Jurnal CoreIT, Vol.2, No.2, Desember 2016
ISSN: 2460-738X (Cetak)

Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)

Wenni Syafitri
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Lancang Kuning
Jl. Yos Sudarso KM. 8, Pekanbaru 28266
wenni20@gmail.com

***Abstrak* – Sistem informasi akademik Universitas XYZ merupakan terobosan terbaru dibidang pelayanan akademik. Sistem ini menyediakan berbagai informasi yang dibutuhkan oleh civitas akademika. Sehingga kebutuhan akan keberlangsungan sistem ini semakin penting. Permasalahan yang pernah ada di SI Akademik Universitas XYZ seperti berkaitan dengan celah kerawanan keamanan informasi. Jika permasalahan ini tidak dapat diperbaiki secara berkelanjutan, alhasil akan memberikan dampak ataupun risiko kepada keberlangsungan sistem ini, khusunya civitas akademika. Penelitian ini menggunakan NIST SP 800-30 sebagai metode yang digunakan untuk menyelesaikan permasalahan tersebut. Maka berdasarkan hasil penelitian yang telah dilakukan, Universitas xyz memiliki 1 tingkat risiko tinggi, 5 tingkat risiko sedang dan 52 tingkat risiko rendah.**

***Kata kunci – Keamanan Informasi, NIST SP 800-30 dan Peniliaian Risiko*.**

PENDAHULUAN

SI AKADEMIK Universitas XYZ atau system informasi Akademik Universitas XYZ merupakan terobosan terbaru dibidang pelayanan akademik. Sistem ini menyediakan berbagai informasi yang dibutuhkan oleh civitas akademika. Sehingga kebutuhan akan keberlangsungan system ini semakin penting.

Permasalahan yang pernah ada di SI Akademik Universitas XYZ seperti berkaitan dengan celah kerawanan keamanan informasi. Jika permasalahan ini tidak dapat diperbaiki secara berkelanjutan, alhasil akan memberikan dampak ataupun risiko kepada keberlangsungan sistem ini, khusunya civitas akademika. Berbagai upaya telah dilakukan pihak Universitas XYZ untuk melibatkan civitas akademika berpartisipasi demi kemajuan SI Akademik. Misalnya membuat grup untuk sosialisasi SI Akademik. Hal ini tentu saja masih kurang efektif demi menyelesaikan permasalahan diatas. Ruang server Universitas XYZ penah mengalami gangguan yang mengakibatkan rusaknya 3 server utama dan peralatan network lainnya. Petir tersebut meninggalkan bekas hangus pada rak *switch*, *mainboard* server dan peralatan lainnya [1].

Menurut [2], [3] dan [4], COBIT framework sebagai audit sistem informasi dan teknologi informasi masih bersifat umum seperti mengukur kematangan implementasi teknologi informasi. Sedangkan menurut [5], [6],[7], [8], [9] dan [10] manajemen risiko keamanan informasi dapat diterapkan sebagai pelindung teknologi informasi dari bahaya keamanan informasi, seperti virus, *hacker* ataupun pencurian data, menimbulkan ancaman besar terhadap asset dan reputasi perusahaan ataupun organisasi. Berdasarkan rekomendasi beberapa penelitian diatas untuk menyelesaikan permasalahan SI Akademik Universitas XYZ dibutuhkan manajemen risiko keamanan informasi.

Ada banyak metode yang dapat digunakan untuk melakukan manajemen risiko keamanan informasi seperti Octave, NIST SP 800-30 dan ISO 27001. Metode OCTAVE terdapat beberapa langkah pengerjaan yaitu persiapan, Identifikasi Aset (Berdasarkan identifikasi ancaman), identifikasi kerawanan infrastruktur dan membuat strategi dan perencanaan keamanan [8]. NIST SP-800-30 Memiliki 9 langkah untuk melakukan analisa risiko yaitu karakterisasi sistem, identifikasi ancaman, identifikasi kerawanan, analisa kontrol, analisa kecenderungan, analisa dampak, penentuan risiko, rekomendasi kontrol dan dokumentasi [10]. metode iso 27001 terdiri dari 4 langkah utama serta bersifat umum yaitu *Plan*, *Do*, *Check* dan *Act* [5].

