AUDIT KEAMANAN DAN MANAJEMEN RESIKO SISTEM INFORMASI AKADEMIK DENGAN FRAMEWORK NIST
(STUDI KASUS : UNIVERSITAS SANGGA BUANA YPKP BANDUNG)

TESIS

Disusun Sebagai Bagian Dari Persyaratan Untuk
Mendapatkan Gelar Magister Komputer
Dari Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI

Oleh :

RANGGA SATRIA PERDANA

NPM : 2015210102

PROGRAM STUDI PASCASARJANA
MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER LIKMI
BANDUNG

2018

AUDIT KEAMANAN DAN MANAJEMEN RESIKO SISTEM INFORMASI AKADEMIK DENGAN FRAMEWORK NIST
(STUDI KASUS : UNIVERSITAS SANGGA BUANA YPKP BANDUNG)

Oleh :

RANGGA SATRIA PERDANA

NPM : 2015210102

Bandung, 4 Januari 2018
Menyetujui,

Dr. Hery Heryanto, S.Kom, M. Kom
Pembimbing

PROGRAM STUDI PASCASARJANA
MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER LIKMI
BANDUNG

2018

DIPERSEMBAHKAN UNTUK ORANG TUA DAN KELUARGATERCINTA

DR. H. ASEP EFFENDI ROCHAENDI, SE., M.SI, PIA,CFRA DAN HJ. HAMMY KUSUMAH,SE

SOLIHIN DAN ASIANI

ISTRI DAN ANAKKU TERCINTA

TYA SEPTIANI ASTUTI

ANAK - ANAKKU

KHANSA TYARA RIZKI SHOLEHAH DAN MOCHAMMAD SATRYA MALIK IBRAHIM

ADIK – ADIKKU

MOCHAMMAD YUSUF KRISHNA SATRIA, ST DAN HANIFAH NURWAHYUNI

TIAN MUHAMMAD SATIBI DAN DINI ANGGRAENI

MUHAMMAD ABDUL AZIZ

ABSTRAK

Persaingan diantara lembaga pendidikan semakin terasa. Informasi yang disediakan oleh lembaga tersebut pun harus dapat dirasakan dengan cepat, tepat dan dapat dipercaya oleh konsumen. Perkembangan teknologi informasi yang diterapkan di dunia pendidikan memiliki dampak yang positif. Semakin berkembangnya teknologi informasi, semakin terasa pula peran yang diberikan oleh teknologi informasi tersebut. Namun, perkembangan teknologi informasi yang cepat membuka celah terjadinya resiko yang merugikan bagi institusi. Untuk itu, perlu dilakukan identifikasi terhadap resiko dan keamanan pada sistem informasi tersebut. Jika manajemen resiko tidak dilakukan, makaakan terjadi masalah pada sistem informasi tersebut. beberapa masalah yang mungkin terjadi adalah hilangnya datadata akan menjadi tidak valid, akurasi data menjadi tidak dapat dipercaya,dan sistem informasi tersebut akan menjadi rentan terhadap ancaman.

Audit keamanan dan manajemen resiko dapat dilakukan dengan menggunakan standar kerangka kerja. NIST merupakan salah satu kerangkan kerja yang biasa digunakan mengidentifikasi keamanan dan resiko pada sistem informasi. Dengan dilakukannya penilaian terhadap keamanan dan resiko pada sistem informasi akademik di Universitas Sanga Buana YPKP Bandung, diharapkan mampu meminimalisir kemungkinan terjadinya resiko pada sistem informasi akademik tersebut.

Hasil audit keamanan sistem informasi akademik dengan *framework* NIST SP 800-26 menunjukkan bahwa keamanan pada sistem informasi akademik tersebut memiliki nilai secara keseluruhan sebesar 72.43 %. Nilai tersebut didapat dari hasil perhitungan berdasarkan 3 (tiga) kategori yang diuji, yaitu pengendalian manajemen (*management control*), pengendalian operasional (*operational control*), pengendalian teknikal (technical control*).* Berdasarkan data tersebut, keamanan sistem informasi yang ada di Unviersitas Sangga Buana YPKP termasuk ke dalam level 3, yaitu *implemented procedures and controls*.

Manajemen resiko yang dilakukan menggunakan tahapan pada NIST SP 800-30, dengan bantuan menggunakan aplikasi *scanning* Acunetix. Berdasarkan hasil *scanning* menggunakan Acunetix, sistem informasi akademik di Universitas Sangga Buana YPKP memiliki kerentanan sebanyak 600 buah. Kerentanan tersebut terbagi menjadi 4 tingkatan kerentanan, yaitu 4 buah kerentanan tingkat tinggi, 40 buah kerentanan tingkat sedang, 13 buah kerentanan tingkat rendah, dan 543 buah kerentanan bersifat informasional.

Kata Kunci : Audit Keamanan, Manajemen Resiko, Sistem Informasi, *framework* NIST, Acunetix

ABSTRACT

Competition among educational institutions is increasingly felt. The information that provided by institutions must be rapidly, accurately, trustworthily felt by costumers. The development of information technology which is applied in the world of education has positive impact. The more information technology develop, the more role given by the information technology. However, fast development of information technology opens the risks that harm to the institution. Therefore, it is necessary to identify the risks and security of information system. If risk management isn't done, same problems might occur: loss of data, data will be invalid, the accuracy of data will be untrustworthy, and the information system will be vulnerable to threats.

Security audit and risk management can be done using standard framework. NIST is one of the framework which usually used to identify the security and risks on information system. The assessment is done to the security and risksin academic information system at USB YPKP Bandung that it is expected to minimize the risks occurs to the academic information system.

The result of security audit on academic information system with NIST SP 800-26 framework shows the security on the system has the whole score as big as 72.43%. the score is obtained from the calculation of 3 categories tested namely Management Control, Operational Control, and Technical Control.Based on the data, the security of information system in USB YPKP belongs to level 3, Implemented Procedures and Controls.

Risk management is done using some stages on NIST SP 800-30, with the help of Acunetix Scanning Application. Based on the result of scanning using Acunetix, academic information system at USB YPKP has 600 pieces of vulnerabilities. These vulnerabilities divided into 4 levels of vulnerability, namely 4 pieces of high level of vulnerabilities, 40 pieces of medium level of vulnerabilities, 13 pieces of low level of vulnerabilities, and 543 pieces of informational vulnerabilities.

Keyword : Security Audit, Risk Management, Information Sistem, Framework NIST, Acunetix

KATA PENGANTAR

Bismillahirrohmaanirrohim

Alhamdulillahhirabbil Alamin. Puji dan syukur penulis panjatkan ke hadirat Allah Swt atas rahmat dan karunia-Nya yang telah diberikan kepada penulis, sehingga dapat menyelesaikan penyusunan laporan Tesis yang berjudul "Audit Keamanan dan Manajemen Resiko Sistem Informasi Akademik Dengan *Framewok* NIST (Studi Kasus : Universitas Sangga Buana YPKP)".

Tujuan dari penyusunan laporan Tesis ini adalah untuk mengembangkan kemampuan menyusun suatu karya tulis ilmiah dari hasil penelitian ilmiah dan mengembangkan kemampuan untuk menganalisis serta memecahkan masalah secara sistematis. Selain itu, tujuan dari Tesis ini adalah untuk menyelesaikan kuliah Pasca Sarjana.

Dengan segala kerendahan hati pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Dr. Hery Heryanto, S.Kom., M.Kom, selaku dosen pembimbing yang telah membimbing dan mengarahkan penulis dalam menyelesaikan laporan Tesis ini.
2. Rektor Universitas Sangga Buana YPKP beserta jajarannya yang memberikan izin penulis untuk melakukan penelitian.
3. Bapak Renol Burjulius ST., M.Kom, CEH., App., selaku Direktur PUDI Universitas Sangga Buana YPKP Bandung.
4. Rekan-rekan Pasca Sarjana STMIK LIKMI angkatan 2015, terima kasih atas dukungan kalian.
5. Istri dan anak tercinta yang selalu menjadi inspirasi dan penyemangat bagi penulis untuk bisa menyelesaikan Tesis ini.
6. Dan semua pihak yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari dalam penulisan Tesis ini masih terdapat kekurangan baik dari segi teknis maupun isinya, hal ini disebabkan oleh keterbatasan ilmu dan pengetahuan penulis. Untuk itu kritik dan saran sangat berguna untuk perbaikan laporan Tesis ini.

Akhirnya penulis berharap semoga laporan Tesis ini memberikan manfaat khususnya bagi penulis dan umumnya bagi pihak-pihak yang tertarik pada bidang ini dan berkeinginan untuk mengembangkannya untuk masa yang akan datang. Aamiin.

Bandung, 4 Januari 2018

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Akhir – akhir ini, persaingan diantara lembaga pendidikan semakin terasa. Sehingga, membuat para pimpinan lembaga pendidikan, khususnya perguruan tinggi harus bisa memenuhi tuntuntan masyarakat terkait kualitas lulusan dan layanan. Kemampuan meningkatkan kualitas dan layanan, khususnya kepada masyarakat akan menjadikan lembaga pendidikan tersebut menjadi pemenang dalam persaingan di era kompetisi ini. Salah satu upaya yang dapat dilakukan dalam meningkatkan daya saing lembaga pendidikan, para pimpinan harus bisa menyediakan informasi yang cepat, tepat, dan dapat dipercaya.

Parameter keberhasilan suatu organisasi, khususnya perguruan tinggi, dapat dilihat dari banyak faktor, baik itu faktor internal maupun eksternal. Faktor internal diantaranya kualitas dosen yang mumpuni, mahasiswa sebagai konsumen, sarana dan fasilitas yang menunjang, serta pelayanan yang memuaskan. Sedangkan faktor eksternal adalah hubungan dengan dunia luar, misalnya dengan perguruan tinggi lain, pemerintah, dan masyarakat. Tentunya, untuk dapat bertahan di dalam persaingan tersebut, dibutuhkan strategi yang dapat ditawarkan kepada para calon konsumen. (Aswati dkk, 2015).

Perkembangan teknologi informasi dalam dunia pendidikan mendapat dampak yang positif. Dengan berkembangnya teknologi informasi, dunia pendidikan mulai memperlihatkan perubahan yang cukup signifikan. Ada perubahan – perubahan cara mengajar yang bekembang dalam dunia pendidikan. Sekarang ini, jarak dan waktu bukanlah sebagai masalah yang berarti untuk transfer ilmu pengetahuan. Banyak *software* dan aplikasi yang dibuat untuk memfasilitasi dalam transfer pengetahuan ini. (Yahya, 2011).

Tujuan diterapkannya sistem informasi dibidang pendidikan adalah untuk kemudahan dan kesempurnaan dalam memberikan pelayanan, informasi yang akurat

dan dapat dipercaya, serta menjadikan perguruan tinggi yang memiiki daya saing yang mumpuni untuk bisa bertahan dalam persaingan. Teknologi informasi memiliki peran yang signifikan dalam peningkatan mutu pelayanan dan daya saing suatu organinsasi.

Beberapa penelitian menunjukkan bahwa sistem informasi beserta asetnya rentan terhadap resiko kerusakan fisik dan logik. Resiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (*natural disaster*), pencurian (*theft*), kebakaran (*fires*), lonjakan listrik (*power surge*), dan perusakan (*vandalism*). Resiko kerusakan logik mengacu kepada akses tidak sah (*unauthorized access*), kerusaka sengaja maupun tidak sengaja pada sistem informasi dan data. (Suduc, 2010).

Untuk itu perlu dilakukan identifikasi ancaman dan analisis risiko untuk meningkatkan keamanan dan mengurangi resiko kerusakan sistem informasi. (Jakaria, 2013). Dengan manajemen resiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa: dampak terhadap finansial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan asetyang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan. (Maulana, 2006)

Jika manajemen resiko tidak dilakukan terhadap sistem informasi akademik tersebut, maka akan terjadi masalah pada sistem informasi akademik tersebut. Masalah yang mungkin terjadi, khususnya di Universitas Sangga Buana YPKP, diantaranya hilangnya data, data akan menjadi tidak valid, akurasi data menjadi tidak dapat dipercaya, dan sistem informasi tersebut akan menjadi sangat rentan terhadap ancaman, baik itu ancaman secara internal maupun eksternal. Aset yang dapat terancam resiko tersebut antara lain informasi nilai mahasiswa, penghitungan, kehadiran dosen dan mahasiswa, penghitungan honorarium dan penggajian dosen dan karyawan, serta koneksi informasi ke pusat data dan informasi Kementrian pendidikan dan ristek (PDPT Dikti). Untuk mengatasi tahap tersebut, berdasarkan hasil survey pendahuluan, diketahui bahwa pimpinan Universitas Sangga Buana YPKP memberikan tugas dan kewenangan kepada

direktorat IT untuk mengelola *hardware*, *software*, maupun *brainware* yang memiliki kompetensi dalam rangka minimalisasi resiko.

NIST merupakan sebuah kerangka kerja yang dipublikasikan oleh *National Institute of Standard and Technology* (NIST). NIST didirikan oleh Samuel W. Stratton padea tahun 1901. NIST melakukan pengukuran, penetapan standard dan teknologi untuk dapat mengoptimalkan peran dari infrastruktur institusi, khususnya dalam bidang IT. NIST memiliki banyak versi, yang masing – masing versi tersebut memiliki topik dan fokus bahasan yang berbeda dan beragam, namun saling berhubungan. Sehingga, dapat dikatakan bahwa NIST merupakan salah satu kerangka kerja yang banyak digunakan oleh perusahaan ataupun institusi di seluruh penjuru dunia. Salah satu kerangka kerja NIST yang sering digunakan dalam menentukan tingkat dari *cybersecurity* dipublikasikan pada Agustus 2001 berjudul "*NIST Special Publication 800-26 : Security Self-Assessment Guide for Information Technology Systems*". Kerangka kerja NIST tersebut diharapkan dapat meningkatkan kemampuan sebuah institusi dalam mengatasi permasalah keamanan komputer, baik pada saat ini maupun masa yang akan datang.

Pengalaman Yayasan Pendidikan Keuangan dan Perbankan (YPKP) mengelola pendidikan lebih dari 44 tahun, semenjak 1968 mengelola Akademik Bank Nasional (ABN) Cabang Bandung , kemudian ABN berubah menjadi AKUBANK YPKP, dan berubah lagi menjadi STIE YPKP, serta mendirikan STT YPKP. Universitas Sangga Buana Yayasan Pendidikan Keuangan dan Perbankan, yang disingkat USB YPKP berdiri sejak dikeluarkannya Surat Keputusan DIKTI nomor 178/D/O/2006, tanggal 24 Agustus 2006 USB YPKP terdiri dari tiga Fakultas, yang merupakan hasil penggabungan Sekolah Tinggi Ilmu Ekonomi (STIE) YPKP (sekarang menjadi Fakultas Ekonomi USB YPKP) dengan Sekolah Tinggi Teknologi (STT) YPKP (sekarang menjadi Fakultas Teknik USB YPKP), ditambah dengan pendirian Fakultas baru, yaitu Fakultas Ilmu Komunikasi dan Administrasi (FIKA).

Berdasarkan permasalahan di atas, maka peneliti tertarik untuk melakukan penelitian dengan judul “Audit Keamanan dan Manajemen Resiko Sistem Informasi Akademik Dengan Framework NIST (Studi Kasus : Universitas Sangga Buana YPKP)”.

1.2 Rumusan Masalah

Adapun permasalahan yang terjadi pada sistem informasi akademik di Universitas Sangga Buana YPKP adalah:

1. Bagaimana sistem keamanan yang diterapkan pada sistem informasi akademik di Universitas Sangga Buana YPKP?
2. Bagaimana manajemen resiko yang dilakukan pada sistem informasi akademik di Universitas Sangga Buana YPKP?
3. Rekomendasi apakah yang dapat diberikan terkait keamanan dan manajemen resiko sistem informasi akademik di Universitas Sangga Buana YPKP Bandung?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang ditemukan, maka penelitian ini bertujuan:

1. Untuk menganalisa sistem kemanan yang diterapkan pada sistem informasi akademik di Universitas Sangga Buana YPKP
2. Untuk menganalisa manajemen resiko yang dilakukan pada sistem informasi akademik di Universitas Sangga Buana YPKP.
3. Untuk memberikan rekomendasi yang terkait dengan keamanan dan manajemen resiko sistem informasi akademik di Universitas Sangga Buana YPKP.

1.4 Ruang Lingkup

Ruang lingkup yang digunakan pada penelitian ini adalah sistem informasi akademik di Universitas Sangga Buana yang merupakan proses pencatatan kegiatan belajar mengajar yang pada akhirnya akan melahirkan data-data seperti data mahasiswa, absensi mahasiswa, data dosen, absensi dosen, honor dosen, nilai mahasiswa, laporan nilai untuk orang tua siswa, dan evaluasi kinerja dosen.

1.5 Metode Penelitian

Dalam penelitian ini akan dilakukan penilaian terhadap keamanan dan manajemen resiko sistem informasi akademik. Untuk dapat melakukan proses penilaian tersebut, beberapa tahapan yang dilakukan adalah.

1. Studi Pustaka

   Studi pustaka merupakan pengumpulan berbagai informasi yang memiliki hubungan dengan topik penelitian. Informasi-informasi tersebut diambil dari berbagai sumber seperti buku, jurnal, artikel, ataupun sumber lain yang tetap memiliki keterkaitan dengan penelitian ini.

2. Pengumpulan Data

   Data yang dibutuhkan untuk melakukan penelitian ini didapat melalui proses penyebaran kuisioner kepada pihak responden sesuai dengan sampel yang sudah ditentukan dari populasi.

3. Analisa Data

   Data yang terkumpul selanjutnya dianalisa dengan menggunakan aplikasi Microsoft Excel.

1.6 Sistematika Penulisan

Sistematika penulisan dibuat untuk mempermudah peneliti untuk menjalankan proses penelitian ini. Sistematika penulisan terdiri sebagai berikut.

BAB I : Pendahuluan

Menjelaskan secara umum latar belakang, rumusan masalah, tujuan penelitian, ruang lingkup (batasan masalah), metode penelitian dan sistematika penulisan.

BAB II : Tinjauan Pustaka

Merupakan kumpulan teori dan informasi yang berkaitan dengan topik penelitian, khususnya yang berkaitan dengan analisis keamanan dan manajemen resiko sistem infomasi akademik.

BAB III : Objek dan Metodologi Penelitian

Berisi profil Universitas Sangga Buana YPKP dan proses bisnis sistem informasi akademik, sample yang akan dijadikan responden dan metode yang akan digunakan pada penelitian.

BAB IV : Analisis dan Pembahasan

Menjabarkan prosedur dalam menganalisa data yang terkumpul dan dilakukan pembahasan untuk dapat memperoleh sesuatu yang diharapkan dari penelitian terhadap sistem informasi akademik di Universitas Sangga Buana YPKP.

BAB V : Kesimpulan dan Saran

Berisi kesimpulan dan saran penulis sesuai dengan hasil penelitian untuk memaksimalkan peran dan keamanan dari sistem informasi akademik yang ada di Universitas Sangga Buana YPKP.

BAB II

TINJAUAN PUSTAKA

2.1 Keamanan Sistem Informasi

Sistem informasi menjadi salah satu aspek penting bagi perusahaan dalam mencapai tujuan dengan bantuan teknologi informasi. Hal tersebut dikarenakan Kerahasiaan informasi menjadi sangat krusial mengingat informasi-informasi tersebut menjadi aset berharga bagi perusahaan.

