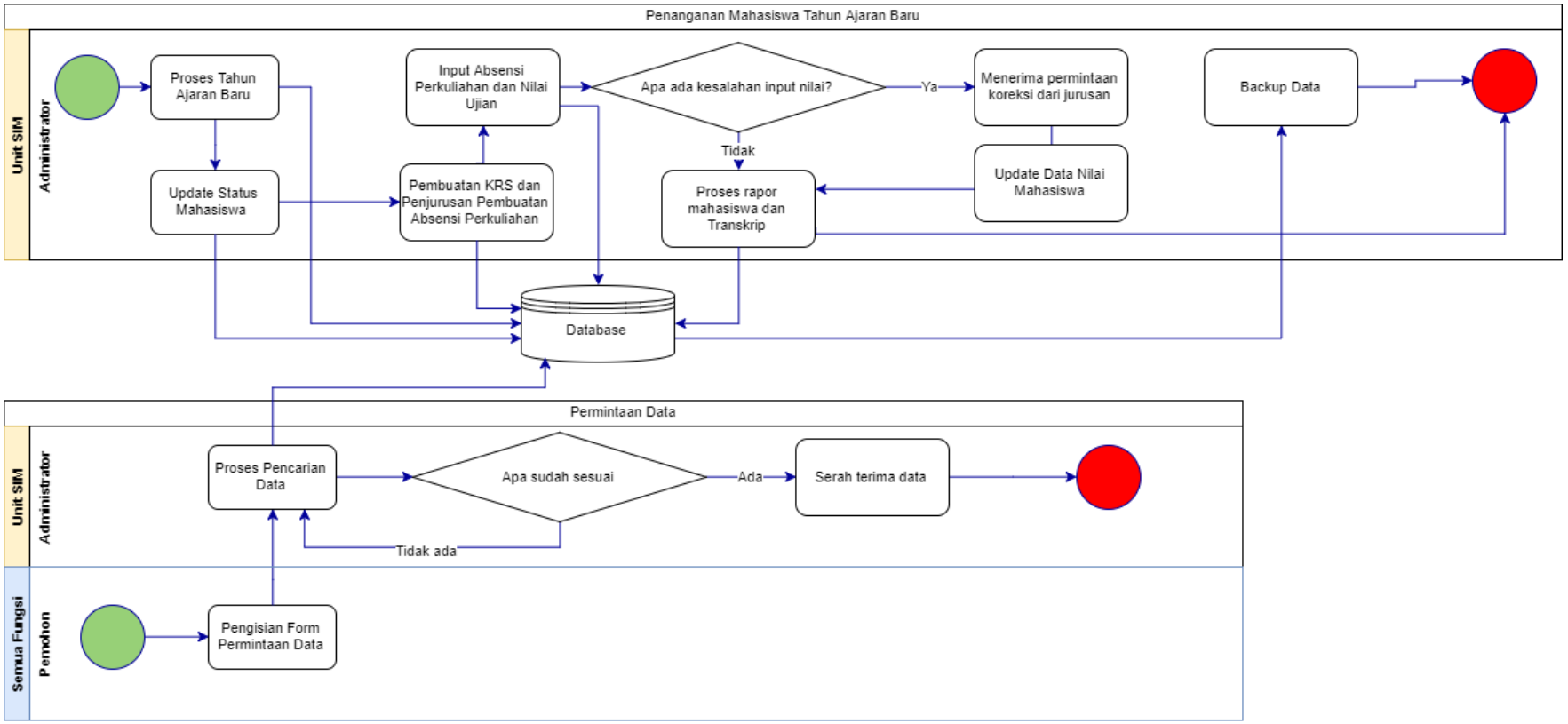


Proses bisnis pemeliharaan Jaringan/Hardware di Unit SIM Politeknik Negeri Bali

Lampiran 3: Proses bisnis Pengendalian Data dan Informasi

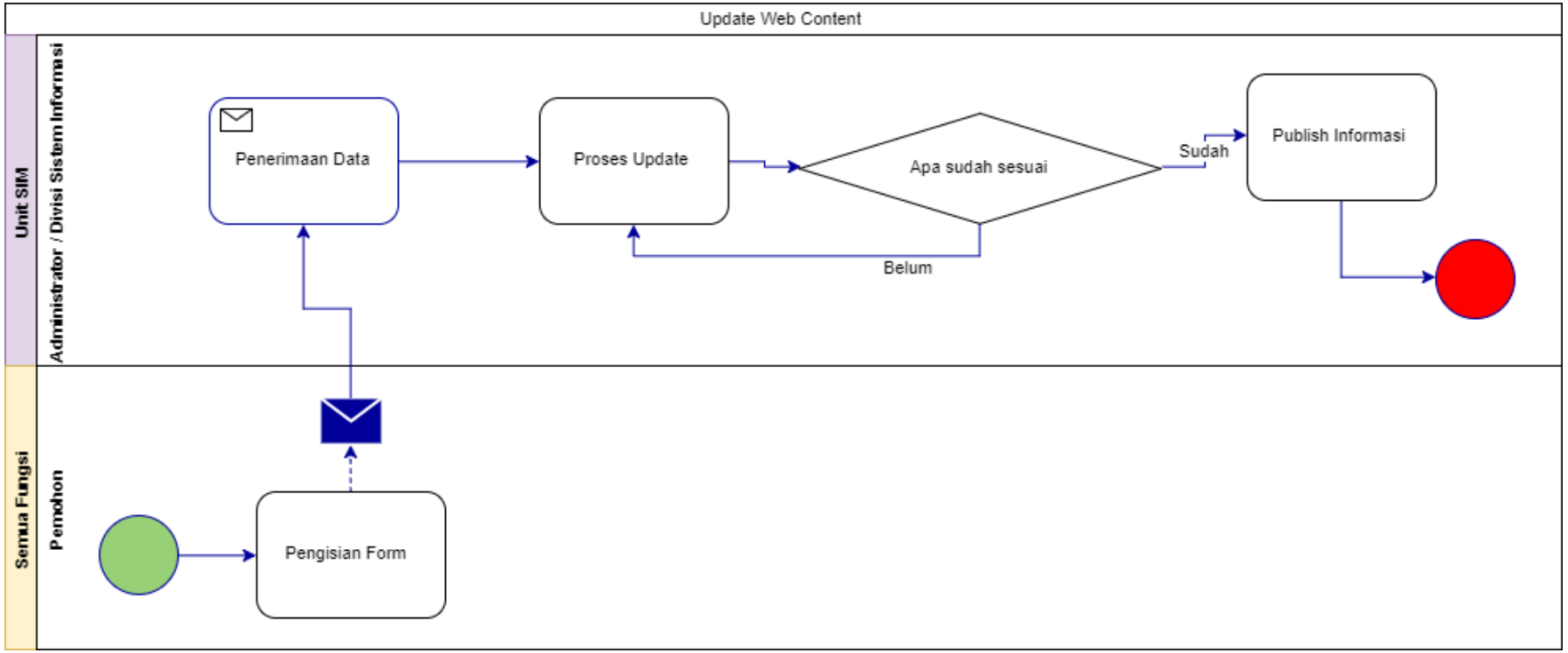


Proses bisnis Penanganan Penerimaan Mahasiswa Baru di Unit SIM Politeknik Negeri Bali