Metode Octave hanya digunakan bagi organisasi (evaluasi organisasi) sedangkan ISO 27001 lebih cenderung mengarahkan kepada manajemen level tingkat atas. NIST SP 800-30 telah terbukti memberikan kontribusi yang lebih seperti: memberikan wawasan keamanan informasi yang sifatnya konsisten dan komprehensif bagi pengambil kebijakan, pemodelan sumber daya yang terstruktur, wawasan keamanan informasi dapat diterima oleh berbagai pengambil resiko, penentuan ancaman dapat diidentifikasi dengan

mudah, pengambil keputusan tidak ragu-ragu untuk mengambil resiko karena setiap resiko telah diselidiki dengan baik [10]. NIST SP 800-30 terbaik dari 3 metode untuk analisa resiko yaitu Mehari, Magerit dan Microsoft's Security Management Guide terutama pada saat melakukan analisa resiko, NIST SP 800-30 memberikan rekomendasi kontrol [11].

Penelitian ini akan menggunakan NIST SP 800-30 sebagai metode yang akan digunakan untuk menyelesaikan permasalahan yang telah disebutkan diatas. Maka, Berdasarkan latar belakang diatas ide penelitian yang akan diusulkan adalah Manajemen Risiko Keamanan Informasi Menggunakan Metode NIST SP 800-30 (Studi Kasus: SI Akademik Universitas XYZ).

BAHAN DAN METODE

A. Keamanan Informasi

Menurut ISO27002 (2005), keamanan informasi adalah melindungi informasi dari berbagai ancaman demi menjamin kelangsungan proses bisnis, meminimalisir risiko bisnis dan memaksimalkan laba investasi dan peluang bisnis. Keamanan informasi dapat dibentuk dengan cara menerapkan suatu set kontrol yang termasuk didalamnya kebijakan, proses, prosedur, struktur oganisasi serta fungsi dari perangkat lunak dan perangkat keras. Kontrol tersebut perlu ditetapkan, dilaksanakan, dipantau, dikaji ulang dan disempurnakan demi menjamin keamanan dan tercapainya tujuan bisnis organisasi.

Keamanan informasi juga didefinisikan sebagai perlidungan informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi atau pengrusakan [12]. Saat ini peran keamanan informasi telah menjadi lebih penting karena telah banyak orang, bisnis dan lembaga pemerintah menyimpan data dalam bentuk digital dengan menggunakan berbagai jenis teknologi.

United Stated National Information System Security mendefinisikan keamanan sistem informasi sebagai perlindungan sistem informasi terhadap akses yang tidak sah atau modifikasi informasi, baik yang terjadi saat penyimpanan, pemprosesan ataupun transit, penolakan layanan terhadap pengguna resmi atau pemberian layanan kepada pengguna yang tidak sah, juga termasuk tindakan-tindakan yang diperlukan untuk mendeteksi dan melawan ancaman tersebut [13].

B. Penilaian Risiko

Menurut Whitman dan Mattord (2006) dalam menggunakan sebuah *framework* manajemen risiko, ada beberapa hal yang harus diperhatikan:

a. Risiko dan dampak sebaiknya dipandang secara keseluruhan dari sudut pandang perspektif bisnis.
b. Risiko berpengaruh secara signifikan jika memiliki dampak terhadap bisnis.
c. *Framework* yang akan digunakan haruslah menyediakan bentuk dasar untuk melakukan evaluasi segala macam risiko, mulai dari insiden keamanan informasi yang besifat kecil hingga yang berpotensi bencana.