Keamanan sistem informasi merupakan hal yang perlu mendapat perhatian saat membangun sebuah sistem informasi. Bayangkan kita membuat sebuah rumah yang lengkap dengan jendela dan pintu, tetapi kita tidak membuat kunci untuk pintu dan jendela. Hal ini dapat menyebabkan seseorang bisa dengan mudah memasuki rumah kita, bahkan mungkin melakukan pencurian. Sama halnya dengan membangun sistem informasi, keamanan sistem informasi digunakan untuk menghindari seseorang yang tidak memiliki akses untuk dapat masuk ke dalam sistem. (Chazar, 2015).

2.1.1 Komponen Keamanan Sistem Informasi

Menurut Simanungkalit (2009), Keamanan Informasi adalah perlindungan informasi dari berbagai macam ancaman agar menjamin kelanjutan usaha / bisnis, mengurangi resiko bisnis dan meningkatkan *return of investment* dan peluang bisnis. Keamanan sistem informasi merupakan suatu kegiatan perlindungan atau pencegahan terhadap gangguan penyalahgunaan informasi yang dilakukan oleh orang-orang yang tidak bertanggung jawab terhadap jalannya suatu sistem. Menurut HARR dalam Simanungkalit (2009) keamanan informasi meliputi perlindungan terhadap tiga aspek, yaitu Kerahasiaan (*Confidentiality*), Integritas (*Integrity*) dan Ketersediaan (*Availability*). Ketiga aspek tersebut dikenal dengan CIA Triad dan menjadi prinsip dasar keamanan informasi.

Gambar 2.1. *CIA Triad* (Kelley, 2017)

Menurut Chazar (2015), penjelasan dari aspek – aspek tersebut adalah sebagai berikut.

1. *Confidentiality* (Kerahasiaan)

   Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenangdan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.

2. *Integrity* (Integritas)

   Aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas ini.

3. *Availability* (Ketersediaan)

   Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan *user* yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana dibutuhkan).

2.1.2 Audit Keamanan Sistem Informasi

Menurut Gondodiyoto (2007) tujuan audit sistem informasi, yaitu :

1. Pengamanan Aset

   Asset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia (*brainware*), file data dan fasilitas lain harus dijaga dengan sistem pengendalian intern yang baik agar tidak terjadi

penyalahgunaan asset perusahaan. Dengan demikian sistem pengamanan asset merupakan suatu hal yang sangat penting yang harus dipenuhi oleh perusahaan.

2. Efektifitas Sistem

   Efektifitas sistem perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut sudah dirancang dengan benar (*doing the right thing*), telah sesuai dengan kebutuhan user. Informasi yang dibutuhkan oleh para manager dapat dipenuhi dengan baik.

3. Efisiensi Sistem

   Efisiensi menjadi sangat penting ketika sumber daya kapasitasnya berbatas. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan user dengan sumber daya informasi yang minimal.

4. Ketersediaan

   Berhubungan dengan ketersediaan dukungan atau layanan teknologi informasi (TI). TI hendaknya dapat mendukung secara continue terhadap proses bisnis (kegiatan perusahaan). Makin sering terjadi gangguan (*System down*) maka berarti tingkat ketersediaan sistem lemah.

5. Kerahasiaan

   Fokusnya ialah pada proteksi terhadap informasi dan supaya terlindung dari akses dari pihak-pihak yang tidak berwenang.

6. Kehandalan

   Berhubungan dengan kesesuaian dan keakuratan bagi manajemen dalam pengelolaan organisasi, pelaporan dan pertanggungjawaban.

7. Menjaga Integritas Data

Integritas data (data integrity) adalah salah satu konsep dasar dari sistem informasi. Data memiliki atribut-atribut seperti : kelengkapan, kebenaran, dan keakuratan.

2.1.3 NIST SP 800-26

Swanson (2001), melalui publikasi khusus *framework* NIST SP 800-26 mengungkapkan ada setidaknya 17 kriteria yang harus dipenuhi sebuah perusahaan dalam menjaga keamanan sistem informasi di perusahaan tersebut. Kriteria tersebut yaitu.

1. *Management Control*
    a. *Risk Management*
    b. *Review of Security Controls*
    c. *Life Cycle*
    d. *Authorize Processing*
    e. *System Security Plan*
2. *Operational Control*
    a. *Personnel Security*
    b. *Physical Security*
    c. *Production, Input/Output Control*
    d. *Contigency Planning*
    e. *Hardware and System Software Maintenance*
    f. *Data Integrity*
    g. *Documentation*
    h. *Security Awarness, Training, And Education*
    i. *Incident Response Capability*
3. *Technical Control*
    a. *Identification and Authentication*
    b. *Logical Access Controls*
    c. *Audit Trails*

Pada NIST SP 800-26 disebutkan bahwa ada 5 tingkatan atau level keamanan pada teknologi informasi. 5 tingkatan tersebut adalah.

1. Level 1 - *Documented Policy* (Kebijakan terdokumentasi)
2. Level 2 - *Documented Procedures* (Prosedur terdokumentasi)
3. Level 3 - *Implemented Procedures and Controls* (prosedur dan pengendalian sudah dilakukan)
4. Level 4 - *Tested and Reviewed Procedures and Controls* (prosedur dan pengendalian sudah diuji dan ditinjau)
5. Level 5 - *Fully Integrated Procedures and Controls* (prosedur dan pengendalian sudah sepenuhnya terintegrasi).

2.2 Manajemen Resiko

Pada subbab ini, akan dijelaskan mengenai hal – hal yang berhubungan dengan manajemen resiko.

2.2.1 Resiko

Definisi risiko adalah akibat negatifdari sebuah kejadian atau suatu keputusan yang diambil dalam kehidupan sehari-hari. (Pinontoan,2010). Darmawi (2006:1) mendefinisikan risiko sebagai kemungkinan akan terjadinya akibat buruk atau akibat yang merugikan, seperti kemungkinan kehilangan, cedera, kebakaran dan sebagainya. Dalam risiko tidak ada metode apapun yang bisa menjamin seratus persen bahwa akibat buruk itu setiap saat dapat dihindarkan, kecuali kalau kegiatan yang mengandung unsur risiko tidak dilakukan.

Menurut Idroes (2008), Risiko merupakan peluang bagi organisasi untuk mencapai tujuannya dengan menerapkan konsep manajemen risiko yang sesuai dengan kebutuhan organisasi. Manajemen risiko didefinisikan sebagai suatu metode logis dan sistematik dalam identifikasi, kuantifikasi, menentukan sikap, menetapkan solusi, serta melakukan monitor dan pelaporan risiko yang berlangsung pada setiap aktivitas atau proses.

2.2.2 Manajemen Resiko

Manajemen resiko merupakan sebuah proses penilaian terhadap resiko, mengambil langkah dalam rangka mengurangi resiko ke tingkat yang dapat diterima, dan menjaga tingkat resiko tersebut (Swanson, 2001). Nurochman (2014) mengatakan, dalam melaksanakan kegiatan manajemen resiko teknologi informasi dan sistem informasi terdapat beberapa kerangka kerja yang merupakan kumpulan prosedur standar dalam mengelola dan memberikan pemahaman untuk kegiatan manajemen risiko yang dilaksanakan secara bertahap. NIST mengeluarkan rekomendasi melalui publikasi khusus framework NIST SP 800-30 tentang "*Risk Management Guide For Information Technology System"*. Terdapat tiga proses dalam manajemen resiko yakni: proses penilaian resiko, proses peringanan (mitigasi) resiko dan proses evaluasi resiko. Masing-masing tahapan proses tersebut memiliki kerangka kerja terstruktur untuk memberikan penjelasan kerangka kerja manajemen risiko teknologi informasi. Proses kerangka kerja NIST meliputi: risk asssessment (penilaian risiko), risk mitigation (peringanan risiko) dan risk evaluation (evaluasi risiko). Penerapan manajemen resiko pada sebuah organisasi bertujuan untuk menghindari segala resiko yang mungkin terjadi pada organisasi tersebut.

Manajemen resiko merupakan proses yang memungkinkan manajer IT untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi (Stoneburner, 2002). Jakaria (2013) menuturkan, tujuan utama melakukan analisis resiko adalah untuk mengukur dampak dari potensi ancaman, menentukan berapa besar kerugian yang diderita akibat hilangnya potensi bisnis. Hasil utama dari analisis resiko dua diantaranya adalah identifikasi resiko dan jumlah biaya berbanding manfaatnya untuk penanggulangan resiko kerusakaan.

Krutz (2006) mengatakan manfaat melakukan analisis resiko antara lain menciptakan rasio *cost-to-value* yang jelas untuk perlindungan keamanan. Hal ini juga mempengaruhi

proses pengambilan keputusan yang berhubungan dengan konfiguras *hardware* dan design sistem *software*.

Blokdijk (2008) mengatakan, suatu upaya dari perencanaan, perngorganisasian, memimpin dan mengendalikan sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian akibat kecelakaan pada biaya yang paling dapat diterima. Untuk memenuhi kebutuhan spesifik organisasi, keberhasilan manajemen resiko harus menyeimbangkan pengendalian resiko dan teknik resiko pembiayaan dengan mempertimbangkan visi, misi, nilai – nilai dan tujuan organisasi.

2.2.3 NIST SP 800-30

Stoneburn (2002), melalui publikasi khusus framework NIST SP 800-30 tentang *Risk Management Guide For Information Technology System* mengatakan, setiap kerangka kerja yang terdapat pada manajemen risiko memiliki tahapan masing – masing. Tahapan – tahapan tersebut adalah.

1. *Risk Assessment*
    a. Identifikasi Sistem

        Langkah pertama dalam penilaian risiko adalah melakukan identifikasi terhadap sistem yang akan diteliti. Mengidentifikasi sistem informasi tersebut bertujuan untuk menentukan ruang lingkup dari proses penilaian risiko, batasan dari wewenang dalam melakukan pengujian, serta mendapatkan informasi terkait sistem informasi tersebut seperti perangkat keras, perangkat lunak, keterhubungan sistem, divisi yang bertanggung jawab, dan personil yang membantu.

    b. Identifikasi Ancaman

        Tujuan dari langkah ini adalah untuk mengidentifikasi sumber ancaman yang dapat terjadi pada sistem informasi untuk dijadikan bahan evaluasi terhadap sistem tersebut. Dalam menilai sumber ancaman, sangat penting untuk mengetahui semua sumber ancaman yang dapat membahayakan bagi sistem

informasi dan lingkungan yang mempengaruhinya. Berdasarkan sumbernya, ancaman terbagi menjadi 3 (tiga) jenis, yaitu ancaman yang berasal dari alam (*natural threat*), ancaman yang berasal dari tingkah laku manusia (*human threat*), dan ancaman yang diakibatkan oleh dampak dari lingkungan sekitar (*environmental threat*).

c. Identifikasi Kerentanan

Tahapan analisis terhadap ancaman harus meliputi analisis terhadap kerentanan yang berhubungan dengan sistem informasi tersebut. Tujuan dari tahapan ini adalah untuk mengidentifikasi dan mengembangkan kerentanan (kelemahan) dari sistem agar dapat mengurangi kemungkinan masuknya ancaman pada sistem. Kerentanan merupakan titik lemah dari sebuah sistem yang berkaitan dengan prosedur pengamanan, perancangan, implementasi, ataupun pengendalian internal.

d. Analisis Pengendalian

Tujuan dari langkah ini adalah untuk menganalisa pengendalian yang sudah diimplementasikan ataupun yang sudah direncanakan untuk diimplementasikan oleh pihak institusi dengan harapan dapat mengurangi atau meghilangkan kemungkinan masuknya ancaman melalui kerentanan atau kelemahan pada sistem. Pada umumnya, terdapat 2 (dua) metode yang dapat digunakan untuk proses pengendalian keamanan pada sistem informasi, yaitu metode pengendalian teknikal dan metode pengendalian non-teknikal. Metode pengendalian teknikal berupa pengamanan pada hal-hal yang berhubungan dengan perangkat keras, perangkat lunak, dan perangkat pendukung. Metode pengendalian non-teknikal berupa pengendalian manajemen dan pengendalian operasional seperti ketentuan pengamanan, prosedur operasional, pengamanan personil, fisik, dan lingkungan sekitar. Berdasarkan sifatnya, pengendalian yang

dilakukan terbagi menjadi pengendalian yang bersifat mencegah dan pengendalian yang bersifat mendeteksi.

e. Penilaian Kecenderungan Risiko

Tingkat kecenderungan terjadinya risiko dapat digambarkan ke dalam 3 (tiga) tingkatan, yaitu.

1) Kecenderungan risiko tingkat tinggi, ketika risiko tersebut memiliki kemungkinan timbul yang tinggi dan pengendalian yang dilakukan oleh pihak institusi berjalan tidak efektif.
2) Kecenderungan risiko tingkat sedang, ketika risiko tersebut memiliki kecenderungan timbul yang sedang dan pengendalian yang dilakukan oleh pihak institusi berjalan efektif sebagian.
3) Kecenderungan risiko tingkat rendah, ketika risiko tersebut memiliki kecenderungan timbul yang rendah dan pengendalian yang dilakukan oleh pihak institusi sudah berjalan dengan baik.

f. Analisis Dampak

Salah satu langkah dalam mengukur tingkat risiko adalah menentukan dampak yang dihasilkan akibat ancaman yang masuk melalui kerentanan pada sistem informasi. Besar dari dampak yang ditimbulkan terbagi menjadi 3 (tiga) tingkatan, yaitu risiko dengan dampak tinggi, risiko dengan dampak sedang, dan risiko dengan dampak rendah. Penilaian dampak risiko tersebut dipengaruhi oleh beberapa faktor diantaranya, seberapa besar biaya yang harus dikeluarkan akibat hilangnya aset institusi, pengaruh risiko terhadap visi, misi dan reputasi institusi di masa depan, serta kemungkinan adanya masalah yang timbul pada kesehatan personil institusi.

g. Penilaian Tingkat Risiko

Tingkat resiko dapat dinilai dengan menggunakan matriks tingkat resiko (*risk-level matrix*). Penilaian menggunakan matriks tingkat resiko dapat ditentukan

berdasarkan tingkat kecenderungan resiko dan dampak dari resiko tersebut. Tabel 2.1 memperlihatkan tingkat resiko dengan menggunakan *risk-level matrix*.

Tabel 2.1 *Risk-Level Matrix*

Likelihood	*Impact*		
	Rendah	Sedang	Tinggi
Tinggi	Rendah	Sedang	Tinggi
Sedang	Rendah	Sedang	Sedang
Rendah	Rendah	Rendah	Rendah

Berdasarkan tabel 2.1 tersebut, dapat terlihat penilaian tingkat resiko yang mungkin terjadi berdasarkan tingkat kecenderungan dan tingkat dampak jika resiko tersebut terjadi. Penjelasan tabel 2.1 tersebut dapat dilihat pada beberapa contoh berikut.

1) Jika sebuah resiko memiliki kecenderungan terjadi rendah dan dampak yang ditimbulkan rendah, maka tingkat resiko tersebut adalah rendah.
2) Jika sebuah resiko memiliki kecenderungan terjadi sedang dan dampak yang ditimbulkan tinggi, maka tingkat resiko tersebut adalah sedang.
3) Jika sebuah resiko memiliki kecenderungan terjadi tinggi dan dampak yang ditimbulkan tinggi, maka tingkat resiko tersebut adalah tinggi.

a. Rekomendasikan Pengendalian

Langkah ini memungkinkan pihak institusi untuk mendapatkan masukan ataupun rekomendasi yang sesuai dan cocok dengan kondisi institusi terkait risiko yang mungkin terjadi pada sistem informasi akademik. Rekomendasi tersebut dimaksudkan untuk meminimalisir atau menghilangkan kecenderungan risiko untuk mempengaruhi sistem informasi yang digunakan dan untuk menguatkan sistem pengamanan pada sistem informasi baik itu dari internal maupun eksternal.

b. Dokumentasi hasil

Ketika tahapan penilaian terhadap risiko selesai dilakukan, hasil yang didapat seharunya didokumentasikan sebagai laporan resmi ataupun sebagai bahan evaluasi institusi di masa yang akan datang.

2. *Risk Mitigation*

   a. Menentukan prioritas pelaksanaan

      Prioritas pelaksanaan untuk mencegah terjadinya resiko dimulai dari tingkat dan kecenderungan resiko yang paling berat.

   b. Mengevaluasi pengendalian yang direkomendasikan

      Proses pengendalian yang dilakukan dievaluasi untuk mendapatkan pengendalian lain agar dapat mengurangi kemungkinan resiko terjadi dengan lebih baik.

   c. Menganalisa biaya dan keuntungan

      Menghitung dan menganalisa alur biaya dan dampak dari proses pengendalian dalam hal keuangan.

   d. Memilih jenis pengendalian

      Menentukan jenis pengendalian lanjutan yang akan dilakukan untuk mengurangi resiko yang tersisa.

   e. Menetapkan tanggung jawab

      Membagi tanggung jawab untuk setiap SDM dengan tujuan memudahkan proses pengendalian.

   f. Mengembangkan rencana implementasi pemeliharaan

      Mengevaluasi dan mengembangkan rencana yang sudah disusun untuk diimplementasikan sebagai proses pemeliharaan.

   g. Mengimplementasikan pengendalian yang dipilih

      Melakukan upaya proses pengendalian setelah dilakukan pengembangan.

3. *Risk Evaluation*

   a. *Good Security Practice*

      Melakukan evaluasi dan pengendalian secara berkala untuk mencegah terjadinya resiko dalam waktu yang relatif lama.

b. *Keys For Success*

Beberapa kunci sukses dalam menerapkan manajemen resiko yaitu.

(1) Komitmen dari manajemen senior

(2) Dukungan penuh dari pihak IT

(3) Pengelolaan yang kompeten dari pihak pengelola resiko

(4) Kesadaran dari para pengguna

(5) Evaluasi dan penilaian secara berkala

Dalam penerapan sistem informasi, secara khusus Gibson (2011) mengemukakan "*risk management is the practice of identifying, assessing, controlling, and mitigating risks*". Manajemen resiko diartikan sebaga kegiatan praktis tentang identifikasi, penilaian, pengontrolan dan peringanan resiko. Pelaksanaan manajemen resiko merupakan tahapan kegiatan organisasi dalam mengidentifikasi dan memandang sumber resiko, kerentanan resiko secara menyeluruh dan terkontrol dengan dilaksanakan evaluasi proses secara berkesinambungan.

2.3 Sistem Informasi

Jogiyanto (2005) mengungkapkan sistem informasi adalah suatu sistem didalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategis dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang dibutuhkan. Gondodiyoto (2007) dalam bukunya mengatakan bahwa sistem informasi dapat didefinisikan sebagai kumpulan elemen-elemen atau sumberdaya dan jaringan prosedur yang saling berkaitan secara terpadu, terintergrasi dalam suatu hubungan hirarkis tertentu, dan bertujuan untuk mengolah data menjadi informasi.

Sutarbi (2005), dalam bukunya yang berjudul Sistem Informasi Manajemen, menuturkan bahwa sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi operasi organisasi yang bersifat manajerial dengan kegiatan strategi dari suatu

organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan – laporan yang diperlukan. Sistem informasi pada umumnya dapat terbentuk dengan beberapa kegiatan operasi tetap berikut.

