Analisa Tingkat Resiko Tata Kelola Teknologi Informasi Perguruan Tinggi Menggunakan Model Framework National Institute of Standards & Technology (NIST) Special Publication 800-30 dan *IT General Control Questionnaire* (ITGCQ) (Studi Kasus PTS. XYZ)

Susilo†
Program Studi Teknik Elektro Fakultas Teknik Universitas Kristen Indonesia Jakarta
E-mail : susilo.suwarno@uki.ac.id
Jl. Mayjen Sutoyo No. 2, Cawang, Jakarta Timur 13630

Abstract *- Information and Communication Technology (ICT) Governance is strongly associated with the successful of an organization's management especially about how to control physical assets, data and information were applied. In organizations, universities (Higher Education) Data and information is extremely important given the orientation of utilization is in the form of shared knowledge, through teaching and learning, research and community service (Tri Dharma). With a potential source of threats posed by humans (Human Threats), natural disasters (Natural Threats), and disruption of the environment (Environmental Threats) can interfere with the management of ICT colleges. NIST Framework Model is implemented by integrating the concept of Information Technology (IT) Risk Management through assessment risk mitigation strategies and recommendations to measure the probability of the threat and the level of impact on the institution. Then, through indepth interviews with ICT department/unit using IT General Control Questionnaire (ITGCQ) and also review operational documents to found risk analysis issues. Risk analysis results are summarized in the form of safeguard implementation plan to reduce the level of IT risk governance PTS. XYZ. More and more ICT management activities that do not have control, the higher the level of risk management of ICT.*
Keywords*: Information Technology Governance, NIST, IT Risk, SDLC, ITGCQ*

Abstrak - Tata Kelola Teknologi Informasi dan Komunikasi (TIK) sangat terkait dengan keberhasilan pengelolaan manajemen sebuah organisasi khususnya bagaimana pengendalian terhadap aset fisik, data dan informasi diterapkan. Dalam organisasi perguruan tinggi (*Higher Education*) data dan informasi adalah hal yang sangat penting mengingat orientasi pemanfaatannya adalah dalam bentuk berbagi pengetahuan (*knowledge sharing*), yaitu melalui kegiatan belajar-mengajar, penelitian serta pengabdian kepada masyarakat (Tri Dharma) termasuk ketersediaan pangkalan data. Dengan potensi sumber ancaman yang diakibatkan oleh manusia (*Human Threats*), bencana alam (*Natural Threats*), dan gangguan lingkungan (*Environmental Threats*) dapat mengganggu pengelolaan TIK perguruan tinggi. Model Framework NIST dengan cara mengintegrasikan konsep *IT Risk Management* melalui kegiatan penilaian (*assesment*) dan rekomendasi strategi mitigasi resiko dapat mengukur tingkat probabilitas ancaman serta tingkat dampaknya bagi institusi. Kemudian, melalui kegiatan wawancara mendalam dengan Pihak Pengelola TIK menggunakan dokumen *IT General Questionnaire* serta review dokumen operasional ditemukan hasil analisa resiko yang dirangkum dalam bentuk rencana penerapan perlindungan yang mampu mengurangi tingkat resiko tata kelola teknologi informasi PTS. XYZ. Semakin banyak kegiatan pengelolaan TIK yang belum memiliki pengendalian, maka semakin tinggi tingkat resiko pengelolaan TIK.
Kata Kunci : Tata Kelola, NIST, *IT Risk*, SDLC,ITGCQ

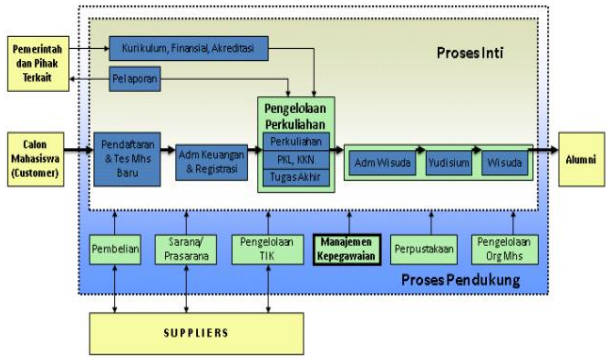
1. PENDAHULUAN

Dalam organisasi perguruan tinggi sangat dituntut tata kelola sistem informasi yang baik dan dapat meningkatkan kegiatan pelayanan pendidikan tinggi bagi masyarakat dan bangsa. Dengan demikian informasi-informasi dapat dikelola dan bermanfaat bagi pengambilan keputusan manajemen perguruan tinggi tersebut, dan disamping itu pengelolaan sistem informasi juga dapat memberikaan manfaat bagi *stakeholder*/sivitas akademika. Dalam kegiatan analisa resiko (*Risk Assesment*) khususnya teknologi informasi harus dapat mengevaluasi resiko yang kemungkinan timbul dalam tata kelola sistem informasi dan keberlangsungan operasional organisasi.

Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko. Pengembangan dan Pengelolaan Teknologi Informasi ini sangat penting untuk peningkatan kompetensi perguruan tinggi, terlebih lagi dengan perluasan akses bagi publik untuk mendapatkan pendidikan tinggi yang layak. Studi penelitian sebelumnya membahas berbagai pendekatan analisa tingkat resiko, namun yang perlu diketahui, tidak semua Perguruan tinggi di Indonesia terotomatisasi secara penuh (*Fully Automated System*) dalam kegiatan pelayanan pendidikan yang ada dengan penggunaan aplikasi sistem informasi. Dalam melakukan analisa

† Corresponding Author

tingkat resiko pada perguruan tinggi, perlu pemahaman bersama mengenai peta umum proses yang ada dalam



perguruan tinggi, khususnya di Indonesia. Peta Umum tersebut terbagi ke dalam Proses Inti dan Pendukung serta Eksternal sehingga sebenarnya menggambarkan garis besar penyelenggaraan kegiatan di perguruan tinggi.

Gambar 1. Peta Umum Proses PT (Lingkar Benua,Workshop Sistem Informasi Perguruan Tinggi, Jogjakarta, 2011)

2. METODE PENELITIAN

2.1 Pedoman NIST SP 800-30

Metodologi *NIST Special Publication 800-30* yang dipublikasikan oleh National Institute of Standard and Technology pada tahun 2002 adalah tentang *Risk Management Guide for Information Technology System*. NIST mampu mengintegrasikan analisis tingkat/level resiko ke setiap bagian siklus hidup pengembangan sistem (SDLC).

2.1.1 Risk Management dalam SDLC

Dalam Pengembangan dan Pengelolaan Sistem Informasi yang ideal secara umum menggunakan SDLC dimana tahapan yang ditempuh itu meliputi :

1. Inisialisasi Kebutuhan
2. Akuisisi dan Pengembangan
3. Implementasi
4. Operasi dan Pemeliharaan
5. Disposal

Kemudian untuk mengukur tingkat resiko yang kemungkinan akan timbul menurut rekomendasi dari NIST digunakan Metode *Risk Management*, adapun tahapan dari *Risk Management* tersebut, meliputi :

1. *Risk Assesment*
2. *Risk Mitigation*
3. *Evaluation and Assesment*
4. *Reporting*

Sehingga dengan demikian untuk menghasilkan rekomendasi yang baik dalam rangka tata kelola sistem informasi dintegrasikan antara Metode Risk Management dengan karakteristik tahapan dalam SDLC. Menurut NIST, ada perbandingan mendasar dari *Risk Management* dan *Risk Assesment*, dan dapat dilihat pada tabel 1.

Khusus pada tahapan identifikasi struktur organisasi perlu dibuat *key responsibilities matrix* bagi penanggung jawab tata kelola teknologi informasi di perguruan tinggi. Hal ini penting mengingat untuk mengukur sejauh mana keterlibatan para stake holder pengembangan sistem terhadap resiko yang kemungkinan timbul.

2.2 Ancaman (Threat) terhadap Sistem

Dalam mengelola sebuah sistem khususnya teknologi informasi, ancaman-ancaman baik yang datang dari luar maupun dalam perlu diantisipasi. Contohnya, bagaimana penyusup (*intruder)* menggunakan teknik dan perangkat lunak yang lebih canggih melakukan penetrasi terhadap jaringan komputer organisasi atau insititusi tertentu. Dalam tata kelola teknologi informasi di perguruan tinggi, memang data-data yang ada belum tergolong *high-classified* seperti data-data rahasia negara. Namun, bagaimanapun juga data-data dalam perguruan tinggi sangat berperan penting untuk peningkatan kompetensi perguruan tinggi. Bentuk ancaman-ancaman yang masuk dalam pertimbangan penilaian resiko, meliputi : *Accidental Disclosure*, kondisi alam, penambahan perangkat lunak, penggunaan bandwith, interferensi listrik, *intentional alteration of data*, kesalahan konfigurasi sistem, dan kegagalan operasi jaringan.

2.3 Penilaian Resiko (*Risk Assesment*)

Dalam melakukan penilaian resiko bagi tata kelola teknologi informasi, format standard sudah ada, namun disesuaikan dengan kondisi yang ada di perguruan tinggi yang bersangkutan. Secara garis besar tahapan yang dalam metodologi Risk Assesment meliputi :

1. Karakterisasi Sistem (*System Characterization*)
2. Identifikasi Ancaman (*Threat Identification*)
3. Identifikasi Kerentanan (*Vulnerability Identification*)
4. Analisa Pengendalian (*Control Analysis*)
5. Penentuan Kemungkinan (*Likelihood*)
6. Analisa Dampak (*Impact Analysis*)
7. Penentuan Resiko (*Risk Determination*)
8. Rekomendasi Pengendalian (*Control Recommendations*)
9. Dokumentasi Hasil Kegiatan (*Results Recomendation*)

2.3.1 Penentuan Kemungkinan (*Likelihood*)

Pemberian rating *Likelihood* menggambarkan probabilitas dari kelemahan sistem (*vulnerability*) yang dapat terjadi. *Rating Level Likelihood* dapat didefinisikan pada Tabel 1 sebagai berikut :

Tabel 1. Definisi Tingkat Kemungkinan

Tingkat Kemungkinan	Definisi Kemungkinan
High	Tingkat/Motivasi Ancaman sangat tinggi dimana pengendalian terhadap

	kemungkinan kelemahan sistem tidak dapat diatasi/tidak efektif
Medium	Tingkat/Motivasi Ancaman cukup tinggi, pengendalian terhadap beberapa kelemahan sistem masih belum dapat diatasi
Low	Tingkat ancaman sangat rendah, dimana pengendalian kelemahan sistem secara umum dapat diatasi.