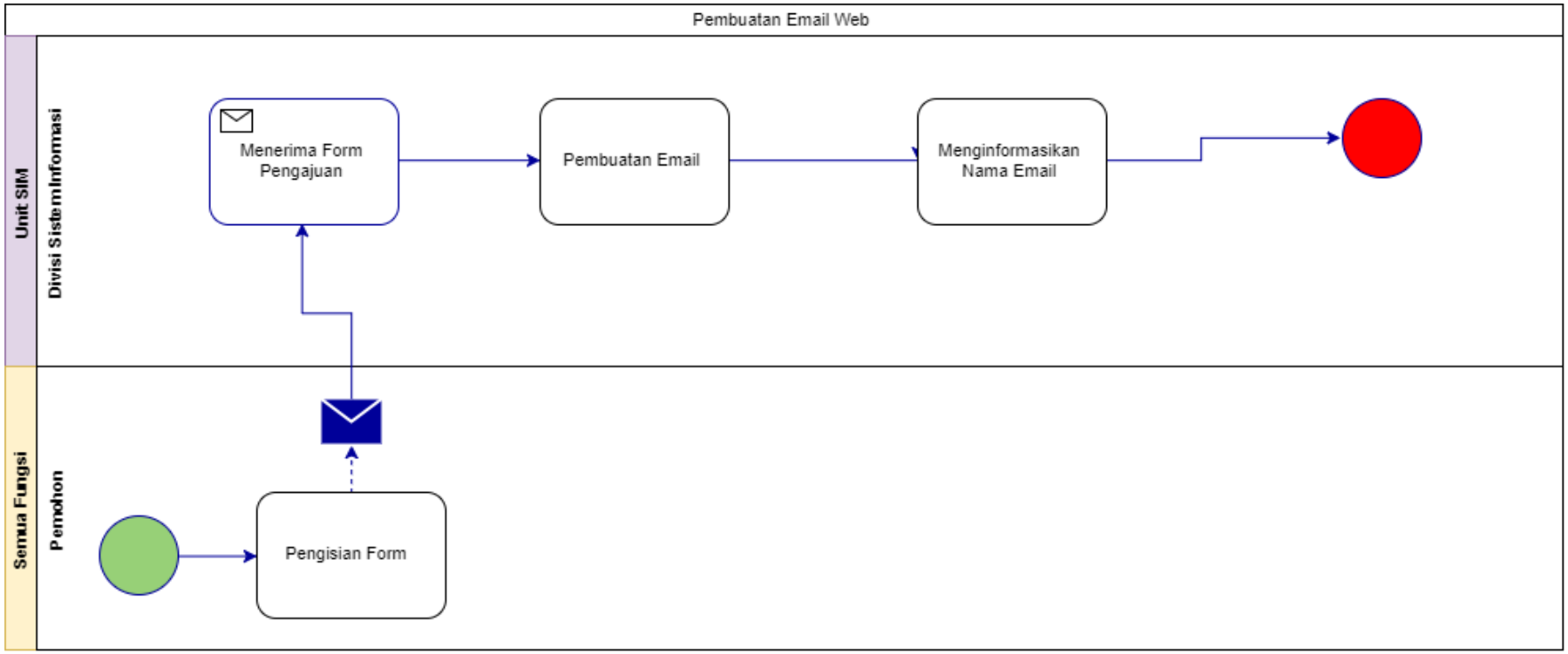


Proses bisnis Penanganan Mahasiswa Tahun Ajaran Baru dan Permintaan Data di Unit SIM Politeknik Negeri Bali

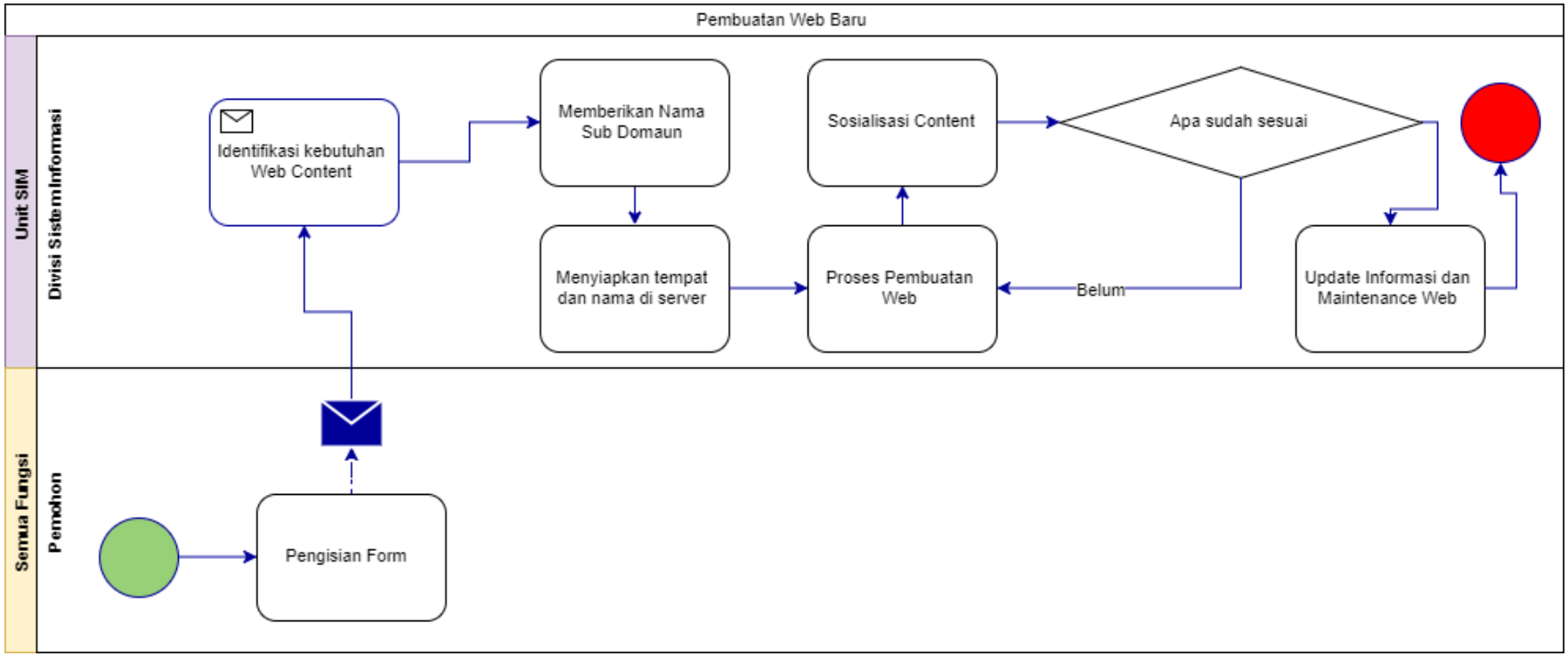
Lampiran 4: Proses bisnis Pengelolaan Website