1. Pengumpulan data
2. Pengelompokan data
3. Penghitungan data
4. Analisa topik data
5. Penyajian laporan

2.3.1 Komponen Sistem Informasi

Hutahaean (2014), dalam bukunya berjudul Konsep Sistem Informasi, menuturkan sistem informasi terdiri dari komponen – komponen yang disebut dengan istilah blok bangunan (*building block*), yaitu

1. Blok Masukan (*input block*)

   Input mewakili data yang masuk ke dalam sistem informasi. Input disini termasuk metode – metode dan media yang digunakan untuk menangkap data yang akan dimasukkan, yang dapat berupa dokumen dasar.

2. Blok Model (*Model Block*)

   Blok ini terdiri dari kombinasi prosedur, logika, dan metode matematik yang akan memanipulasi data input dan data yang tersimpan di basis data dengan cara yang sudah tertentu untuk menghasilkan keluaran yang sudah diinginkan.

3. Blok Keluaran (*Output Block*)

   Produk dari sistem informasi adalah keluaran yang merupakan informasi yang berkualitas dan dokumentasi yang berguna untuk semua tingkatan manajemen serta semua pemakai sistem.

4. Blok Teknologi (*Technology Block*)

   Teknologi digunakan untuk menerima input, menjalankan model, menyimpan dan mengakses data, menghasilkan dan mengirimkan keluaran dan membantu pengendalian diri secara keseluruhan. Teknologi terdiri dari unsur utama.

   a. Teknisi (*humanware* dan *brainware*)
   b. Perangkat lunak (*software*)
   c. Perangkat keras (*Hardware*)

5. Blok Basis Data (*Database Block*)

   Merupakan kumpulan dari data yang saling berhubungan satu dengan yang lainnya, tersimpan di perangkat keras komputer dan digunakan perangkat lunak untuk memanipulasinya.

6. Blok Kendali (*Control Block*)

   Banyak faktor yang dapat merusak sistem informasi, misalnya bencana alam, api, temperature tinggi, air, debu, kecurangan-kecurangan, kejanggalan sistem itu sendiri, kesalahan-kesalahan, ketidakefisienan, sabotase dan sebagainya. Beberapa pengendalian perlu dirancang dan diterapkan untuk meyakinkan bahwa hal-hal yang dapat merusak sistem dapat dicegah atau bila terlanjur terjadi kesalahan dapat langsung diatasi.

2.3.2 Sistem Informasi Akademik

Tantra (2012) menyebutkan bahwa sistem informasi merupakan cara yang terorganisir, untuk mengumpulkan, memasukkan, dan memproses data dan menyimpannya, mengelola, mengontrol dan melaporkannya sehingga dapat mendukung perusahaan atau organisasi untuk mencapa tujuan. Menurut Satoto (2008), sistem Informasi Akademik (SIA) adalah perangkat lunak yang digunakan untuk menyajikan informasi dan menata administrasi yang berhubungan dengan kegiatan akademis. Dengan penggunaan perangkat lunak seperti ini diharapkan kegiatan administrasi

akademis dapat dikelola dengan baik dan informasi yang diperlukan dapat diperoleh dengan mudah dan cepat.

Menurut Davis (dalam Arifin, 2002) mengatakan data atau informasi merupakan kelompok teratur, studi yang mewakili kuantitas tindakan, benda dan sebagainya. Data berbentuk karakter yang dapat berupa alphabet, angka maupun symbol-simbol khusus. Data merupakan kelompok teratur yang refresentatif tidakan, barang/benda dan sebagainya. Mewakili kuantitas tindakan bisa juga dimaksudkan bahwa data tersebut merupakan hasil laporan kerja yang disajikan dalam bentuk laporan dengan karakter kuantitas atau banyaknya kegiatan ataupun tindakan yang dilakukan dalam perusahaan. Data atau informasi juga dapat mewakili benda/barang yang disajikan dalam bentuk laporan (mewakili keadaan benda/jasa).

Pengelolaan data bidang studi dan kurikulum mempermudah pencarian informasi akan salah satu bidang studi. Penyajian yang baik dalam klasifikasi (kriteria) tertentu dan menarik (meskipun tetap formal) akan dapat menampung data yang lebih besar dan menghasilkan informasi yang lebih berguna. Jika cara ini dipilih, Sejumlah informasi tambahan seharusnya dapat disertakan atau diberikan link ke perguruan tinggi penyelenggara. Misalnya tentang dosen pengajar dan perbedaan/persamaan materi. Secara terdistribusi Data dikelola oleh masing-masing, tetapi ada *gateway* ataupun penyajian yang disepakati bersama untuk kemudahan pembaca. Departemen pendidikan atau pemerintah juga memperoleh hak mengakses. Bila diperlukan pengumpulan data untuk arsip, dapat dilakukan melalui internet setiap saat dan mengurangi kebutuhan pertukaran data melalui media tercetak (*paperless*). Kegiatan perkuliahan dilakukan setiap semester mencakup: a) pendaftaran peserta kuliah pada semester yang akan berlangsung; b) perkuliahan yang sedang berjalan, yaitu materi dan tugas; dan c) ujian atau evaluasi atas hasil perkuliahan. (Lukum, 2013).

2.4 Studi Empiris

Penelitian ini memiliki keterkaitan dengan beberapa penelitian yang sudah dilakukan sebelumnya. Tabel 2.2 berikut ini menggambarkan mengenai penelitian terkait. Jurnal 1 tulisan Ucu Nugraha pada tahun 20016 melakukan implementasi kerangka kerja NIST 800-30 dengan tujuan untuk dapat menilai resiko yang dapat terjadi pada perguruan tinggi secara umum. Jurnal 2 yang diteliti oleh Arif Nurochman pada tahun 2014 menjelakan penerapan kerangkan kerja NIST 800-30 di perpustakaan milik Universitas Gadjah Mada sebagai standar penilaian dalam manajemen resiko sistem informasi.

Jurnal 3 yang dibuat oleh Wenni Syafitri pada tahun 2016 mengungkapkan penerapan kerangka kerja NIST 800-30 pada sistem informasi akademik di salah satu universitas. Jurnal 4 dibuat oleh Yana Aditia Gerhana dkk, menyebutkan penggunaan COBIT 4.1 dan NIST 800-30 sebagai beberapa standar penilaian terhadap resiko yang mungkin terjadi pada sistem informasi yang ada di Rumah Sakit Umum dr. Slamet Garut. Jurnal 5 yang diteliti oleh Wahyu S. Prabowo dkk, menyampaikan penerapan kerangka kerja NIST 800-30 yang dilakukan di Lembaga Ilmu Pengetahuan Indonesia (LIPI) dengan tujuan untuk memaksimalkan peran dan manfaat dari penggunaan teknologi dan mengurangi kemungkinan terjadinya resiko yang dapat merugikan lembaga.

Tabel 2.2 Studi Empiris

Penulis	Tahun	Judul	Kesimpulan Penelitian
Ucu Nugraha	2016	Manajemen Resiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST 800-30	Implementasikan kerangka kerja NIST 800-30 untuk mengetahui resiko yang mungkin terjadi dan memberikan rekomendasi yang sesuai dengan hasil penelitian
Arif Nurochman	2014	Manajemen Resiko Sistem Informasi Perpustakaan (Studi Kasus Di Perpustakaan Universitas Gadjah Mada)	Penerapan kerangka kerja NIST 800-30 di perpustakaan Universitas Gadjah Mada sebagai standar penilaian pengelolaan resiko
Wenni Syafitri	2016	Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus : Sistem Informasi Akademik Universitas XYZ)	Penerapan Kerangka Kerja NIST 800-30 pada Universitas XYZ dan menemukan total 58 resiko yang mungkin bisa terjadi

Penulis	Tahun	Judul	Kesimpulan Penelitian
Yana Aditia Gerhana Erdiansyah Undang Syarifudin	2011	Penilaian ResikoTeknologi Informasi dan Keamanan Sistem Informasi dengan Menggunakan *Framework* COBIT 4.1 dan *Guidelines* NIST SP 800-30 (Studi Kasus : Rumah Sakit Umum Dr Slamet Garut)	Penerapan *Framework* COBIT 4.1 dan NIST 800-30 sebagai standard model audit sistem informasi Rumah Sakit Umum dr. Slamet Garut
Wahyu S. Prabowo Widyawan Noor A. Setiawan M. Hanif Muslim Yoga S. Utama	2017	Manajemen Resiko Infrastruktur *Cloud* Pemerintah Menggunakan NIST *Framework* Studi Kasus Lembaga Ilmu Pengetahuan Indonesia (LIPI)	Penerapan standar manajemen resiko NIST untuk mengoptimalkan manfaat dari teknologi yang terdapat di LIPI

BAB III

OBJEK DAN METODE PENELITIAN

3.1 Universitas Sangga Buana Yayasan Pendidikan Keuangan dan Perbankan (USB YPKP)

3.1.1 Universitas Sangga Buana YPKP

Pengalaman Yayasan Pendidikan Keuangan dan Perbankan (YPKP) mengelola pendidikan lebih dari 44 tahun, semenjak 1968 mengelola Akademik Bank Nasional (ABN) Cabang Bandung , kemudian ABN berubah menjadi AKUBANK YPKP, dan berubah lagi menjadi STIE YPKP, serta mendirikan STT YPKP. Universitas Sangga Buana Yayasan Pendidikan Keuangan dan Perbankan, yang disingkat USB YPKP berdiri sejak dikeluarkannya Surat Keputusan DIKTI nomor 178/D/O/2006, tanggal 24 Agustus 2006 USB YPKP terdiri dari tiga Fakultas, yang merupakan hasil penggabungan Sekolah Tinggi Ilmu Ekonomi (STIE) YPKP (sekarang menjadi Fakultas Ekonomi USB YPKP) dengan Sekolah Tinggi Teknologi (STT) YPKP (sekarang menjadi Fakultas Teknik USB YPKP), ditambah dengan pendirian Fakultas baru, yaitu Fakultas Ilmu Komunikasi dan Administrasi (FIKA).

3.1.2 Visi

Menjadi Universitas yang unggul dan terkemuka serta mampu menghasilkan lulusan yang berkualitas dan berakhlak mulia dalam bidang ekonomi, teknik dan komunikasi serta dapat menyesuaikan diri terhadap perubahan global.

3.1.3 Misi

1. Menyelenggarakan Pendidikan kajian ekonomi, sosial, dan teknik secara profesional sesuai dengan perkembangan ilmu pengetahuan dan teknologi yang menghasilkan tenaga terdidik yang berakhlak mulia dan memiliki daya saing global.

2. Menciptakan dan membangun academik dan scientific atmosphere yang berbasis pada kajian ekonomi, sosial dan teknologi yang sesuai dengan ilmu pengetahuan, teknologi dan kesenian tertentu.
3. Melaksanakan pelayanan akademik secara profesional dan paripurna yang berbasis teknologi canggih.
4. Melaksanakan penelitian dan pengembangan serta penerapan ilmu ekonomi, sosial, dan teknologi
5. Melaksanakan 11 (sebelas) indikator pembinaan dan pengembangan Pendidikan Tinggi cq. Perguruan tinggi
6. Mempersiapkan dan meningkatkan mutu kesepuluh komponen yang menjadi penilaian BAN-PT.
7. Membantu mengembangkan kehidupan masyarakat dengan menerapkan ilmu pengetahuan dan teknologi yang relavan.

3.1.4 Tujuan

Pendirian USB YPKP bertujuan mencerdaskan kehidupan bangsa dan menunjang nilai-nilai luhur bangsa dalam mengelola program pendidikan dari Diploma, Sarjana dan Pascasarjana dalam upaya mencapai masyarakat adil, makmur dan sejahtera yang diridhoi oleh Allah SWT.

3.1.5 Program Kerja / Rencana Kegiatan Direktorat Pusat Data dan Informasi (PUDI)

Program kerja yang sudah disusun dan siap dilaksanakan oleh pihak Universitas Sangga Buana YPKP adalah sebagai berikut.

1. Menghitung/*feasibility study* kebutuhan dana untuk membangun/rehabilitasi Direktorat Sistem Informasi dan Multimedia.
2. Pengajuan proposal dana bantuan ke DIKTI dan Yayasan untuk pembangunan Direktorat Sistem Informasi dan Multimedia.

3. Investasi pembangunan Direktorat Sistem Informasi dan Multimedia dengan pendanaan Yayasan atau bantuan DIKTI.
4. Penyediaan sasaran dan prasarana untuk kebutuhan Direktorat Sistem Informasi dan Multimedia.Raker membehas mengenai upaya peningkatan fungsi dan peran Direktorat Sistem Informasi dan Multimedia.
5. *Recruitment* SDM untuk pengelola Direktorat Sistem Informasi dan Multimedia.
6. *Training and development* SDM Direktorat Sistem Informasi dan Multimedia.
7. Pelatihan (*training*) SDM USB YPKP untuk memahami pengoperasian beberapa *software* komputer, internet, intranet, *download – upload* data, dll dalam memanfaarkan sistem informasi yang ada.
8. Pengoperasian kembali terminal-terminal komputer di kampus untuk mendistribusikan informasi
9. Membuat buku tata tertib penggunaan/pemanfaatan sistem informasi melui Direktorat Sistem Informasi dan Multimedia.Lomba pembuatan/desain *website* USB YPKP
10. Raker membahas pembangunan Direktorat Sistem Informasi dan Multimedia secara komprehensif
11. Penyempurnaan dan *maintenace website* USB YPKP
12. Penyediaan layanan informasi akademik, keuangan, dll. Secara *online*
13. *Louncing* untuk sosialisasi beberapa layanan informasi dari Direktorat Sistem Informasi dan Multimedia.

3.1.6 Sistem Informasi Akademik (SIA) USB YPKP

Universitas Sangga Buana YPKP merupakan perguruan tinggi yang sudah mulai memanfaatkan perkembangan teknologi informasi sebagai *booster* untuk memberikan sebuah pelayanan yang ideal bagi seluruh *stakeholders*. Harapannya tentu saja adalah untuk menerapkan konsep perguruan tinggi berbasis IT dan memberikan pelayanan yang terbaik, khususnya bagi masyarakat selaku konsumen potensial. Salah satu bagian

yang sudah menerapkan teknologi informasi adalah akademik, yang biasa dikenal dengan sistem informasi akademik.

Sistem informasi akademik digunakan untuk melakukan proses pencatatan kegiatan belajar mengajar saat perkuliahan berlangsung. Proses pencatatan kegiatan belajar mengajar di Universitas Sangga Buana YPKP menggunakan data absensi mahasiswa dan dosen menggunakan teknologi sidik jari (*fingerprint*) sebagai input yang akan diolah. Data input tersebut akan terhubung dengan 3 bagian, yaitu pertama adalah fakultas yang merupakan tempat pengolahan data untuk menghasilkan data output seperti persentase absensi mahasiswa, nilai mahasiswa, perwalian mahasiswa, nilai untuk dilaporkan kepada orang tua siswa, absensi dosen, dan evaluasi kinerja dosen. Kedua adalah bagian keuangan yang berhubungan dengan penerimaan pembayaran uang kuliah oleh mahasiswa. Ketiga adalah bagian kepegawaian yang ditugaskan untuk menghitung jumlah gaji dan honorarium dosen pengajar.

Universitas Sangga Buana YPKP melakukan penerapan dengan menggunakan aplikasi TI yang dapat membantu kinerja institusi, meningkatkan mutu pembelajaran yang berkualitas kepada mahasiswa/i. Sistem yang digunakan oleh Universitas Sangga Buana YPKP adalah Sistem Presensi, sistem ini digunakan untuk proses perkuliahan yang berlangsung menggunakan mesin *finger print* yang berfungsi untuk mengontrol kehadiran mahasiswa dan dosen di Universitas Sangga Buana YPKP. Sistem Absensi pada Universitas Sangga Buana tergolong baru karena implementasinya baru dilakukan satu semester kebelakang. Pentingnya Sistem Absensi untuk proses absensi perkuliahan menjadikan sistem tersebut harus dalam kondisi yang optimal. Masih banyak kendala yang dialami diantaranya jadwal pengganti yang tidak muncul pada sistem meskipun telah disetting sehingga Dosen dan Mahasiswa tidak dapat melakukan absensi *finger print, finger* tidak terdeteksi dan kegagalan dalam melakukan absensi.

3.2 Metode Penelitian

Metode penelitian merupakan susunan langkah kerja yang dibuat secara berurutan untuk dapat mencapai tujuan yang diharapkan. Tahapan dalam penelitian ini secara garis besar pada gambar 3.1.

1. Persiapan Penelitian

   Persiapan penelitian ini berupa menentukan latar belakang dan mengidentifikasi masalah (tercantum pada bab 1), serta studi literatur dan observasi teori-teori seperti yang tercantum pada bab 2.

2. Menentukan Kriteria Penilaian dan Merancang Kuesioner

   Kriteria penelitian ditentukan berdasarkan *Framework* NIST *Special Publication* 800-26 yang dipublikasikan oleh *National Institute of Standards and Technology* dan dijadikan dasar untuk merancang kuesioner.

3. *Risk Assessment*

   Risk Assessment dilakukan berdasarkan tahapan yang terdapat pada *framework* NIST *Special Publication* 800-30.

4. Menentukan Responden

   Responden yang ditunjuk adalah struktural rektorat, fakultas, dan program studi. Struktural rektorat terdiri dari rektor beserta jajarannya, biro akademik, keuangan, kepegawaian, dan direktur PUDI beserta staffnya. Responden dari fakultas yaitu dekan fakultas dan responden dari program studi yaitu ketua program studi.

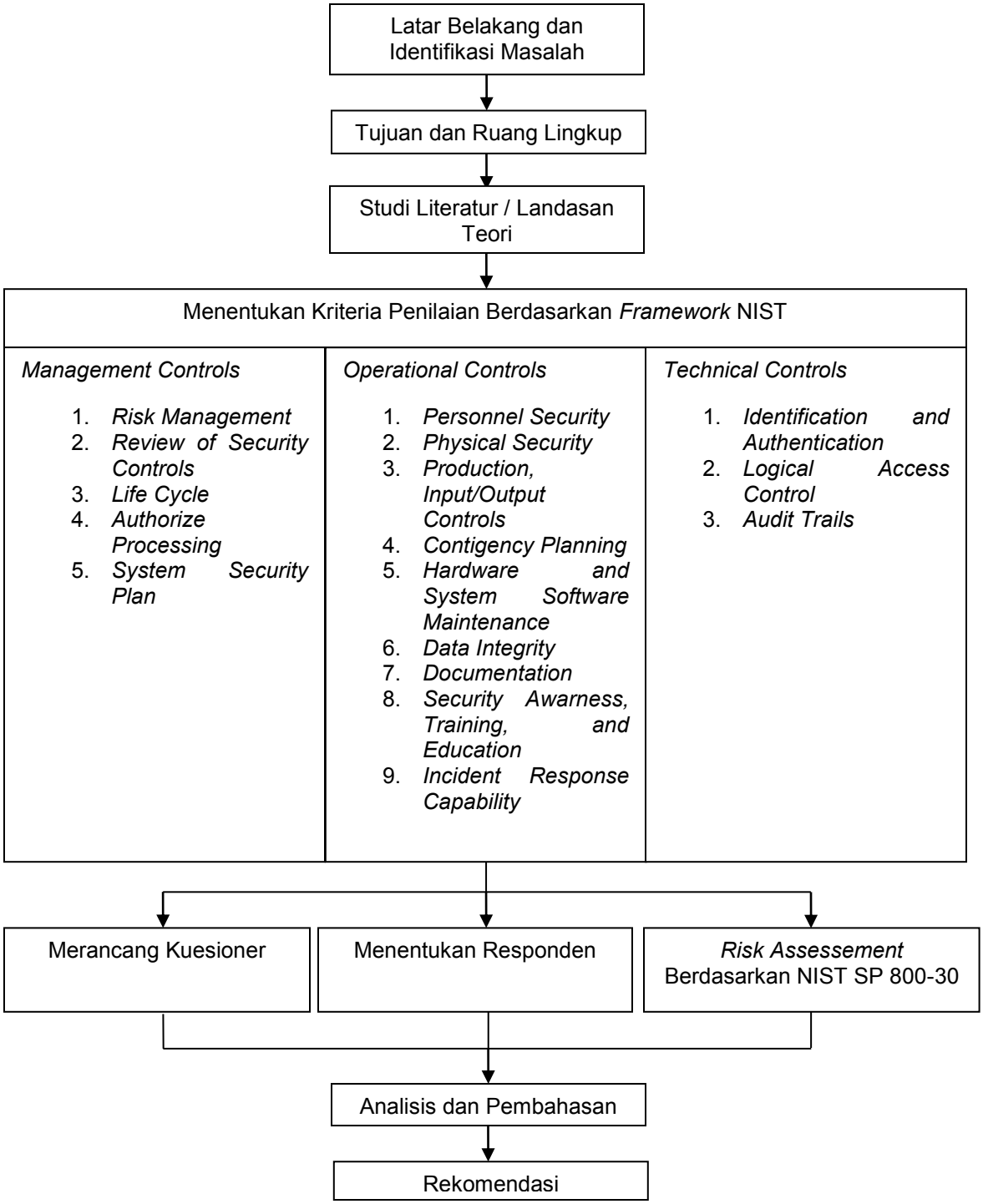
5. Analisa Data dan Pembahasan

   Data yang sudah diisi oleh para responden melalui kuisioner diolah dan dianalisa untuk dapat menarik kesimpulan terkait kondisi objek penelitian.

