ANALISIS KEAMANAN DAN MANAJEMEN RESIKO ASET INFORMASI PADA SISTEM INFORMASI AKADEMIK DI POLITEKNIK TEDC BANDUNG MENGGUNAKAN *FRAMEWORK NIST* SP 800-30

Shandy Tresnawati
Teknik Komputer, Politeknik TEDC Bandung
Email: shandy.tresnawati@gmail.com

Abstrak
Politeknik TEDC Bandung adalah sebuah politeknik swasta yang terletak di Jl. Pesantren KM 02 Cimahi. Merupakan Politeknik dengan 12 program studi dan memiliki mahasiswa sebanyak 1500 orang. Sistem informasi merupakan sebuah kebutuhan untuk institusi pendidikan seperti Politeknik TEDC Bandung karena di zaman globalisasi seperti sekarang ini pelayanan serta proses bisnis yang mumpuni menjadi keharusan ditengah persaingan bisnis dengan universitas lain. Sistem Informasi Akademik (Siakad) Politeknik TEDC Bandung, telah dipakai sejak tahun 2012 dan telah membantu serta menampung data-data seputar akademik, tingkat resiko pun bertambah seiring dengan berkembangnya sistem informasi akademik ini. Tercatat serangan virus dan kegagalan server yang paling mendominasi selama 3 tahun terakhir ini. Karena itulah analisis keamanan sistem untuk sistem informasi pun sangat diperlukan untuk dapat menjaga sistem dan data yang ada didalamnya agar mengetahui langkah-langkah mitigasi yang harus dilakukan saat ancaman atau resiko menyerang sistem. Analisis keamanan dan manajemen resiko ini menggunakan metode NIST SP 800-30 dengan tiga pendekatan utama yaitu *Risk Assessment* (Penilaian Resiko), *Risk Mitigation* (Mitigasi Resiko) dan *Evaluation Assesment* (Evaluasi).

Kata Kunci: NIST SP 800-30, manajemen resiko, sistem informasi akademik

Abstract
Polytechnic TEDC Bandung is a private polytechnic located in Pesantren Street KM 02 Cimahi. It is a Polytechnic with 12 study programs and has more than 1300 students. Information systems are a necessity for educational institutions such as Polytechnic TEDC Bandung because in this globalization era, service and business processes that are qualified to become a necessity in the midst of business competition with another universities. Academic Information System (Siakad) in Polytechnic TEDC Bandung has been used since 2012 and has helped and accommodated academic's data, it is mean the level of risk also increases along with the development of this academic information system. virus attacks and server failures have been dominated for almost past 3 years. Because of that, analysis of security system for information systems is very necessary to do to be able to maintain the system and data contained in it to know the mitigation steps that must be done when the threat or risk attacking the system. This security analysis and risk management uses the NIST SP 800-30 method with three main approaches: Risk Assessment, Risk Mitigation and Evaluation Assessment.

Keywords: *NIST SP 800-30, risk management, academic information system*

I. PENDAHULUAN

Peranan teknologi informasi dan komunikasi dalam dunia pendidikan juga sangat besar, khususnya dalam hal penunjang proses belajar-mengajar dan efisiensi pekerjaan akademik maupun administratif. Perguruan tinggi sebagai salah satu institusi pendidikan sudah selayaknya mampu untuk memanfaatkan teknologi informasi dan komunikasi dalam menunjang berbagai aktivitasnya. Politeknik TEDC Bandung sebagai salah satu Politeknik swasta di Indonesia sudah sejak lima tahun terakhir ini melakukan implementasi dan adaptasi teknologi informasi dan komunikasi. Sistem informasi akademik adalah salah satu sistem informasi yang sangat penting bagi Politeknik TEDC Bandung karena meliputi data-data penting bukan hanya ratusan bahkan ribuan mahasiswa serta memuat data-data dosen pengampu mata kuliah.

Menurut Peltier (2001:21), Risiko adalah seseorang atau sesuatu yang membuat atau menyarankan sebuah bahaya. Sedangkan menurut Alberts, Dorofee, Stevens and Woody (2001:43), *Risk is the possibility of suffering harm or loss*.

Menurut Djojosoedarso (2003:2), pengertian Risiko adalah suatu variasi dari hasil-hasil yang dapat terjadi selama periode tertentu.