Menurut Jones dan Ashenden (2005) terdapat formula untuk mengukur risiko yaitu:

```
Risiko = Threat x Vulnerability x Impact
```

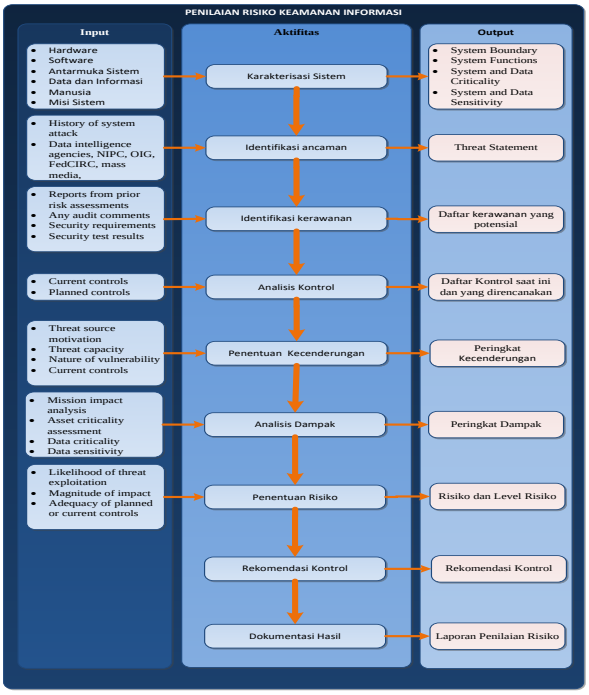
Maksud pernyataan dari formula diatas adalah *threat* akan melakukan eksploitasi *vulnerability* sehingga dapat menyebabkan *impact* terhadap sistem, sehingga menjadikan hal tersebut sebagai risiko terhadap organisasi. Oleh karena itu jika tidak ditemukan *threat*, *vulnerability* dan *impact* maka tidak terdapat risiko.

NIST 800-30 adalah dokumen standar yang dikembangkan oleh *National Institute of Standards and Technology* yang mana merupakan kelanjutan dari tanggung jawab hukum di bawah undang-undang *Computer Security Act* tahun 1987 dan *the Information Technology Management Reform Act* tahun 1996. NIST 800-30 terdapat dua tahap penting yaitu penilaian risiko dan mitigasi risiko. Tahapan penilaian risiko berdasarkan NIST 800-30 yaitu (Syalim, Hori, dan Sakurai, 2009):

1. *System Characterization*
   Pada tahapan ini, batas-batas dari sistem TI harus diidentifikasi, termasuk didalamnya sumber daya dan informasi.
2. *Threat Identification*
   Pertimbangan atas kemungkinan untuk muncul ancaman seperti sumber, potensi kerawanan dan kontrol yang ada.
3. *Vulnerability Identification*
   Identifikasi terhadap kerawanan digunakan untuk pengembangan dari daftar kerawanan sistem yang dapat dimanfaatkan nantinya.
4. *Control Analysis*
   Analisis terhadap kontrol yang telah dilaksanakan atau direncanakan untuk implementasi oleh organisasi untuk minimalisir atau menghilangkan kemungkinan-kemungkinan pengembangan dari ancaman.
5. *Likelihood Determination*
   Proses rangking terhadap potensi dari kerawanandapat dilaksanakan dalam lingkungan dari kerawanan tersebut. Faktor

yang menjadi pertimbangan adalah ancaman (sumber dan kemampuan), sifat dari kerawanan serta keberadaan dan efektifitas kontrol jika diterapkan.

6. *Impact Analysis*
   Tahapan ini digunakan untuk menentukan dampak negatif yang dihasilkan dari keberhasilan penerapan kerawanan.
7. *Risk Determination*
   Penilaian tingkat risiko pada sistem IT dilakukan pada langkah ini.
8. *Control Recommendations*
   Tahapan ini menilai kontrol yang mana dapat mengurangi atau menghilangkan risiko yang telah teridentifikasi. kontrol yang direkomendasikan sebaiknya harus dapat mengurangi tingkat risiko pada sistem IT dan data, kepada tingkat risiko yang dapat diterima.
9. *Results Documentation*
   Pada tahap ini, dilakukan pengembangan laporan hasil penilaian risiko (sumber ancaman, kerawanan, risiko *yang* dinilai dan kontrol yang direkomendasikan).



