ISSN: 2477-5126
e-ISSN: 2548-9356

Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1
(Studi Kasus: STMIK Sumedang)

Fathoni Mahardika[*)]
Jurusan Manajemen Informatika, STMIK Sumedang
Jln. Angkrek Situ No.19 Sumedang 45323, Indonesia
email: [1]fathoni@stmik-sumedang.ac.id

***Abstract* - STMIK Sumedang have problems in the use of IT policies, among others: (1) are still common information security incidents that cause disruption of the business process of the company, (2) Not adan supervision and planning the best way to manage information security in STMIK Sumedang. Risk Management using NIST SP 800-30 Revision 1. This standard is used as a reference to the management of risk and anticipate the risk that the loss does not occur to the organization. So the risk can be managed to a level that can be received by the organization. It is expected that will reduce the impact of the incident of the system and information technology in higher education institutions, protect the business process of the organization is important from security threats, minimize the risk of loss and avoid serious failure of the information in STMIK Sumedang. The result STMIK Sumedang have risk level moderately, while for the browning assessment (maturity) information security, organization STMIK Sumedang have browning level on low value where the security level that is only planned without any documentation and risk management control in the form of a standard procedure security policy.**

***Abstrak* – STMIK Sumedang memiliki permasalahan dalam penggunaan TI antara lain : (1) Masih sering terjadinya insiden keamanan informasi yang menyebabkan terganggunya proses bisnis perusahaan, (2) Belum adanya pengawasan dan perencanaan yang tepat dalam pengelolaan keamanan informasi di STMIK Sumedang. Manajemen risiko menggunakan NIST SP 800-30 Revisi 1. Standar ini digunakan sebagai acuan melakukan manajemen risiko, mengantisipasi risiko agar kerugian tidak terjadi terhadap organisasi. Sehingga risiko dapat dikelola ke level yang dapat diterima organisasi. Diharapkan akan mengurangi dampak insiden sistem dan teknologi informasi di institusi perguruan tinggi, melindungi proses bisnis organisasi yang penting dari ancaman keamanan, meminimalisir risiko kerugian serta menghindari kegagalan serius terhadap informasi yang ada di STMIK Sumedang. Hasilnya STMIK Sumedang memiliki level risiko *Moderate*, Sedangkan untuk penilaian kematangan (*maturity*) keamanan informasi, Organisasi STMIK Sumedang mempunyai level kematangan pada nilai rendah dimana tingkatan keamanan yang ada hanya direncanakan tanpa adanya dokumentasi dan kontrol penanganan risiko dalam bentuk sebuah prosedur standar kebijakan keamanan.**

Kata Kunci* – Keamanan Informasi, Manajemen Risiko, NIST SP 800-30 Rev1, ISO / IEC 27002, *Control Security Standards Information Security Policy

*) Penulis korespondensi (Fathoni Mahardika)
Email: fathoni@stmik-sumedang.ac.id

I. PENDAHULUAN

Penggunaan Teknologi Informasi di Perguruan Tinggi telah memberikan kemudahan, terutama dalam hal pengaksesan suatu informasi dengan sangat cepat dan murah yang dikemas dalam sebuah Sistem Informasi digital. Akan tetapi dengan perkembangan teknologi informasi tersebut maka semakin besar keinginan orang untuk mendapatkan akses ke informasi dan mengendalikannya. Maka munculah individu atau kelompok baik itu dari pihak internal atau eksternal yang menggunakan aset informasi demi berbagai tujuan dan mengerahkan segala upaya untuk mendapatkan aset informasi dengan berbagai cara. TI dapat digunakan untuk memelihara anonimitas, hal ini mempermudah seseorang untuk melakukan tindakan tidak etis dan kriminal, termasuk perusakan aset Teknologi Informasi dan perolehan informasi secara ilegal. Berdasarkan hasil laporan Iwan Sumantri (ID-SIRTI) tentang Insiden Serangan Website domain Indonesia Tahun 2013 bahwa serangan terhadap domain website *ac.id* (akademik indonesia) adalah sebesar 18,98 % dimana *ac.id* merupakan domain ke-2 yang paling banyak mengalami serangan keamanan selain domain *go.id*. Oleh sebab itu, maka perlu peningkatan pengamanan terhadap asset informasi yang ada di perguruan tinggi salah satunya berupa *website* [3].