Dari definisi tersebut dapat disimpulkan bahwa Risiko selalu dihubungkan dengan kemungkinan terjadinya sesuatu yang merugikan yang tidak diduga/tidak diinginkan. Kerugian tersebut sebenarnya merupakan bentuk ketidakpastian yang seharusnya dipahami dan dikelola secara efektif oleh organisasi sebagai bagian dari strategi sehingga dapat menjadi nilai tambah dan mendukung pencapaian tujuan organisasi. Secara garis besar Manajemen risiko dibentuk dengan memperhatikan dua hal lain yaitu gangguan ancaman (*threat*) serta konsekuensi (*consequences*), dan lebih dalam lagi ancaman dapat dijabarkan lagi menjadi beberapa komponen pembentuk ancaman.

II. LANDASAN TEORI

Menurut Alberts dan Dorefee (2004:8), manajemen risiko adalah proses yang berkelanjutan dalam mengenal risiko dan mengimplementasikan rencana untuk menunjukannya. Pendapat lain mengatakan, *Risk is the Likelihood that a threat will occur* (*Rainer, Turban, Potter*, 2007). Manajemen risiko secara umum didefinisikan sebagai proses, mengidentifikasi, mengukur dan memastikan risiko dan mengembangkan strategi untuk mengelola risiko tersebut.

Penentu resiko adalah metode untuk menilai tingkatan pengambilan resiko pada sistem Teknologi Informasi. Untuk mengukur resiko maka sebuah *risk* scale dan *Risk-Level Matrix* harus dikembangkan. Penentuan akhir dari misi resiko diperoleh dari perkalian antara tingkatan penilaian kemungkinan ancaman dan dampak dari ancaman. Berikut adalah *Risk Scale* dan *Risk Level Matrix* yang sesuai dengan metode NIST SP 300-80.

Tabel 1. *Risk-Level Matrix*

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

Risk Scale: *High* (>50 to 100): *Medium* (>10 to 50): *Low* (1 to 10)

Pada matrix diatas diperlihatkan bagaimana keseluruhan tingkat resiko untuk *High*, *Medium*, dan *Low* diperoleh. Penentuan dari tingkat resiko atau evaluasi ini bersifat subjektif. Dasar pemikiran untuk pertimbangan ini dapat dijelaskan dalam kaitannya dengan kemungkinan penilaian untuk setiap tingkatan kemungkinan ancaman dan penilaian evaluasi untuk setiap tingkatan dari dampaknya.

Tabel 2. *Risk Scale and Necessary Actions*

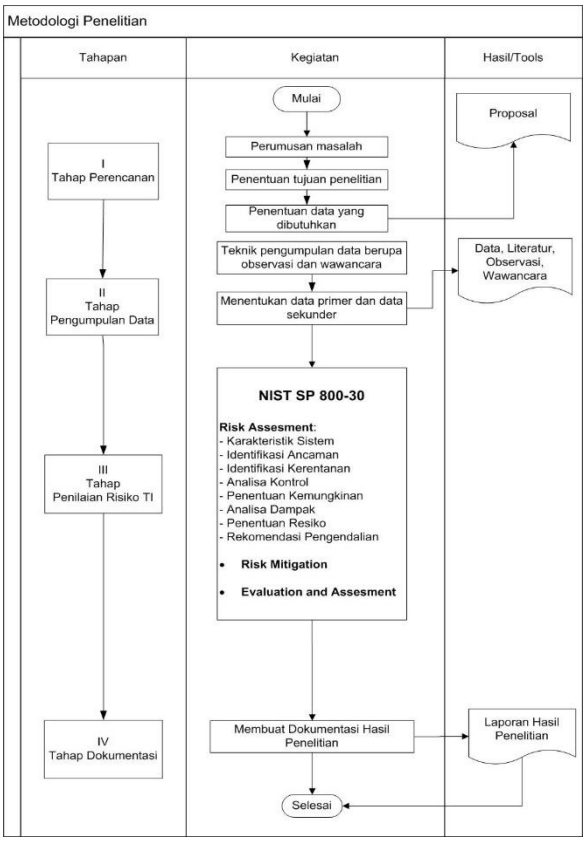
Risk Level	***Risk Description and Necessary Actions***
High	*If an observation or finding is evaluated as a High risk, there is a strong need for corrective measures. An existing system may continue to operate, but acorrective action plan must be put in place as soon as possible.*
Medium	*In an observation is rated as Medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.*
Low	*If an observation is described as Low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.*