Proses bisnis *update* Web Content di Unit SIM Politeknik Negeri Bali

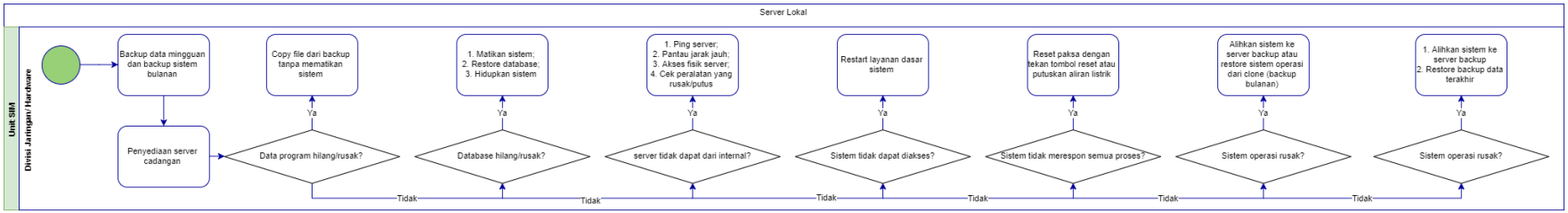


Proses bisnis Pembuatan Email Web di Unit SIM Politeknik Negeri Bali

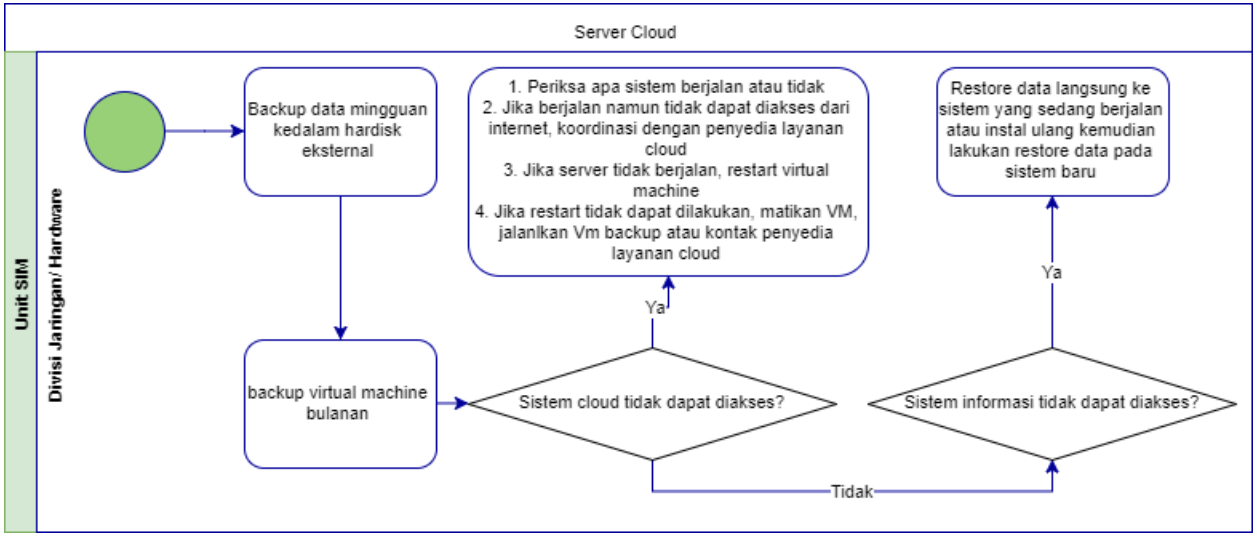


Proses bisnis Pembuatan Web Baru di Unit SIM Politeknik Negeri Bali

Lampiran 5: Proses bisnis penanganan *Disaster Recovery* Planning

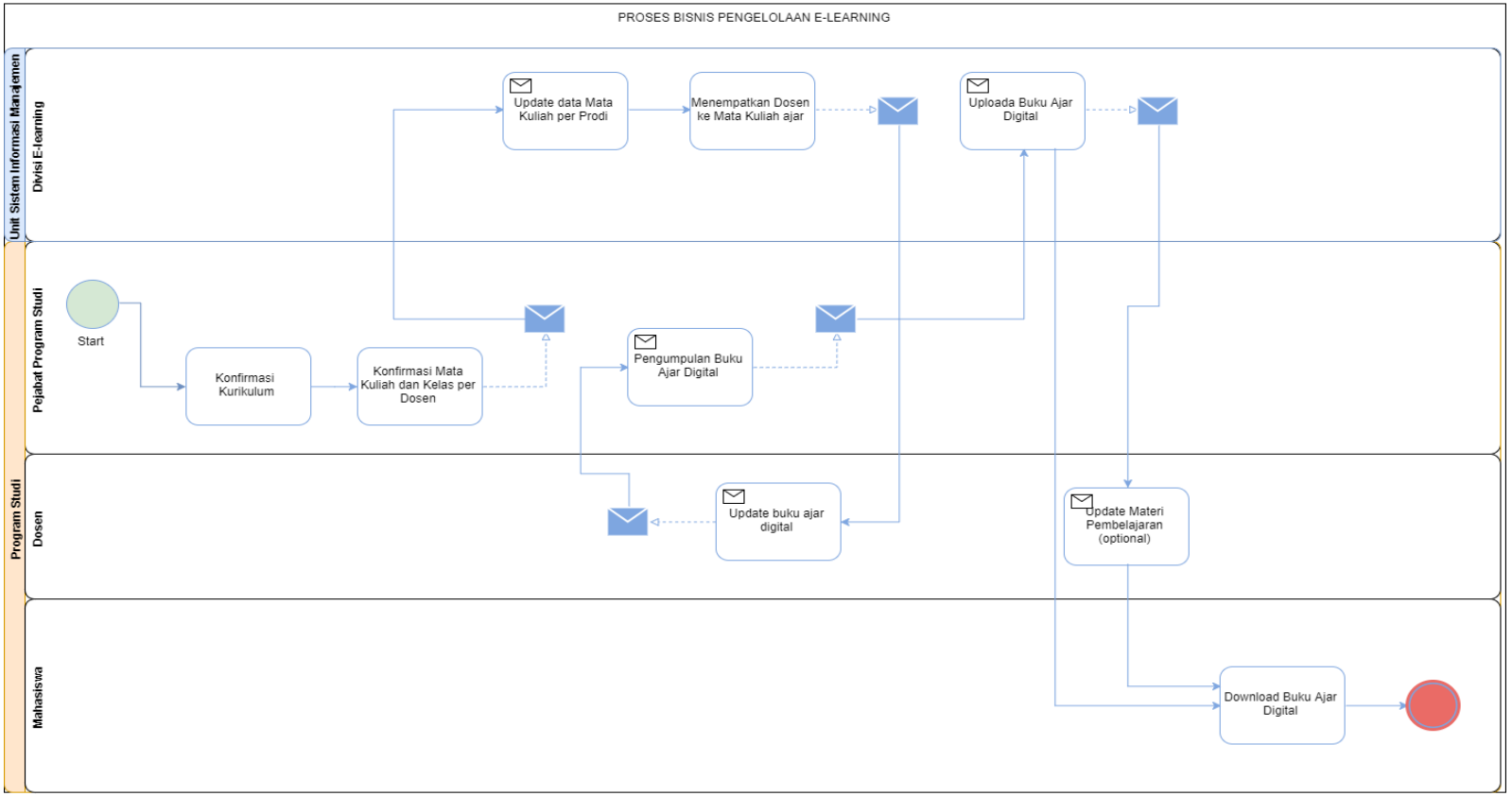


Proses bisnis penanganan Server Lokal



Proses bisnis penanganan Server Cloud

Lampiran 6: Proses bisnis Pengelolaan *E-learning*



Proses bisnis pengelolaan *E-learning* di Unit SIM Politeknik Negeri Bali

Lampiran 7: Kuesioner Penelitian Tesis (Pembobotan AHP)

Institut Teknologi Sepuluh Nopember (ITS)

Fakultas Bisnis dan Manajemen Teknologi
Program Studi Magister Manajemen Teknologi
Bidang Keahlian Manajemen Teknologi Informasi

KUESIONER PENELITIAN TESIS

Judul Penelitian Tesis:

AUDIT MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PERGURUAN TINGGI MENGGUNAKAN KERANGKA KERJA COBIT 5

Kuisioner ini dibuat untuk menyelesaikan Tesis di Fakultas Bisnis dan Manajemen Teknologi, Program Studi Magister Manajemen Teknologi, Bidang Keahlian Manajemen Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS). Untuk kepentingan penelitian, identitas responden dijamin kerahasiaannya. Atas dasar tersebut, saya mohon kepada Bapak/Ibu responden untuk mengisi kuisioner ini dengan obyektif dan sebenar-benarnya.

Tujuan Kuesioner:

Kuesioner ini dilakukan untuk mengetahui tingkat kepentingan setiap kriteria guna mendapatkan bobot untuk prioritas respon terhadap risiko terkait Teknologi Informasi (TI) menggunakan Analytical Hierarchy Process (AHP).

Responden:

Mengacu pada hasil pemetaan peran Menggunakan Kerangka Kerja COBIT 5 yang telah disesuaikan dengan kondisi di Politeknik Negeri Bali (**Tabel 1 dan Tabel 2**), kuesioner ini ditujukan kepada **7 responden**, antara lain: Pembantu Direktur I, Ketua Unit Sistem Informasi Manajemen (SIM), Sekretaris Unit SIM, Ketua Divisi Sistem dan Jaringan Unit SIM, Ketua Divisi Sistem Informasi Unit SIM, Ketua Divisi *E-learning* Unit SIM dan Ketua Pejabat Pengelola Informasi dan Dokumentasi (PPID) (**Tabel 3**).

Isi Kuisioner:

Adapun data isian dalam kuisioner ini adalah sebagai berikut:

A. Data responden
B. Pengisian data matriks perbandingan berpasangan antar kriteria pada prioritas respon terhadap risiko TI

Atas perhatian dan ketersediaan Bapak/Ibu dalam mengisi kuisioner ini, saya ucapkan terima kasih.

Peneliti,

Ida Bagus Gde Kresna Adi Jaya

Mahasiswa Magister MMT ITS

Email : kresnaadijaya@gmail.com

Tabel 1 Hasil pemetaan peran pada COBIT 5 dengan peran di Politeknik Negeri Bali

Peran Pada Cobit 5.0	Peran Pada Politeknik Negeri Bali
Board	Direktur
Chief Excutive Officer	Direktur
Chief Financial Officer	Pembantu Direktur II
Chief Operating Officer	Pembantu Direktur I
Business Executive	Ketua Unit Sistem Information Manajemen (SIM)
Business Process Owner	Sekretaris Unit Sistem Information Manajemen (SIM)
Strategy (IT Executive) Committee	Sekretaris Unit Sistem Information Manajemen (SIM)
(Project and Programme) Steering Committees	Unit SIM dan Team Unit Layanan Pengadaan
Project Managament Officer	-
Value Management Office	Sekretaris Unit SIM
Chief Risk Officer	Pembantu Direktur I
Chief Information Security Officer	Ketua Unit Sistem Information Manajemen (SIM)
Architecture Board	Direktur
Enterpise Risk Committee	Sekretaris Unit Sistem Information Manajemen (SIM)
Head Human Resource	Ketua Bagian Administrasi Akademik dan Kemahasisswaaan (BAAK)
Compliance	Jajaran Pembantu Direktur
Audit	SPI, Unit Perncanaan dan UPMA
Chief Information Officer	Ketua Unit Sistem Information Manajemen (SIM)
Head Architecture	Ketua Unit Sistem Information Manajemen (SIM)
Head Development	Ketua Unit Sistem Information Manajemen (SIM)
Head IT Operations	Ketua Unit Sistem Information Manajemen (SIM)
Head IT Administration	Ketua Unit Sistem Information Manajemen (SIM)
Service Manager	3 ketua Divisi dari Unit SIM
Information Security Manager	Ketua Pejabat Pengelolaa Informasi dan Dokumentasi (PPID)
Business Continuity Manager	Ketua Unit Sistem Information Manajemen (SIM)
Privacy Manager	Ketua Pejabat Pengelolaa Informasi dan Dokumentasi (PPID)

(Sumber: Hasil interview peneliti dengan Sekretaris Unit SIM Politeknik Negeri Bali, 2017)

Tabel 2 Hasil pemetaan RACI Chart Menggunakan Kerangka Kerja COBIT 5.