Gambar 1. Penilaian Risiko NIST SP 800-30

ANALISA RESIKO

A. *System Characterization*

Server SI Akademik telah berpindah dari Universitas XYZ ke provider internet sejak 3 bulan yang lalu. Pihak provider hanya bertanggung jawab terhadap ketersediaan layanan, misalnya listrik dan internet. Sehingga perbaikan ataupun *maintenaince* diserahkan sepenuhnya oleh Universitas XYZ. Salah satu contohnya yaitu melakukan akses secara remote ke dalam server untuk melakukan backup database. Backup tersebut dilakukan secara berkala minimal 1 bulan sekali, kemudian hasil backup tersebut dipindahkan ke DVD.

B. *Threat Identification*

Identifikasi terhadap ancaman pada Universitas XYZ dapat dilihat pada **Tabel 1**.

Tabel 1. Identifikasi ancaman pada Universitas XYZ

No	Sumber Ancaman	Jenis Ancaman
1	Individu di luar organisasi	*Information Disclosure, Blind SQL Injection, Denial Of Service, CSRF, Session fixation, cookie disclosure, Clickjacking, Spam, Network and Port Scanning, Network Sniffing, malware, Virus* dan *Social Engineering*
2	Individu di dalam organisasi (pegawai, dosen, mahasiswa)	*Information Disclosure, Blind SQL Injection, Denial Of Service, CSRF, Session fixation, cookie disclosure, Clickjacking, Spam, Network and Port Scanning, Network Sniffing, malware, Virus dan Social Engineering*
3	Perlengkapan TI (media penyimpanan pada server)	Gagal fungsi media penyimpanan, seperti : *disk error* atau *disk full*.
4	Perlengkapan TI (jaringan komunikasi data)	Gagal melakukan komunikasi dikarenakan terdapat Serangan *Wireless Jamming, Flood/collusion,* perusakan secara langsung perangkat atau jalur komunikasi data.
5	Pemprosesan data sistem informasi	Kegagalan sistem informasi
6	Kebakaran	Sistem mati, data hilang dan infrastruktur IT rusak

No	Sumber Ancaman	Jenis Ancaman
7	Gempa bumi	Sistem mati, data hilang dan infrastruktur IT rusak
8	Banjir	Sistem mati, data hilang dan infrastruktur IT rusak
9	Hubungan arus pendek Listrik	Sistem mati dan data hilang

C. Vulnerability Identification

Identifikasi terhadap celah kerawanan pada SI Akademik Universitas XYZ menggunakan tools penetration testing Acunetix dan tool assessment NIST SP 800-26. Hasil identifikasi celah kerawanan oleh Acunetix adalah sebanyak 7 celah kerawanan dikategorikan tinggi dan sedang, serta sebanyak 17 kerawanan dan 28 kerawanan dikategorikan rendah dah informasi. Berdasarkan hasil tersebut Acunetix menilai bahwa Celah kerawanan SIAkademik Universitas XYZ berada pada level 3 (HIGH).

Hasil assessment menggunakan tool NIST SP 800-26 berdasarkan *system characterization*, yaitu hanya sebatas akses secara logic tidak secara fisikal. Hal ini dikarenakan server dari SI Akademik berada pihak ketiga. Tools NIST SP 800-26 terdiri atas 17 kriteria assessment dan masing-masing kriteria memiliki subkriteria yang berbeda pula. Adapun kriteria yang dipenuhi oleh Sistem Informasi Universitas XYZ dapat dilihat pada **Tabel 2**. Berdasarkan tabel tersebut dari 17 kriteria hanya 10 kriteria yang dapat terpenuhi namun tidak semua sub kriteria yang terpenuhi secara maksimal.

