Manajemen Risiko Pada Pusat Data Perguruan Tinggi Dengan Kerangka Kerja NIST 800-30 (Studi Kasus: Universitas Kristen Duta Wacana)

Halim Budi Santoso[1], Lussy Ernawati[2]

***Abstrak*— Pusat data pada Perguruan Tinggi menangani pengelolaan data dan informasi untuk kepentingan operasional dan pelayanan aktivitas pengajaran, penelitian, pengabdian, keuangan, kemahasiswaan, dan sebagai media penyimpanan. Dalam Pusat data juga terdapat peralatan yang lain yang mendukung kegiatan server atau komputer untuk tetap berjalan dengan baik. Pusat data merupakan aset yang yang harus dilindungi keamanan data dan informasinya dari setiap risiko dan ancaman yang ada. Risiko dan ancaman tidak hanya terjadi pada sistem operasi, aplikasi, file dan data saja tetapi risiko dan ancaman terhadap lokasi fisik dari pusat data tersebut ditempatkan. Kerangka kerja NIST 800-30 sebagai acuan dan prosedur kerja dalam melakukan penilaian risiko pusat data. NIST 800-30 memberikan 9 tahapan yaitu karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, analisa pengendalian, penentuan kemungkinan, analisa dampak, penentuan risiko, rekomendasi pengendalian dan dokumentasi hasil. Hasil penentuan risiko dibagi dalam 3 kategori tinggi, rendah dan sedang. Tinggi, sumber ancaman yang sangat merugikan organisasi. Kategori risiko tinggi dalam pusat data, disebabkan dari internal Universitas Kristen Duta Wacana sendiri, pemahaman tentang teknologi informasi karyawan masih rendah. Kategori sedang, memiliki potensi kerugian terhadap organisasi tetapi masih dapat dilakukan pengendalian untuk menghambat ancaman yang akan timbul. Fluktuasi sumberdaya listrik yang sering terjadi dapat dicegah dengan memasang UPS dan genset dalam pusat data. Kategori rendah, tidak terlalu memberikan kerugian terhadap pusat data, pengendalian bisa dilakukan oleh unit pengembangan dan pemeliharaan Universitas Kristen Duta Wacana sendiri.**

***Kata Kunci:* Pusat data, Risiko, Ancaman, NIST 800-30**

***Abstract*— Data center for Higher Education handles data and information management for operational and services, such as teaching, research, empowerment, finance, students, and as a storage media. Data center is also as a tools to support server activity or computer to run well. Data center is an important asset which needed to be protected for its data and information from every risk and vulnerability. Risk and vulnerability for data center not only in operating system but also physical location of its data center. NIST 800-30 framework as an reference and working procedure to assess risk for data center. NIST 800-30 gives 9 steps: system characteristic, threat and vulnerability identification, control assessment, probabilities determination, risk assessment, control recommendation, and result documentation. Risk assessment is divided into 3 category high, medium, and low. High when threat resources can harm and bring loss to organization. High risk category is caused by Duta Wacana Christian University Internal, low understanding of its human resources. Medium risk category has possibilities to bring loss to organization but it is still able to be controlled to inhibit threat. Fluctuation in electrical resources can be prevented by installing UPS and Genset in the data center. Low risk category is not able to bring some losses to development and maintenance unit of Duta Wacana Christian University.**

Keyword: Data center, Risk, Theft, NIST 800-30

[1]*Dosen, Sistem Informasi, Universitas Kristen Duta Wacana, Dr. Wahidin Sudiro Husodo No. 5 – 25 Yogyakarta 55224 INDONESIA (tlp: 0274 – 563929 ext.115; fax: 0274 – 513235; email: hbudi@staff.ukdw.ac.id)*

[2]*Dosen, Sistem Informasi, Universitas Kristen Duta Wacana, Dr. Wahidin Sudiro Husodo No. 5 – 25 Yogyakarta 55224 INDONESIA (tlp: 0274 – 563929 ext.313; fax: 0274 – 513235; email: lussy@staff.ukdw.ac.id)*

I. PENDAHULUAN

Aktivitas Perguruan Tinggi menghasilkan banyak data seperti data aktivitas pengajaran, penelitian, pengabdian, keuangan, dan kemahasiswaan. Perkembangan teknologi informasi ini mendukung pelayanan kepada mahasiswa dan pemangku kepentingan menjadi lebih efisien dan efektif. Penggunaan teknologi informasi di lingkungan perguruan tinggi, seperti pelayanan akademik, keuangan, manajemen pembelajaran, dan integrasi data, dapat meningkatkan produktivitas, ketersediaan informasi bagi stakeholder Perguruan Tinggi.

Teknologi informasi, bagi Perguruan tinggi merupakan salah satu komponen penting dalam pengelolaan sistem informasi,. Akan tetapi pemanfaatan teknologi informasi dalam pengelolaan sistem informasi bisa tidak sesuai harapan dan akan muncul risiko yang dapat menganggu keberlangsungan sistem informasi sehingga dapat mengakibatkan kerugian [1].

Seiring dengan perkembangan dan penggunaan teknologi informasi, data yang dimiliki oleh perguruan tinggi tersimpan ke dalam bentuk digital. Untuk membantu dalam pengelolaan data tersebut, sebuah Perguruan Tinggi membentuk sebuah tempat data yang di sebut dengan pusat data atau *electronic data center*. Pada Perguruan Tinggi, Pusat Data disebut juga sebagai Pusat Komputerisasi yang mendukung teknologi informasi.

Pusat data di lingkungan perguruan tinggi merupakan salah satu *repository* terintegrasi untuk data perguruan tinggi. Di dalam pusat data tersebut, data perguruan tinggi, baik data operasional maupun strategis tersimpan. Data ini tentunya bermanfaat bukan hanya untuk kepentingan pelayanan terhadap mahasiswa, tetapi juga untuk pemberian data kepada pihak lain yang berwenang, seperti pemerintah dan pemangku kepentingan lainnya. Selain itu, data yang terdapat dalam perguruan tinggi juga berperan dalam proses akreditasi institusi perguruan tinggi.

Pusat data perguruan tinggi juga membantu untuk meningkatkan kualitas pelayanan administrasi di lingkungan perguruan tinggi. Dengan demikian, pelayanan administrasi pendidikan menjadi teruji tingkat validitasnya, efisien, efektif, dan di dukung oleh keakuratan data, kecepatan pengolahan data, serta keamanan yang terjamin. Keberadaan pusat data juga sebagai tindak lanjut atas penggunaan teknologi informasi dan komunikasi di lingkungan perguruan tinggi. Oleh karena itu, pusat data di lingkungan perguruan tinggi menjadi sangat penting. Pusat data perlu di jaga keamanan dan informasi yang ada di dalamnya. Pusat data merupakan salah satu aset yang penting bagi perguruan tinggi. Hal ini juga berlaku bagi Universitas Kristen Duta Wacana

Pusat data Universitas Kristen Duta Wacana merupakan salah satu aset yang harus dilindungi untuk keamanan data dan informasi selain menangani pengelolaan data untuk kepentingan operasional, juga sebagai media penyimpanan dan pendistribusian data baik ke internal dan eksternal. Pusat data juga memiliki berbagai tantangan tentang keamanan basis data, kemanan aplikasi, keamanan jaringan, kinerja sistem, infrastruktur yang semakin komplek dan keamanan lingkungannya secara fisik. Dalam menghadapi tantangan tersebut diperlukan sistem pengendalian untuk menghadapi segala risiko yang akan terjadi.