APO 12 *Manage Risk*												
Key Management Practice	*Business Process Owner*	*Project Management Officer*	*Chief Risk Officer*	*Chief Information Security Officer*	*Head Architecht*	*Head Development*	*Head IT Operation*	*Head IT Administration*	*Service Manager*	*Information Security Manager*	*Business Continuity Manager*	*Privacy Officer*
APO12.06 ***Respond to Risk***	R	R	R	R	R	R	R	R	R	R	R	R

(Sumber: ISACA, 2012. COBIT 5 – *Enabling Process*)

Berdasarkan hasil pemetaan RACI *Chart* Menggunakan Kerangka Kerja COBIT 5 pada Tabel 2, pihak yang terlibat didalam proses pengisian kuesioner adalah sebagai berikut:

Tabel 3 Responden pengisian kuesioner

Business Process Owner	Sekretaris Unit Sistem Information Manajemen (SIM)
Project Management Officer	-
Chief Risk Officer	Pembantu Direktur I
Chief Information Security Officer	Ketua Unit Sistem Information Manajemen (SIM)
Head Architecht	Ketua Unit Sistem Information Manajemen (SIM)
Head Development	Ketua Unit Sistem Information Manajemen (SIM)
Head IT Operation	Ketua Unit Sistem Information Manajemen (SIM)
Head IT Administration	Ketua Unit Sistem Information Manajemen (SIM)
Service Manager	3 ketua Divisi dari Unit SIM
Information Security Manager	Ketua Pejabat Pengelolaa Informasi dan Dokumentasi (PPID)
Business Continuity Manager	Ketua Unit Sistem Information Manajemen (SIM)
Privacy Officer	Ketua Pejabat Pengelolaa Informasi dan Dokumentasi (PPID)

(Sumber: Peneliti, 2017)

KUESIONER PENELITIAN TESIS

AUDIT MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PERGURUAN TINGGI MENGGUNAKAN KERANGKA KERJA COBIT 5

Tanggal Pengisian: : …….

Nama Pakar : …….

Jabatan : …….

Unit/ Instansi : …….

Tanda Tangan : …….

Peneliti:

Ida Bagus Gde Kresna Adi Jaya

Dosen Pembimbing:

Dr. Tech. Ir. R. V. Hari Ginardi, M.Sc.

Dr. Rita Ambarwati, S., S.E., M.MT.

BIDANG KEAHLIAN MANAJEMEN TEKNOLOGI INFORMASI
PROGRAM STUDI MAGISTER MANAJEMEN TEKNOLOGI
FAKULTAS BISNIS DAN MANAJEMEN TEKNOLOGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER

2018

Kepada
Yth. Bapak/Ibu
Ditempat

Dengan hormat,

Sehubungan dengan penelitian saya yang berjudul "Audit Manajemen Risiko Teknologi Informasi pada Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5", di bawah bimbingan Dr. Tech. Ir. R. V. Hari Ginardi, M.Sc. dan Dr. Rita Ambarwati, S.E., M.MT., saya Ida Bagus Gde Kresna Adi Jaya mahasiswa Magister Manajemen Teknologi, Institut Teknologi Sepuluh Nopember bermaksud menyampaikan permohonan kepada Bapak/Ibu untuk menjadi pakar pada penelitian ini guna memberikan *judgement* atas pertimbangan pembobotab kriteria didalam prioritas respon terhadap risiko terkait Teknologi Informasi (TI).

Tujuan penelitian ini untuk mendapatkan dokumen profil risiko TI yang harapannya dapat membantu Politeknik Negeri Bali, selaku objek penelitian saya dalam mengidentifikasi, menganalisis risiko, dan pemprioritaskan respon terhadap risiko terkait TI.

Semua informasi yang diberikan akan dirahasiakan dan hanya digunakan untuk kepentingan akademik. Terima kasih atas kesediaan dan partisipasi Bapak/Ibu dalam pengisisan kuesioner untuk mendukung penelitian saya.

Surabaya, Januari 2018
Hormat Saya,

Ida Bagus Gde Kresna Adi Jaya

PETUNJUK PENGISIAN KUESIONER

1. Pada pengisian kuesioner ini, Bapak/Ibu dimohon untuk **mengisi Tabel 5** guna membandingkan antara dua elemen, yaitu **Elemen A** (kolom 1) dengan **Elemen B** (baris 1). Nilai perbandingan antara kedua elemen tersebut ditandai dengan angka yang sesuai dengan **Tabel 4**.
2. Nilai perbandingan yang diberikan mulai dari skala **1** sampai **9**. Keterangan dari skala yang digunakan dapat dilihat pada **Tabel 4**.
3. Contoh pengisian tabel matriks perbandingan yang **BENAR** dapat dilihat pada **Tabel 6** dan **Tabel 7**.