6. Rekomendasi

   Hasil dari analisis data dan pembahasan dari penelitian yang berupa rekomendasi dari peneliti. Rekomendasi ini diberikan untuk memaksimalkan peran dari sistem

informasi akademik di Unversitas Sangga Buana dan mengurangi kemungkinan terjadinya kerentanan yang bisa jadi timbul di masa yang akan datang.



Gambar 3.1 Tahapan Penelitian

3.3 Populasi

Populasi penelitian merupakan unsur penting dalam penelitian. Jika tidak ada populasi, maka data yang dibutuhkan tidak akan ada, yang menyebabkan tidak adanya penelitian yang dilakukan. Populasi penelitian merupakan kumpulan individu dengan kualitas serta ciri tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya (Iskandar, 2005). Populasi adalah keseluruhan data yang menjadi pusat perhatian seorang peneliti dalam ruang lingkup dan waktu yang telah ditentukan (Margono,2010). Berdasarkan uraian tersebut, maka dapat disimpulkan bahwa populasi adalah sekolompok orang, benda, atau hal lain yang memenuhi syarat – syarat tertentu yang berkaitan dengan masalah dalam penelitian. Maka dari itu, yang menjadi populasi dalam penelitian ini adalah Universitas Sangga Buana YPKP.

3.4 Sampel

Sampel merupakan bagian dari jumlah dan karakteristik yang dimiliki oleh populasi tersebut (Sugiyono, 2006). Sampel adalah sebagian atau wakil yang diteliti (Arikunto, 2002). Sampel dipilih dengan menggunakan teknik *purposive sampling*, yaitu suatu teknik penetapan sampel dengan yang dikehendaki peneliti sehingga sampel tersebut dapat mewakili karakteristik populasi yang telah dikenal sebelumnya (Nursalam, 2003). Berdasarkan hal tersebut, yang menjadi sampel pada penelitian ini adalah dosen struktural rektorat, fakultas, program studi dan staff PUDI sebagai pengendali utama sistem informasi akademik di Universitas Sangga Buana YPKP. Itu dikarenakan sistem informasi akademik langsung terhubung dengan pihak rektorat, fakultas, dan PUDI. Tabel 3.1 merupakan rincian responden berdasarkan jabatan strukturalnya.

Tabel 3.1 Responden Berdasarkan Jabatan Struktural di USB YPKP

No.	Jabatan	Jumlah Responden
1	Rektorat	11
2	Fakultas dan Prodi	20
3	Staff PUDI	9
TOTAL		40

3.5 Operasionalisasi Variabel Penelitian

Operasionalisasi variabel penelitian ini dibuat untuk mempermudah dalam menentukan jumlah pernyataan yang dibutuhkan dalam kuesioner. Operasionalisasi variable penelitian ini berisikan kategori beserta sub-kategori penilaian sesuai dengan kerangka kerja yang akan digunakan. Operasionalisasi variabel penelitian dapat dilihat pada tabel 3.2.

Tabel 3.2 Operasionalisasi Variabel Penelitian

Kategori	Subkategori	Skala Ukur	Item
Pengendalian Manajemen (*Management Control*)	*Risk Management*	Likert	1-2
	Review of Security Control		3-4
	Life Cycle		5-6
	Authorize Processing		7-8
	System Security Plan		9-10
Pengendalian Operasional (*Operasional Control*)	*Personnel Security*		11-12
	Physical Security		13-14
	Production, Input/Output Control		15-16
	Contigency Planning		17-18
	Hardware and Software Maintenance		19-20
	Data Integrity		21-22
	Documentation		23-24
	Security Awarness, Training and Education		25-26
	Incident Response Capability		27-28
Pengendalian Teknikal (*Techincal Control*)	*Identification and Authentication*		29-30
	Logical Access Control		31-32
	Audit Trails		33-34

3.6 Uji Validitas

Iskandar (2005) mengatakan bahwa validitas suatu alat ukur didefinisikan sebagai sifat suatuukuran yang memungkinkan peneliti beranggapan bahwa alat ukur itu dapat digunakan untuk mengukur karakter yang hendak diukurnya. Validitas adalah suatu ukuran yang menunjukkan tingkat keakuratan alat ukur. Suatu alat ukur dikatakan valid jika alat ukur itu menghasilkan ukuran yang tepat dalam suatu pengukuran masalah tertentu, dan tidak valid untuk mengukur masalah lain. Alat ukur yang valid dan akurat mempunyai validitas yang tinggi, sebaliknya alat ukur yang kurang valid memiliki validitas yang rendah. Pada umumnya, validitas alat ukur bergantung pada faktor logika dan pembuktian statistik.

Sugiyono (2010) mengatakan, untuk menguji validitas terhadap alat ukur yang berupa kuesioner, dapat dilakukan dengan cara mengkorelasikan skor butir alat ukur dengan skor totalnya. Rumus yang digunakan untuk menguji validitas instrumen adalah rumus korelasi *Pearson Product Moment.*

$$r_{hitung} = \frac{n\left(\sum XY\right) - \left(\sum X\right)\left(\sum Y\right)}{\sqrt{\left[n\left(\sum X^2\right) - \left(\sum X\right)^2\right]\left[n\left(\sum Y^2\right) - \left(\sum Y\right)^2\right]}}$$

Rumus *Pearson Product Moment* (3.1)

Untuk memudahkan perhitungan uji validitas ini, peneliti menggunakan *software Microsoft Excel*.

3.7 Uji Reliabilitas

Ghozali (2012) menyatakan bahwa reliabilitas adalah alat untuk mengukur suatu kuesioner yang merupakan indikator dari variabel atau konstruk. Suatu kuesioner dinyatakan reliabel atau handal jika jawaban seseorang terhadap penyataan adalah konsisten atau stabil dari waktu ke waktu. Pengujian reliabilitas sebuah instrument penilaian dapat dilakukan dengan teknik belah dua dan Spearman Brown dengan rumus sebagai berikut.

$$r_{11} = \frac{2r_b}{1 + r_b}$$

Rumus Spearman Brown (3.2)

Dalam teknik belah dua (*split Half*), butir-butir pernyataan pada kuesioner dibagi menjadi 2 kelompok, kelompok ganjil dan kelompok genap. Kedua kelompok pernyataan tersebut dihitung total skornya dan kemudian dicari korelasi antara kedua total skor tersebut. Untuk memudahkan perhitungan uji reliabilitas ini, peneliti menggunakan *software Microsoft Excel*.

BAB IV

ANALISIS DAN PEMBAHASAN

4.1 Proses Pengumpulan dan Perhitungan Data Kuesioner

Data penelitian didapatkan dari kuesioner yang diberikan kepada responden yang sudah ditentukan. Responden tersebut ditetapkan karena sistem informasi akademik langsung terhubung beberapa bagian, yaitu rektorat, fakultas, prodi, dan pihak PUDI. Oleh karena itu, para responden tersebut dianggap sebagai pengendali utama dari sistem informasi akademik yang ada di Universitas Sangga Buana YPKP Bandung. Responden yang ditetapkan terdiri dari struktural rektorat, fakultas, program studi, dan staff PUDI. Jumlah keseluruhan struktural dan staff PUDI sebanyak 79 orang dan dari jumlah tersebut diambil sebanyak 40 responden, yang terbagi menjadi 11 orang responden dari struktural rektorat, 20 orang responden dari fakultas dan prodi, serta 9 orang dari staff PUDI. Jumlah tersebut mencapai setengah dari jumlah struktural dan staff PUDI yang ada di Universitas Sangga Buana YPKP. Jumlah tersebut ditentukan untuk mengurangi kemungkinan terjadinya penyimpangan yang cukup besar apabila jumlah responden yang ditentukan hanya sedikit.

Selama proses pengumpulan data penelitian tersebut, peneliti mendampingi responden, dengan tujuan untuk menjaga tingkat akurasi dalam pengisian agar dapat mengurangi kemungkinan terjadinya perbedaan pandangan terhadap masing – masing pernyataan pada kuesioner tersebut. Data yang diperoleh dari para responden dapat dikatakan valid. Hal tersebut dikarenakan setiap responden yang mendapatkan dan mengisi kuesioner tersebut didampingi dan diberi pengarahan oleh peneliti dengan bantuan dari direktur PUDI.

Setiap sub kriteria penilaian masing – masing diwakili oleh 2 buah pernyataan yang diambil dari pernyataan utnuk kuesioner yang disediakan oleh *framework* NIST *Special*

Publication 800-26. Setiap pernyataan menggunakan skala linkert, yang artinya masing – masing pernyataan memiliki nilai antara 1 (tidak setuju/TS) hingga 5 (sangat setuju/SS). Nilai pada kuesioner tersebut kemudian dikalkulasikan untuk menghitung nilai rata – rata dengan menggunakan aplikasi *Microsoft Excel*. Nilai rata – rata tersebut menggambarkan tingkat keamanan sistem informasi akademik di Universitas Sangga Buana YPKP berdasarkan nilai tiap kategori dan nilai dari pemahaman responden berdasarkan jabatan struktual di USB YPKP.

4.2 Hasil Perhitungan Tingkat Keamanan

Pengukuran tingkat keamanan ini dilakukan setelah peneliti mendapatkan kembali kuesioner yang sudah dilengkapi dengan data dari responden. Perhitungan tersebut dilakukan dengan menggunakan aplikasi *Microsoft Excel*. Data yang diharapkan didapat dari proses penghitungan tersebut adalah nilai rata – rata yang nantinya mencerminkan tingkat keamanan sistem informasi akademik di Universitas Sangga Buana YPKP. Perhitungan tersebut dibagi menjadi 2 (dua) bagian, yaitu berdasarkan kategori dan berdasarkan jabatan struktural. Perhitungan berdasarkan kategori dilakukan untuk menilai tingkat keamanan pada sistem informasi akademik di Universitas Sangga Buana YPKP, sedangkan perhitungan berdasarkan jabatan struktural dilakukan untuk melihat apakah terdapat perbedaan pandangan terhadap sistem informasi akademik yang digunakan sesuai dengan tingkatan jabatan strukturalnya. Hal tersebut dilakukan dengan harapan dapat menilai keberhasilan dari pelatihan rutin yang dilakukan oleh pihak institusi.

4.2.1 Hasil Perhitungan Tingkat Pengendalian Manajemen (*Management Control*)

Data hasil penilaian responden melalui kuesioner dikumpulkan dan dimasukkan sesuai dengan kategori masing – masing. Data yang dikumpulakan berasal dari responden yang sudah ditetapkan sebelumnya, yaitu struktural rektorat, fakultas dan prodi, serta staff PUDI. Masing – masing sub kretirea memiliki 2 pernyataan yang mewakili.

Tabel 4.1 Perhitungan Data Kuesioner Kategori Pengendalian Manajemen

No.	Sub Kriteria Pertanyaan	Skala *Likert*					Jumlah Data	Rata – Rata	Persentase (%)
		5	4	3	2	1			
1	*Risk Management*	14	30	28	7	1	80	3,6125	72,25
2	*Review of Security Control*	13	36	22	8	1	80	3,6500	73,00
3	*Life Cycle*	12	33	26	7	2	80	3,5750	71,50
4	*Authorize Processing*	13	26	27	8	6	80	3,4000	68,00
5	*System Security Plan*	14	27	24	13	2	80	3,4750	69,50
Jumlah		66	152	127	43	12	400	17,7125	354,25
Rata-rata Keseluruhan								3,5425	70,85

Tabel 4.1 menunjukan hasil dari data yang didapat melalui pernyataan pada kuesioner berdasarkan penilaian dari total 40 (empat puluh) responden. Hasil tersebut menunjukkan tingkat keamanan dari sistem informasi akademik untuk kategori pengendalian manajemen (*Management Control*).

Nilai persentase dihitung dengan rumus = (Nilai rata – rata/nilai maksimal)*100%. Berdasarkan data pada tabel 4.1, nilai yang diperoleh untuk setiap sub kategori bernilai antara 3,4000 – 3,7000 dan persentase sub kategori antara 68,00% – 73,00%, dengan nilai rata – rata nilai keseluruhan untuk kategori pengendalian manajemen (*manajemen control*) mencapai angka 3,5425 atau dengan persentase 70,85%. Hal ini menunjukkan bahwa tingkat keamanan yang sudah diimplementasikan untuk kategori pengendalian manajemen (*management control*) sudah berada pada level 3, yaitu prosedur dan pengendalian sudah diimplementasikan secara konsisten.

4.2.2 Hasil Perhitungan Tingkat Pengendalian Operasional (*Operational Control*)

Data yang dikumpulakan berasal dari responden yang sudah ditetapkan sebelumnya, yaitu struktural rektorat, fakultas dan prodi, serta staff PUDI. Masing-masing sub kretirea memiliki 2 pernyataan yang mewakili.

Tabel 4.2 Perhitungan Data Kuesioner Kategori Pengendalian Operasional

No.	Sub Kriteria Pertanyaan	Skala *Likert*					Jumlah Data	Rata – Rata	Persentase (%)
		5	4	3	2	1			
1	*Personnel Security*	16	26	25	11	2	80	3,5375	70,75
2	*Physical Security*	11	28	29	12	0	80	3,4750	69,50
3	*Prodoction, Input/Out Control*	8	30	32	10	0	80	3,4500	69,00
4	*Contigency Planning*	14	31	26	9	0	80	3,6250	72,50
5	*Hardware and Software Maintenance*	23	34	18	4	1	80	3,9250	78,50
6	*Data Integrity*	14	34	22	9	1	80	3,6375	72,75
7	*Documentation*	15	31	21	13	0	80	3,6000	72,00
8	*Security, Awarness, Training, and Education*	17	28	22	11	2	80	3,5875	71,75
9	*Incident Response Capability*	17	27	20	14	2	80	3,5375	70,75
Jumlah		135	269	215	93	8	720	32,3750	647,5
Rata-rata Keseluruhan								3,5972	71,94

Tabel 4.2 menunjukan hasil dari data yang didapat melalui pernyataan pada kuesioner berdasarkan penilaian dari total 40 (empat puluh) responden. Hasil tersebut menunjukkan tingkat keamanan dari sistem informasi akademik yang ada di Universitas Sangga Buana YPKP Bandung untuk katergori pengendalian operasional (*Operational Control*).

Nilai persentase dihitung dengan rumus = (Nilai rata – rata/nilai maksimal)*100%. Berdasarkan data pada tabel 4.2, nilai yang diperoleh untuk setiap sub kategori bernilai antara 3,4000 – 4,0000 dan persentase sub kategori antara 69,00% – 79,00%, dengan nilai rata – rata nilai keseluruhan untuk kategori pengendalian operasional (*Operational control*) mencapai angka 3,5972 atau dengan persentase 71,94%. Hal ini menunjukkan bahwa tingkat keamanan yang sudah diimplementasikan untuk kategori pengendalian operasional (*operational control*) sudah berada pada level 3, yaitu prosedur dan pengendalian sudah diimplementasikan secara konsisten.

4.2.3 Hasil Perhitungan Tingkat Pengendalian Teknikal (*Technical Control*)

Data hasil penilaian responden melalui kuesioner dikumpulkan dan dimasukkan sesuai dengan kategori masing-masing. Data yang dikumpulakan berasal dari responden yang sudah ditetapkan sebelumnya, yaitu struktural rektorat, fakultas dan prodi, serta staff PUDI. Masing-masing sub kretirea memiliki 2 pernyataan yang mewakili.

Tabel 4.3 Perhitungan Data Kuesioner Kategori Pengendalian Teknikal

No.	Sub Kriteria Pertanyaan	Skala *Likert*					Jumlah Data	Rata-Rata	Persentase (%)
		5	4	3	2	1			
1	*Identification and Authentification*	13	36	22	9	0	80	3,6625	73.25
2	*Logical Access Control*	15	32	25	8	0	80	3,6750	73.50
3	*Audit Trails*	17	31	26	6	0	80	3,7375	74.75
Jumlah		45	99	73	23	0	240	11,0750	221,5
Rata-rata Keseluruhan								3,6917	73,83

Tabel 4.3 menunjukan hasil dari data yang didapat melalui pernyataan pada kuesioner berdasarkan penilaian dari total 40 (empat puluh) responden. Hasil tersebut menunjukkan tingkat keamanan dari sistem informasi akademik yang ada di Universitas Sangga Buana YPKP Bandung untuk kategori pengendalian teknikal (*Technical Control*).

Nilai persentase dihitung dengan rumus = (Nilai rata-rata/nilai maksimal)*100%. Berdasarkan data pada tabel 4.3, nilai yang diperoleh untuk setiap sub kategori bernilai antara 3,6000 – 3,8000 dan persentase sub kategori antara 73,00% – 75,00%, dengan nilai rata-rata nilai keseluruhan untuk kategori pengendalian manajemen (*manajemen control*) mencapai angka 3,6917 atau dengan persentase 73,83%. Hal ini menunjukkan bahwa tingkat keamanan yang sudah diimplementasikan untuk kategori pengendalian operasional (*operational control*) sudah berada pada level 3, yaitu prosedur dan pengendalian sudah diimplementasikan secara konsisten.

4.2.4 Hasil Perhitungan Tingkat Keamanan Keseluruhan

Hasil pengukuran kuesioner dihitung dari nilai rata-rata masing-masing kategori. Hal ini dilakukan untuk mengetahui tingkat keamanan pada sistem informasi akademik yang ada di Universitas Sangga Buana YPKP secara keseluruhan. Tabel 4.4 menunjukan

hasil dari perhitungan nilai rata-rata keseluruhan audit keamanan sistem informasi akademik di Universitas Sangga Buana YPKP.