Risiko-risiko yang muncul tersebut perlu diatasi, sehingga tidak menghambat kinerja sistem informasi dan pusat data . Risiko – risiko yang dihadapi juga dapat merugikan perguruan tinggi itu sendiri, baik kerugian secara material maupun secara inmaterial. Oleh karena itu, risiko – risiko yang muncul dari pusat data perlu di atur sehingga dapat meminimalisasi dampak kerugian yang akan timbul apabila resiko tersebut benar – benar terjadi.

Di dalam penelitian ini, akan dilakukan kajian terhadap resiko – resiko yang muncul untuk pusat data . Selain itu, akan dilakukan beberapa langkah pengendalian yang dapat di lakukan untuk mengantisipasi segala resiko yang ada. Penelitian ini menggunakan kerangka kerja NIST SP 800-30 untuk melakukan manajemen resiko.

II. TINJAUAN PUSTAKA

A. Konsep Risiko Teknologi Informasi

Aset Teknologi Informasi, seperti layaknya aset lainnya di dalam perusahaan perlu dijaga dari berbagai macam ancaman. Aset teknologi informasi dapat dikategorikan menjadi beberapa macam, yaitu diantaranya perangkat keras, perangkat lunak, sistem informasi, jaringan komputer, informasi, data, dan manusia / sumber daya manusia. Sumber daya manusia tak kalah penting dari aset – aset lainnya dan bukan dianggap sebagai beban bagi perusahaan.

Risiko menurut Australian / New Zealand Standard [2] merupakan kesempatan terjadinya sesuatu, seperti sumber daya manusia, finansial, hukum, manajemen, peristiwa alam, kegiatan operasi, masyarakat, politik, ataupun teknologi yang akan berdampak terhadap obyektif tertentu. Atau dengan kata lain, risiko adalah kemungkinan terjadinya peristiwa yang membawa akibat yang tidak diinginkan atas tujuan, strategi, sasaran, dan / atau target. Dampak dari suatu risiko dapat bervariasi, seperti di level strategik, operasional, pelaporan, dan ketaatan. Berdasarkan pengertian tersebut, tentunya risiko juga dapat menimpa aset teknologi informasi yang dimiliki oleh perusahaan. Dampak yang yang di hasilkan oleh risiko aset teknologi informasi juga bervariasi, mulai dari level strategik, operasional, pelaporan, dan ketaatan [2]. Oleh karena itu, risiko aset teknologi informasi adalah kemungkinan terjadinya peristiwa atas aset teknologi informasi, seperti perangkat keras, perangkat lunak, sistem informasi, jaringan komputer, informasi, data, dan sumber daya manusia, yang membawa dampak yang tidak diinginkan atas tujuan, strategi, sasaran, dan / atau aset teknologi informasi.

Aset Teknologi Informasi seperti halnya aset lain harus di jaga. Organisasi atau perusahaan, sebagai pemiliki aset, harus mampu untuk melindungi selusuh aset tersebut dari berbagai macam ancaman (*threats*) dan kerentanan (*vulnerability*). Ancaman dan kerentanan memiliki beberapa perbedaan di tinjau oleh Krutz dan Vines [3].

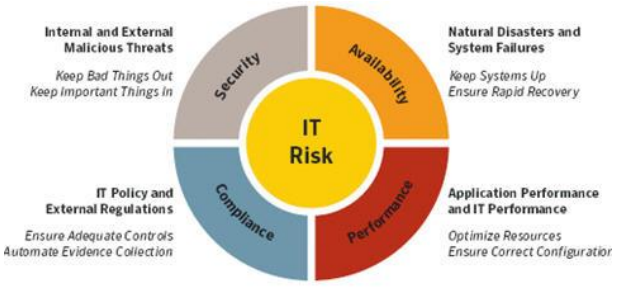
Ancaman merupakan setiap peristiwa yang jika terjadi, dapat menyebabkan kerusakan pada sistem dan membuat hilangnya kerahasiaan, ketersediaan, ataupun integritas. Ancaman bisa berbahaya, seperti modifikasi yang disengaja terhadap informasi sensitif – atau tidak sengaja – seperti kesalahan dalam perhitungan transaksi atau penghapusan file [3]. Di sisi lain, kerentanan adalah kelemahan dalam sistem yang dapat di eksploitasi oleh

ancaman. Kerentanan dapat dinilai sesuai dengan tingkat risiko terhadap organisasi, baik secara internal maupun eksternal [3].

Selain konsep ancaman dan kerentanan, risiko teknologi informasi juga dapat di bedakan berdasarkan penyebab risiko tersebut dan dampak yang di timbulkan bagi teknologi informasi. Risiko yang terjadi dapat berupa risiko fisik ataupun risiko logik. Berdasarkan kategori tersebut, risiko fisik lebih banyak berdampak terhadap perangkat keras teknologi informasi dan kaitannya dengan beberapa kejadian lainnya [4]. Beberapa contoh risiko yang dapat dikaitkan dengan kerusakan fisik adalah bencana alam (*natural disaster*), pencurian (*theft*), kebakaran (*fires*), lonjakan arus listrik (*power surge*), dan perusakan (*vandalism*). Bencana alam dapat di kategorikan sebagai risiko kerusakan fisik karena apabila bencana alam terjadi, aset teknologi informasi yang dapat terdampak adalah infrastruktur teknologi informasi dan perangkat keras. Sedangkan pencurian merupakan salah satu hal yang juga berkaitan dengan perangkat keras dan komponen dalam teknologi informasi. Akan tetapi, pencurian lain yang juga akan memberikan dampak adalah pencurian terhadap perangkat lunak, data, dan informasi yang dimiliki oleh organisasi / perusahaan.

Berbeda dengan risiko kerusakan fisik, risiko lainnya adalah risiko yang bersifat kerusakan logik. Risiko ini lebih mengacu pada proses yang terjadi dalam sistem informasi dan data [4]. Risiko kerusakan logik merupakan salah satu penyebab kegagalan dari sistem informasi. Selain itu, pencurian dan penghapusan terhadap data juga merupakan salah satu risiko kerusakan logik. Risiko kerusakan logik dapat di sebabkan oleh berbagai hal, baik dari eksternal maupun internal. Dari pihak eksternal, virus dan malware merupakan ancaman yang dapat menyebabkan terjadinya risiko kerusakan logik. Sedangkan dari faktor internal, pencurian terhadap kode program dan data yang dilakukan oleh karyawan juga dapat menyebabkan kerusakan logik.