Tabel 4 Keterangan skala pada AHP

Nilai Perbandingan (A terhadap B)	Keterangan
1	**Elemen A** sama penting dengan **B**
3	**Elemen A** sedikit lebih penting dari **B**, atau sebaliknya
5	**Elemen A** lebih penting dari **B**, atau sebaliknya
7	**Elemen A** sangat lebih penting dari **B**, atau sebaliknya
9	**Elemen A** mutlak lebih penting dari **B**, atau sebaliknya
2,4,6,8	Diberikan apabila ada perbedaan (ragu-ragu) dengan standar yang diuraikan diatas
1/(1 s/d 9)	Kebalikan nilai tingkat kepentingan dari skala 1-9

(Sumber: Saaty, 1986)

Tabel 5 Matriks Perbandingan Berpasangan Antar Kriteria pada Prioritas Respon terhadap Risiko TI

Kriteria	Durasi Proyek (DUP)	Anggaran (ANG)	Keuntungan (KEU)
Durasi Proyek (DUP)[1]			
Anggaran (ANG)[2]			
Keuntungan			

(Sumber: Kriteria didapat dari penelitian yang dilakukan oleh Oztaysi, 2014: Karasakal & Aker, 2017)

[1] Total waktu yang diperlukan dari awal mulai perencanaan hingga aksi terhadap respon risiko telah dilaksanakan (Oztaysi, 2014)

[2] Total biaya yang dikeluarkan untuk menutupi biaya implementasi dan biaya pendukung lainnya (Oztaysi, 2014)

(KEU)[3]			

Tabel 6 Contoh pengisian matriks perbandingan berpasangan yang **BENAR**

Kriteria	Durasi Proyek (DUP)	Anggaran (ANG)	Keuntungan (KEU)
Durasi Proyek (DUP)		**1/3**	**5**
Anggaran (ANG)			**7**
Keuntungan (KEU)			

Tabel 7 Contoh pengisian matriks perbandingan berpasangan yang **BENAR** (2)

Kriteria	Durasi Proyek (DUP)	Anggaran (ANG)	Keuntungan (KEU)
Durasi Proyek (DUP)		**1/3**	**1/5**
Anggaran (ANG)			**1/7**
Keuntungan (KEU)			

Tabel 8 Contoh pengisian matriks perbandingan berpasangan yang **SALAH**

Kriteria	Durasi Proyek (DUP)	Anggaran (ANG)	Keuntungan (KEU)
Durasi Proyek (DUP)	**1/3**	**5**	**3**
Anggaran (ANG)	**1/5**	**3**	**7**

[3] Keuntungan yang diperoleh oleh pihak Politeknik Negeri Bali, khususnya Unit Sistem Informasi Manajemen dalam hal peningkatan produktivitas (Karasakal & Aker, 2017).

Keuntungan (KEU)	**7**	**5**	**3**

Tabel 9 Contoh pengisian matriks perbandingan berpasangan yang **SALAH** (2)

Kriteria	Durasi Proyek (DUP)	Anggaran (ANG)	Keuntungan (KEU)
Durasi Proyek (DUP)		√	√
Anggaran (ANG)			√
Keuntungan (KEU)			

Lampiran 8: Hasil usulan pemrioritasan respon risiko kategori "Sedang"

8.A. Hasil kalkulasi pemrioritasan respon risiko kategori sedang

Kode Respon Risiko	Kriteria AHP			Total Bobot
	17,45%	26,75%	55,80%	
	Durasi	Anggaran	Keuntungan	
R0201-03	1	2	1	1,267489361
R0201-04	1	1	3	2,116063672
R0201-05	1	1	4	2,674095508
R0201-07	2	2	4	3,116063672
R0201-14	1	1	3	2,116063672
R0201-18	1	2	3	2,383553033
R0201-19	1	2	4	2,941584869
R0201-20	1	2	3	2,383553033
R0202-02	2	1	1	1,558031836
R0202-03	2	1	1	1,558031836
R0202-16	2	2	3	2,558031836
R0202-17	1	1	3	2,116063672
R0202-21	1	1	4	2,674095508
R0202-24	2	2	4	3,116063672
R0202-25	1	1	3	2,116063672
R0202-26	1	2	2	1,825521197
R0202-27	1	2	3	2,383553033
R0202-28	1	1	2	1,558031836
R0202-29	1	2	2	1,825521197
R0202-30	1	2	3	2,383553033
R0202-31	1	1	2	1,558031836
R0303-05	1	2	4	2,941584869
R0303-21	2	2	3	2,558031836
R0303-24	1	2	3	2,383553033
R0303-25	1	2	3	2,383553033

Kode Respon Risiko	Kriteria AHP			Total Bobot
	17,45%	26,75%	55,80%	
	Durasi	Anggaran	Keuntungan	
R0303-26	1	2	4	2,941584869
R0303-27	1	2	4	2,941584869
R0303-29	1	2	5	3,499616705
R0303-30	1	2	5	3,499616705
R0303-35	3	2	4	3,290542475
R0401-04	1	1	4	2,674095508
R0401-05	1	1	2	1,558031836
R0401-06	1	1	4	2,674095508
R0402-01	1	1	4	2,674095508
R0402-06	1	1	2	1,558031836
R0402-07	1	1	3	2,116063672
R0402-08	1	1	3	2,116063672
R0403-03	1	1	4	2,674095508
R0403-04	1	1	3	2,116063672
R0501-01	1	1	1	1
R0501-09	1	2	2	1,825521197
R0502-01	1	2	2	1,825521197
R0503-09	2	2	5	3,674095508
R0503-10	2	2	5	3,674095508
R0601-02	2	2	3	2,558031836
R0601-05	1	3	4	3,20907423
R0602-02	1	2	3	2,383553033
R0602-03	1	2	3	2,383553033
R0602-04	1	2	3	2,383553033
R0701-02	1	1	1	1
R0701-03	1	2	3	2,383553033
R0701-07	1	1	3	2,116063672

Kode Respon Risiko	Kriteria AHP			Total Bobot
	17,45%	26,75%	55,80%	
	Durasi	Anggaran	Keuntungan	
R0701-08	1	1	3	2,116063672
R0701-09	1	1	3	2,116063672
R0701-10	1	1	3	2,116063672
R0701-11	1	1	3	2,116063672
R0701-13	1	1	3	2,116063672

8.B. Hasil pengurutan pemrioritasan respon risiko kategori sedang

Urutan	Kode Respon Risiko	Total Bobot
1	R0503-09	3,674095508
2	R0503-10	3,674095508
3	R0303-29	3,499616705
4	R0303-30	3,499616705
5	R0303-35	3,290542475
6	R0601-05	3,20907423
7	R0201-07	3,116063672
8	R0202-24	3,116063672
9	R0201-19	2,941584869
10	R0303-05	2,941584869
11	R0303-26	2,941584869
12	R0303-27	2,941584869
13	R0201-05	2,674095508
14	R0202-21	2,674095508
15	R0401-04	2,674095508
16	R0401-06	2,674095508
17	R0402-01	2,674095508
18	R0403-03	2,674095508