Dalam perjalanannya Perguruan tinggi membutuhkan sumber informasi yang mutakhir dan selalu terkini. Pengembangan implementasi teknologi informasi di perguruan tinggi merupakan upaya yang sudah seharusnya dilakukan. Aktivitas utama dalam perguruan tinggi sesuai dengan fungsi utamanya yaitu sebagai penyelenggara pendidikan adalah layanan akademik. Dalam pelaksanaan layanan akademik ini perlu adanya penggunaan TI yang dapat mendukung tercapainya sasaran dari layanan akademik tersebut dalam organisasi STMIK Sumedang. Hal tersebut juga berlaku pada penggunaan teknologi informasi di STMIK Sumedang. STMIK Sumedang sebagai salah satu lembaga pendidikan yang menyelenggarakan pendidikan tinggi di Sumedang, menggunakan teknologi informasi sebagai inti usaha yang memberikan pendidikan berdasarkan kurikulum yang berbasis kompetensi teknologi informasi dan komputer, dan Penunjang usaha dalam penggunakan teknologi informasi sebagai sarana dan prasarana untuk memberikan layanan kepada mahasiswa, dosen dan seluruh stafnya.

Dalam melakukan tugas pengelolaan TI, STMIK Sumedang sudah didukung oleh *server* akademik yang didalamnya berisi Sistem Informasi Akademik, Sistem

Informasi Keuangan Mahasiswa, *SMS Gateway*, yang dihubungkan dengan jaringan melalui yang dilakukan oleh bagian UPT LPSI. Namun terdapat permasalahan dalam penggunaan dan pemanfaatan TI yang ada saat ini antara lain: (1) Masih sering terjadinya insiden keamanan informasi yang menyebabkan terganggunya proses bisnis perusahaan. Sebagian insiden yang terjadi dapat diatasi secara langsung (*reaktif*) dilapangan, tetapi insiden lainnya membutuhkan perencanaan dan waktu yang tidak sedikit untuk menyelesaikannya; (2) Belum adanya pengawasan dan perencanaan yang tepat dalam pengelolaan keamanan data dan informasi di STMIK Sumedang. Dilihat dari sudut pandang pemakai informasi yang dihasilkan oleh sistem informasi akademik dimana informasi yang dihasilkan akan sangat lambat dan sering terjadi kesalahan dan kerusakan data.

Kejadian (*incident*), atau *vulnerability* yang terjadi diatas merupakan risiko yang dapat mengganggu proses bisnis STMIK Sumedang. Dengan pertimbangan *incident*, dan *vulnerability* yang sering terjadi maka diperlukan penanganan risiko, dan penilaian risiko dilakukan dalam proses manajemen risiko keamanan informasi sehingga risiko yang ada bisa ditangani dan dikendalikan. Manajemen risiko keamanan informasi adalah metode untuk penilaian dan mitigasi risiko terhadap aspek kebutuhan keamanan informasi yang memuat 3 unsur penting yaitu: *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan). Tiga unsur penting dari aspek keamanan tersebut sangat rawan terhadap ancaman serangan-serangan yang mengancam keberadaanya baik serangan terhadap sumber-sumber informasi baik secara fisik dan melalui akses secara jaringan.

Dalam penelitian ini manajemen risiko keamanan informasi yang digunakan mengacu pada *framework* NIST (*National Institute Standard Technology*) dikembangkan oleh *US Department of Commerce*. NIST merupakan Organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standar, dan teknologi untuk meningkatkan fasilitas dan kualitas kehidupan. NIST mengeluarkan alat, teknik dan metode untuk penilaian dan perencanaan keamanan informasi berbasis risiko.