Tabel 2. Kriteria *vulnerability* yang terpenuhi

No	Kriteria NIST SP 800-26	Kode Sub Kriteria NIST SP 800-26
1	*Risk Management*	1.1,1.1.1,1.1.2,1.1.3,1.1.4 dan 1.2, 1.2.2,1.2.3
2	*Review of security controls*	2.1.1,2.1.2 dam 2.1.3
7	*Physical & Environment Protection*	7.1.7, 7.1.10, 7.1.12, 7.1.13, 7.1.14, 7.1.16, 7.1.18, 7.2.2, 7.3.1
8	*Production, In-Out Controls*	8.1.1, 8.2, 8.2.2, 8.2.4, 8.2.9, 8.2.10
9	*Contingency Planning*	9.1.1 dan 9.2.6
10	*Hardware and System*	10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.2.1,
	Software Maintenance	10.2.2, 10.2.3, 10.2.9, 10.2.11, 10.3.1
11	*Data Integrity*	11.1, 11.1.1 dan 11.1.2
12	*Documentation*	12.1.4, 12.1.5, 12.1.8, 12.2.1
14	*Incident Response Capability*	14.1.1, 14.1.2, 14.1.3, 14.1.6, 14.2.1
16	*Logical Access Control*	16.1.2, 16.1.3, 16.1.5, 16.2.2, 16.2.4, 16.2.5, 16.2.8, 16.2.9, 16.2.10, 16.2.12

D. Control Analysis

Pada tahapan ini, system informasi universitas XYZ memiliki control analysis yang dieksekusi oleh pihak ketiga atau vendor. Sehingga akses ke sistem informasi akademik lebih terbatas.

E. Likelihood Determination

Penentuan likelihood pada penelitian ini dapat dilihat pada **Tabel 3**.

Tabel 3. Tingkat Likelihood

Tingkat Likelihood	
Tidak Pernah	LOW (1)
Sekali Setahun	MEDIUM (2)
Sekali Seminggu atau lebih sering	HIGH (3)

F. Impact Analysis

Penentuan Impact pada penelitian ini dapat dilihat pada **Tabel 4**.

Tabel 4. Tingkat Impact

Tingkat Impact	
Dampak tidak berpengaruh terhadap organisasi	LOW (1)
Memiliki pengaruh besar namun organisasi tidak terancam	MEDIUM (2)
Memberikan pengaruh yang besar terhadap organisasi	HIGH (3)

G. Risk Determination

Penentuan Impact pada penelitian ini dapat dilihat pada **Tabel 5**.

Tabel 5. Risk Determination

	Dampak		
Likelihood	***Rendah***	***Sedang***	***Tinggi***
Tinggi	Low	Medium	Tinggi
Sedang	Low	Medium	Medium
Rendah	Low	Low	Low

Tabel 6 merupakan hasil dokumentasi penilaian risiko berbasis keamanan informasi pada universitas xyz.

Tabel 6. Risk Documentation

No	Kode Kontrol Objectif	Likelihood	Impact	Risk
1	7.1.18	3	3	Tinggi
2	7.1.12	2	3	Sedang
3	7.1.13	2	3	Sedang
4	7.1.14	2	3	Sedang
5	7.1.16	2	3	Sedang
6	10.2.9	2	3	Sedang
7	1.1	1	2	Rendah
8	1.1.1	1	2	Rendah
9	1.1.3	1	1	Rendah
10	1.1.4	3	1	Rendah
11	1.2	3	1	Rendah
12	1.2.2	3	1	Rendah
13	1.2.3	1	1	Rendah
14	2.1.1	2	1	Rendah
15	2.1.2	2	1	Rendah
16	2.1.3	2	1	Rendah
17	7.1.7	2	1	Rendah
18	7.1.10	2	1	Rendah
19	7.2.2	3	1	Rendah
20	7.3.1	3	1	Rendah
21	8.1.1	2	1	Rendah
22	8.2	2	1	Rendah
23	8.2.2	2	1	Rendah
24	8.2.4	2	1	Rendah
25	8.2.9	2	1	Rendah
26	8.2.10	2	1	Rendah
27	9.1.1	2	1	Rendah
28	10.1.1	2	1	Rendah
29	10.1.2	2	1	Rendah
30	10.1.3	2	1	Rendah
31	10.1.4	2	1	Rendah
32	10.1.5	2	1	Rendah
33	10.2.1	2	1	Rendah
34	10.2.2	2	1	Rendah
35	10.2.3	2	1	Rendah
36	10.2.11	1	3	Rendah
37	10.3.1	1	1	Rendah
38	11.1.1	3	1	Rendah
39	11.1.2	3	1	Rendah
40	12.1.4	2	1	Rendah
41	12.1.5	2	1	Rendah
42	12.1.9	3	1	Rendah
43	12.2.1	1	1	Rendah
44	14.1.1	1	1	Rendah
45	14.1.2	1	1	Rendah
46	14.1.3	1	1	Rendah
47	14.1.6	1	1	Rendah
48	14.2.1	1	1	Rendah
49	16.1.2	1	1	Rendah
50	16.1.3	2	1	Rendah
51	16.1.5	1	1	Rendah
52	16.2.2	1	1	Rendah
53	16.2.4	3	1	Rendah
54	16.2.5	2	1	Rendah
55	16.2.8	1	1	Rendah
56	16.2.9	3	1	Rendah
57	16.2.10	3	1	Rendah
58	16.2.12	1	1	Rendah