Tabel 4.4 Perhitungan Data Kuesioner Keseluruhan Kategori

No.	Sub Kriteria Pertanyaan	Rata-Rata	Persentase (%)
1	*Management Control*	3.5425	70.85
2	*Operational Control*	3.5972	72.61
3	*Technical Control*	3.9617	73.83
Rata – Rata Total		3.7005	72.43

Nilai persentase dihitung dengan rumus = (Nilai rata – rata/nilai maksimal)*100%. Berdasarkan data pada tabel 4.4, nilai yang diperoleh untuk kategori bernilai antara 3,5000 – 4,0000 dan persentase kategori antara 70,00% – 74,00%, dengan nilai rata – rata nilai keseluruhan mencapai angka 3,7005 atau dengan persentase 72.43%. Hal ini menunjukkan bahwa tingkat keamanan yang sudah diimplementasikan untuk kategori pengendalian operasional (*operational control*) sudah berada pada level 3, yaitu prosedur dan pengendalian sudah diimplementasikan secara konsisten.

4.2.5 Hasil Perhitungan Tingkat Keamanan Berdasarkan Jabatan Struktural

Data hasil penilaian responden melalui kuesioner dikumpulkan dan dimasukkan sesuai dengan kategori masing-masing. Data yang dikumpulakan berasal dari responden yang sudah ditetapkan sebelumnya, yaitu struktural rektorat, fakultas dan prodi, serta staff PUDI. Masing-masing sub kretirea memiliki 2 pernyataan yang mewakili. Sehingga, total data yang didapat dari 40 (empat puluh) responden sebanyak 80 data. Tabel 4.5 menunjukkan perhitungan data kuesioner berdasarkan jabatan struktural.

Tabel 4.5 Perhitungan Data Kuesioner Berdasarkan Jabatan Struktural

No.	Jabatan Struktural	Skala *Likert*					Jumlah Data	Rata-Rata	Persentase (%)
		5	4	3	2	1			
1	Rektorat	55	181	73	56	9	374	3,5802	71,60
2	Fakultas dan Prodi	103	245	257	67	8	680	3,5412	70,82
3	Staff PUDI	88	94	85	36	3	306	3,7451	74,90
Jumlah		246	520	415	159	20	1360	10,8665	217,32
Rata-rata								3,6222	72,44

Hasil perhitungan data kuesioner pada sub bab ini berfokus pada penilaian terhadap tingkat keamanan sistem informasi akademik di Universitas Sangga Buana YPKP berdasarkan tingkat jabatan struktural para responden. Perhitungan berdasarkan jabatan

struktural dilakukan untuk melihat apakah terdapat perbedaan pandangan terhadap sistem informasi akademik yang digunakan sesuai dengan tingkatan jabatan strukturalnya. Hal tersebut dilakukan dengan harapan dapat menilai keberhasilan dari pelatihan rutin tentang sistem informasi akademik yang dilakukan oleh pihak institusi.

Berdasarkan data pada tabel 4.5, nilai yang diperoleh untuk kategori bernilai antara 3,5000 – 3,7500 dan persentase kategori antara 70,00% – 75,00%, dengan nilai rata – rata nilai keseluruhan mencapai angka 3,6222 atau dengan persentase 72.44%. Hal ini menunjukkan bahwa setiap responden untuk setiap tingkatan jabatan struktural sudah mendapatkan pemahaman dari pelatihan rutin tentang sistem informasi akademik di Universitas Sangga Buana YPKP yang diselenggarakan oleh pihak institusi.

4.3 *Risk Assessment* Berbasis NIST SP 800-30

Dalam penelitian ini, dilakukan tahapan *risk assessment* sesuai dengan yang tercantum pada NIST SP 800-30. Tahapan berdasarkan NIST SP 800-30 berjumlah 9 tahapan. Tahapan tersebut adalah sebagai berikut.

4.3.1 Identifikasi Sistem

Sistem informasi akademik di Universitas Sangga Buana YPKP Bandung memasuki tahun ke-2 sejak digunakan Sistem pada server sia.usbypkp.ac.id menggunakan 2 jenis *hardware* yang digunakan sebagai server lokal dan server publik. Untuk server lokal, menggunakan Fujitsu *Single Processor* dengan *memory* 8 GB dan berbentuk *tower server*. Untuk server publik, menggunakan DELL *Double Processor* 12 *core* dengan *memory* 32 GB dan berbentuk *rack server*. *Software* yang digunakan adalah PHP 5.6 Apache 2 sebagai *web engine*, SQL Server sebagai *database*, dan Sun Solaris 10 sebagai *Operating System*. Sistem informasi akademik ini dibangun dengan tujuan untuk mengikuti visi dan misi yang sudah dicanangkan oleh Universitas Sangga Buana YPKP Bandung.

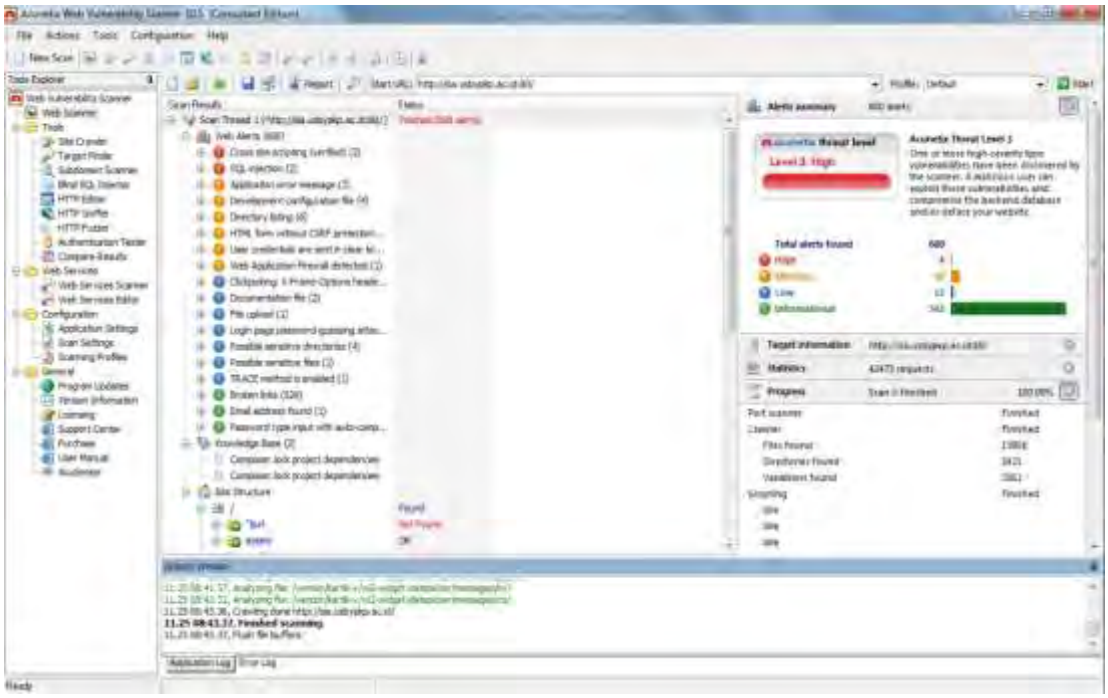
4.3.2 Identifikasi Ancaman

Pada umumnya, berdasarkan yang tercantum pada *framework* NIST SP 800-30, ancaman yang dapat mengganggu proses bisnis sistem informasi terbagi menjadi 3 (tiga) jenis ancaman. Ketiga jenis ancaman tersebut yaitu ancaman alam (*natural threat*), ancaman manusia (*human threat*), dan ancaman lingkungan (*environmental threat*).

1. Ancaman alam (*natural threat)* merupakan ancaman yang bersumber dari alam. Beberapa contoh diantaranya yaitu banjir, kebakaran, gempa bumi, tornado, dan longsor.
2. Ancaman manusia (*human threat*) merupakan ancaman yang bersumber dari tingkah laku manusia dan dapat dikatakan dilakukan dengan kesengajaan untuk mendapatkan keuntungan. Beberapa contoh diantaranya yaitu *hacker*, *blackmailing*, *cybercrime*, *cracker*, dan *system penetration*.
3. Ancaman lingkungan (*environmental threat*) merupakan ancaman yang mungkin terjadi dikarenakan kondisi lingkungan yang memungkinkan ancaman tersebut menjadi nyata. Beberapa contoh diantaranya suhu ruangan yang panas, listrik padam, dan kerusakan fisik pada server.

4.3.3 Identifikasi Kerentanan

Kerentanan yang terdapat pada sia.usbypkp.ac.id diuji melalui proses *scanning* dengan menggunakan *tool* Acunetix. Gambar 4.1 menunjukkan hasil dari proses *scanning* yang dilakukan dengan menggunakan aplikasi Acunetix. Proses *scanning* tersebut dilakukan terhadap website sia.usbypkp.ac.id.



Gambar 4.1 Hasil *Scanning* Terhadap website sia.usbypkp.ac.id Berbasis Acunetix

Gambar 4.1 merupakan hasil *scanning* pada website sia.usbypkp.ac.id, menunjukkan bahwa sistem informasi akademik yang ada di Universitas Sangga Buana memiliki tingkat kerentanan yang sangat tinggi (level 3). Hal itu dibuktikan dengan temuan pada proses *scanning* dengan jumlah total kerentanan mencapai 600 buah, dengan rincian 4 buah kerentanan dengan tingkat resiko tinggi, 40 buah kerentanan dengan resiko medium, 13 buah kerentanan dengan tingkat resiko rendah, dan 543 buah yang bersifat *informational*. Sehingga, tingkat kerentanan yang ada pada sistem informasi akademik tersebut mencapai level 3 atau tinggi.

1. Kerentanan tingkat tinggi

   Pada sia.usbypkp.ac.id terdapat 4 buah kerentanan tingkat tinggi yang terdiri dari 2 jenis kerentanan yang berbeda, yaitu.

   a. *Cross Site Scripting*

      Pada sia.usbypkp.ac.id, Acunetix mendeteksi 2 buah kerentanan jenis *Cross Site Scripting*. *Cross Site Scripting* adalah sebuah kerentanan yang menyebabkan

sesorang untuk dapat memasukkan kode tertentu kedalam akun *user* lain. Hal ini biasanya terjadi karena perbedaan versi pada *browser user*. Penyerang yang masuk melalui kerentanan ini akan mengeksekusi sejumlah *script* dengan tujuan untuk mengakses *cookies* pada *browser* pengguna, mengubah konten pada halaman yang sedang dibuka oleh *user*, bahkan orang tersebut dapat berpura – pura sebagai korbannya.

b. SQL *Injection*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 2 buah kerentanan jenis SQL *injection*. SQL *injection* adalah sebuah kerentanan yang memungkinkan bagi seseorang untuk mengganti sejumlah data dengan cara memanipulasi data input *user*. Hal ini biasanya terjadi ketika aplikasi berbasis web menerima data input *user* yang langsung terhubung dengan SQL *statement* tanpa ada penyaringan yang memadai untuk mencegah karakter berbahaya.

2. Kerentanan tingkat sedang

Pada sia.usbypkp.ac.id terdapat total 40 buah jenis kerentanan tingkat sedang yang terdiri atas 6 jenis kerentanan yang berbeda, yaitu.

a. *Application Error Massage*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 3 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan pada halaman tertentu memunculkan informasi – informasi yang bersifat sensitif, bahkan memunculkan pula lokasi dari informasi tersebut.

b. *Development Configuration File*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 4 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan data yang memuat konfigurasi sistem dapat ditemukan dengan mudah. Data konfigurasi tersebut mungkin saja menampilkan informasi-informasi yang bersifat sensitif, sehingga memungkinkan seseorang untuk dapat merusak informasi tersebut.

c. *Direcroty Listing*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 6 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan server web menampilkan data yang terdapat pada direktori. Pada dasarnya, data yang terdapat pada direktori tersebut sangat jarang ditampilkan pada website melalui sebuah link.

d. *HTML Form Without CSRF Protection*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 23 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan adanya kemungkinan digunakannya *commend* ilegal oleh *user* yang dipercaya oleh website tersebut.

e. *User Credentials are Sent in Clear Text*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 3 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan tanda pengenal *user* dikirimkan melalui *channel* yang tidak terenkripsi.

f. *Web Application Firewall Detected*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 1 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan terdeteksinya *Firewall* yang digunakan untuk melindungi sistem. Dengan digunakannya *Firewall* tersebut, ada kemungkinan kesalahan dari sistem untuk menampilkan informasi yang diinginkan.

3. Kerentanan tingkat rendah

Pada sia.usbypkp.ac.id terdapat total 13 buah jenis kerentanan tingkat sedang yang terdiri atas 7 jenis kerentanan yang berbeda, yaitu.

a. *Clickjacking*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 1 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan ada kemungkinan terjadinya pencurian data dari *user* ketika *user* tersebut melakukan proses clicking pada website

tersebut. Hal itu terjadi disaat ada yang menyusupi website tersebut dan memasukkan sebuah kamuflase terhadap website aslinya.

b. *Documentation File*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 2 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan adanya dokumentasi terhadap data yang berhubungan dengan aplikasi web yang digunakan dapat diidentifikasi dengan mudah.

c. *File Upload*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 1 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan pihak *user* dapat melakukan proses *upload* dengan mudah. Jika tidak dapat ditangani dengan baik, maka aka nada kemungkinan file yang dimasukkan merupakan file yang dapat menakibatkan kerugian bagi institusi.

d. *Login Page Password-Guessing Attack*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 3 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan adanya kemungkinan terjadinya perubahan kata sandi dari akun yang digunakan oleh *user*. Perubahan kata sandi itu dapat dilakukan setelah melakukan percobaan secara sistematik dengan menggunakan kombinasi huruf, angka, dan symbol.

e. *Possible Sensitive Directory*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 4 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan adanya direktori sensitif yang mudah untuk diketahui meskipun tidak terhubung langsung dengan website. Data – data tersebut dapat digunakan sebagai alat untuk mengidentifikasi target yang dituju.

f. *Possible Sensitive File*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 1 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan adanya data sensitive yang dapat

dengan mudah untuk diketahui meskipun tidak terhubung langsung dengan website. Sama seperti *possible sensitive directory*, hal ini juga digunakan sebagai alat untuk mengidentifikasi sistem yang menjadi target.

g. TRACE *Method*

Pada sia.usbypkp.ac.id, Acunetix mendeteksi 1 buah kerentanan jenis ini. Kerentanan jenis ini muncul dikarenakan informasi yang bersifat sensitif dapat dibaca dari setiap domain yang mendukung HTTP TRACE *method* tersebut.

4.3.4 Analisis Pengendalian

Proses pengendalian oleh pihak PUDI adalah dengan menggunakan *Firewall*. Hal ini bertujuan untuk menjaga segala sesuatu yang ada pada sistem tersebut. *Firewall* yang digunakan saat ini adalah IPCop dengan versi 2.1.9. Versi tersebut merupakan versi IPCop yang paling terakhir dan paling stabil untuk saat ini. Hingga saat ini, proses pengendalian menggunakan IPCop tersebut sudah maksimal. Sejumlah kerentanan yang mungkin dimanfaatkan secara ilegal sangat sulit ditembus dan dapat dengan cepat terdeteksi jika terdapat aktifitas yang mencurigakan terhadap sistem informasi akademik.

Pelatihan rutin kepada para *user*, baik itu internal maupun eksternal, dilakukan untuk memberikan pengetahuan kepada *user* tentang sistem informasi akademik dan meningkatkan kesadaran para *user* untuk menjaga keamanan data pada sistem informasi akademik dan menjaga kenyamanan para *user* lain saat mengakses sistem informasi akademik tersebut. Untuk mencegah kerugian akibat hilangnya data, pihak institusi sudah melakukan *backup* data secara terpisah dari server dan data tersebut disimpan ke dalam DVD. Pihak institusi pun selalu berusaha menjalankan setiap aktifitas sesuai dengan SOP yang berlaku.

4.3.5 Penilaian Kecenderungan Resiko

Kecenderungan terhadap terjadinya resiko dapat dilihat sesuai dengan jenis ancaman yang mungkin menyerang, baik itu terhadap sistem maupun terhadap fisik

servernya. Kecenderungan akan ancaman tersebut terhadap Universitas Sangga Buana YPKP adalah sebagai berikut.

1. *Natural threat* hampir tidak pernah terjadi. Hal tersebut dikarenakan lokasi Universitas Sangga Buana YPKP berada di lokasi yang terhindar dari kemungkinan terjadinya bencana. Selain itu, drainase yang ada di sekitar Universitas Sangga Buana YPKP sudah berfungsi dengan maksimal, sehingga potensi terjadinya banjir dapat dikurangi. Untuk kebakaran, pihak institusi sudah melakukan semua kegiatan berdasar SOP (standar operasional prosedur) dengan sangat baik, sehingga dapat meminimalisir kemungkinan terjadinya kebakaran. Karena hal tersebut, kecenderungan terjadinya *natural threat* dapat dikategorikan rendah (*low*).
2. *Human threat* terjadi karena tindakan sengaja oleh seorang atau sekolompok manusia. Tindakan tersebut dilakukan dengan mengincar targetnya, baik itu melewati sistem ataupun langsung kepada fisik dari server sistem informasi akademik. Universitas Sangga Buana sudah mengantisipasi hal tersebut. Sistem yang ada di Universitas Sangga Buana YPKP memanfaatkan *system protection* dengan menggunakan *firewall* IPCop versi 2.1.9. Sedangkan untuk keamanan fisik server, pihak PUDI sudah menempatkan fisik server di tempat yang tertutup dan sulit terjangkau oleh orang asing dan juga sudah terpasang CCTV di ruang server tersebut. Oleh karena itu, kecenderungan terjadinya *human threat* dapat dikategorikan rendah (*low*).
3. *Environmental threat* dapat terjadi jika keadaan yang ada di sekitar sistem/server mendukung terjadinya ancaman tersebut. Untuk menghindari hal tersebut, pihak institusi melalui bagian PUDI sudah menerapkan semua proses yang berhubungan dengan sistem informasi sesuai dengan SOP yang berlaku. Oleh karena itu, kecenderungan terjadinya *environmental threat* dapat dikategorikan rendah (*low*).

4.3.6 Analisis Dampak

Dampak yang ditimbulkan akibat dari terjadinya resiko pada sistem informasi akademik dapat menyerang *hardwre*, *software*, maupun data dan informasi yang tersimpan dalam server. Dampak tersebut bergantung pada resiko yang terjadi. Beberapa dampak yang dapat terjadi antara lain.

1. Banjir menyebabkan fisik *hardware* server rusak, sehingga data dan informasi yang tersimpan akan hilang dan pihak institusi akan mengalami kerugian investasi karena kerusakan server tersebut.
2. Kebakaran dapat menyebabkan dampak yang lebih parah dibandingkan dengan banjir. Hal tersebut dikarenakan yang akan mengalami dampak kerusakan bukan hanya server, namun juga ruangan untuk menyimpan server tersebut pun harus dibangun ulang. Investasi yang harus dilakukan institusi untuk membentuk kembali sistem informasi tersebut pun akan semakin besar.
3. Dampak yang timbul akibat masuknya *hacker* pada sistem informasi akademik adalah menyerang sistem informasi tersebut dari dalam sistem informasi itu sendiri. Hal yang dapat dilakukan ketika sudah dapat masuk ke dalam sistem informasi tersebut diantaranya melakukan perubahan pada data dan informasi yang tersimpan, merusak sistem yang sudah dirancang, dan terjadi pencurian data penting milik institusi.
4. Suhu ruangan server yang meningkat dapat menyebabkan *hardware* server menjadi panas, bahkan dapat menyebabkan kerusakan pada *hardware* server tersebut. hal tersebut dapat mengakibatkan proses bisnis pada sistem informasi akademik akan terhenti.
5. Mati lampu pun mengakibatkan semua proses bisnis yang melibatkan sistem informasi di Universitas Sangga Buana YPKP menjadi terhenti dikarenakan server sistem informasi akademik pun tidak dapat digunakan.