Standar yang akan digunakan didalam penelitian ini adalah NIST SP 800-30. Standar ini digunakan sebagai acuan dalam melakukan manajemen risiko keamanan informasi, yang bertujuan untuk mengantisipasi terhadap risiko agar kerugian tidak terjadi kepada organisasi. Sehingga risiko dapat di identifikasi, dinilai dan dikurangi dampak risikonya ke level yang dapat diterima organisasi. NIST SP 800-30 dipilih sebagai acuan manajemen risiko dalam penggunaan sistem dan teknologi informasi di perguruan tinggi. Dengan dilakukannya manajemen risiko diharapkan akan mengurangi dampak insiden sistem dan teknologi informasi di institusi perguruan tinggi, melindungi proses bisnis organisasi yang penting dari ancaman keamanan, meminimalisir risiko kerugian serta menghindari kegagalan serius terhadap informasi yang ada di organisasi STMIK Sumedang.

Tujuan *Framework* NIST SP 800-30 adalah memberikan petunjuk program secara terpadu, untuk seluruh organisasi dalam mengelola risiko keamanan informasi operasi organisasi (yaitu, misi, fungsi, *image*, dan reputasi), asset organisasi, individu, operasi yang dihasilkan organisasi dan terhadap penggunaan sistem informasi/teknologi informasi [9],[10]. Publikasi khusus 800-30 menyediakan pendekatan terstruktur, tapi fleksibel dalam mengelola risiko yang luas, dengan rincian yang spesifik dalam menilai, menanggapi, dan melakukan pemantauan risiko secara terus-menerus sehingga risiko bisa di evaluasi oleh pihak manajemen di organisasi STMIK Sumedang. Setelah dilakukan manajemen risiko maka diperlukan *control* keamanan sebagai dasar acuan bahwa risiko dilakukan mitigasi, diterima/ditransfer oleh pihak manajemen. *Control* keamanan dikembangkan dari ISO 27002. Setelah itu dilakukan maturity keamanan informasi organisasi STMIK Sumedang menggunakan *control* yang dikembangkan dari ISO 27002. Dari hasil penilaian *maturity* ini menjadi dasar dibuatnya rekomendasi standar kebijakan keamanan informasi di STMIK Sumedang, baik itu informasi yang ada di lembaga atau informasi yang dikelola Sistem dan Teknologi Informasi yang digunakan di STMIK Sumedang.

II. PENELITIAN YANG TERKAIT

Menurut Slay & Koronios (2006), manajemen risiko adalah proses yang berjalan untuk mengukur kemungkinan munculnya suatu kejadian yang membahayakan, mengimplementasikan pengukuran untuk mengurangi risiko atas kejadian yang muncul dan memastikan organisasi yang bersangkutan merespon dan meminimalisasi dampak yang terjadi [20]. Menurut Djohanputro (2008), manajemen risiko merupakan proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternatif penanganan risiko, dan memonitor dan mengendalikan penanganan risiko [18].

Menurut Fahmi (2010), manajemen risiko adalah suatu bidang ilmu yang membahas tentang bagaimana suatu organisasi menerapkan ukuran dalam memetakan berbagai permasalahan yang ada dengan menempatkan berbagai pendekatan manajemen secara komprehensif dan sistematis [19]. Sehingga dapat disimpulkan dari beberapa definisi diatas, bahwa definisi manajemen risiko adalah sebagai berikut: (a) segala proses pengelolaan risiko yang mencakup identifikasi, evaluasi, mitigasi dan pengendalian risiko terutama yang berhubungan dengan menyangkut keamanan informasi yang dapat mengancam kelangsungan usaha, strategi visi misi dan aktivitas organisasi untuk masa sekarang beserta masa yang akan dating; (b) setiap proses pengukuran serta penilaian terhadap sesuatu yang belum pasti serta memberikan strategi untuk mengelolanya, beberapa cara ataupun strategi yang biasanya digunakan antara lain memindahkan ketidakpastian/risiko kepada pihak luar, mengurangi hal-hal yang sekiranya dapat memberikan nilai negative atau risiko, dan bersedia menerima segala konsekuensi dari risiko yang akan terjadi.