KESIMPULAN

Berdasarkan hasil penilaian risiko berbasis keamanan informasi, universitas xyz memiliki 1 tingkat risiko tinggi, 5 tingkat risiko sedang dan 52 tingkat risiko rendah.

REFERENSI

[1] D. Setiawan och M. P. Halilintar, ”Analisis Gangguan Sambaran Petir Terhadap Kerusakan Perangkat IT Pusat Komputer Universitas Lancang Kuning Menggunakan Metode Collection Volume,” Pekanbaru, 2015.

[2] T. Iskandar och I. Hermadi, ”Audit Proses Perencanaan dan Implementasi Sistem Informasi PT Bank XYZ, Tbk dengan Menggunakan Cobit Framework,” Jurnal Aplikasi Manajemen (JAM), vol. 12, nr 14, pp. 572-581, 2014.

[3] A. Setiawan, ”EVALUASI PENERAPAN TEKNOLOGI INFORMASI DI PERGURUAN TINGGI SWASTA YOGYAKARTA DENGAN MENGGUNAKAN MODEL COBIT FRAMEWORK,” Seminar Nasional Aplikasi Teknologi Informasi (SNATI), pp. A15-A20, 2008.

[4] D. Fitrianah och Y. G. Sucahyo, ”AUDIT SISTEM INFORMASI/TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA COBIT UNTUK EVALUASI MANAJEMEN TEKNOLOGI INFORMASI DI UNIVERSITAS XYZ,” Jurnal Sistem Informasi MTI-UI, vol. 4, nr 1, pp. 37-46.

[5] M. Utomo, A. H. N. Ali och I. Affandi, ”Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I,” JURNAL TEKNIK ITS, vol. 1, nr 1, pp. A288-A293, 2012.

[6] T. Neubauer och M. Pehn, ”Workshop-based Security Safeguard Selection with AURUM,” International Journal on Advances in Security, vol. 3, nr 3, pp. 123-134, 2010.
[7] B. Karabacak och I. Sogukpinar, ”ISRAM: information security risk analysis method,” Computers & Security, vol. 24, nr 2, pp. 147-159, 2005.
[8] B. Supradono, ”MANAJEMEN RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION),” Media Elektrika, vol. 2, nr 1, pp. 5-8, 2009.
[9] K. J. S. Hoo, ”HOW MUCH IS ENOUGH? A RISK MANAGEMENT APPROACH TO COMPUTER SECURITY,” STANFORD UNIVERSITY, Stanford, 2000.
[10] A. Ekelhart, S. Fenz och T. Neubauer, ”AURUM: A Framework for Information Security Risk Management,” i Hawaii International Conference on System Sciences, Hawaii, 2009.
[11] A. Syalim, Y. Hori och K. Sakurai, ”Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft’s Security Management Guide,” i International Conference on Availability, Reliability and Security, Fukuoka, 2009.
[12] A. Klai, ”Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies,” i MIPRO, Opatija, Croatia, 2010.
[13] D. J. White, Managing Information in the Public Sector, M.E.Sharpe, 2007.