4.3.7 Penilaian Tingkat Resiko

Berdasarkan data pada tabel 2.1, tingkat resiko yang mungkin terjadi terhadap sistem yang ada di Universitas Sangga Buana YPKP dapat ditentukan. Tingkat resiko pada Universitas Sangga Buana tersebut yaitu.

1. Banjir merupakan salah satu ancaman yang termasuk ke dalam ancaman alam. Universitas Sangga Buana berada pada lokasi yang sangat jarang terkena banjir, daerah tersebut diketahui sudah memiliki sistem drainase yang sangat baik dan ruang server sudah berada di lokas yang cukup tinggi dari daratan. Oleh karena itu, kecenderungan terjadinya banjir dikategorikan rendah. Namun, dampak yang ditimbulkan jika banjir tersebut terjadi adalah rusaknya server sistem informasi akademik di Universitas Sangga Buana YPKP dan hilangnya data serta informasi yang berkaitan dengan sistem informasi tersebut. Pihak institusi pun harus menambahkan *budget* untuk mendapatkan *hardware* server yang baru. Maka dari itu, dampak yang ditimbulkan akibat banjir termasuk kedalam kategori tinggi. Berdasarkan tabel 2.1, tingkat resiko banjir terhadap sistem informasi Universitas Sangga Buana YPKP adalah rendah.
2. Kebakaran menjadi ancaman yang serius jika terjadi. Hal tersebut dikarenakan dampak yang ditimbulkan akibat kebakaran terhadap sistem informasi Universitas Sangga Buana. Rusaknya server, hilangnya data dan informasi, serta terhambatnya proses bisnis di Universitas Sangga Buana merupakan dampak akibat kebakaran. Dampak tersebut termasuk ke dalam kategori tinggi. Namun, pihak institusi sudah melakukan pencegahan agar dapat meminimalisir terjadinya kebakaran, diantaranya dengan melakukan semua aktifitas dengan mengikuti SOP yang berlaku, melakukan pengecekan secara berkala terhadap hal – hal yang dianggap berpotensi menyebabkan kebakaran, memasang alat peringatan kebakaran dan meningkatkan kesadaran akan keselematan kerja melalui seminar ataupun pelatihan secara rutin. Oleh karena itu, tingkat kecenderungan terjadinya kebakaran dapat diminimalisir.

Bedasarkan hal tersebut, tingkat resiko kebakaran di Universitas Sangga Buana YPKP dapat dikategorikan sebagai resiko dengan tingkat rendah.

3. *Hacker* termasuk ancaman yang memiliki dampak tinggi. Akibat adanya *hacker*, data dan informasi milik sebuah institusi ataupun perusahan dapat dihilangkan, diubah, bahkan dicuri. Hal itu dapat mengganggu proses bisnis yang ada di institusi tersebut. *Hacker* akan selalu mencoba jalur baru untuk dapat masuk ke dalam sistem informasi yang sudah menjadi targetnya. Pihak institusi harus dapat mencegah masuknya *hacker* tersebut. Maka dari itu, beberapa hal sudah dilakukan pihak institusi, khususnya PUDI. Pemasangan *firewall* IPCop versi terbaru merupakan salah satu cara yang dilakukan pihak PUDI untuk menutup ruang gerak dari para *hacker* tersebut. setiap serangan yang dilakukan akan sangat sulit menembus sistem pertahan *firewall* tersebut. Pelatihan rutin kepada para *user* pun terus dilakukan untuk meningkatkan kesadaran untuk menjaga keamanan sistem informasi akademik. Selain itu, adanya daftar akses pada sistem informasi Universitas Sangga Buana merupakan satu hal positif yang dilakukan karena dapat mengetahui para *user* yang melakukan akses pada sistem informasi tersebut. Maka dari itu, tingkat resiko terjadinya *hacker* pada sistem informasi akademik di Universitas Sangga Buana YPKP termasuk ke dalam kategori rendah.
4. Beberapa ancaman yang berasal dari lingkungan diantaranya panasnya suhu ruangan dan mati lampu. Panasnya suhu ruangan dapat meningkatkan suhu pada server, yang mengakibatkan *hardware* server tersebut terjadi *error* bahkan meledak. Dampak tersebut termasuk ke dalam kelompok tinggi, karena dapat memberikan kerugian bagi institusi untuk mendapatkan server yang baru dengan waktu yang sangat singkat. Untuk menghindari hal tersebut, pihak institusi memasang *air conditioning* (AC) pada ruang server dan menutup ruang server untuk menjaga suhu pada ruang server tersebut. Mati lampu yang tidak terduga pun dapat mengganggu proses bisnis di Universitas Sangga Buana YPKP. Untuk dapat mencegah hal

tersebut, generator listrik (genset) disiapkan sebagai persedian listrik cadangan. Hal – hal tersebut diharapkan dapat meminimalisir terjadinya hal – hal tersebut, sehingga kecenderungan terjadinya suhu ruang server yang meningkat dan mati lampu menajadi rendah. Berdasarkan hal tersebut, tingkat resiko tersebut adalah rendah.

4.3.8 Rekomendasi Pengendalian

Ancaman mungkin saja menjadi resiko yang dapat berbahaya bagi proses bisnis yang ada di Universitas Sangga Buana YPKP. Hal tersebut dikarenakan sistem informasi yang digunakan sudah menjadi sesuatu hal yang krusial untuk meningkatkan pelayanan di dunia pendidikan. Perannya yang begitu penting bagi institusi menjadikan setiap data dan informasi yang tersimpan dalam sistem informasi tersebut menjadi sesuatu yang sensitif. Untuk dapat meminimalisir kemungkinan terjadinya resiko tersebut, pihak institusi, khusunya pihak PUDI, harus selalu memperbaharui *system protection* yang digunakan menjadi versi yang terbaru. Pihak PUDI pun harus selalu melakukan pengujian sistem secara berkala untuk mengetahui kerentanan yang ada pada sistem informasi akademik. Selain itu, setiap orang yang terlibat dalam proses bisnis tersebut harus berperan aktif dalam menjaga keamanan sistem informasi akademik tersebut. Untuk itu, pihak institusi diharapkan mampu memberikan pelatihan rutin untuk dapat meningkatkan kesadaran dan pengetahuan para *user*.

Untuk menjaga data jika terjadi kehilangan atau pencurian data dan informasi, pihak institusi harus melakukan *backup* data. *Backup* data yang dilakukan dapat menggunakan tempat penyimpanan sesuai dengan kebutuhan pihak institusi. Salah satunya dengan menyimpan semua data dengan menggunakan DVD.

4.3.9 Dokumentasi Hasil

Sistem informasi akademik yang diterapkan oleh Universitas Sangga Buana bertujuan untuk mencapai visi misi yang sudah ditetapkan oleh pihak institusi. Sistem informasi akademik memiliki peran yang sangat penting dalam menunjang perkembangan pelayanan pendidikan yang diusung oleh pihak institusi. Oleh karena itu,

tingkat keamanan yang dilakukan oleh pihak institusi, khususnya pihak PUDI, harus memadai dan sesuai dengan kebutuhan untuk menangkal terjadinya resiko. Kerentanan yang ada pada sistem informasi akademik pun harus dapat teridentifikasi, mengingat cepatnya perkembangan teknologi informasi.

Terdapat beberapa ancaman yang bisa jadi menyerang sistem informasi akademik di Universitas Sangga Buana YPKP. Ancaman yang mengganggu proses bisnis sistem informasi akademik tersebut terbagi menjadi 3 (tiga) kelompok, yaitu,

1. Ancaman alam (*natural threat*), contohnya banjir, kebakaran, gempa bumi.
2. Ancaman manusia (*human threat*), contohnya *hacker, blackmailing*, *cybercrime*.
3. Ancaman lingkungan (*environmental threat*), contohnya suhu ruangan yang panas, listrik padam, kerusakan server.

Sistem informasi akademik yang ada di Universtas Sangga Buana pun masih dalam tahap pengembangan. Oleh karena itu, masih ditemukan kerentanan pada sistem informasi akademik tersebut. kerentanan yang ditemukan dengan proses *scanning* menggunakan *tool* Acunetix berjumlah 600 buah, kerentanan tersebut terbagi menjadi 4 tingkatan kerentanan, yaitu 4 buah kerentanan dengan tingkat tinggi, 40 buah kerentanan tingkat sedang, 13 buah kerentanan tingkat rendah, dan 543 buah kerentanan yang bersifat informational.

Untuk dapat meminimalisir kecenderungan terjadinya resiko dan meminimalkan kerugian yang didapat, pihak institusi harus melakukan langkah antisipasi. Beberapa langkah tersebut diantaranya dengan selalu memperbaharui *firewall* yang menjadi *system protection* pada sistem informasi akademik, melakukan pengujian secara berkala untuk melihat tingkat kerentanan sistem, memberikan pelatihan mengenai pentingnya peran sistem informasi akademik kepada *user* secara rutin, dan melakukan *backup* data dan informasi untuk mengantisipasi hilangnya data.

4.4 Rekomendasi

Dari hasil pencapaian tingkat keamanan sistem informasi akademik yang ada pada Universitas Sangga Buana YPKP Bandung memiliki nilai rata – rata 72.43 % atau pada level 3 (*Implemented Procedures and Controls*). Berdasarkan *framework NIST* SP 800-26, untuk dapat mencapai level 4 (*Tested and Review Procedures and Controls*) sebaiknya dilakukan beberapa aktifitas sesuai dengan kriterianya, yaitu.

1. Pihak institusi melakukan efisiensi program untuk mengevaluasi kecukupan dan efektifitas kebijakan keamanan, prosedur, dan pengendalian.
2. Pihak institusi menjalankan mekanisme prosedur untuk mengidentifikasi kerentanan yang timbul dengan menggunakan *security alerts*.
3. Pihak institusi mengembangkan proses pelaporan kelemahan pada sistem keamanan dan meyakini proses pembaharuan berjalan dengan efektif.
4. Pihak institusi melakukan investigasi terhadap latar belakang dari staff IT sebelum diberikan tugas dan tanggung jawab untuk menjaga keamanan sistem informasi akademik.
5. Pihak institusi meningkatkan tingkat kesadaran dan memberikan edukasi pada *user* dengan mengadakan pelatihan rutin terkait sistem informasi akademik.
6. Pihak institusi meminta penjelasan secara detail terkait proposal dari pihak IT untuk dapat mengembangkan produr pengamanan terhadap sistem informasi akademik.
7. Pihak Institusi melakukan pengujian secara berkala untuk dapat mengetahui kerentanan yang dapat timbul pada sistem informasi akademik.
8. Pihak institusi melakukan penilaian terhadap resiko secara berkala.
9. Pihak institusi melakukan *backup* data secara berkala.
10. Pihak institusi menambahkan *air conditioner (AC)* dan kamera CCTV pada ruang server.
11. Pihak institusi mendokumentasikan secara menyeluruh terkait setiap aktivitas yang dilakukan pihak *user*.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kerangka Kerja NIST SP 800-26 memberikan penjelasan mengenai tingkat keamanan teknologi informasi yang diterapkan pada sebuah institusi. NIST SP 800-26 menyebutkan 3 kategori penilaian keamanan teknologi informasi, yaitu pengendalian manajemen (*Management Control*), pengendalian operasional (*Operational Management*), dan pengendalian teknikal (*Technical Control*). Dari hasil penelitian yang dilakukan pada sistem informasi akademik di Universitas Sangga Buana YPKP, dapat disimpulkan bahwa.

1. Berdasarkan penilaian hasil audit pada sistem informasi akademik Universitas Sangga Buana YPKP, dapat disimpulkan bahwa keamanan pada sistem informasi akademik tersebut berada pada level 3, *implemented procedures and control*.
2. Penilaian kerentanan dan resiko dengan menggunakan aplikasi Acunetix pada website sia.usbypkp.ac.id menghasilkan 600 buah kerentanan yang ada pada sistem informasi akademik tersebut. Rinciannya, 4 buah kerentanan dengan tingkat resiko tinggi, 40 buah kerentanan dengan tingkat resiko medium, 13 buah kerentanan dengan tingkat resiko rendah, dan 543 buah kerentanan yang bersifat informasional.
3. Rekomendasi yang dapat diberikan terkait hasil penilitian antara lain melakukan pengujian *scanning* pada sistem informasi akademik secara berkala, melakukan *backup* data secara rutin, meningkatkan sistem pengamanan pada sistem informasi akademik, memenuhi kebutuhan terkait fasilitas untuk menjaga kestabilan server, dan mendokumentasikan setiap aktifitas yang berkaitan dengan sistem informasi akademik.

5.2 Saran

Dari hasil penelitian di Universitas Sangga Buana YPKP Bandung, saran dari hasil pembahasan tersebut antara lain.

1. Audit keamanan sistem informasi sangat dibutuhkan bagi pihak institusi dikarenakan sistem informasi yang digunakan masih baru diterapkan dan masih dalam tahap pengembangan. Diharapkan dengan diterapkannya audit keamanan tersebut, setiap aktifitas perubahan yang dilakukan pada proses bisnis sistem informasi tersebut dapat meningkatkan dan peran sistem informasi dapat optimal.
2. Meningkatkan sistem keamanan untuk dapat memaksimalkan sistem informasi yang ada saat ini dan mengembangkannya sehingga dapat mencapai tingkatan keamanan yang lebih tinggi berdasarkan *framework* NIST SP 800-26.

DAFTAR PUSTAKA

Arifin, Mochamad. 2002. *Pemanfaatan Media Web Site Sebagai Sistem Informasi Akademik dan Sarana Pembelajaran Mandiri dalam Pengaruhnya dengan Prestasi Belajar Mahaiswa*, Jurnal STIKOM Vol.6 No. 2 Sept 2002.

Arikunto, Suharsimi. 2002. *Prosedur Penelitian Suatu Pendekatan Praktik*. Jakarta : Rineka Cipta

Aswati, Safrian, dkk. 2015. *Peranan Sistem Informasi dalam Perguruan Tinggi*. Jurnal Teknologi dan Sistem Informasi Vol 1. No. 2.

Blokdijk, Gerard et al. 2008. *Complete Risk Management Toolkit Guide for Information Technology Processes and System*. Brisbane.

Chazar, Chalifa. 2015. *Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005*. Jurnal Informasi Vol. VII No. 2.

Darmawi, Herman. 2006. *Manajemen Risiko*. Jakarta:Bumi Aksara.

Gerhana, Yana Aditia dkk. 2011. *Penilaian Resiko Teknologi Informasi dan Keamanan Sistem Informasi Dengan Menggunakan Framework Cobit 4.1 dan Guidelines NIST SP 800-30 (Studi Kasus : Rumah Sakit Umum dr. Slamet Garut).* ISSN 1979-8911. Vol. V No. 1-2.

Ghozali, Imam. 2012. *Aplikasi Analisis Multivariate dengan Program IBM SPSS 20.* Badan Penerbit Universitas Diponegoro.

Gibson, Danil. 2011. *Managing Risk in Information Systems*. Sudbury: Jones & Bartlett Learning.

Gondodiyoto, Sanyoto. 2007. *Audit Sistem Informasi*. Jakarta : Mitra Wacana Media.

Hutahaean, Jeperson. 2014. *Konsep Sistem Informasi*. Yogyakarta : Deepublish.

Idroes, Ferry N. 2008. *Manajemen Risiko perbankan:Pemahaman Pendekatan 3 pilar Kesepakatan Bassel II Terkait Aplikasi Regulasi dan Pelaksanaannya di Indonesia*. Jakarta: Rajawali Pers.

Iskandar, Jusman. 2005. *Metode Penelitian Administrasi*. Bandung : Puspaga.

Jakaria, Deni Ahmad dkk. 2013. *Manajemen Resiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Actave Allegro*. Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 2013.

Jogiyanto. 2005. Dalam *Analisa dan Desain Sistem Informasi* (hal. 11). Surabaya: Informatika.

Krutz, R. L. dan D. R. Vines. 2006. *The CISSP Prep Guide – Mastering the Ten Domains of Computer Security*. CA: Wiley Computer Publishing John Wiley & Sons, Inc.

Lukum, Astin. 2013. *Implementasi Sistem Informasi Akademik Universitas Negri Gorontalo*. Jurnal Entropi Vol. VIII No. 1.

Margono, S. 2010. *Metodologi Penelitian Pendidikan*. Jakarta : Rineka Cipta.

Maulana, M. M. dan S. H. Supangkat. 2006. *Pemodelan Framework Manajemen Resiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang*. Prosiding Konfrensi Nasional Teknologi Informasi dan Komunikasi untuk Indonesia, 121 – 126.

Nugraha, Ucu. 2016. *Manajemen Resiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST 800-30*. Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)

Nurochman, Arif. 2014. *Manajemen Resiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan Universitas Gadjah Mada Yogyakarta)*. Berkala Ilmu Perpustakaan dan Informasi Vol. X No. 2

Nursalam. 2002. Manajemen Keperawatan Aplikasi dalam Praktika Keperawatan Profesional. Jakarta : Salemba Medika.

Pinontoan, Jimmy H. 2010. *Manajemen Risiko TI - Konsep-konsep Majalah PC Media*.

Prabowo, Wahyu S. 2017. *Manajemen Resiko Infrastruktur Cloud Pemerintah Menggunakan NIST Framework Studi Kasus Lembaga Ilmu Pengetahuan Indonesia (LIPI)*. Jurnal Penelitian Pos dan Informatika. ISSN : 2476-9266.

Satoto, Kodrat Iman. 2008. *Analisis keamanan Sistem Informasi Akademik Berbasis Web di Fakultas Teknik Universitas Diponegoro*. Seminar Nasional Aplikasi Sains dan Teknologi 2008.

Simanungkalit, S.Juliandry. 2009. *Perancangan Manajemen Keamanan Sistem Informasi Studi Kasus Depkominfo.* Tesis. Jakarta. Fakultas Ilmu Komputer Program Studi Magister Teknologi Informasi UI.

Stoneburner, et al. 2002, *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30.

Suduc, A. M., et al. 2010. *Audit for Information System Security* . Journal Informatica Economica, 14(1), 43 – 48.

Sugiyono. 2006. *Metode Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif dan R&D)*. Bandung : Alfabeta.

Sugiyono. 2010. *Statistika Untuk Penelitian*. Bandung. Alfabeta.

Sutabri, Tata. 2005. Sistem Informasi Manajemen. Yogyakarta. Andi

Swanson, Marianne. 2001. *Security Self-Assessment Guide for Information Technology Systems*. NIST Special Publication 800-26.

Syafitri. Wenni. 2016. *Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus : Sistem Informasi Akademik Universitas XYZ)*. Jurnal CoreIT, Vol. 2 No. 2.

Tantra, Rudy. 2012. *Manajemen Proyek Sistem Informasi*. Yogyakarta:Penerbit Andi.

Yahya, Dede, 2011, *Perkembangan Teknologi Informasi dan Komunikasi di bidang Pendidikan di Indonesia.*

Kelley, K. Brian, 2009, *Security Basic – The C-I-A Triad,* http://www.sqlservercentral.com/blogs/brian_kelley/2009/04/20/security-basics-the-c-i-a-triad/. Diakses pada 23 November 2017.