Pada tabel I memperlihatkan penelitian yang berhubungan dengan penelitian yang peneliti lakukan:

TABEL I
PENELITIAN TERKAIT

No	Judul dan Hasil Penelitian	Perbedaan
1.	Penerapan Manajemen Risiko Untuk Meningkatkan Keamanan Informasi [25] (Studi Kasus: Divisi IT Security PT.XYZ) Carolina Rizky Putri, Binus University	Framework yang digunakan dalam manajemen risiko keamanan informasi
2	*Information Technology Risk Assessment: Octave S Approach* [2] Bambang Gunawan, Alumni, Binus University Merry, Alumni, Binus University, Nelly, Faculty Member, Binus University	Metode Penilaian Risiko Kemanan Informasi, dalam penelitian berikut ini menggunakan metode Octave-S. Octave-S menitip beratkan penilaian risiko untuk pengolahan data.
3.	Implementasi *Framework* Manajemen Risiko terhadap Penggunaan Teknologi Informasi Perbankan [8] Hendra Shandi Firmansyah STMIK Jabar Bandung	Objek Penelitian terhadap penggunaan IT di perbankan
4.	Manajemen Risiko Sistem Informasi Akademik pada perguruan Tinggi menggunakan *Octave Allegro*. [16] Deni Ahmad Jakaria, STMIK DCI Tasikmalaya R Teduh Dirgahayu, UII Yogyakarta	*Octave Allegro* memfokuskan pada asset informasi dan data yang mendukung informasi tersebut.
5.	Pembuatan Rencana Keamanan Informasi Berdasarkan Analisis Dan Mitigasi Risiko Teknologi Informasi [1] Aan Albone Jurusan Teknik Informatika, Universitas Pasundan Bandung, Indonesia	Hanya melakukan perencanaan keamanan informasi, tidak menghasilkan sebuah kebijakan keamanan informasi
6.	*Information Security Management in Australian University – An Exploratory Analysis* [26] Tim Lane, AssocDip IT, BMangt&Prof.Studies. Thesis submitted for the degree of Master of Information Technology QUT Faculty of Information Technology School of Software Engineering and Data Communication Januari 2007	Hanya menghasilkan penelitian deskriptif, kebijakan keamanan informasi dibuat berdasarkan survey online tentang penggunaan framework keamanan informasi.
7.	Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metoda Octave (Operationally Critical Threat, Asset, And Vulnerability Evaluation) [6] Bambang Supradono Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Semarang	Metoda Octave sebagai alat untuk mengukur risiko keamanan informasi
8	Mengukur Keamanan Informasi: Studi Komparasi ISO 27002 dan NIST SP 800-55 [4] Maryuni, Bekti Susanto,. Program Studi Manajemen Informatika, AMIK BSI YOGYAKARTA. Seminar Nasional Teknologi Informasi dan Komunikasi 2013. Yogyakarta	Metode dan hasil penelitian yang berbeda
9	Pengukuran Risiko Aset Teknologi Informasi Berbasis PBI Pada Sektor Perbankan di Indonesia. [5] Rudy M. Harahap, Marisa Caroline Subita, Shinta Octavia Fakultas Ilmu Komputer Universitas Bina Nusantara. 2009	Penggunaan metode, framework, dan alat ukur untuk menghasilkan risiko. Output dan objek yang berbeda
10	Sistem Manajemen Keamanan Informasi Pada Organisasi Kesehatan Berdasarkan ISO 27799. [7] Susanto, B. M., & Wahyudi, M.*Seminar Nasional Ilmu Komputer* (ss. 65-72). Semarang: Graha Ilmu. 2012.	Penggunaan metode dan langkah penilaian risiko Sama-sama menghasilkan kebijakan.

Dalam penelitian ini manajemen risiko keamanan informasi yang digunakan mengacu pada framework NIST (*National Institute Standard Technology*) dikembangkan

oleh *US Department of Commerce*. NIST merupakan Organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standar, dan teknologi untuk meningkatkan fasilitas dan kualitas kehidupan. NIST mengeluarkan alat, teknik dan metode untuk penilaian dan perencanaan keamanan informasi berbasis risiko. Kaitan dengan penelitian yang sudah ada yaitu sama-sama melakukan manajemen risiko keamanan informasi, yang menjadi perbedaan yaitu penggabungan framework NIST SP800-30 dengan ISO 27002 dengan melakukan *maturity* sehingga dihasilkan kebijakan keamanan informasi yang bisa diterapkan di STMIK Sumedang.