Berbeda dengan Jakaria, Dirgahayu, dan Hendrik [4] yang mengklasifikasikan hanya menjadi 2 jenis risiko berdasarkan kerusakan, Farber [5] mengklasifikasikan berdasarkan jenis serangan dan risiko yang ada. Gambar 1 di bawah ini menunjukan klasifikasi risiko dari Teknologi Informasi:



Gambar 1: Klasifikasi Risiko (Farber, 2008)

Gambar 1 di atas menunjukan klasifikasi risiko teknologi informasi menurut Farber [5]. Dari gambar 1 tersebut, terdapat 4 jenis risiko, yaitu: (1) *Availability Risk*; (2) *Performance Risk*; (3) *Compliance Risk*; dan (4) *Internal dan External Malicious Threats*. *Availability Risk* merupakan risiko yang disebabkan oleh adanya bencana alam dan kegagalan dari sistem. Sedangkan untuk *Performance Risk* merupakan risiko yang mengancam terhadap performa dari aplikasi dan teknologi informasi, termasuk di dalamnya perangkat keras dan lunak. Yang termasuk dalam compliance adalah risiko yang muncul sebagai akibat dari adanya ketidakpatuhan terhadap peraturan yang ada. Dan yang terakhir adalah security yang berupa keamanan teknologi informasi, termasuk didalamnya keamanan data dan informasi yang ada.

B. Manajemen Risiko

Risiko merupakan peluang terjadinya sesuatu yang mempunyai dampak terhadap sasaran [6]. Pengertian lain disiebutkan bahwa risiko merupakan gabungan antara kemungkinan sebuah kejadian beserta konsekuensinya, baik konsekuensi positif maupun konsekuensi negative [7]. Oleh karena itu, risiko seringkali memiliki kaitan terhadap efek negative dari adanya suatu kejadian. Menurut Risnandar, risiko yang membawa dampak negative di akibatkan oleh suatu kerawanan (*vulnerability*).

Risiko juga merupakan efek dari ketidakpastian sasaran [8]. Sedangkan efek ini merupakan penyimpangan dari pengharapan positif dan atau negatif. Dengan kata lain, risiko merupakan kemungkinan situasi atau keadaan yang dapat mengancam pencapaian tujuan serta sasaran sebuah organisasi atau individu [9]. Berdasarkan pengertian tersebut, risiko seharusnya dapat di antisipasi. Untuk mengantisipasi hal tersebut, diperlukan suatu manajemen risiko yang dapat melakukan identifikasi risiko dan memberikan pengendalian terhadap risiko tersebut.

Manajemen risiko adalah identifikasi, penilaian, dan prioritas risiko diikuti oleh aplikasi terkoordinasi dan ekonomis dari sumber daya untuk meminimalkan, memantau, dan mengendalikan probabilitas dan / atau dampak peristiwa yang tidak diinginkan [10]. Manajemen risiko merupakan proses iteratif yang terdiri dari langkah – langkah yang terdefinisi yang bertujuan mengidentifikasi dan mengelola risiko dengan baik.

Penelitian terkait dengan manajemen risiko teknologi informasi telah dilakukan beberapa peneliti. Framework yang digunakan dan berkaitan dengan risiko adalah ISO 31000 Risk Management. Kerangka kerja ISO 31000 ini digunakan untuk melakukan manajemen risiko terhadap teknologi informasi perbankan. Gustini dan Sulisti [11] menggunakan kerangka kerja ISO 31000 untuk melakukan manajemen risiko teknologi informasi pada bank bengkulu. Sebagai hasilnya, penerapan manajemen risiko di Bank Bengkulu memiliki kualitas yang memuaskan. Penilaian ini di dasarkan pada proses yang dilakukan, yaitu dimulai dari tahapan penyusunan strategi, program, kebijakan, sasaran, dan implementasi.

Kerangka kerja manajemen risiko lainnya adalah NIST 800-30. National Institute of Standards and Technology (NIST) merupakan organisasi pemerintahan Amerika Serikat yang bertujuan untuk menyusun panduan manajemen risiko di bidang teknologi informasi. Manajemen risiko merupakan suatu proses yang memungkinkan pemimpin organisasi untuk dapat menyeimbangkan biaya operasional dan ekonomi yang dikeluarkan untuk mengurangi risiko dan mencapai keuntungan dengan melindungi sistem teknologi informasi dan data yang mendukung misi atau tujuan bisnis organisasi [1].

Menurut NIST [12], manajemen risiko adalah sebuah proses yang mengijinkan manager IT untuk menyeimbangkan antara operasional dan biaya ekonomis dari ukuran protektif dan mencapai misi untuk melakukan proteksi terhadap sistem dan data teknologi informasi yang mendukung misi organisasi. Manajemen risiko yang efektif harus dapat terintegrasi dengan daur hidup perangkat lunak (system development life cycle) [12]. Oleh karena itu, manajemen risiko dari teknologi informasi harus dimulai sejak pertama kali sistem dikembangkan / dibangun.

Pada tahap inisiasi pengembangan sistem, manajemen risiko harus dapat mengidentifikasi kebutuhan keamanan dan operasional keamanan sistem [12]. Selain itu, manajemen risiko juga harus mampu di desain untuk mendukung analisa keamanan dari sistem teknologi informasi yang akan sedikit banyak mempengaruhi desain dan rancangan arsitektur teknologi informasi. Pada tahap implementasi, manajemen risiko juga harus mampu untuk memberikan keputusan terkait dengan identifikasi risiko dalam proses implementasi dan operasional. Manajemen risiko ini harus mampu di evaluasi secara berkala / reakreditasi untuk melihat perubahan – perubahan yang mungkin terjadi pada saat proses implementasi. Sebagai akhirnya, aktivitas manajemen risiko di jalankan untuk komponen sistem yang dapat ditimpa untuk menyakinkan bahwa perangkat lunak yang ada dapat di minimalisasikan kerugian akibat risiko yang ada [12].

Beberapa tahapan yang digunakan untuk melakukan manajemen risiko menggunakan kerangka kerja NIST 800-30 adalah:

1. Karakteristik dari sistem
2. Identifikasi ancaman
3. Identifikasi kerentanan
4. Analisa Pengendalian
5. Penentuan kemungkinan
6. Analisa dampak
7. Penentuan risiko
8. Rekomendasi pengendalian
9. Dokumentasi hasil.

Penggunaan kerangka kerja NIST 800-30 ini telah dilakukan oleh Nugraha [1]. Di dalam penelitiannya, Nugraha [1] melakukan identifikasi risiko untuk sistem informasi yang terdapat di lingkungan perguruan tinggi. Sebagaimana menggunakan 3 langkah manajemen risiko dengan menggunakan kerangka kerja NIST 800-30, yaitu : (1) penilaian risiko; (2) peringanan risiko; dan (3) evaluasi risiko. Sebagai hasil dari penelitian ini adalah rekomendasi untuk mengurangi risiko yang akan terjadi pada sistem informasi di kalangan perguruan tinggi.