Swastika, Vanessa Mayrahma, 2015, *Perkembangan Teknologi di Indonesia,* http://www.kompasiana.com/vanessams/perkembangan-teknologi-di-indonesia_55547634b67e615e14ba545b. Diakses 22 Februari 2017

LAMPIRAN-LAMPIRAN

LAMPIRAN 1

KUESIONER PENELITIAN

Kuesioner Analisis Keamanan Sistem Informasi Akademik (SIA)

Universitas Sangga Buana (USB) YPKP

Tanggal Penelitian : ……

I. Petunjuk Pengisian

1. Bacalah penyataan berikut dengan seksama dan pilih jawaban Anda yang sesuai dengan ***kondisi nyata*** yang terjadi dan Anda ketahui.
2. Berikan tanda ceklis (v) pada salah satu pilihan yang dianggap paling sesuai dengan kondisi yang ada.
   Penjelasan Pilihan : TS = Tidak Setuju; KS = Kurang Setuju; CS = Cukup Setuju; S = Setuju; SS = Sangat Setuju

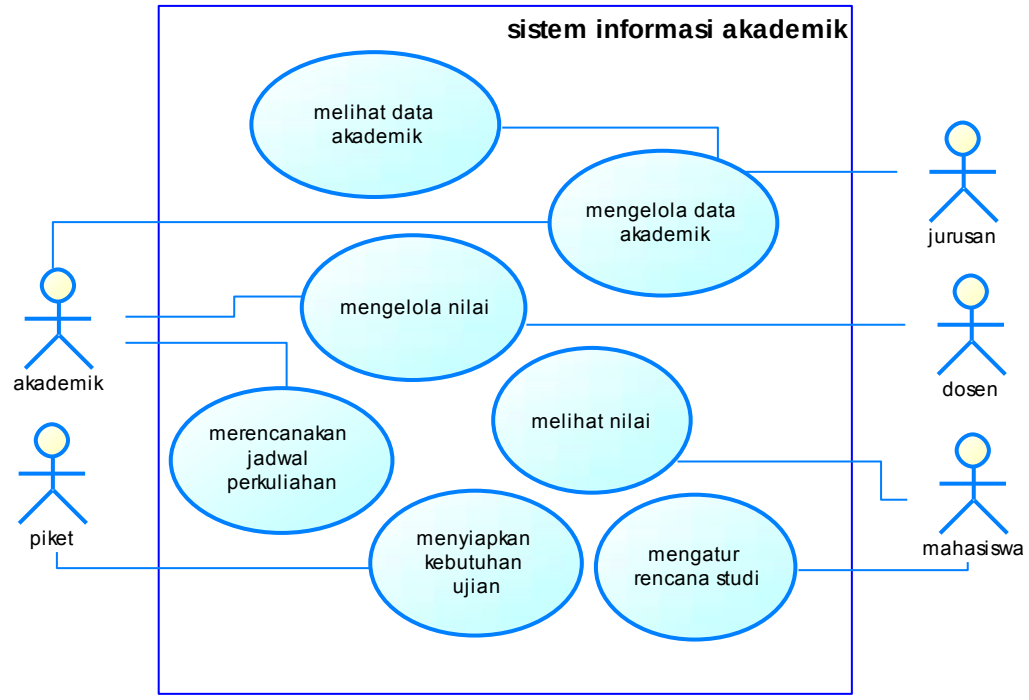
No	Pernyataan	Penilaian				
		TS	KS	CS	S	SS
Management Control – Risk Management						
1	Penilaian resiko yang mungkin terjadi kepada sistem informasi akademik dilakukan secara berkala					
2	Konfigurasi / pengaturan sistem saat ini sudah didokumentasikan					
Management Control – Review of Security Control						
3	Melakukan review / peninjauan ulang terhadap kontrol keamanan pada sistem informasi akademik					
4	Pihak institusi / manajemen yakin aktifitas yang dilakukan terkait keamanan sistem informasi akademik sudah dilakukan dengan benar dan efektif					
Management Control – Life Cycle						
5	Metodologi proses pengembangan sistem sudah dilakukan					
6	Melakukan pengujian terhadap perubahan yang terjadi pada sistem informasi akademik selama proses implementasi sebelum disetujui					
Management Control – Authorize Processing						
7	Sistem informasi akademik sudah tersertifikasi					
8	Pengoprasian sistem informasi akademik sudah sesuai dengan prosedur yang ada					
Management Control – System Security Plan						
9	Rencana keamanan sistem informasi akademik terdokumentasi dan semua sistem yang ada saling berkaitan					
10	Rencana kontrol keamanan sistem informasi akademik sudah berjalan					
Operational Control – Personnel Security						
11	Penugasan terhadap kontrol keamanan sistem informasi akademik sudah terbagi					
12	Proses seleksi terhadap staff kontrol dilakukan sesuai dengan kebutuhan untuk posisi kontrol sistem informasi akademik					

No	Pernyataan	Penilaian				
		TS	KS	CS	S	SS
Operational Control – Physical Security						
13	Kontrol keamanan yang dilakukan terhadap fisik dari sistem informasi akademik sesuai dengan tingkat kerusakan akibat resiko yang terjadi					
14	Data terlindungi dari segala bentuk gangguan					
Operational Control – Production, Input/Output Controls						
15	Pihak pengguna (user) sistem informasi akademik memberikan support terkait sistem tersebut					
16	Adanya kontrol media pada sistem informasi akademik					
Operational Control – Contigency Planning						
17	Perencanaan terkait kontrol keamaan pada perusahaan secara menyeluruh dikembangkan dan didokumentasikan					
18	Kerentanan pada pengoprasian sistem informasi akademik dapat teridentifikasi					
Operational Control – Hardware and System Software Maintenance						
19	Adanya pembatasan akses terhadap hardware dan software sistem					
20	Melakukan proses otorisasi, pengujian, dan persetujuan dengan pihak perusahaan terkait hardware dan software yang baru ataupun diperbaharui sebelum diimplementasikan					
Operational Control – Data Integrity						
21	Software untuk mendeteksi dan menghilangkan virus sudah terpasang dan sudah digunakan					
22	Adanya integritas data dan validasi kontrol untuk memastikan sistem berfungsi sesuai dengan yang diharapkan					
Operational Control - Documentation						
23	Terdapat dokumentasi yang cukup untuk menjalaskan cara penggunaan software atau hardware					
24	Pengamanan resmi dan prosedur pengoprasian sistem informasi akademik terdokumentasi					
Operational Control – Security Awarness, Training, and Education						
25	Staff institusi sudah mendapatkan pelatihan yang cukup untuk memenuhi tanggung jawab sebagai pengendali keamanan sistem informasi akademik					
26	Pelatihan staff institusi terdokumentasi dan termonitor					
Operational Control – Incident Response Capability						
27	Adanya respon untuk memberikan bantuan kepada user ketika terjadi kesalahan pada sistem					
28	Kesalahan yang berkaitan dengan informasi dibagikan sesuai dengan bagiannya					
Technical Control – Identification and Authentication						
29	Menerapkan proses otorisasi perorangan menggunakan password, token, atau perangkat lain					

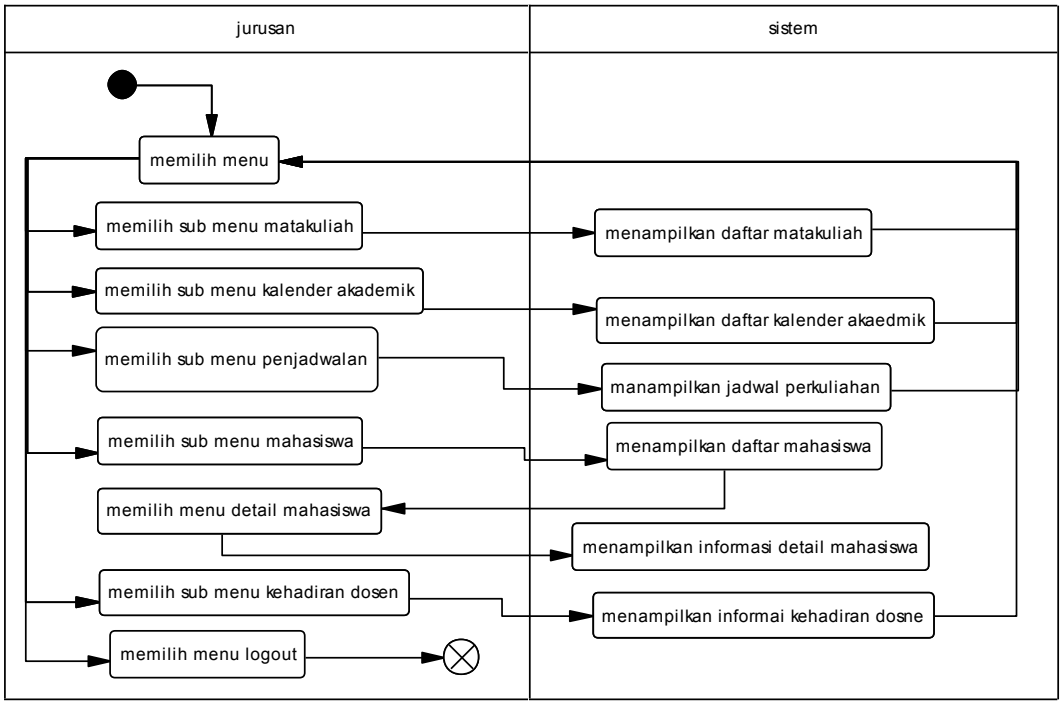
No	Pernyataan	Penilaian				
		TS	KS	CS	S	SS
30	Kontrol akses memaksa terjadinya pemisahan tugas					
Technical Control – Logical Access Control						
31	Melakukan kontrol ketika pihak eksternal mengakses sistem informasi akademik institusi untuk melindungi integritas sistem dan kenyamanan publik					
32	Kontrol kemanan dapat mendeteksi pengakses yang tidak dikenal					
Technical Control – Audit Trails						
33	Aktifitas yang melibatkan akses dan modifikasi pada sistem informasi akademik tercatat dan termonitor					
34	Melakukan proses investigasi dam penindakan apabila terdapat aktifitas yang mencurigakan pada sistem informasi akademik					

LAMPIRAN 2

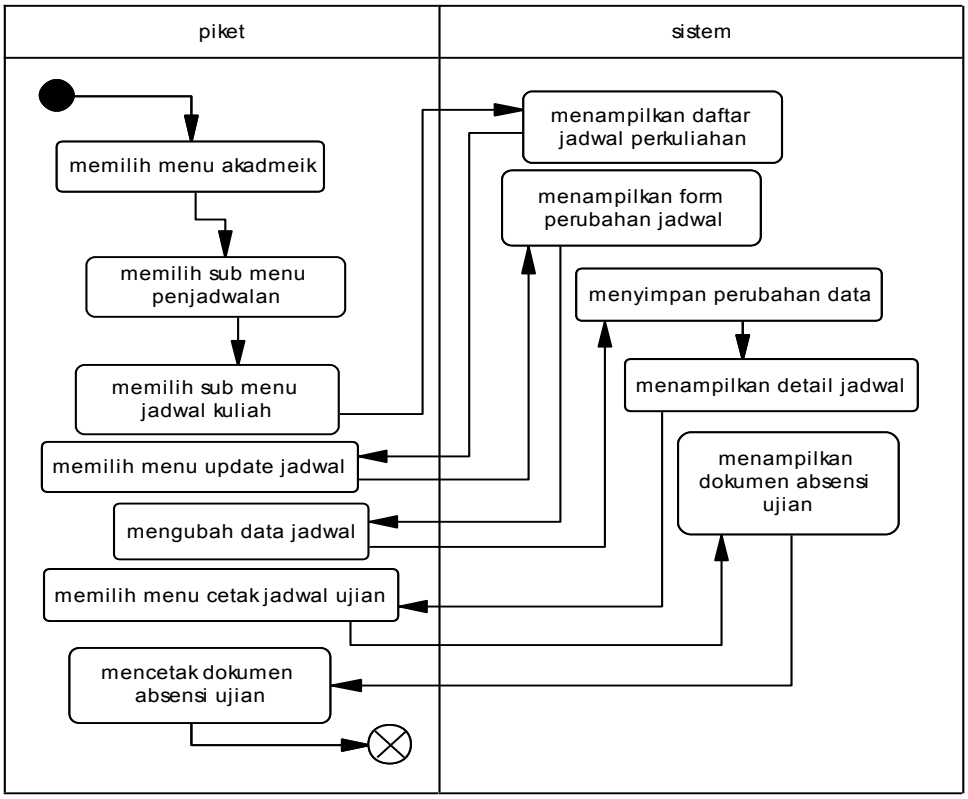
USE CASE AND ACTIVITY DIAGRAM



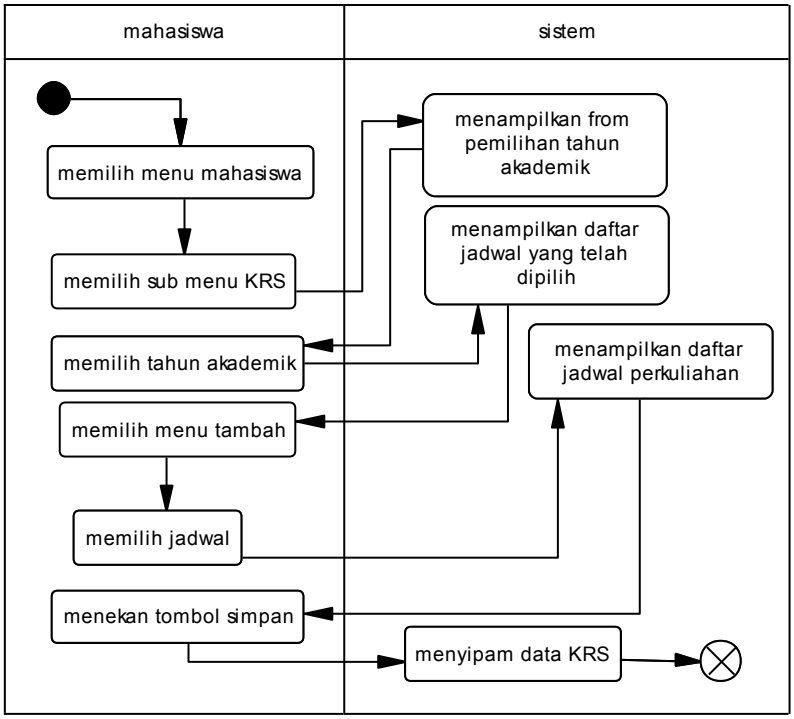
Gambar 3.1 *Use Case Diagram* Sistem Informasi Akademik Universitas Sangga Buana YPKP



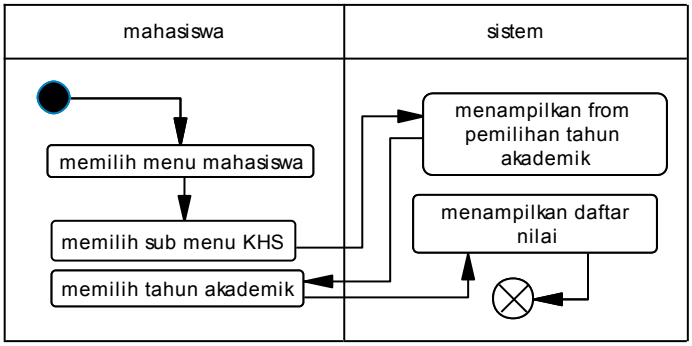
Gambar 3.2 *Activity Diagram* Melihat Data Akademik



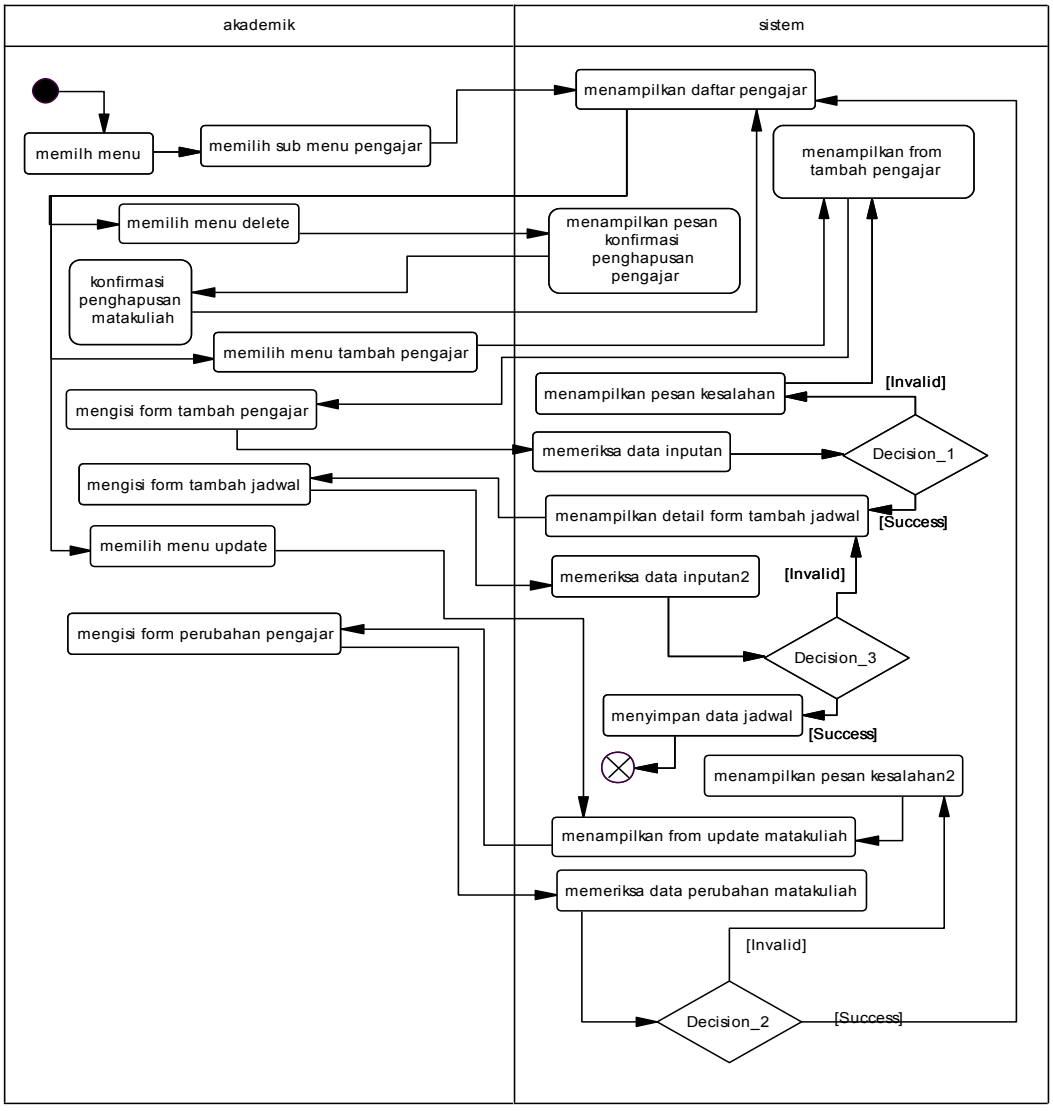
Gambar 3.3 *Activity Diagram* Menyiapkan Kebutuhan Ujian