Urutan	Kode Respon Risiko	Total Bobot
19	R0202-16	2,558031836
20	R0303-21	2,558031836
21	R0601-02	2,558031836
22	R0201-18	2,383553033
23	R0201-20	2,383553033
24	R0202-27	2,383553033
25	R0202-30	2,383553033
26	R0303-24	2,383553033
27	R0303-25	2,383553033
28	R0602-02	2,383553033
29	R0602-03	2,383553033
30	R0602-04	2,383553033
31	R0701-03	2,383553033
32	R0201-04	2,116063672
33	R0201-14	2,116063672
34	R0202-17	2,116063672
35	R0202-25	2,116063672
36	R0402-07	2,116063672
37	R0402-08	2,116063672
38	R0403-04	2,116063672
39	R0701-07	2,116063672
40	R0701-08	2,116063672
41	R0701-09	2,116063672
42	R0701-10	2,116063672
43	R0701-11	2,116063672
44	R0701-13	2,116063672
45	R0202-26	1,825521197
46	R0202-29	1,825521197

Urutan	Kode Respon Risiko	Total Bobot
47	R0501-09	1,825521197
48	R0502-01	1,825521197
49	R0202-28	1,558031836
50	R0202-31	1,558031836
51	R0401-05	1,558031836
52	R0402-06	1,558031836
53	R0202-02	1,558031836
54	R0202-03	1,558031836
55	R0201-03	1,267489361
56	R0501-01	1
57	R0701-02	1

8.C. Hasil pengurutan pemrioritasan respon risiko kategori sedang

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
R0503-09	Programmer yang kurang paham dalam mengerti kemauan pemohon tersebut harus meminta bantuan kepada personel yang telah berpengalaman dalam memahami kemauan pemohon.	Pengelolaan Website Politeknik – Pembuatan Website Baru
R0503-10	Programmer dapat berdiskusi dengan divisi sistem informasi dalam pengembangan website, agar website yang dikembangkan tidak terlalu sulit secara teknis.	Pengelolaan Website Politeknik – Pembuatan Website Baru

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
R0303-29	Project Manager harus segera menyusun rencana untuk dilakukannya user *Transfer*ance test.	Pengembangan Software
R0303-30	Melakukan *Transfer*ance test dengan merilis versi beta agar dapat dilihat bug atau kelengkapannya terlebih dahulu sebelum dirilis versi finalnya	Pengembangan Software
R0303-35	Divisi sistem informasi bekerja sama dengan ketua SIM dalam merancang ketetapan untuk wajibnya dilakukan evaluasi terhadap dampak dari penggunaan aplikasi dari sisi pengguna	Pengembangan Software
R0601-05	Mengganti sistem operasi pada server lokal dengan sistem operasi yang baru	Penanganan Disaster Recovery
R0201-07	Unit SIM diharapkan menggalakkan prosedur keselamatan kerja dengan mengedukasi divisinya agar selalu mengutamakan keselamatan dalam bekerja	Pemeliharaan Jaringan/ Hardware
R0202-24	Menggalakkan prosedur keselamatan kerja dengan mengedukasi divisinya agar selalu mengutamakan keselamatan dalam bekerja	Pengembangan Jaringan/ Hardware
R0201-19	Unit help desk harus dapat mendistribusikan kembali surat	Pemeliharaan Jaringan/ Hardware

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
	pemberitahuan tersebut dengan baik ke pihak pelapor.	
R0303-05	Divisi sistem informasi bekerja sama dengan ketua SIM dalam membuat usulan proposal pengembangan software	Pengembangan Software
R0303-26	Project Manager memindahkan penjaminan mutu yang sebelumnya dipertanggungjawabkan kepada PM ditujukan kepada dosen Teknik Informatika yang telah terbukti memiliki pengalaman dan kinerja yang lebih baik	Pengembangan Software
R0303-27	Project Manager bekerja sama dengan personel yang telah berpengalaman dalam melakukan application penetration test (Ethical Hacking) dan *Transfer*ance test untuk membantu personel lainnya jika mengalami kesulitan	Pengembangan Software
R0201-05	Unit organisasi harus membuat prosedur tertulis untuk pengelolaan insiden dan permintaan layanan.	Pemeliharaan Jaringan/ Hardware
R0202-21	Teknisi dipandu oleh teknisi yang lebih senior atau yang lebih berpengalaman dalam hal pemasangan jaringan/hardware	Pengembangan Jaringan/ Hardware

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
R0401-04	Menggunakan PHP Data Object (PDO) saat membuat program untuk mengatasi SQL injection saat login	Pengendalian Data dan Informasi – Penanganan Penerimaan Mahasiswa Baru
R0401-06	Mengembalikan sistem ke keadaan semula dengan menghilangkan seluruh script malicious yang diinputkan	Pengendalian Data dan Informasi – Penanganan Penerimaan Mahasiswa Baru
R0402-01	Mengembalikan sistem ke keadaan semula dengan menghilangkan seluruh script malicious yang diinputkan.	Pengendalian Data dan Informasi – Penanganan Mahasiswa Tahun Ajar Baru
R0403-03	Mengembalikan sistem ke keadaan semula dengan menghilangkan seluruh script malicious yang diinputkan.	Pengendalian Data dan Informasi – Prosedur Penanganan Permintaan Data
R0202-16	Divisi mengawasi jalannya proses lelang melalui LPSE	Pengembangan Jaringan/ Hardware
R0303-21	Analyst harus mengerjakan kembali proyek tersebut dengan menerapkan SDLC didalamnya.	Pengembangan Software
R0601-02	Melakukan *Transfer* knowledge dengan cara membuat panduan mengenai langkah-langkah dalam melakukan *backup* server lokal	Penanganan Disaster Recovery
R0201-18	Unit help desk harus melakukan kerja sama dengan teknisi sistem dan	Pemeliharaan Jaringan/ Hardware

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
	jaringan dalam membuat surat pemberitahuan, agar informasi yang diberikan jelas.	
R0201-20	Help desk harus mencatat hasil perbaikan dan disimpan ke dalam arsip, guna memenuhi prosedur yang telah dibuat	Pemeliharaan Jaringan/ Hardware
R0202-27	Membuat kesepakatan kepada supplier berkaitan dengan masa garansi dari jaringan/hardware yang telah terpasang	Pengembangan Jaringan/ Hardware
R0202-30	Teknisi harus membawa checklist kegiatan agar tidak lupa melakukan pelaporan bahwa jaringan/jardware telah terpasang dan siap untuk digunakan	Pengembangan Jaringan/ Hardware
R0303-24	Personel yang kurang paham dalam membaca SRS menggunakan metode MVC tersebut harus meminta bantuan kepada personel yang telah berpengalaman dalam memahami SRS menggunakan metode MVC.	Pengembangan Software
R0303-25	Programmer dapat berdiskusi dengan divisi sistem informasi dalam pengembangan aplikasi, agar aplikasi yang dikembangkan tidak terlalu sulit secara teknis	Pengembangan Software