2.3.2 Analisa Dampak (*Impact Analysis*)

Pengukuran ini dilakukan akibat dampak yang ditimbulkan dari sumber ancaman (*Threat-Source*) yang mengeksploitasi kelemahan sistem khususnya terhadap keberadaan sistem dan data penting bagi organisasi. Konsekuensi yang kemungkinan timbul dari ancaman ini antara lain : modifikasi data secara ilegal, data rahasia menjadi tidak terproteksi sehingga informasi yang diolah dari data tersebut menjadi tidak valid. Kekuatan dampak tersebut dapat diukur dengan pendefinisian pada Tabel 2 sebagai berikut :

Tabel 2. Tingkat Dampak

Tingkat Dampak	Definisi Dampak
High	1) Dapat mengakibatkan kerugian yang sangat mahal dari banyak aset berwujud 2) Dapat menganggu misi dan reputasi organisasi 3) Dapat mengakibatkan kematian manusia atau luka berat
Medium	1) Dapat mengakibatkan kerugian dari banyak aset berwujud 2) Dapat menganggu misi dan reputasi organisasi 3) Dapat mengakibatkan luka ringan
Low	Dapat mengakibatkan kerugian dari beberapa aset berwujud

2.3.3 Matriks Tingkat Resiko (*Risk Level*)

Dengan menggunakan Matriks Tingkat Resiko akan menggambarkan kondisi resiko aktual bagaimana implementasi tata kelola di perguruan tinggi yang bersangkutan. Dan formulasi deskripsi level dapat dilihat pada Tabel 3 berikut :

Tabel 3. Risk Level Matrix 3 x 3 (R = L x I)

Threat Likelihood	*Impact*		
	Low (10)	*Medium* (50)	*High* (100)
High (1.0)	*Low* 10 x 1.0 = 10	*Medium* 50 x 1.0 = 50	*High* 100 x 1.0 = 100
Medium (0.5)	*Low* 10 x 0.5 = 5	*Medium* 50 x 0.5 = 25	*Medium* 100 x 0.5 = 50
Low (0.1)	*Low* 10 x 0.1 = 1	*Low* 50 x 0.1 = 5	*Low* 100 x 0.1 = 10

Ket. Skala resiko : High (>50 – 100), Medium (>10 – 50, Low (1-10) Dalam memberikan penilaian skor dampak (Impact) dari resiko didasarkan pada kriteria Tabel 4.

Tabel 4. Tingkat Resiko

Tingkat Resiko	Definisi Resiko
High	Sistem yang berjalan tetap beroperasi, namun tindakan perbaikan harus segera dilakukan.
Medium	Tindakan perbaikan dilakukan sesuai periode waktu yang direncanakan
Low	Tindakan perbaikan masih perlu dilakukan atau resiko tersebut masih bisa ditoleransi/diterima

2.3.4 Opsi Mitigasi Resiko (*Risk Mitigation*)

Mitigasi resiko merupakan metodologi sistematis yang digunakan oleh manajemen senior untuk mengurangi resiko melaksanakan misi organisasi. Langkah mitigasi resiko merupakan strategi untuk menghadapi resiko yang ada, dan opsi-opsi yang bisa dipilih terdiri dari 4 cara, antara lain :

1. Menerima Resiko (*Risk Asumption*)
2. Pencegahan Resiko (*Risk Avoidance*)
3. Membatasi level resiko (*Risk Limitation*)
4. Mentransfer Resiko (*Risk Transference*)

Proses Mitigasi Resiko merupakan proses kedua dari manajemen resiko dimana melibatkan proses memprioritaskan, mengevaluasi, dan menerapkan rekomendasi pengendalian pengurangan resiko dari proses penilaian resiko yang sebelumnya telah dilakukan.

2.4 Desain Penelitian

Desain penelitian dimaksudkan mengetahui dengan pasti informasi atas pengendalian resiko yang sudah ada dalam pengelolaan teknologi informasi dan komunikasi pada perguruan tinggi terkait, karena akan sangat mempengaruhi hasil analisa dampak dan tingkat resiko. Hasil Analisa Dampak dan tingkat resiko tersebut menjadi starting point dalam menentukan strategi mitigasi resiko yang akan direkomendasikan dan dijalankan pada organisasi pengelola perguruan tinggi, khususnya pada unit tata kelola teknologi informasi dan komunikasi.

Penjelasan Tahapan Desain Penelitian, dapat dijelaskan sebagai berikut :

1. **Perencanaan Kerja Penelitian** : Rencana kerja penelitian dibuat untuk memastikan bahwa penelitian memiliki tahapan/fase sehingga waktu yang diharapkan untuk menyelesaikan penelitian dapat dicapai.