III. METODE PENELITIAN

A. Pendekatan Penelitian

Pendekatan yang digunakan dalam penyusunan penelitian ini adalah dengan menggunakan pendekatan kualitatif. Menurut (Sugiyono, 2009:15), Metode penelitian kualitatif adalah metode penelitian yang berlandaskan pada filsafat postpositifsime, digunakan untuk meneliti pada kondisi objek yang alamiah (sebagai lawannya adalah eksperimen) dimana peneliti adalah sebagai instrument kunci, pengambilan sample sumber dan data dilakukan secara purposive dan snowbaal, teknik pengumpulan data dilakukan dengan triangulasi (gabungan) analisis data bersifat induktif / kualitatif, dan hasil penelitian kualitatif lebih menekankan pada makna daripada generalisasi [23]. Metode yang dipakai berupa studi kasus pada STMIK Sumedang.

B. Pengumpulan Data

Dalam proses pengumpulan data antara lain dengan mencari ke berbagai sumber terpercaya, sebagai berikut :

a) *Metodologi Pustaka:* Dengan mengumpulkan data dari berbagai sumber dan referensi berupa buku, handout, modul perkuliahan, browsing dari website atau mencari sumber lain dari berbagai perpustakaan baik itu perpustakaan kampus, umum, daerah, atau digital library (e-library). Sumber utama yaitu Buku, website yang menjelaskan tentang Manajemen Risiko khususnya memuat penjelasan metode NIST SP 800-30 sebagai dasar materi untuk pengukuran dan manajemen risiko di STMIK Sumedang.

b) *Metodologi Lapangan*

- *Wawancara atau Interview*: Proses memperoleh data dengan cara tanya jawab secara langsung melalui pihak yang berkepentingan dalam perusahaan sehingga didapatkan data yang berkualitas. Wawancara dilakukan terhadap pihak atau manajemen yang memahami tentang tugas pengelolaan keamanan informasi atau teknologi informasi yaitu Ka.UPT LPSI.
- *Observasi*: Dengan melakukan pengamatan dan peninjauan secara langsung terhadap objek yang akan diteliti penulis yang berkaitan dengan organisasi serta kondisi TI dan SI yang dipakai organisasi mencakup hardware, software, network, dan application yang diterapkan STMIK Sumedang melalui pengelolaan UPT LPSI.

C. Teknik Analisis

Penelitian tentang manajemen risiko ini pada dasarnya merupakan penelitian eksploratif artinya penelitian dilakukan dengan cara menggali informasi tentang pengelolaan keamanan informasi di STMIK Sumedang, dan hasil penelitian disampaikan dalam bentuk deskripsi yang bersifat kualitatif maupun kuantitatif. Teknis analisis dilakukan dengan melakukan penilaian kematangan (*maturity*) keamanan informasi organisasi STMIK Sumedang yang dianalisis secara kuantitatif melalui pengisian kuisioner oleh UPT.LPSI, sedangkan rekomendasi draft kebijakan keamanan informasi tindak lanjutnya dianalisis secara kualitatif yang diambil dari hasil penilaian kematangan (maturity) [11].

Teknik analisis kualitatif menggunakan *spreadsheet* Microsoft Excel untuk mengolah data asset TI berupa software, hardware, dan infrastruktur jaringan. untuk menjawab dan menjelaskan perumusan masalah manajemen risiko, penilaian tingkat kematangan (*maturity level*) dan pembuatan draft standar kebijakan keamanan informasi dari hasil kematangan keamanan informasi di organisasi STMIK Sumedang. [12]