Sumber: NIST SP 800-30

Skala resiko ini (skor *High*, *Medium*, dan *Low*) menguraikan tingkatan atau derajat resiko pada suatu sistem Teknologi Informasi, fasilitas atau prosedur dapat dijadikan arahan jika memberikan *vunerability.*

III. METODE PENELITIAN

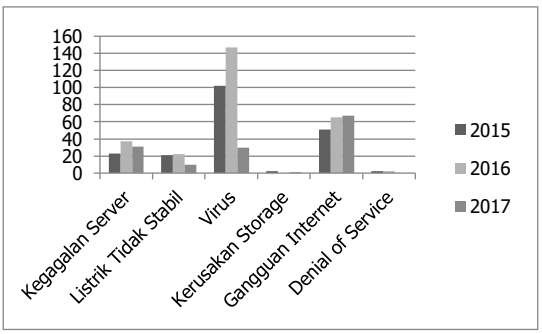
Metodologi utama yang digunakan dalam penelitian mengacu kepada metode NIST SP (National Institute of Standard Technology Special Publication) 800-30. NIST (*National Institute of Standard and Technology*) mengeluarkan rekomendasi melalui publikasi khusus 800-30 tentang *Risk Management Guide for Information Technology Sistem.* Berikut adalah metode keseluruhan untuk menentukan resiko system informasi akademik di Politeknik TEDC Bandung.



Gambar 1. Digram alir penelitian

IV. HASIL PEMBAHASAN

Sumber ancaman adalah keadaan atau peristiwa yang memiliki potensi untuk menyebabkan kerusakan pada sistem TI. Tujuan dari tahapan ini adalah mengidentifikasi ancaman yang mungkin masuk ke dalam sistem dan lingkungannya. Suatu *threat-source* digambarkan sebagai keadaan atau peristiwa yang pada umumnya berasal dari alam, manusia atau lingkungan. Pada grafik berikut terlihat kategori *event* atau kejadian terbesar dari tahun 2015 sampai Februari 2017 berupa serangan *virus* atau malware.



Gambar 2. Grafik kategori *event*

Berikut adalah resiko-resiko yang telah dan mungkin terjadi akibat adanya ancaman pada tahap identifikasi ancaman, besarnya resiko dan kontrol yang dilakukan saat ini. Adapun rekomendasi kontrol dilanjutkan pada proses mitigasi risiko, dimana prosedur dan teknis keamanan sebagai kontrol yang direkomendasikan akan dievaluasi, diprioritaskan, dan diimplementasikan. Hasil rekomendasi langkah pengamanan resiko pada Sistem Informasi Akademik Politeknik TEDC Bandung dapat dilihat sebagai berikut:

- **Resiko:** Kegagalan pada server, **Dampak**: Melambatnya *server*, *over capacity* menyebabkan *server* tidak dapat diakses, ***Risk Likelihood Rating:*** *High*, ***Risk Impact Rating:*** *High*, ***Overall Risk Rating:*** *High*, **Kontrol Saat Ini:** Mematikan *server* dan melakukan pengecekan secara keseluruhan, Memastikan semua kabel dalam keadaan yang baik dan dalam posisi yang benar, Memastikan *hardware* terutama hardisk dalam baik, **Rekomendasi:** Melakukan pengecekan system secara keseluruhan secara berkala, minimal 6 bulan sekali.
- **Resiko:** Ketidakstabilan Listrik, **Dampak:** Sistem mati total, ***Risk Likelihood Rating:*** *High*, ***Risk Impact Rating:*** *High*, ***Overall Risk Rating:*** *High*, **Kontrol Saat Ini:** Menghubungi pihak terkait (PLN), **Rekomendasi:** *Server* dan *workstation* di akademik harus dilengkapi dengan UPS (*Uninterruptible power supply*).
- **Resiko:** Data terinfeksi virus sehingga mengacaukan link dan data-data lainnya ketika di save, **Dampak:** Data *error*, tidak bisa diakses dan mengacaukan system, ***Risk Likelihood Rating:*** *High*, ***Risk Impact Rating:*** *Medium*, ***Overall Risk Rating:*** *Medium*, **Kontrol Saat Ini:** Melakukan estimasi terhadap pengaruh secara teknis, Mengidentifikasi sistem yang terinfeksi, Disinfeksi, mengkarantina, menghapus, dan mengganti *file* yang terinfeksi, Mengkonfirmasikan bahwa sistem yang terkena telah berfungsi normal, **Rekomendasi:** Pengecekan terhadap sistem secara berkala dan meng-*update antivirus* secara berkala.
- **Resiko:** *Denial of system.* **Dampak:** Sistem *crash*, tidak dapat diakses dan *server* lambat karena serangan *hacker*, ***Risk Likelihood Rating:*** *Low*, ***Risk Impact Rating:*** *High*, ***Overall Risk Rating:*** *Low*, **Kontrol Saat**