2. **Karakterisasi Sistem** : Pada tahapan ini dilakukan Identifikasi profil organisasi pengelola teknologi informasi dilakukan untuk memastikan keberadaaan proses bisnis (*business process*), prosedur standard dan kebijakan terkait pengelolaan teknologi informasi dalam lingkungan perguruan tinggi bersangkutan. Identifikasi profil organisasi dibutuhkan untuk jenis-jenis kategori pengelolaan yang akan digunakan untuk penyusunan item penelitian resiko.
3. **Penyusunan Item Penilaian Resiko** : Berdasarkan identifikasi profil organisasi, maka item sumber ancaman, potensi kerentanan dan tindakan ancaman dapat disusun sesuai kategorisasi pengelolaan teknologi informasi
4. **Penilaian Resiko** : Masing-masing item penilaian resiko akan diberikan skor sesuai tingkat/level yang terjadi pada sistem yang telah berjalan serta potensi-potensi dan dampak resiko yang akan terjadi di masa yang akan datang.
5. **Identifikasi Opsi Mitigasi Resiko** : Resiko akan diurutkan mulai dari tingkat resiko yang paling tinggi (*High*) hingga yang paling rendah (Low) dan akan diprioritaskan penanganannya melalui pemilihan opsi mitigasi resiko yang akan direncanakan.
6. **Rekomendasi dan Penerapan Strategi Mitigasi Resiko** : Rekomendasi opsi mitigasi resiko yang disesuaikan dengan misi dan sasaran organisasi, dirumuskan dalam bentuk Rencana Penerapan Perlindungan (*Safeguard Implementation Plan*) sehingga tata kelola teknologi informasi perguruan tinggi XYZ menjadi semakin lebih baik, khususnya dalam mendukung kegiatan-kegiatan pengajaran, penelitian dan pengabdian masyarakat.
7. **Presentasi Penelitian** : sesuai hasil *assesment* maka rekomendasi dan penerapan strategi mitigasi resiko akan dipaparkan melalui rapat strategis, sehingga masalah penelitian dapat diketahui solusi pemecahannya.

2.5 Teknik Pengumpulan Data Penelitian

Dalam penelitian ini ada beberapa teknik pengumpulan data yang digunakan, antara lain : **a. Penyebaran Kuestioner**, teknik ini digunakan untuk mendapatkan informasi efesiensi dan efektivitas pelayanan teknologi informasi dari back-end user (technical) dan front-end user(non-technical).

b. ***Interview On-Site***, teknik ini digunakan untuk mendapatkan informasi bagaimana sistem beroperasi dan dikelola oleh personil teknologi informasi dan dimungkinkan adanya kegiatan evaluasi terhadap lingkungan fisik.

c. Review Dokumen, teknik ini digunakan untuk mendapatkan administrasi sistem dikelola dengan baik atau tidak termasuk kebijakan tertulis yang ada. Pada teknik ini juga dapat didapatkan pengendalian dan rencana pengamanan sistem teknologi informasi.

d. **Penggunaan *Automated-Scanning Tool***, teknik yang memudahkan mendapatkan informasi tentang informasi sistem secara cepat melalui kegiatan *penetration testing* dan hasil evaluasi terhadapnya.

2.6 Penetapan Strategi Mitigasi Resiko

Manajemen senior sebagai pemilik misi, dengan mengetahui resiko potensial dan rekomendasi pengendalian resiko menjadi dasar pengambilan keputusan kapan dan tindakan mitigasi resiko yang harus dilakukan.

3. PEMBAHASAN

3.1 Karakterisasi Sistem

Proses awal pengukuran resiko dimulai dari mengidentifikasi keberadaan sistem teknologi informasi dan aset-aset yang ada didalamnya, karena orientasi pengenalan sistem sangat diperlukan untuk memastikan pengukuran resiko dilakukan sesuai dengan tujuan dan misi dari sistem teknologi informasi. Salah satu instrument penting dalam pengawasan dan pengendalian manajemen atas aset milik organisasi, adalah dengan diselenggarakannya pencatatan tersruktur yang berkesinambungan dan laporan secara periodik (bulanan/tahunan) tentang keberadaan maupun perubahan aset (barang-barang atau peralatan) yang dioperasikan. Sistem administrasi yang demikian adalah sangat penting dalam pengelolaan sistem informasi terutama karena mobilitasnya yang tinggi serta kemajuan teknologi informasi yang sangat pesat. Identifikasi karakterisasi sistem, dibagi ke dalam 2 (dua) kategori penting, yaitu :

1. Profil organisasi pengelola TIK : Struktur, Kebijakan, Standard, Dokumen Operasional.
2. Aset Teknologi Informasi : hardware, software/aplikasi, pengguna sistem.

3.2 Identifikasi Ancaman (*Threat*)

Identifikasi sumber ancaman PTS XYZ akan dibagi ke dalam 3 kategori, yaitu : kondisi alam, kondisi Manusia, dan kondisi Lingkungan. Kemudian, untuk menggambarkan alasan/motivasi dan tindakan ancaman yang kemungkinan terjadi disajikan tabel 5. Pada tabel tersebut di bawah ini yang diidentifikasi sebagai potensi dan sumber ancaman yang ada karena dinamika perkembangan organisasi.