D. Alat Penelitian

Alat penelitian yang digunakan dalam membantu proses penelitian yang dilakukan adalah dengan menggunakan wawancara dan kuisioner yang diambil berdasarkan literature yang ada didalam NIST SP 800-30 Revision 1, ISO 27002:2005 [13] [14] [15]. Adapun alasan yang mendasari pemakaian alat penelitian tersebut adalah sebagai berikut: (1) Wawancara merupakan salah satu alat penelitian yang digunakan untuk pendekatan penelitian kualitatif. Sehingga hasil wawancara bisa menghasilkan informasi berupa *threat*, *vulnerabillity*, *likelyhood*, *impact*, dan *level of Risk*; (2) Kuisioner merupakan salah satu alat penelitian yang dapat digunakan untuk melakukan penilaian kematangan keamanan informasi. Objek yang menjadi kuisioner yaitu Ka.UPT LPSI beserta staff UPT; (3) Responden yang digunakan dalam penelitian ini adalah UPT LPSI yang mempunyai kewenangan dan tanggung jawab terhadap pengelolaan TI yang ada di STMIK Sumedang; (4) Mengumpulkan langsung responden untuk memberikan penjelasan hasil wawancara, pengisian kuisioner penilaian kematangan, dan istilah-istilah asing dan masukan yang tepat yang dapat dipahami oleh responden; (5) Analisis untuk maturity dilakukan dengan cara membandingkan tingkat maturity yang ada pada saat ini dengan tingkat maturity yang dituju. Tingkat maturity yang dituju pada dasar merupakan tingkat maturity rata-rata institusi yang berada pada level 3.

IV. HASIL PEMBAHASAN

Sebelum dilakukan manajemen risiko dapat dijelaskan bahwa STMIK Sumedang hanya melakukan perencanaan keamanan tanpa adanya dokumentasi secara jelas, hal ini bisa dijelaskan pada pembahasan dibawah ini.

A. Hasil Penilaian

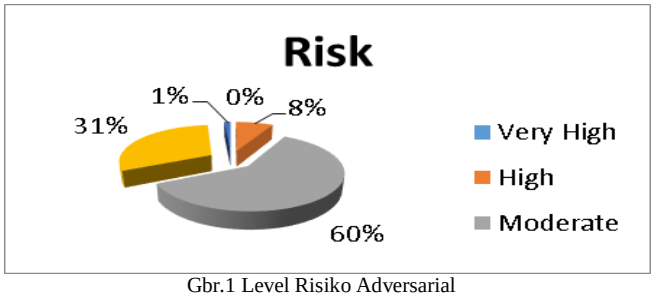
Berdasarkan hasil penilaian risiko pada tahapan sebelumnya dapat dihasilkan asset yang harus ditangani dalam proses mitigasi risiko yaitu sebagai berikut:

Hasil mitigasi risiko dibuat dalam bentuk 2 risiko yaitu Risiko Adversarial dan Risiko Non-Adversarial. Hal ini

ISSN: 2477-5126
e-ISSN: 2548-9356

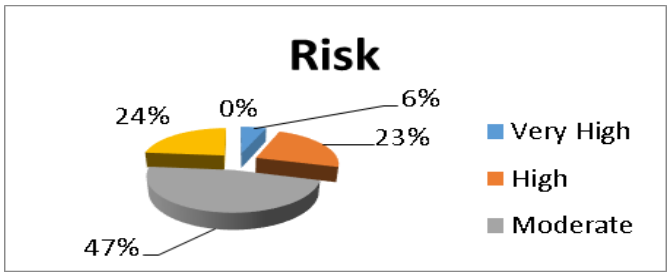
disesuaikan dengan kebutuhan yang ada dalam framework NIST SP 800-30 Revisi 1 [13].

Pada tabel Risiko Adversarial, dilakukan mitigasi risiko oleh pihak manajemen yang bertanggung jawab dalam penanganan risiko. Dari hasil analisis kualitatif dapat dihasilkan bahwa STMIK Sumedang terutama menyangkut risiko adversarial mempunyai risiko keamanan informasi yang *Moderate*, hal ini bisa di gambarkan pada grafik berikut ini:



Gbr.1 Level Risiko Adversarial

Pada Risiko *Non-Adversarial* pihak manajemen melakukan mitigasi risiko oleh pihak yang bertanggung jawab dalam menangani risiko tersebut. Dari hasil analisis kualitatif dapat dihasilkan bahwa STMIK Sumedang terutama menyangkut risiko non-adversarial mempunyai risiko keamanan informasi yang Moderate, hal ini bisa di gambarkan pada grafik berikut ini:



Gbr. 2 Level Risiko Non Adversarial

Untuk membuat sebuah kebijakan keamanan informasi maka sebelumnya diperlukan penilaian *maturity* keamanan informasi [9-15]. Dalam tahapan ini akan dilakukan penilian proses misi/bisnis organisasi terutama yang terkait dengan Keamanan informasi dalam Organisasi STMIK Sumedang. Dalam penilaian *maturity*, dilakukan Analisis kualitatif dimana penulis melakukan penilaian dengan menggunakan teknik wawancara langsung. Yang menjadi objek penilaian adalah Ka UPT LPSI dan Staf UPT. Berdasarkan kuisioner dari UPT.LPSI yang mempunyai tanggung jawab dalam pengelolaan layanan TI dan SI di STMIK Sumedang dapat dihasilkan sebuah level kematangan program keamanan informasi di STMIK Sumedang dari *Score Card* terdiri dari penilaian berdasarkan control dan implementasi yang dikembangkan dari ISO 27002, meliputi:

1. Manajemen Risiko (*Risk Management*).
2. Kebijakan Keamanan (*Security Policy*).
3. Pengorganisasian Keamanan Informasi (*Organization Of Information Security*).
4. Manajemen Aset (*Asset Management*) .
5. Keamanan Sumber Daya Manusia (*Human Resource Security*).
6. Keamanan Fisik dan Lingkungan (*Physical and Environmental Security*).
7. Manajemen Komunikasi dan Operasional (*Communication and Operations Management*).
8. Kontrol Akses (*Acces Control*).
9. Akuisisi Pengembangan dan Pemeliharaan Sistem Informasi (*Information Systems Acquisition, Development, and Maintenance*).
10. Manajemen Insiden Keamanan Informasi (*Information Security Incident Management*).
11. Manajemen Kelangsungan Bisnis (*Business Continuity Management*).
12. Kepatuhan (*Compliance*).

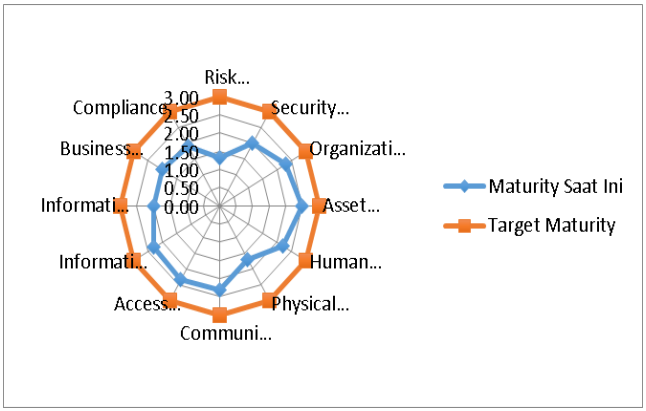
TABEL II
LEVEL MATURITY

ISO Keamanan	Hasil Maturity	Target Maturity	GAP
Risk Management	1.33	3.00	1.67
Security Policy	2.00	3.00	1.00
Organization Of Information Security	2.30	3.00	0.70
Asset Management	2.50	3.00	0.50
Human Resource Security	2.20	3.00	0.80
Physical and Environmental Security	1.71	3.00	1.29
Communication and Operations Management	2.32	3.00	0.68
Access Control	2.33	3.00	0.67
Information Systems Acquisition, Development, and Maintenance	2.29	3.00	0.71
Information Security Incident Managements	2.00	3.00	1.00
Business Continuity Managements	2.00	3.00	1.00
Compliance	1.88	3.00	1.12
Rata-rata	2.18	3.00	0.82

Dari tabel terdapat GAP (Selisih) yang menggambarkan bahwa STMIK Sumedang belum menerapkan control dan prosedur keamanan informasi, GAP diatas membandingkan antara kematangan keamanan informasi saat ini dengan target kematangan keamanan informasi yang dituju. Untuk menutupi GAP tersebut akan dilakukan mapping berdasarkan hasil kematangan saat ini, hasilnya berupa rekomendasi kebijakan yang dikembangkan berdasarkan *control* yang ada pada ISO 27002.