C. Pusat Data

Pusat data dikenal sebagai kumpulan *server* atau ruang komputer, Pusat data dari sebagian besar organisasi untuk penyimpanan, pengoperarsian, pengelolaan ada di ruang server [13]. Pusat data merupakan fasilitas yang memiliki kemampuan untuk mengatur, mengelola dan menyelenggarakan layanan teknologi informasi dan komunikasi dalam bentuk layanan. Pusat data dapat dikatakan menjadi suatu aset yang penting bagi suatu perusahaan. Dengan melakukan pengelolaan pusat data secara efisien, perusahaan dapat meningkatkan efektivitas dari proses pemeliharaan bisnis yang ada. Perusahaan dapat

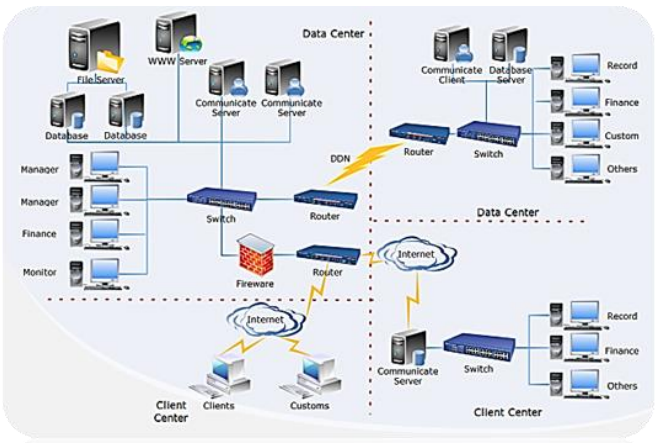
Dalam Pusat data terdapat infrastruktur, koneksi jaringan, pengelolan database dan alokasi sumberdaya untuk keperluan ketersediaan layanan jangka panjang, kehandalan dan keamanan aset teknologi informasi dan komunikasi. Pusat data Perguruan Tinggi akan menjadi pusat layanan teknologi informasi dan komunikasi yang menjadi aset vital bagi proses layanan, baik untuk layanan sistem informasi dan akses bagi pihak-pihak yang berkepentingan.

Pusat data sebagai media penyimpanan data, harus dapat memenuhi syarat 3C agar pusat data tersebut dapat berjalan dengan baik:

1. Comprehensive (Komprehensif): perencanaan data untuk organisasi harus bersifat universal dan unik agar dapat melawan berbagai macam ancaman dan tantangan
2. Convenience (Kenyamanan): pusat data harus dapat menjadi pendukung kegiatan operasional Teknologi Informasi dengan mudah.
3. Costs (Biaya): pengelolaan biaya di dalam lingkungan pusat data harus dapat berjalan dengan baik.

Kumpulan server dan sistem penyimpanan data membutuhkan fasilitas untuk menampung semua sumber daya yang dimiliki. Fasilitas tersebut harus memenuhi kondisi server yang memungkinkan untuk melakukan pengaturan sumber daya, pengaturan udara serta memiliki sistem pengamanan fisik. Fasilitas yang menjadi pusat penampungan data ini memiliki beberapa kriteria khusus dalam perancangannya, antara lain:

1. *Availibility*, Pusat data mampu menjalankan operasi secara berkelanjutan dan terus menerus dalam kondisi apapun.
2. *Scalability* dan *Flexibility*, Pusat data mampu beradaptasi dengan pertambahan kebutuhan atau teknologi baru tanpa merubah substansi pusat data secara keseluruhan.
3. *Security*, Pusat data mampu melindungi aset data yang tersimpan pada server secara fisik maupun non-fisik.



Gambar 2. Electronic data center Network Diagram

Pada gambar 2 diatas merupakan salah satu infrastruktur pusat data. Tampak pada gambar tersebut bahwa di dalam pusat data, beberapa komputer terkoneksi satu sama lain. Selain itu, proses lalu lintas data juga berada dalam pusat data. Di dalam pusat data tersebut terdapat beberapa server basis data yang terkoneksi satu sama lain. Hal ini juga berlaku untuk perguruan tinggi

sebagai salah satu organisasi dengan banyak sistem informasi yang terlibat di dalamnya.

Perguruan tinggi sebagai salah satu organisasi juga memiliki beberapa data yang harus dirawat dan dijaga. Data akademik, seperti data mahasiswa, data perkuliahan, materi perkuliahan, evaluasi pembelajaran, dll merupakan salah satu aset yang sangat berharga bagi perguruan tinggi. Selain itu, perguruan tinggi juga menyimpan beberapa data lain terkait data keuangan dan pembiayaan di lingkungan perguruan tinggi.

Pusat data bagi perguruan tinggi akan dapat menciptakan simpul – simpul jaringan pendidikan yang membuat instansi perguruan tinggi di Indonesia bukan bersaing secara fisik, tetapi dapat berkolaborasi untuk dapat mewujudkan cita – cita bangsa ini. Perguruan Tinggi akan memanfaatkan pusat data juga untuk memberikan akses terhadap bahan ajar yang dapat dibagikan, tukar menukar pengetahuan, terwujudnya jenjang pendidikan, dan tentu saja aksesbilitas bagi orang yang terlibat di dalamnya menjadi lebih mudah [14].

III. METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah melakukan wawancara dan observasi. Selain itu, penelitian ini juga melakukan kajian pustaka terhadap beberapa sumber yang digunakan. Kerangka kerja NIST 800-30 digunakan sebagai acuan dan prosedur kerja dalam melakukan penilaian terhadap risiko yang ada. Beberapa tahapan yang dipergunakan dalam manajemen risiko pusat data adalah:

1. Karakteristik dari sistem
2. Identifikasi ancaman
3. Identifikasi kerentanan
4. Analisa Pengendalian
5. Penentuan kemungkinan
6. Analisa dampak
7. Penentuan risiko
8. Rekomendasi pengendalian
9. Dokumentasi hasil.

Untuk melakukan pengumpulan data, peneliti melakukan pengumpulan data dengan melakukan wawancara dan observasi. Selain itu, pada penelitian ini juga dilakukan penggalian informasi melalui wawancara yang ada. Beberapa orang yang dilakukan wawancara adalah administrator jaringan, administrator aplikasi, administrator basis data, dan beberapa pengguna. Peneliti juga melakukan kajian terhadap pustaka – pustaka pendukung penelitian.

IV. ANALISA DAN HASIL PENELITIAN

A. Sistem Karakteristik

Karakteristik dari sistem yang digunakan di Universitas Kristen Duta Wacana sangat fleksibel, sehingga sangat mudah disesuaikan dengan kebutuhan internal Universitas Kristen Duta Wacana. Pengelolaan dan pengembangan pusat data di Universitas Kristen Duta Wacana dilakukan oleh unit pengembangan sistem yang ada di Universitas Kristen Duta Wacana. Pemeliharaan pusat data, untuk teknologi informasi dilakukan secara periodik. Sistem informasi akan di-backup setiap bulan kemudian akan di copy ke DVD setiap semester dan untuk hardware akan dilakukan peremajaan setiap 2-3 tahun.