Tabel 5. Sumber Ancaman Manusia, Motivasi & Tindakan

Sumber Ancaman	Motivasi	Tindakan
Hacker, Cracker	Tantangan Ego Memberontak	Hacking Social engineering Gangguan sistem Akses terhadap sistem
Kriminal	Perusakan Informasi Penyingkapan informasi secara	Tindak Kriminal Perbuatan Curang

	ilegal Keuntungan moneter Merubah data	Penyuapan Spoofing Intrusi atas Sistem

Sumber Ancaman	Tindakan
Power Failure	Gangguan sistem
Kebakaran	Gangguan sistem
Kerusuhan	Gangguan sistem
Sistem Pendingin	Gangguan sistem
Kondisi Bangunan/Ruangan	Gangguan sistem

Teroris	Surat kaleng (*Blackmail*) Perusakan Peledakan Balas dendam	Bom/teror Perang informasi Penyerangan sistem Penembusan atas sistem Gangguan sistem
Mata-mata	Persaingan usaha Mata-mata ekonomi	Pencurian informasi Social engineering Penembusan atas sistem
Orang dalam Organsiasi	Keingintahuan Ego Mata-mata Balas dendam Kelalaian kerja	Surat kaleng (*Blackmail*) Sabotase atas sistem Bug sistem Pencurian/Penipuan Perubahan data Malicious Code (malware) Penyalahgunaan komputer

Sumber ancaman manusia pada tabel tersebut di atas, merupakan gambaran yang didapat dari hasil analisa terhadap network operasional report selama 3 (tiga) tahun terakhir juga berdasarkan hasil assesment terhadap back-end user dan dalam hal ini adalah pada unit network operation center PTS. XYZ.

Banjir	Gangguan sistem
Gempa Bumi	Gangguan sistem
Badai, Angin Ribut	Gangguan sistem
Kilat/Petir	Gangguan sistem

Selain daripada itu, sumber ancaman lain juga disebabkan oleh kondisi geografis sistem itu ditempatkan, dan secara umum sumber ancaman alam yang bisa menggangu keberlangsungan operasi sistem dapat dilihat pada Tabel 6.

Tabel 6. Ancaman Alam

Ancaman dari kondisi alam dalam skala yang massive dan besar juga bisa menyebabkan gangguan operasional sistem, beberapa infrastuktur jaringan universitas ada yang dikonfigurasi mulai dari didalam tanah sampai dengan di atas bangunan, oleh karena 4 (empat) potensi sumber ancaman, menjadi pertimbangan resiko yang harus dianalisa dampaknya bagi keberlangsungan sistem.

Tabel 7. Ancaman Lingkungan

Kondisi fisik dari fasilitas teknologi informasi mulai dari cabling sampai pada ruang data center harus bisa diantisipasi resiko yang akan dan mungkin timbul pada saat yang akan datang terutama dari ancaman lingkungan di sekitar lokasi fasilitas teknologi informasi universitas. Dengan mengetahui potensi sumber ancaman tersebut bisa menyebabkan ekploitasi terhadap sistem karena dapat diketahui kerentanan/kelemahan sistem yang ada saat ini dan yang akan datang.

3.3 Identifikasi Kerentanan (Vulnerability)

Analisis terhadap potensi sumber ancaman juga harus diikuti dengan analisa terhadap kelemahan-kelemahan sistem, karena pada saatnya kelemahan-kelemahan ini akan menjadi pemicu tindakan (action) terhadap keberadaan sistem. Ada 2(dua) hal penting yang perlu dipertimbangkan dalam mengidentifikasi kerentanan/kelemahan sistem, yaitu : 1. Banyak sistem teknologi informasi memiliki lubang dan bug keamanan yang tidak diketahui, dan menggunakan password setting sistem yang kurang aman; 2. Banyak kerentanan pada sistem diakibatkan kesalahan konfigurasi oleh administrator system. Adapun kerentanan ini teridentifikasi berdasarkan dokumentasi laporan sistem yang sudah ada sebelumnya serta site visit lokasi data center dan pusat pengolahand datam pada setiap fakultas/biro/unit/lembaga, yaitu : - *Checklist Maintenance Data Center* - N*etwork Operational Reports* - *Operating System Event Viewer/Logs* - *Web Statistic Reports* - *Vulnerability Scanning Tool* untuk testing penetrasi jaringan Dengan hasil observasi tersebut, identifikasi potensi kelemahan diperoleh sebagai berikut :

Kerentanan/Kelemahan Sistem	Sumber Ancaman	Tindakan
akun user tidak aktif belum dihapus	Karyawan yang diberhentikan	Akses terhadap jaringan dan data penting organisasi.
Hot fixes, service packs, security Patch terbaru sistem operasi belum diupdate	Unauthorized user (Hacker, Karyawan tidak aktif, teroris, tindakan	Akses terhadap beberapa data sensitif akibat kelemaha

	kriminal)	n sistem yg ada
Data Center tidak menggunakan fire supression system (alarm, extinguisher)	Kebakaran, Kelalaian staf data center/yang diberi wewenang masuk ke ruang data center	Kebakaran terjadi dalam ruang data center
Data center tidak menggunakan pengatur suhu ruangan	Kelalaian staf data center/yang diberi wewenang masuk ke ruang data center	Gangguan terhadap hardware sistem (overheat)
Data Center tidak memiliki fasilitas backup power	Power Failure	Kerusakan terhadap hardware sistem
Data Center tidak memiliki fasilitas backup dan recovery file dan data	Kelalaian User menghilangkan data	Data Corrupted, Gangguan terhadap sistem pengolahan data
Koneksi Internet tidak memiliki proxy server backup	Power Failure	Gangguan terhadap sistem jaringan internet