Ini: Melaporkan insiden kepada staf internal, Medokumentasikan bukti yang ada, Mengkonfirmasi bahwa sistem masih dapat berfungsi secara normal, Penanggulangan ancaman, Mendokumentaskan paska insiden, **Rekomendasi:** Melakukan analisis sistem secara keseluruhan secara bertahap agar segala sesuatu yang mencurigakan akan dapat terdeteksi sedini mungkin.

- **Resiko:** Kerusakan media *storage* dan *hardware,* **Dampak:** Rusak atau hilangnya sebagian atau seluruh data sensitif, ***Risk Likelihood Rating:*** Low, ***Risk Impact Rating:*** *High,* ***Overall Risk Rating:*** *Low*, **Kontrol Saat Ini:** Melakukan pemeriksaan secara berkala, **Rekomendasi:** Pengamanan terhadap *server* dan system.
- **Resiko:** Gangguan pada koneksi internet, **Dampak:** Sistem dan data di *server* tidak dapat diakses, ***Risk Likelihood Rating:*** *High,* ***Risk Impact Rating:*** *Medium,* ***Overall Risk Rating:*** *Medium,* **Kontrol Saat Ini:** Melakukan pemeriksaan jaringan secara berkala, Berkoordinasi dengan pihak *provider*, **Rekomendasi:** Memberikan pengarahan kepada karyawan secara berkala.
- **Resiko:** Bencana alam (Banjir, Longsor, Kebakaran), **Dampak:** Rusaknya infrastruktur Jaringan dan *hardware* pendukung, ***Risk Likelihood Rating:*** *Medium,* ***Risk Impact Rating:*** *High,* ***Overall Risk Rating:*** *High,* **Kontrol Saat Ini:** Tidak ada, **Rekomendasi:** Melakukan pemeriksaan dan peremajaan *hardware* secara berkala.
- **Resiko:** Bencana yang disengaja (Kebakaran, perusakan atau pencurian asset informasi yang dilakukan secara sengaja), **Dampak:** *Hardware* mengalami kerusakan secara total, kerusakan infrastruktur jaringan, hilangnya sebagian atau seluruh data sensitif, ***Risk Likelihood Rating:*** *High,* ***Risk Impact Rating:*** *High,* ***Overall Risk Rating:*** *High,* **Kontrol Saat Ini:** Kamera CCTV yang terpasang di beberapa titik, **Rekomendasi:** Melakukan pengecekan jaringan dan bekerjasama dengan pihak *provider*. Memperketat penjagaan, membatasi orang yang keluar masuk di area kampus.
- **Resiko:** Perusakan sistem dan pencurian data oleh *hacker*, **Dampak:** Sistem dan data pada *server* tidak dapat diakses, sistem mengalami kegagalan, ***Risk Likelihood Rating:*** *High,* ***Risk Impact Rating:*** *Medium,* ***Overall Risk Rating:*** *Medium,* **Kontrol Saat Ini:** *Firewall,* **Rekomendasi:** Meningkatkan keamanan *server*, membatasi keluar masuknya orang kedalam *server*.
- **Resiko:** Penyalahgunaan Data, **Dampak:** Informasi personal yang dapat disalahgunakan atau dapat merugikan *user* dan institusi. ***Risk Likelihood Rating:*** *High,* ***Risk Impact Rating:*** *Medium,* ***Overall Risk Rating:*** *Medium,* **Kontrol Saat Ini:** Tidak ada. **Rekomendasi:** Memberikan pengarahan kepada *user* tentang bahayanya penyalahgunaan data.
- **Resiko:** *Unauthorized user* (Pengguna yang tidak memiliki izin akses), **Dampak:** Bocornya informasi yang bersifat personal, ***Risk Likelihood Rating:*** *High,* ***Risk Impact Rating:*** *Low,* ***Overall Risk Rating:*** *Low,* **Kontrol Saat Ini:** Admin memberikan password untuk user yang diberikan izin akses, **Rekomendasi:** Memberikan pengarahan kepada semua pihak termasuk pemimpin politeknik tentang bahayanya penyalahgunaan data.
- **Resiko:** *Human error* (Kesalahan manusia), **Dampak:** Bocornya informasil, terhapusnya data secara tidak sengaja, masuknya virus atau *malware*, ***Risk Likelihood Rating:*** *High,* ***Risk Impact Rating:*** *Medium,* ***Overall Risk Rating:*** *Medium,* **Kontrol Saat Ini:** Memberikan pengarahan pada karyawan tentang penggunaan sistem yang benar, melakukan pengecekan system secara berkala, **Rekomendasi:** Memberikan pengarahan secara berkala terhadap karyawan terkait tentang tata cara penggunaan sistem yang baik.

V. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan terhadap aset informasi pada sistem informasi akademik di politeknik TEDC Bandung, maka dapat disimpulkan:

1. Telah dikelompokan antara resiko dan ancaman yang sudah terjadi (dari tahun 2015 sampai februari 2017) dan yang belum terjadi pada Sistem Informasi Akademik (Siakad) di Politeknik TEDC Bandung serta telah berhasil diukur resiko mana saja yang akan berdampak terhadap proses bisnis di politeknik TEDC Bandung. Virus dan kegagalan server menjadi dua hal yang sering terjadi dan membuat sistem terganggu.

2. Dari segi keamanan server dan komputer kerja (*workstation*) di unit akademik, pihak institusi hanya mengandalkan *antvirus*. Walaupun kasus *Denial of Service* (seseorang yang ingin membuat sistem *crash*/ lambat dengan cara mengirim *bug* dengan tujuan mengganggu lalu lintas data) atau yang ingin menyerang server hanya beberapa kali terjadi dalam 3 tahun terakhir ini, tetapi membuat pihak pengelola selalu waspada karena data yang ada di server meliputi data Akademik, Keuangan dan PDPT (Pangkalan Data Perguruan Tinggi) yang sangat penting untuk institusi pendidikan seperti Politeknik TEDC Bandung dalam menjalankan proses bisnisnya.
3. Dengan diadakannya penelitian ini, pihak pengelola merasakan betapa pentingnya membuat kebijakan-kebijakan formal dalam segi keamanan aset informasi di lingkungan Politeknik TEDC Bandung, sehingga selalu ada langkah-langkah solusi mitigasi terhadap resiko yang sedang dan yang akan terjadi.

DAFTAR PUSTAKA

Alberts, C., Dorofee, A., Stevens, J., Woody, C. (2005*). Crtitical Asset for Applications. U.S. Patent & Trademark Office by Carnegie Mellon University, U.S. Alter, Steven. Information Systems a Management Perspective.* Addison Wesley Longman, Inc, 1996.

Boyce and Jennings.(2002). *Information Assurance: Managing Organizational IT Security Risk*. Washington DC: Butterworth – Heinemann.

Kemenkominfo. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*

Nugraha, Ucu.(2015). *Manajemen Resiko Sistem Informasi pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-30*. Seminar Nasional Telekomunikasi dan Informasi.

Peltier, Thomas R.(2001). *Information Security Risk Analysis*. Auerbach/CRC Press Release, Washington D.C

Stoneburner Gary, Goguen Alice and Feringa Alexis, 2002, "*NIST Special Publication 800-30* "*Risk Management Guide for Information TechnologySystem",* NIST U.S.Department of Commerce, Gaithersburg.