Pengembangan sistem informasi dilakukan sesuai kebutuhan dari Universitas Kristen Duta Wacana sendiri, guna mendukung berbagai aktivitas seluruh sivitas akademika, mendukung fungsi proses belajar mengajar dan untuk pengolahan administrasi umum Universitas Kristen Duta Wacana.

B. Identifikasi Ancaman

Beberapa ancaman yang dapat terjadi di lingkungan Universitas Kristen Duta Wacana berdasarkan sumber ancaman dapat di bedakan menjadi 3 (tiga), yaitu: (1) Ancaman yang berasal dari kejadian alam; (2) Ancaman yang berasal dari manusia; (3) Ancaman lingkungan. Tabel I di bawah ini menunjukan jenis ancaman yang mungkin terjadi di Universitas Kristen Duta Wacana:

TABEL 1. JENIS KERENTANAN DALAM IMPLEMENTASI TEKNOLOGI INFORMASI DI UNIVERSITAS KRISTEN DUTA WACANA

No	Ancaman
1	Ancaman yang berasal dari alam: • Gempa bumi • Gunung meletus • Tsunami • Angin putting beliung
2	Ancaman manusia: • Hak akses ke dalam pusat data belum di batasi. • Belum terdapat pembatasan akses ke dalam pusat data • Penyalahgunaan wewenang dalam pemanfaatan aplikasi. Seperti yang diketahui, aplikasi yang dikembangkan di Universitas Kristen Duta Wacana masih terdapat beberapa kekurangan. Hal ini tentunya menjadi ancaman tersendiri dalam memanfaatkan aplikasi dan informasi yang terkandung di dalamnya. • Pengambilan data yang tidak sesuai dengan prosedur kerja. • SQL Injection • Bandwidth Flooding
3	Ancaman Lingkungan: • Kegagalan aliran arus listrik • Hewan tikus yang sering terlihat di atap – atap ruang pusat data • Arus listrik yang tidak stabil di beberapa instalasi • Ancaman dari virus, worms, dan trojan.

Tabel 1 di atas menunjukan ancaman yang terdapat di Pusat Data Universitas Kristen Duta Wacana. Terdapat ancaman yang berasal dari alam yaitu gempa bumi, gunung meletus, tsunami, dan angin puting beliung. Universitas Kristen Duta Wacana terletak di Yogyakarta dan di Yogyakarta terdapat beberapa bencana yang pernah terjadi dan kemungkinan akan dapat terjadi kembali. Gempa bumi dan gunung meletus merupakan ancaman. Daerah Istimewa Yogyakarta terkenal dengan salah satu gunung berapi teraktif yaitu gunung merapi yang terletak di sebelah utara Yogyakarta. Selain itu, juga terdapat beberapa pantai di daerah selatan yang juga dapat berpotensi menimbulkan bencana tsunami.

Selain ancaman dari alam, terdapat ancaman dari manusia. Pusat Data Universitas Kristen Duta Wacana belum menerapkan prosedur dan hak akses untuk dapat masuk ke Pusat Data . Oleh karena itu, hal ini tentunya menjadi ancaman yang sangat rawan. Tidak adanya pemisahan hak akses ke dalam pusat data dapat seseorang

dengan mudahnya memasuki pusat data . Sedangkan untuk ancaman yang berasal dari lingkungan berasal dari aliran arus listrik. Selain itu, di dalam pusat data masih sering terlihat hewan tikus yang terdapat di atap – atap pusat data.

C. Identifikasi Kerentanan

Beberapa kerentanan yang teridentifikasi dapat dikategorikan menjadi 4, yaitu: (1) kerentanan terhadap konfigurasi perangkat keras; (2) kerentanan terhadap perangkat lunak dan aplikasi; (3) kerentanan terhadap kebijakan dan prosedur sistem informasi; (4) kerentanan pada sumber daya manusia. Tabel II di bawah ini menunjukan jenis kerentanan untuk pusat data di Universitas Kristen Duta Wacana.

TABEL 2. JENIS KERENTANAN PUSAT DATA UNIVERSITAS KRISTEN DUTA WACANA

No	Kerentanan
1	Kerentanan terhadap perangkat keras • Pembagian akses terhadap penggunaan perangkat keras yang ada • Tidak berfungsinya dengan baik firewall untuk mencegah serangan trojan, virus, dan malware. • Belum terdapat prosedur untuk melakukan penanganan terhadap perangkat keras • Pencurian perangkat keras yang disebabkan oleh akses ke pusat data belum aman
2	Kerentanan terhadap perangkat lunak dan aplikasi • Integrasi dalam data yang memungkinkan memiliki data yang sama dan selalu diperbaharui • Integrasi sistem yang belum dapat terlaksana dengan baik • Konflik antar sistem informasi yang disebabkan oleh tidak terintegrasinya sistem yang ada • Pengembangan sistem informasi yang masih kurang benar dan hanya dilakukan secara terpisah tanpa melihat kebutuhan beberapa tahun mendatang.
3	Kerentanan terhadap kebijakan dan prosedur pusat data • Prosedur akses ke pusat data belum ada • Kebijakan dalam pengembangan Sistem Informasi hanya berjalan modular dan belum diterapkan secara terintegrasi • Dukungan pihak rektorat dan yayasan terhadap Teknologi Informasi yang masih kurang. • Unit yang menangani Teknologi Informasi masih bersifat operasional dan bukan merupakan unit strategis. • Prosedur backup di lingkungan Universitas Kristen Duta Wacana yang masih belum sempurna.
4	Kerentanan terhadap Sumber Daya Manusia: • Kurangnya sumber daya manusia yang menangani pusat data . Sumber daya manusia yang menangani pengembangan sistem juga merangkap sebagai perawatan sistem.

Tabel 2 diatas menunjukan jenis kerentanan yang terjadi dalam pusat data Universitas Kristen Duta Wacana. Dari kerentanan perangkat keras, penanganan akses terhadap perangkat keras menjadi salah satu kendala yang harus di hadapi. Kurang ketatnya pengawasan terhadap akses ke perangkat keras juga rawan terhadap pencurian perangkat keras itu sendiri. Selain itu, untuk kerentanan terhadap perangkat lunak dan aplikasi di sebabkan oleh sebagian data yang tidak terintegrasi. Hal ini disebabkan karena pengembangan sistem yang dilakukan secara tidak terintegrasi dan dilihat per modular saja.

Di dalam Tabel II juga di jelaskan kerentanan terhadap kebijakan dan prosedur terhadap pusat data . Prosedur kerja yang belum sempurna dan tidak di perbaharui menjadi salah satu ancaman dari sisi kebijakan dan prosedur. Selain itu, kurangnya sumber daya manusia juga menjadi salah satu kerentanan. Hal ini menyebabkan ketergantungan yang sangat tinggi terhadap sumber daya manusia yang selama ini menangani pusat data . Ketergantungan ini juga dapat menyebabkan tidak adanya sumber daya manusia yang dapat berfungsi sebagai cadangan apabila terdapat suatu permasalahan terhadap sumber daya manusia yang ada selama ini.