3.4 Analisa Kontrol (*Control Analysis*)

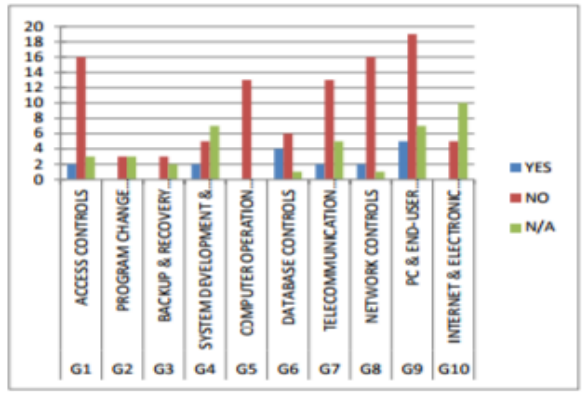
Analisis terhadap potensi sumber ancaman juga harus diikuti dengan analisa terhadap kelemahan-kelemahan sistem, karena pada saatnya kelemahan-kelemahan ini akan menjadi pemicu tindakan (action) terhadap keberadaan sistem. Ada 2(dua) hal penting yang perlu dipertimbangkan dalam mengidentifikasi kerentanan/kelemahan sistem, yaitu : Pengendalian dilakukan untuk meminimalisir atau bahkan mengeliminasi kemungkinan ancaman yang dapat mengeksploitasi kelemahan sistem. Metode pengendalian dibagi ke dalam dua bagian :

1. ***Technical Control***, yaitu meliputi gambaran tentang mekanisme kontrol akses, mekanisme authentikasi, metode enkripsi termasuk penggunaan perangkat lunak deteksi intrusi (*Intrusion Detection Software*).
2. ***Non-Technical Control***, yaitu kebijakan keamanan, prosedur operasional termasuk personal, aset fisik dan keamanan lingkungan.

Evaluasi umum terhadap pengendalian pengelolaaan teknologi informasi universitas XYZ disajikan melalui hasil *IT - General Control Questionnaire*.

Tabel 8. *IT General Control Questionnaire Summary*

CODE	CONTROL DESCRIPTION	YES	NO	N/A
G1	Access Controls	2	16	3
G2	Program Change Controls	0	3	3
G3	Backup& Recovery Controls	0	3	2
G4	System Development& Acquisition Controls	2	5	7
G5	Computer Operation Controls	0	13	0
G6	Database Controls	4	6	1
G7	Telecommunication Controls	2	13	5
G8	Network Controls	2	16	1
G9	PC & End-User Computing (EUC) Controls	5	19	7
G10	Internet& Electronic Commerce Controls	0	5	10
Total		17	99	39



Gambar 2. Grafik Pengendalian Sistem

Tabel 8. dan Gambar 2 di atas memberi gambaran item-item pengendalian sistem apa saja yang sudah diterapkan dan belum diterapkan untuk mendukung kebutuhan teknologi informasi pada PTS XYZ.

3.5 Penentuan Resiko (*Risk Determination*)

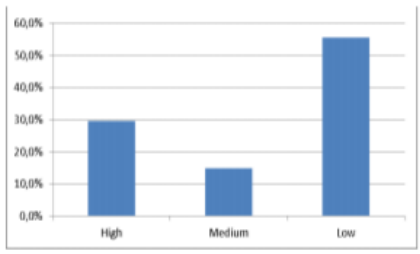
Tingkat resiko dapat dapat ditentukan melalui hasil pemberian skor dengan mengalikan nilai tingkat kemungkinan (L) dengan nilai tingkat dampak (I).Setelah pemetaan tingkat resiko diperoleh, maka dilakukan prioritas mulai dari tingkat tinggi (H) sampai dengan tingkat rendah (L).

Tabel 9. Tingkat Resiko

No.	Deskripsi Ancaman	Tingkat Resiko
1	Malware/Malicious Code	100 (High)
2	Human Error	100 (High)
3	Utilitas – Air	100 (High)
4	Utilitas – Listrik	100 (High)
5	Kebakaran	100 (High)
6	Kerusakan Aplikasi	100 (High)
7	Kerusakan Operasi Hardware	100 (High)
8	Kegagalan Dukungan Vendor	100 (High)
9	Konektivitas Jaringan	50 (Medium)
10	Kerusakan Perangkat Lunak Sistem	50 (Medium)
11	Demo Pekerja	50 (Medium)
12	Banjir	50 (Medium)
13	Terorisme – Senjata Biologis	10 (Low)
14	Terorisme – Senjata Kimia	10 (Low)
15	Terorisme – Radiologi	10 (Low)
16	Terorisme – Nuklir	10 (Low)
17	Terorisme – Ancaman Bom	10 (Low)
18	Kriminal – Pencurian Aset	10 (Low)
19	Kriminal – Perusakan Aset	10 (Low)
20	Kriminal – Vandalisme	10 (Low)
21	Kriminal – Spionase	10 (Low)
22	Kriminal – Penculikan	10 (Low)
23	Gempa Bumi	10 (Low)
24	Utilitas – Gas	5 (Low)
25	Utilitas – Comm. Link	5 (Low)
26	Badai/Angin Ribut	5 (Low)

Dengan melihat sajian data pada tabel 9, maka 8 (Delapan) item (29,6%) berskala resiko tinggi (*High*) menjadi prioritas utama untuk dilakukan segera rencana dan tindakan perbaikan walaupun sistem kemungkinan masih bisa berjalan, seperti terlihat pada gambar 3.