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
R0602-02	Mengecek kembali mengapa melalui jaringan internal, server *cloud* tidak dapat diakses	Penanganan Disaster Recovery
R0602-03	Mengecek kembali mengapa server tidak dapat diakses dari luar jaringan Politeknik Negeri Bali	Penanganan Disaster Recovery
R0602-04	Mengecek kembali mengapa ada beberapa source file yang hilang dengan menonaktifkan VM yang bermasalah dan menjalankan machine backup	Penanganan Disaster Recovery
R0701-03	Pemberian data/file oleh administrator prodi dilakukan via drop box/ google drive untuk menghindari virus yang dibawa dari flashdik/hardisk eksternal kepada Administrtaor E-learning	Pengelolaan E-learning
R0201-04	Help desk harus langsung menangani permintaan yang masuk dengan cepat.	Pemeliharaan Jaringan/ Hardware
R0201-14	Ketua SIM meminta bantuan untuk bekerja sama dengan divisi sistem dan jaringan terkait dengan permasalahan yang tidak dimengerti.	Pemeliharaan Jaringan/ Hardware
R0202-17	Melakukan survey terhadap supplier berdasarkan pengalaman supplier	Pengembangan Jaringan/ Hardware

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
	tersebut, proyek yang pernah ditangani, dan reputasinya	
R0202-25	Divisi Sistem dan jaringan menunjuk perwakilannya yang tidak sibuk dengan membawa catatan apabila perwakilannya tersebut tidak mengerti tentang TI	Pengembangan Jaringan/ Hardware
R0402-07	Meminta bantuan kepada divisi/staff lain untuk membantu membuat atau meminta kembali dokumen permintaan koreksi yang hilang/rusak	Pengendalian Data dan Informasi – Penanganan Mahasiswa Tahun Ajar Baru
R0402-08	Meminta bantuan kepada divisi/staff lain untuk membantu membuat atau meminta kembali dokumen permintaan koreksi yang hilang/rusak.	Pengendalian Data dan Informasi – Penanganan Mahasiswa Tahun Ajar Baru
R0403-04	Mengaktifkan fitur auto scan pada PC Administrator	Pengendalian Data dan Informasi – Prosedur Penanganan Permintaan Data
R0701-07	Mengecek kembali mata kuliah per prodi yang telah di *update* sebelum di submit kedalam aplikasi e-learning	Pengelolaan E-learning
R0701-08	Mengecek kembali dosen ajar apakah sudah sesuai dengan mata kuliah ajar di sebelum di submit kedalam aplikasi e-learning	Pengelolaan E-learning

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
R0701-09	Mengecek kembali proses *update* buku ajar digital yang telah di *update* sebelum di submit kedalam aplikasi e-learning	Pengelolaan E-learning
R0701-10	Mengecek kembali buku ajar digital yang telah dikumpulkan sebelum diserahkan ke Admin *E-learning*	Pengelolaan E-learning
R0701-11	Mengecek kembali buku ajar digital yang telah di upload sebelum di submit kedalam aplikasi e-learning	Pengelolaan E-learning
R0701-13	Menyediakan informasi pada Aplikasi *E-learning* tentang tata cara mengunduh buku ajar	Pengelolaan E-learning
R0202-26	Membawa panduan cara melakukan uji coba terhadap jaringan/hardware yang telah terpasang	Pengembangan Jaringan/ Hardware
R0202-29	Teknisi harus membawa checklist kegiatan agar tidak lupa melakukan pelaporan bahwa jaringan/hardware telah mengalami perubahan konfigurasi.	Pengembangan Jaringan/ Hardware
R0501-09	Memberikan berita acara susulan mengenai *update* content kepada pemohon	Pengelolaan Website Politeknik – *update* Web Content
R0502-01	Membuat kembali form pengelolaan website dan mengumpulkan kembali	Pengelolaan Website Politeknik – Pembuatan Email Politeknik

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
	permhonan pembuatan email yang hilang.	
R0202-28	Teknisi harus menginformasikan kepada Ketua Unit agar dilakukan pengecekan ulang terhadap pemasangan yang dilakukan oleh teknisi	Pengembangan Jaringan/ Hardware
R0202-31	Menugaskan mahasiswa yang sedang melakukan kegiatan PKL untuk melakukan pengecekan jaringan/hardware berkala	Pengembangan Jaringan/ Hardware
R0401-05	Merubah username dan password yang lama dan tidak mencentang remember my password pada web browser	Pengendalian Data dan Informasi – Penanganan Penerimaan Mahasiswa Baru
R0402-06	Meminta bantuan ke teknisi/programmer untuk memberikan perlindungan yang lebih ke database dengan cara merubah password berkala untuk database.	Pengendalian Data dan Informasi – Penanganan Mahasiswa Tahun Ajar Baru
R0202-02	Teknisi harus segera mengisi formulir pengembangan.	Pengembangan Jaringan/ Hardware
R0202-03	Teknisi harus segera mengisi formulir pengembangan karena berdampak pada kelengkapan arsip.	Pengembangan Jaringan/ Hardware

Kode Respon Risiko	Deskripsi Respon Risiko	Proses Bisnis
R0201-03	Help desk menghubungi pelapor untuk mencari informasi kembali guna mengisi formulir kerusakan	Pemeliharaan Jaringan/ Hardware
R0501-01	Menginstall anti virus yang memiliki bebas lisensi	Pengelolaan Website Politeknik – *update* Web Content
R0701-02	Memasang anti-virus yang memiliki bebas lisensi sehingga dapat mengurangi frekuensi terserang virus	Pengelolaan E-learning

Lampiran 9: Profil Risiko TI di Politeknik Negeri Bali

Lampiran Profil Risiko berada di dokumen terpisah. Dokumen Profil Risiko TI terdapat di Perpustakaan Magister Manajemen Teknologi, Institut Teknologi Sepuluh Nopember (MMT – ITS). Bagi pembaca yang berminat untuk membaca dokumen Profil Risiko TI di Politeknik Negeri Bali tanpa harus ke Perpustakaan MMT – ITS, dapat menghubungi peneliti di kresnaadijaya@gmail.com.