D. Analisa Pengendalian

Pada tahapan analisa pengendalian dalam penilaian risiko pusat data Universitas Kristen Duta Wacana adalah bagaimana merancang untuk mencegah dan mendeteksi ancaman terhadap pusat data. Apa yang harus dilakukan Universitas Kristen DutaWacana dalam menyiapkan pusat datanya ketika terjadi bencana.

Berikut pengendalian risiko di lingkungan pusat data Universitas Kristen Duta Wacana:

a) Lokasi Fisik

Lokasi fisik Pusat data jauh dari tempat kerja karyawan dan bahaya yang alami, seperti pabrik, pipa air, banjir, gempa serta jauh dari arus lalu lintas normal, seperti pada lantai tertinggi bangunan.

1) Kontruksi Bangunan

Pusat Data Universitas Kristen Duta Wacana terletak di dalam kompleks kampus Universitas Kristen Duta Wacana. Konstruksi bangunan yang digunakan sebagai Pusat Data dibangun pada tahun 2005 dan memiliki konstruksi yang kuat.

2) Akses

Pusat Data Universitas Kristen Duta Wacana terletak di dalam satu ruang yang belum dibatasi oleh hak akses. Selain itu, Pusat Data ini terletak satu ruang dengan Pusat Teknologi Informasi yang menangani sistem informasi di lingkungan Universitas Kristen Duta Wacana.

3) Pemadam Kebakaran

Kebakaran adalah salah satu bencana alami yang dapat mengancam peralatan komputer, yang dapat menyebabkan kehilangan data. Setiap ruangan pusat data di lengkapi dengan Alat Pemadam Api Ringan. Akan tetapi, Alat Pemadam Api Ringan ini jarang dilakukan perbaikan dan pengecekan. Oleh karena itu, risiko akan muncul ketika terjadi kebakaran.

4) Power Supply

Berfungsi sebagai penyuplai tegangan listrik langsung kepada komponen-komponen PC dan peralatan yang berada dalam Pusat data

b) Sistem Operasi

Sistem Operasi sebagai program pengendalian komputer, sistem operasi akan membagi dan memberikan akses pengguna untuk sumberdaya yang ada dalam komputer, seperti *processors*, *main memory*, *database* dan printer. Keamanan sistem operasi meliputi kebijakan, prosedur dan pengendalian yang menentukan siapa yang dapat mengakses sistem operasi, file, program dan printer. Dari antara komponen keamanan Sistem Informasi, berikut ini adalah gambaran yang ada untuk Universitas Kristen Duta Wacana

1) Logon Procedure

Logon prosedur adalah prosedur pertama yang harus dilakukan ketika pengguna akan masuk dalam sistem operasi. Pengguna akan disajikan kotak dialog yang meminta ID dan *password* pengguna, kemudian sistem akan membandingkan ID dan *password* ke database pengguna apakah mempunyai otorisasi atau tidak.

2) Access Token

Token dalam sistem operasi adalah wadah yang berisi informasi mengenai pengguna, termasuk ID, *password*, user group dan hak istimewa yang diberikan kepada pengguna.

3) Access Control List

Access Control List dalam sistem operasi memberikan akses ke sumberdaya sistem, seperti direktori, file dan program. Pengendalian akan terjadi, ketiga pengguna akan mengakses sumberdaya, sistem akan membandingkan ID dan hak istimewa, apakah pengguna mempunyai otorisasi terhadap sumberdaya sistem.

c) Keseluruhan Sistem

1) Hak Akses

Hak Akses sistem diberikan kepada karyawan untuk mengakses file dan aplikasi yang merupakan tugas dari karyawan tersebut.

2) Password

Password merupakan kode rahasia yang dimiliki setiap pengguna yang akan mengakses sistem. Apabila ada karyawan yang akan mengakses sistem dan *password* salah, sistem tetap terkunci. Jadi *password* memberikan keamanan terhadap sistem.

3) Virus

Virus merupakan ancaman terhadap sistem, dapat merusak perangkat lunak komputer. Pusat data Universitas Kristen Duta Wacana pernah terkena serangan virus yang membuat sumberdaya pada komputer menjadi berkurang secara signifikan.

Untuk menanggulangi virus, pusat data Universitas Kristen Duta Wacana menggunakan anti virus McAfee dan secara berkala anti virus tersebut akan diupdate oleh admin jaringan Universitas Kristen Duta Wacana.

4) Electronic Audit Trail

Server Universitas Kristen Duta Wacana mempunyai catatan akitivitas pengguna pada saat mengakses aplikasi. *Electronic Audit Trail* digunakan untuk mengetahui siapa saja pengguna yang sudah masuk ke dalam sistem dan mengakses aplikasi, serta untuk mencegah dan mendeteksi penyalahgunaan sumberdaya sistem.

5) Prosedur Backup

Backup dilakukan setiap minggu terhadap semua aplikasi. Backup dilakukan oleh unit pengembangan dan pemeliharaan sistem Universitas Kristen Duta Wacana. Berikut prosedur backup pusat data Universitas Kristen Duta Wacana:

- Setiap staf unit pengembangan dan pemeliharaan sistem setiap hari Jumat akan melakukan backup di HD Eksternal/PC masing-masing sesuai bagiannya.
- Setiap 1 bulan sekali semua backup akan dijadikan 1 dan di copy ke dalam DVD rangkap 2.

E. Penentuan Kemungkinan

Identifikasi ancaman dan kerentanan yang dilakukan pada bagian A dan B diperlukan untuk menentukan besaran tingkat kemungkinan terjadinya risiko tersebut. Tingkat kemungkinan terbagi menjadi 3 kategori, yaitu: (1) Tinggi: risiko di katakan tinggi apabila risiko tersebut memiliki motivasi yang tinggi untuk dapat merugikan organisasi. Pengendalian yang dilakukan tidak efektif untuk mencegah terjadinya risiko yang ada; (2) Sedang: risiko memiliki motivasi untuk merugikan pihak Universitas Kristen Duta Wacana. Pihak universitas memiliki pengendalian untuk mencegah terjadinya risiko yang ada; (3) Rendah: risiko yang ada tidak memiliki motivasi untuk merugikan pihak Universitas Kristen Duta Wacana. Selain itu, pihak universitas memiliki kemampuan untuk mengurangi peluang terjadinya risiko tersebut.