Kemudian, 4 (Empat) item (14,8%) berskala resiko sedang (*Medium*) menjadi prioritas selanjutnya, dimana rencana dan tindakan perbaikan dilakukan secara bertahap sesuai periode waktu perbaikan sistem yang direncanakan. Selanjutnya, 15 (Lima belas) item (55,6%) berskala resiko rendah (*Low*) merupakan prioritas lainnya yang harus diputuskan apakah masih dibutuhkan perbaikan atau menerima resiko tersebut.



Gambar 3. Prosentase Resiko

3.6 *IT General Control Questionnaire* (ITGCQ)

ITGCQ merupakan standar dalam memenuhi kegiatan audit untuk terlebih dahulu menginventarisir segala kebijakan, aturan dan sistem yang dimiliki oleh auditee dengan melakukan wawancara sekaligus melengkapi jawaban atas pernyataan yang telah terstruktur dalam suatu daftar questioner dengan tujuan untuk mengetahui apakah dalam pengelolaannya unit atau bagian tersebut sudah memiliki internal control yang memadai. Karena lemahnya internal control sangat memungkinkan terjadinya kerugian maupun kegagalan misinya suatu organisasi tanpa terdeteksi sebelumnya. Hal yang sama juga dapat terjadi pada setiap organisasi atau unit khususnya pengelola teknologi informasi.

Berdasarkan hasil jawaban atas 155 instrumen control yang terstruktur dalam *IT General Control Questionnaire* dimaksud ternyata hanya 17 items (11%) instrument control yang ada, sedang selebihnya 138 items (89%) tidak ada di pengelola teknologi informasi. Data tersebut menunjukkan bahwa pengelolaan teknologi informasi pada unit terkait adalah sangat lemah dan harus segera ditanggulangi.

3.7 Rekomendasi Pengendalian

Sesuai dengan materi kuestionaire pengendalian teknologi informasi, proses observasi sistem, dan hasil wawancara yang disesuaikan dengan metodologi tahapan pada NIST SP 800-30, maka pada tahapan-tahapan yang dilalui telah dihasilkan rekomendasi pengendalian sesuai dengan 8 (Delapan) Prioritas utama yang merupakan kegiatan utama pengelolaan teknologi informasi pada PTS. XYZ.

3.7.1 Kontrol Teknis (Technical Control)

a) Membuat dan Menerapkan kontrol sistem data center maintenance check-list;
b) Dengan banyaknya kegagalan sistem beroperasi menandakan buruknya kontrol terhadap data center dan sistem jaringan. Untuk itu diperlukan automatic network scanning tool & report system untuk membantu memonitoring dan memberikan alternatif solusi penanganan resiko sistem bagi administrator sistem atau pengguna yang ditugaskan menangani masalah tersebut;
c) Rotasi ataupun limitasi user yang mengakses ruang data center sebagai upaya untuk mengurangi akses langsung terhadap aset kritis data center;
d) Perencanaan dan Pengadaan Fire Supression System;
e) Perencanaan dan Pengadaan Monitoring CCTV System untuk mengantisipasi tindakan kriminal dan pengawasan asset teknologi informasi.

3.7.2 Kontrol Non Teknis

a) Penegasan Struktur Organisasi & Job Description tiap Unit/Bagian Pengelolaan Teknologi Informasi untuk memastikan bentuk pertanggungjawaban masing-masing pengelola dan pengguna sistem;
b) Pembuatan dan Implementasi S.O.P Teknologi Informasi untuk memastikan semua berjalan dengan baik dan tercatat secara administratif;

c) Perencanaan dan Pelaksanaan Training User dalam rangka pemanfaatan teknologi informasi yang benar dan tepat sasaran;
d) Pembuatan Rencana Strategis TIK termasuk *Disaster Recovery Plan*, sehingga bisa diketahui tahapan prioritas pengembangan dan pengelolaan sistem yang harus dilakukan termasuk evaluasi terhadapnya;

e) Perlu dibuat *IT Safeguard Implementation Plan* dalam rangka pengamanan aset teknologi informasi untuk jangka menengah dan jangka panjang, sehingga dapat mendukung rencana keberlanjutan usaha perguruan tinggi (*Business Continuity Plan*).

3.8 Perancangan Strategi Mitigasi Resiko

Keberhasilan pemilihan strategi mitigasi resiko yang efektif, dapat menurunkan tingkat resiko pengelolaan TIK Perguruan tinggi. Untuk itu, setelah pengukuran resiko dari setiap ancaman diperingkatkan khusus pada tingkat *high* sampai dengan tingkat *medium*, maka strategi mitigasi resiko dapat dipetakan dalam bentuk "*Safeguard Implementation Plan*" atau rencana penerapan perlindungan (tabel 10 dan tabel 11).