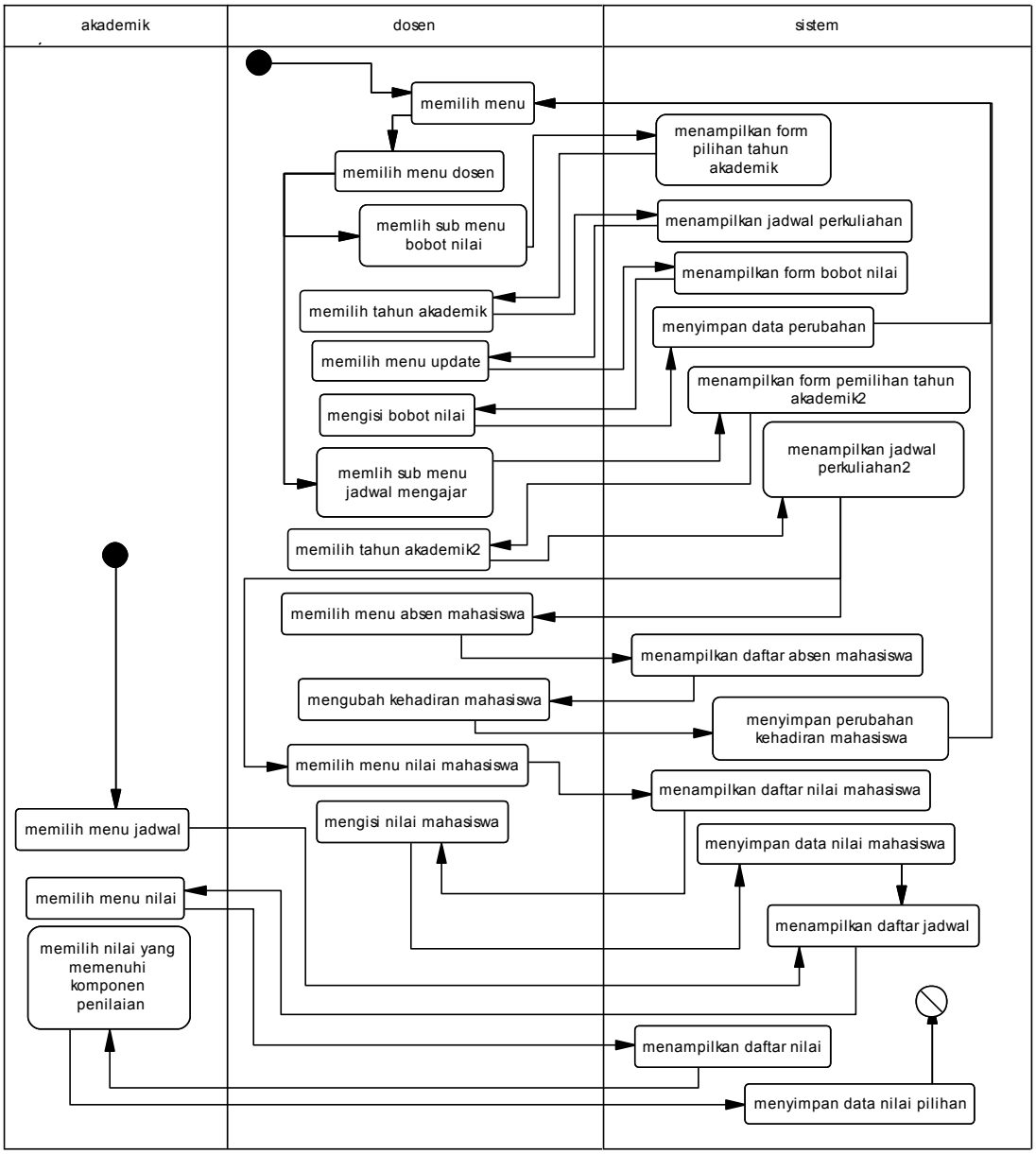
Gambar 3.4 *Activity Diagram* Mengatur Rencana Studi



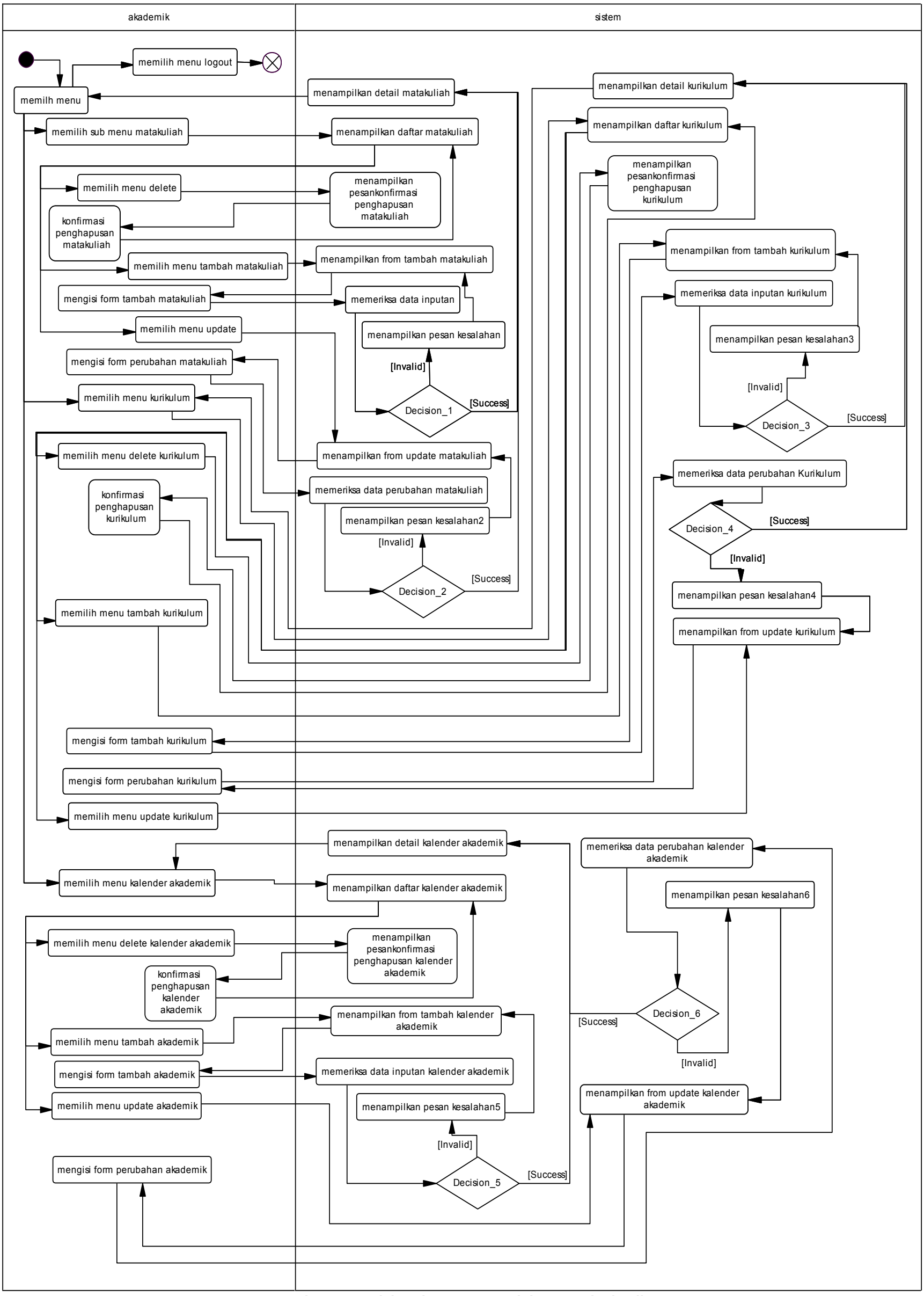
Gambar 3.5 *Activity Diagram* Melihat Nilai



Gambar 3.6 *Activity Diagram* Merencanakan Jadwal Kuliah



Gambar 3.7 *Activity Diagram* Mengelola Nilai



Gambar 3.8 *Activity Diagram* Mengelola Data Akademik

LAMPIRAN 3

DATA HASIL KUESIONER

	Risk Management	*Review of Security Control*	*Life Cycle*	*Authorize Processing*	*System Security Plan*	*Personnel Security*	*Physical Security*	*Production, Input/Output Control*	*Contigency Planning*	*Hardware and Software Maintenance*	*Data Integrity*	*Documentation*	*Security Awarness, Training, and Education*	*Incident Response Capability*	*Identification and Authentication*	*Logical Access Control*	*Audit Trails*	*Rata - Rata*
Rektorat	3	4	4	3	3	4	3	3	3	3	3	4	3	3	3	3	3	3.5802
	4	3	4	3	3	4	3	3	3	3	3	4	3	3	3	3	3	
	4	4	4	4	4	3	2	3	2	5	4	5	2	3	5	3	5	
	4	2	2	4	2	3	3	4	4	4	3	4	4	2	4	5	2	
	5	4	4	3	5	4	4	4	4	5	4	5	5	5	4	5	5	
	5	5	4	5	5	4	5	4	5	5	4	5	4	4	5	5	4	
	1	1	2	1	2	1	2	2	2	2	2	2	2	2	2	2	2	
	2	3	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	
	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	
	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	
	4	5	4	5	4	4	4	4	5	5	5	5	5	4	5	4	5	
	4	4	5	4	5	4	5	4	5	4	4	5	5	4	4	5	4	
	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	
	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	
	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	
	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	
	4	4	4	4	5	4	4	5	4	5	5	4	5	5	5	5	5	
	4	4	5	5	4	4	4	4	4	5	4	4	4	5	5	5	4	
	4	4	5	5	4	4	4	4	4	5	4	4	4	5	5	5	4	
	4	2	3	1	3	3	3	4	3	2	2	3	3	3	2	2	3	
	2	2	1	3	1	3	3	3	2	1	1	2	2	2	3	2	2	
	4	5	3	3	4	3	3	3	3	3	2	2	3	2	4	3	3	
	4	4	3	4	2	2	2	3	3	3	3	2	3	4	3	3	3	
Fakultas dan Prodi	3	2	3	3	4	3	3	2	3	3	3	2	1	3	3	3	3	3.5412
	3	4	3	2	3	3	2	3	3	3	3	2	1	4	3	3	3	
	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	2	5	
	5	5	1	1	4	5	3	2	5	5	5	3	4	5	5	5	5	
	5	3	3	3	4	3	3	4	4	4	3	3	4	4	4	4	4	
	3	3	2	4	4	3	3	3	3	4	4	4	4	4	4	4	4	
	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	
	4	3	4	3	4	4	4	4	4	4	4	4	3	4	4	4	4	
	2	4	3	4	2	5	4	3	3	5	2	4	4	2	4	2	5	
	3	4	4	4	3	5	4	3	4	5	3	2	4	3	3	3	4	
	2	3	2	1	3	5	3	3	4	4	4	4	2	1	2	2	4	
	3	4	3	1	3	5	3	3	3	3	5	3	3	1	3	4	5	
	3	2	4	4	5	3	2	3	4	4	2	3	4	2	4	5	3	
	3	4	5	3	2	4	3	3	5	4	3	2	4	2	3	3	3	
	3	3	4	3	2	2	2	3	2	3	2	3	2	2	3	3	3	
	3	4	2	4	3	2	4	3	3	3	4	2	2	4	2	3	3	

	Risk Management	*Review of Security Control*	*Life Cycle*	*Authorize Processing*	*System Security Plan*	*Personnel Security*	*Physical Security*	*Production, Input/Output Control*	*Contigency Planning*	*Hardware and Software Maintenance*	*Data Integrity*	*Documentation*	*Security Awarness, Training, and Education*	*Incident Response Capability*	*Identification and Authentication*	*Logical Access Control*	*Audit Trails*	*Rata - Rata*
	3	3	3	3	3	2	3	3	2	4	2	4	3	4	2	3	4	
	4	4	4	3	2	3	3	3	2	5	3	4	3	2	3	4	4	
	3	2	4	2	3	5	5	2	3	4	5	4	4	4	4	4	3	
	3	4	3	3	4	4	4	3	4	3	5	3	3	5	4	4	5	
	4	4	5	4	3	4	3	4	5	5	4	5	2	4	3	3	3	
	5	3	3	4	5	4	3	5	4	3	4	3	2	5	4	3	3	
	4	4	3	2	2	2	3	3	4	4	3	2	3	3	4	4	4	
	3	3	4	3	3	3	2	3	4	4	3	3	3	2	4	4	4	
	4	5	4	2	5	5	4	5	4	4	5	5	5	5	4	5	4	
	4	4	3	5	4	4	5	5	3	4	4	4	5	4	4	5	5	
	5	5	3	2	3	3	3	3	4	5	4	2	4	3	4	4	4	
	3	3	3	3	3	3	3	3	4	5	4	3	4	3	3	4	3	
	3	4	4	4	4	4	4	2	3	5	4	4	4	3	3	4	4	
	5	3	3	4	3	3	3	3	4	4	4	4	2	3	4	5	4	
	5	3	3	3	3	3	3	3	3	4	3	3	3	3	4	4	3	
	4	3	3	3	3	3	3	3	4	3	4	3	3	3	4	4	3	
	2	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	
	3	3	2	3	3	3	3	2	3	4	3	3	3	3	3	3	3	
	2	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	
	3	3	2	3	3	3	3	2	3	4	3	3	3	3	3	3	3	
	5	5	4	3	5	4	4	5	5	4	4	3	4	5	4	3	2	
	4	4	3	5	4	5	5	4	4	5	3	5	3	5	4	3	2	
	3	4	4	3	4	4	4	4	4	4	4	4	4	3	4	4	4	
	3	3	4	3	4	3	3	4	3	3	4	4	4	4	4	3	4	
	3	4	3	3	5	5	5	4	4	5	4	4	5	4	5	4	4	
	3	3	4	4	4	5	5	4	5	4	5	4	5	4	4	5	5	
Staff PUDI	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	3.7451
	4	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	
	3	5	4	5	4	3	2	4	3	3	4	3	3	4	3	4	3	
	4	4	3	4	3	3	4	3	2	5	3	4	3	3	3	3	3	
	2	2	4	2	2	2	3	4	3	4	5	4	5	5	5	4	4	
	5	2	5	4	2	2	4	2	4	4	4	5	4	2	3	4	4	
	4	4	3	2	3	2	3	3	3	4	3	3	4	3	2	3	4	
	4	3	4	3	3	3	4	2	3	2	3	3	2	2	2	3	3	
	3	3	3	3	2	2	2	3	3	4	3	3	3	4	3	3	3	
	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	
	5	5	5	4	5	4	4	4	4	3	5	4	5	5	5	5	5	
	5	4	5	5	5	5	4	4	4	5	5	4	4	5	4	4	5	
	2	4	4	1	1	2	2	2	2	3	3	3	4	3	2	3	3	
	3	3	3	2	2	1	2	3	3	3	2	3	3	2	3	2	3	

	Risk Management	*Review of Security Control*	*Life Cycle*	*Authorize Processing*	*System Security Plan*	*Personnel Security*	*Physical Security*	*Production, Input/Output Control*	*Contigency Planning*	*Hardware and Software Maintenance*	*Data Integrity*	*Documentation*	*Security Awarness, Training, and Education*	*Incident Response Capability*	*Identification and Authentication*	*Logical Access Control*	*Audit Trails*	*Rata - Rata*
	4	4	5	4	5	4	4	4	5	5	4	4	5	5	4	4	4	
	4	4	4	5	4	4	4	4	5	4	4	5	5	4	4	4	4	
	3	5	5	5	5	5	5	4	5	4	4	5	5	4	4	4	5	
	4	4	4	5	4	5	4	4	4	5	4	5	5	5	5	4	5	
Rata - Rata	3.6125	3.6500	3.5750	3.4000	3.4750	3.5375	3.4750	3.4500	3.6250	3.9250	3.6375	3.6000	3.5875	3.5375	3.6625	3.6750	3.7375	3.6222

Uji Validitas

	Risk Management	*Review of Security Control*	*Life Cycle*	*Authorize Processing*	*System Security Plan*	*Personnel Security*	*Physical Security*	*Production, Input/Output Control*	*Contigency Planning*	*Hardware and Software Maintenance*	*Data Integrity*	*Documentation*
Risk Management	1											
Review of Security Control	0.422719731	1										
Life Cycle	0.319748709	0.369910075	1									
Authorize Processing	0.351955959	0.364016211	0.469467578	1								
System Security Plan	0.470817299	0.467975126	0.402890051	0.457320015	1							
Personnel Security	0.259224992	0.478091798	0.352899637	0.348039877	0.58863756	1						
Physical Security	0.341900398	0.398033251	0.415644877	0.509588514	0.557187833	0.698565126	1					
Production, Input/Output Control	0.424446911	0.437658676	0.438224829	0.496970779	0.605025923	0.471629656	0.509370724	1				
Contigency Planning	0.476394746	0.435307329	0.450771993	0.390758717	0.566348672	0.591697659	0.554728814	0.540687557	1			
Hardware and Software Maintenance	0.387460308	0.453895467	0.376923202	0.41843402	0.397681187	0.482788665	0.453994496	0.325733765	0.4873461	1		
Data Integrity	0.389469759	0.451616832	0.423824547	0.273035585	0.562402394	0.573049434	0.554039871	0.463204728	0.579133131	0.46819418	1	
Documentation	0.346600593	0.294798602	0.544802052	0.512309085	0.475150841	0.512652778	0.599233564	0.51560895	0.415593926	0.56402703	0.527431726	1
Security Awarness, Training, and Education	0.277249207	0.413491891	0.48710721	0.360230345	0.469331781	0.470223939	0.614826063	0.542031002	0.553362472	0.535441487	0.53561924	0.552642698
Incident Response Capability	0.437078164	0.444585342	0.349905008	0.427093678	0.629792863	0.399644957	0.502932425	0.630695591	0.463323237	0.385279653	0.621846617	0.430819907
Identification and Authentication	0.474280343	0.414795524	0.35857466	0.474474871	0.587182308	0.514528645	0.482496554	0.581128452	0.566722628	0.549123343	0.593699944	0.515979293
Logical Access Control	0.458647992	0.291390261	0.345204418	0.348625904	0.491839832	0.351586991	0.42246638	0.381198322	0.502749972	0.450092744	0.606240153	0.428178655
Audit Trails	0.309487852	0.480405606	0.398733139	0.289748681	0.467350926	0.513103371	0.470715364	0.366198684	0.398192216	0.526491847	0.643855383	0.523537337
Jumlah	0.590624077	0.632023407	0.624797885	0.631008933	0.769216227	0.717959641	0.758858166	0.725869176	0.744030844	0.685213133	0.76885913	0.730260323
r tabel	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222
	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid

	Security Awarness, Training, and Education	*Incident Response Capability*	*Identification and Authentication*	*Logical Access Control*	*Audit Trails*	*Jumlah*
Risk Management						
Review of Security Control						
Life Cycle						
Authorize Processing						
System Security Plan						
Personnel Security						
Physical Security						
Production, Input/Output Control						
Contigency Planning						
Hardware and Software Maintenance						
Data Integrity						
Documentation						
Security Awarness, Training, and Education	1					
Incident Response Capability	0.493904708	1				
Identification and Authentication	0.596440676	0.5839513	1			
Logical Access Control	0.580703765	0.426897036	0.625465998	1		
Audit Trails	0.577573334	0.385465041	0.565960421	0.498718257	1	
Jumlah	0.754005573	0.722034357	0.786556499	0.679034964	0.695554881	1
r tabel	0.219812222	0.219812222	0.219812222	0.219812222	0.219812222	
	Valid	Valid	Valid	Valid	Valid	

UJI RELIABILITAS

Spearman Brown	0.970953
Reliabilitas	Sangat Tinggi