Dari hal tersebut diatas, maka risiko yang ada dapat di identifikasi kemungkinan terjadinya melalui tabel III berikut ini:

TABEL 3. IDENTIFIKASI KEMUNGKINAN TERHADAP RISIKO YANG ADA

No	Risiko
1	Lokasi Fisik • Konstruksi bangunan (Rendah) • Akses (Rendah) • Pemadam Kebakaran (Rendah) • Power Supply (Sedang)
2	Sistem Operasi • *Logon* Procedure (Rendah) • Access Token (Rendah) • Access Control List (Rendah)
3	Keseluruhan Sistem • Hak Akses (Tinggi) • *Password* (Tinggi) • Virus (Tinggi) • Electronic Audit Trail (Tinggi)

Tabel 3 diatas menunjukan identifikasi kemungkinan terjadinya risiko. Lokasi fisik rata-rata mempunyai risiko yang rendah terhadap bencana dan ancaman lain, konstruksi bangunan Universitas Kristen Duta Wacana sudah memenuhi arsitektur tahan gempa dan kokoh. Untuk akses ke lokasi pusat data tidak semua karyawan Universitas Kristen Duta Wacana dapat mengaksesnya dan hanya dibatasi untuk karyawan-karyawan yang bekerja pada unit pengembangan dan pemeliharaan sistem. Alat pemadam kebakaran dan AC sudah tersedia di dalam pusat data. Untuk daya listrik sering terjadi gangguan fluktuasi daya, sehingga didalam pusat data diperlukan sumber daya yang bersifat sementara seperti UPS yang hanya bertahan selama 10-15 menit.

Sistem operasi dan sistem keseluruhan mempunyai risiko rendah dan tinggi. Risiko dalam sistem operasi pusat data terjadinya rendah, hanya karyawan yang paham tentang teknologi informasi saja yang diijinkan mengakses sistem operasi pusat data.

Beberapa karyawan Universitas Kristen Duta Wacana yang diberikan hak akses terhadap aplikasi pusat data belum mempunyai pemahaman akan pentingnya hak akses dan *password* yang harus dijaga, banyak karyawan yang masih menggunakan *password* yang mudah ditebak oleh orang lain, seperti tanggal lahir atau ekstension nomor telpon unit kerjanya dan tidak secara periodik mengubah *password* tersebut. Begitu juga dengan virus, sangat tinggi terjadi untuk menyerang pusat data, karyawan ketika menerima email terkadang tidak memahami email apa yang diterima hanya asal di download dan dijalankan.

F. Analisa Dampak

Dari adanya ancaman dan kerentanan tersebut, dapat di lakukan analisa dampak dari masing – masing ancaman sebagai berikut:

TABEL 4. RISIKO DAN DAMPAK TERHADAP PUSAT DATA

Pusat data	Jenis Risiko	Dampak
Lokasi Fisik	Konstruksi Bangunan yang tidak kuat	Bangunan runtuh dan mengakibatkan kerusakan pusat data
	Akses ke ruang Pusat data	Pengambilan data, perusakan fisik perangkat keras pusat data
	Pemadam Kebakaran	Terjadinya kebakaran pusat data
	Power Supply	Melemahnya daya Fluktuasi daya dan frekuensi daya. Hal ini mengakibatkan media penyimpanan menjadi kurang reliabel.
Sistem Operasi	*Logon* Procedure	Individu yang memiliki hak akses menyalahgunakan hak istimewa yang dimiliki
	Access Token	Mengotak atik sistem operasi dengan tujuan akan merusak sistem keamanan operasi
	Access Control List	Individu yang memiliki hak akses menyalahgunakan hak istimewa yang dimiliki
Sistem Keseluruhan	Hak Akses	Individu yang memiliki hak istimewa mengakses data dan program melakukan pengcopyan data yang bersifat rahasia.
	Password	Penyalahgunaan *password* dari orang yang tidak berwenang
	Virus	Menggandakan /menyalin dirinya sendiri dan menyusup kedalam program atau dokumen Merusak/menghilang kan sistem, aplikasi dan file
	Electronic Audit Trail	Penyalahgunaan wewenang Akses yang tidak diotorisasi oleh pengguna

Dari Tabel 4 diatas dapat menunjukan risiko dan dampaknya terhadap pusat data , dimana di dalam pusat data tersebut terdapat data – data Universitas Kristen Duta Wacana yang bersifat rahasia dan mendukung kegiatan operasional universitas.

G. Penentuan Risiko

Hasil dari Tabel III identifikasi kemungkinan risiko pada pusat data, dapat dijadikan sebagai penentuan risiko. Penentuan risiko dibagi dalam 3 kategori tinggi, rendah dan sedang. Tinggi, sumber ancaman yang sangat merugikan organisasi. Kategori risiko tinggi dalam pusat data Universitas Kristen Duta Wacana, disebabkan dari internal Universitas Kristen Duta Wacana sendiri, pemahaman tentang teknologi informasi karyawan masih rendah, untuk itu diperlukan pelatihan-pelatihan teknologi informasi terhadap karyawan serta pemahaman akan ancaman yang bisa terjadi pada pusat data Universitas Kristen Duta Wacana apabila tidak dilakukan prosedur yang benar dalam mengakses pusat data.

Kategori sedang, memiliki potensi kerugian terhadap organisasi juga, tetapi masih dapat dilakukan pengendalian untuk menghambat ancaman yang akan timbul. Fluktuasi sumberdaya listrik yang sering terjadi dapat dicegah dengan memasang UPS dan genset dalam pusat data.

Kategori rendah, tidak terlalu memberikan kerugian terhadap pusat data Universitas Kristen Duta Wacana, pengendalian bisa dilakukan oleh unit pengembangan dan pemeliharaan Universitas Kristen Duta Wacana sendiri. Karyawan di unit ini sudah kompeten dalam bidang teknologi informasi dan sudah memahami risiko-risiko yang akan terjadi dan Universitas Kristen Duta Wacana juga mempunyai karyawan yang ahli dalam bidang konstruksi bangunan.

Kemungkinan risiko yang menentukan dapat diidentifikasi pada pusat data Universitas Kristen Duta Wacana sebagai berikut 1. *Password* dan virus memiliki tingkat kemungkinan risiko tinggi, 2. Sumber daya listrik memiliki tingkat kemungkinan risiko sedang, dan 3. Lokasi fisik dan sistem operasi memiliki tingkat kemungkinan risiko rendah.

H. Rekomendasi Pengendalian

Pengendalian risiko adalah bagian dari manajemen risiko yang melibatkan penerapan kebijakan, standar, prosedur perubahan fisik untuk menghilangkan atau mengurangi risiko yang kurang baik. Pengendalian Resiko memiliki tingkat keefektifan, kehandalan dan proteksi tertinggi di antara pengendalian lainnya. Dan pada urutan hierarki setelahnya, tingkat keefektifan, kehandalan dan proteksi menurun seperti diilustrasikan pada