Tabel 10. Tingkat Resiko : Medium

No.	Deskripsi Ancaman	Tingkat Resiko	Opsi Mitigasi Resiko	Selected Planned Control	Responsible Person
1	Konektivitas Jaringan	50 (Medium)	Risk Avoidance	Sistem Network Backup Policy & Procedure	NS
2	Kerusakan Perangkat Lunak Sistem	50 (Medium)	Risk Avoidance	Sistem Backup Software Policy & Procedure	SS
3	Demo Pekerja	50 (Medium)	Risk Transfer	Replacement Table Chart	MTIK, SEKUN
4	Banjir	50 (Medium)	Risk Transfer	Disaster Recovery Plan	MTIK, SEKUN

Tabel 11. Tingkat Resiko : *High*

No.	Deskripsi Ancaman	Tingkat Resiko	Opsi Mitigasi Resiko	Selected Planned Control	Responsible Person
1	Malware/Malicious Code	100 (High)	Risk Avoidance	Security Policy & Procedure	NS Manager
2	Human Error	100 (High)	Risk Limitation	Training Policy & Procedure	EDP Manager
3	Utilitas – Air	100 (High)	Risk Avoidance	Data Center Facilities Maintenance Policy & Procedure	SEKUN
4	Utilitas – Listrik	100 (High)	Risk Avoidance	Data Center Facilities Maintenance Policy & Procedure	SEKUN
5	Kebakaran	100 (High)	Risk Avoidance	Data Center Facilities Maintenance Policy & Procedure	SEKUN
6	Kerusakan Aplikasi	100 (High)	Risk Avoidance	Sistem Backup Application Policy & Procedure	SS
7	Kegagalan Operasi Hardware	100 (High)	Risk Avoidance	Sistem Backup Hardware Policy & Procedure	TS
8	Kegagalan Dukungan Vendor	100 (High)	Risk Avoidance	Sistem 3rd Party Policy & Procedure	MTIK

4. KESIMPULAN & SARAN

4.1 Kesimpulan

Dari hasil evaluasi atas sistem dan metode kerja baik administratif maupun operasional dalam Sistem Teknologi Informasi Universitas yang dikelola, disimpulkan bahwa :

1) Hasil Pengukuran Resiko menggambarkan bahwa, tingkat resiko tata kelola teknologi informasi PTS XYZ berada pada level *High Risk*;
2) Strategi Resiko yang diterapkan mengacu pada rencana implementasi perlindungan, yaitu dengan menghindari resiko (*risk avoidance*).

4.2 Saran

1) Agar pimpinan universitas harus me-monitoring dan meng-evaluasi secara periodik terhadap penerapan safeguard implementation plan yang dilakukan oleh organisasi pengelola teknologi informasi supaya fungsi-fungsi di dalamnya dapat berperan secara maksimal, baik dari segi teknis maupun administratif sehingga fungsi supervisi, pengawasan dan pengendalian dapat berjalan sebagaimana mestinya;
2) Perlu dilakukan penelitian sejenis khususnya yang dimana pengukuran menggunakan Risk Level Matrix 5x5 dan melibatkan lebih banyak perguruan tinggi sebagai obyek penelitian.

DAFTAR PUSTAKA

[1] Stoneburner, Gary. 2002. *Risk Management Guide for Information Technology System*. USA:NIST Special Publication 800-30.

[2] Purwanto, Yudha. 2010. Audit Teknologi Informasi dengan COBIT 4.1 dan *IS Risk Assesment* (Studi Kasus Bagian Pengolahan Data PTS XYZ. Bali: Konferensi Nasional Sistem dan Informatika 2010.

[3] Firmansyah, Hendra Sandhi. 2010. Implementasi Framework Manajemen Resiko Penggunaan Teknologi Informasi Perbankan. Bandung: Seminar Munas Aptikom 2010.

[4] Nikolic, Bozo. Dimitrijevic, Ljiljana Ruzic. 2009. Risk Assesment of Information Technology Systems. The Higher Education Technical School of Professional Studie Issues In Informing Science and Technology Vol. 6 2009: Novi Sad, Serbia.

[5] Moeller, Robert R. 2005. *Brink's Modern Internal Auditing 6th Edition*. USA:John Wiley & Sons.

[6] Maulana, M. Mahreza. 2006. Pemodelan Framework Manajemen Resiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. Bandung : Prosiding Konferensi

Nasional Teknologi Informasi & Komunikasi untuk Indonesia.
[7] McGehee, Brad. 2009. *Brad's Sure Guide to SQL Server Maintenance Plans*. Simple Talk Publishing.
[8] Creswell, J. W. 1998. *Qualitatif Inquiry and Research Design*. Sage Publications, Inc: California.

UCAPAN TERIMA KASIH

[1] Bapak Dr. Iwan Krisnadi,MBA., sebagai pembimbing thesis Magister Teknik Elektro Universitas Mercu Buana Jakarta.
[2] Bapak Ir. Bambang Widodo, MT, selaku Ketua Program Studi Teknik Elektro Fakultas Teknik UKI.
[3] Bapak-Ibu Rekan-rekan Dosen Fakultas Teknik UKI.