TABEL 5. REKOMENDASI PENGENDALIAN

Pusat data	Jenis Risiko	Pengendalian
Lokasi Fisik	Konstruksi Bangunan	Konstruksi bangunan yang kokoh, dengan memperhatikan standar arsitektur bangunan, tahan api Bangunan ditempatkan pada area yang memperkecil bahaya. Saluran komunikasi dibawah tanah Jendela bangunan tidak terbuka. Sistem *filtration* udara harus ada dan mampu mengeluarkan debu, rayap dan serbuk-serbuk kotoran yang lain.
	Akses ke ruang Pusat data	Pintu masuk ke Pusat data dengan menggunakan: *keypad* atau s*wipe card*, akses monitor menggunakan CCTV` Para programmer dan analis menggunakan *sign-in logs* ketika

		membutuhkan akses untuk memperbaiki program.
	Pemadam Kebakaran	Alarm otomatis dan manual ditempatkan pada lokasi disekitas instalasi. Sistem deteksi harus bias mendeteksi asap, panas, dan gas yang mudah terbakar Sistem pemadam kebakaran otomatis mengeluarkan jenis *suppressant* yang sesuai lokasi Pusat data . Pintu keluar kebakaran diberi tanda yang jelas dan diberi penjelasan selama kebakaran.
	Power Supply	Peralatan yang digunakan untuk megendalikan masalah ini dengan menggunakan alat pengatur voltase, generator, dan baterai. Backup power supply memiliki kapasitas yang cukup untuk menjalankan komputer dan pengaturan suhu udara
Sistem Operasi	*Logon* Procedure	Pengguna akan diberikan ID dan *Password* yang berguna ketika memulai proses akan diberikan kotak dialog yang meminta ID dan *password* pengguna, yang akan dibandingkan ke database sah pengguna.
	Access Token	Sistem akan membandingkan mengenai infomasi pengguna, termasuk ID dan *password*, use grup dan hak istimewa yang diberikan oleh pengguna.
	Access Control List	Akses ke sumber daya sistem seperti direktori, file dan program dikendalikan oleh daftar pengendalian akses yang ditugaskan ke setiap sumberdaya
Sistem Keseluruhan	Hak Akses	Manajemen harus memastikan bahwa individu telah melakukan segala sesuatu yang merupakan tugasnya Meninjau ulang hak istimewa dari suatu pemilihan grup pengguna dan individu untuk menentukan jika hak akses mereka sesuai dengan diskripsi tugas dan posisi mereka
	Password	Sistem akan menunda akses, apabila pemakai memberikan *password* yang salah Prosedur untuk mengidentifikasi kelemahan pasword Penggantian *password* secara berkala
	Virus	Secara rutin melakukan scan virus komputer pada file server` Anti virus disetiap server yang selalu diperbaharui
	Electronic Audit Trail	Menyediakan audit trail log.

Dari Tabel 5 di atas, terdapat beberapa rekomendasi pengendalian yang dapat membantu dalam mengurangi peluang terjadinya risiko. Beberapa pengendalian yang ada.

I. Dokumentasi Hasil

Hasil dari penilaian risiko yang ada di dokumentasikan untuk mendapatkan manajemen risiko pusat data, khususnya bagi Universitas Kristen Duta Wacana. Manajemen risiko ini akan dapat digunakan sebagai acuan untuk membuat dokumen rencana pemulihan pasca bencana (*Disaster Recovery Planning*)

V. KESIMPULAN

Berdasarkan hasil paparan yang telah disampaikan, dapat disajikan manajemen risiko pusat data perguruan tinggi Universitas Kristen Duta Wacana diperoleh kesimpulan sebagai berikut:

1. Identifikasi ancaman yang bersumber dari alam, manusiadan lingkungan serta identifikasi kerentanan yang dikategorikan menjadi 4 bagian, yaitu konfigurasi perangkat keras, perangkat lunak dan aplikasi, kebijakan dan prosedur sistem informasi dan sumberdaya manusia.
2. Proses pengendalian terhadap risiko pusat data dirancang untuk mencegah dan mendeteksi ancaman terhadap pusat data serta menyiapkan rencana proses pemulihan bencana.
3. Hasil dari penentuan risiko, menunjukkan tingkat risiko tinggi pada pemakaian *password*, penyebaran virus yang dilakukan oleh karyawan, sehingga diperlukan pelatihan teknologi informasi dan pemahaman mengakses aplikasi dalam pusat sesui prosedur yang telah ditetapkan. Backup yang dilakukan juga mempunyai risiko yang tinggi, dengan menggunakan DVD yang sewaktu-waktu dapat hilang atau rusak.
4. Manajemen risiko dengan menggunakan kerangka kerja NIST 300-80 dapat digunakan sebagai acuan dan prosedur kerja dalam melakukan penilaian terhadap risiko.

Saran yang disampaikan dari kesimpulan diatas, sebagai berikut:

1. Pendokumentasian hasil pengendalian, penanganan risiko dan evaluasi risiko.
2. Membuat dokumen rencana pemulihan pasca bencana (*Disaster Recovery Planning*)

DAFTAR PUSTAKA

[1] Nugraha, Ucu (2016). Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST 800-300. Seminar Nasional Telekomunikasi dan Informatika (SELISIK) ISSN: 2503-2844.

[2] AS/NZS (2004). Risk Management Guidelines: Companion to AS/NZS 4360 : 2004. Sydney: Standards Australia Internasional.

[3] Krutz, R. L., & Vines, D. R. (2006). *The CISSP Preparation Guide - Mastering the Ten Domains of Computer Security.* CA: Wiley Computer Publishing Wiley & Sons, Inc.

[4] Jakaria, D. A., Dirgahayu, R. T., & Hendrik. (2013). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metode Octave Allegro. *Seminar Nasional Aplikasi Teknologi Informasi* (pp. E-37 - E-42). Yogyakarta: Universitas Islam Indonesia.

[5] Farber, D. (2008, January 31). *The State of IT Risk Management*. Retrieved from ZDNet: http://www.zdnet.com/article/the-state-of-it-risk-management.

[6] Oktaviani, I., Hapsara, M., & Luthfi, E. T. (2014). Analisis Risiko Implementasi TI Menggunakan COBIT 41 (Studi Kasus : STMIK DUTA BANGSA SURAKARTA). *Duta.com, 7*(1).

[7] Hopkin, P. (2010). *Fundamentals of Risk Management: Understanding, Evaluating, and Implementing Effective Risk Management.* London: Kogan Page.

[8] AIRMIC (2010). A Structured Approach to Enterprise Risk Management and the Requirement of ISO 31000. The Association of Insurance and Risk Managemers, London.

[9] Abisay, Nurhadi (2013). Manajemen Risiko Berbasis ISO 31000:2009. *Jurnal Teknik Industri*. Pp. 116-119.

[10] Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46.2009

[11] Gustini, Dian Wulandari, Sulisti Afriani. (2014). Analisis Manajemen Risiko Pada Kantor Pusat PT. Bank Bengkulu. *Ekombis Review, Vol. 2, No. 1, pp. 105-121*

[12] National Institute of Standard and Technology. (2002). Risk Management Guide for Information Technology.

[13] Bullock, Michael (2009). Evaluating Electronic data center Colocation Options: Expert Tips. http://www.datacenterscanada.com/pdf/CIO - Electronic data center Definition and Solutions.pdf

[14] Mardhani, 2016. Pusat Data untuk Pemerintahan. Departemen Ilmu Komputer dan Elektronika, F MIPA UGM 2016.