Sedangkan gambar 3 menjelaskan tentang gambar level kematangan *(Maturity)* yang dimiliki STMIK Sumedang dalam bentuk diagram radar. Hasil penilaian kematangan bersumber dari kuisioner dan wawancara dengan Ka.UPT LPSI dan Staf UPT LPSI.

ISSN: 2477-5126
e-ISSN: 2548-9356



Gbr. 3 Diagram Radar Informasi

Dari hasil penilaian *maturity* keamanan informasi yang ada di organisasi STMIK Sumedang menggambarkan bahwa nilai yang ada berada di kisaran yang cukup rendah yaitu rata-rata nilainya adalah 2.18 atau berada pada level 2, dimana menurut kematangan level kebijakan yang ada hanya ada pada proses perencanaan atau pihak manajemen hanya melakukan control ditempat tanpa adanya dokumentasi atau tidak ada standar control yang mengikuti standar tertentu.
Pencapaian kematangan dilakukan sebagai upaya mengatasi atau meminimalisir perbedaan (*gap*) berdasarkan tingkat kematangan control Keamanan Informasi yang telah diidentifikasikan sebelumnya. Dimana penerapan kontrol keamanan yang dikelola oleh UPT LPSI saat ini masih memiliki tingkat kematangan yang di bawah tingkat kematangan yang diharapkan. Penetapan pencapaian kematangan diperlukan dengan pertimbangan sebagai berikut: Tahapan kematangan ini dilakukan secara alamiah dalam melakukan proses perbaikan, tiap proses merupakan tahapan pembelajaran yang mana tiap tahapan kematangan harus dilaksanakan [17].

Penetapan pencapaian kematangan diperlukan dengan pertimbangan sebagai berikut:

1. Tahapan kematangan ini dilakukan secara alamiah dalam melakukan proses perbaikan, tiap proses merupakan tahapan pembelajaran yang mana tiap tahapan kematangan harus dilaksanakan.
2. Perbaikan dilakukan secara bertahap sesuai dengan skala prioritas yang di STMIK Sumedang. Yang mempunyai nilai kematangan lebih rendah, mendapat prioritas yang lebih tinggi untuk dilakukan perbaikan.
3. Dengan perbaikan yang bertahap ini, maka proses pembelajaran untuk menuju tingkat kematangan 3 dalam organisasi dapat dilakukan.

Selain melakukan tindakan-tindakan rekomendasi kebijakan dan perbaikan tersebut, UPT LPSI harus melaksanakan, mendokumentasikan, mensosialisasikan, mereview serta menggunakan perangkat aplikasi atau tools untuk mengoptimalkan kebijakan keamanan informasi yang dibangun. Adapun usulan tools untuk optimalisasi yang direkomendasikan dalam penerapan kebijakan keamanan yaitu [24]:

1. *Risk Management Tools*: Risk Management Studio. *RM Studio* adalah perangkat lunak manajemen risiko yang dapat digunakan oleh organisasi untuk menerapkan proses manajemen risiko dan menerapkan kebijakan Keamanan Informasi.
2. *Kali Linux*: Tools OS for Security (Penetration Test). Kali Linux adalah *Operating System* yang digunakan untuk melakukan pengujian terhadap keamanan system computer, jaringan computer, database, dan aplikasi.
3. *Tools Audit Kemanan Informasi*: Accunetix Web Vulnerability Scanner. Merupakan tools untuk melakukan *scanning* pada sebuah aplikasi web dimana hasilnya bisa mengetahui celah keamanan, dan kerentanan yang dimiliki aplikasi web tersebut.
4. *Tools audit keamanan informasi*: ZenMap Scanner. *Zenmap* merupakan *tools* untuk melakukan audit keamanan untuk mengeksplorasi kerentanan pada jaringan komputer.
5. *Tools audit keamanan informasi*: *Wireshark*. *Wireshark* marupakan tools audit untuk melakukan sniffing terhadap kerentanan jaringan dalam sebuah organisasi. Dengan *wireshark*, celah keamanan dalam sebuah sistem bisa diketahui karena *tools* ini bisa menangkap *packet data* yang ada dalam jaringan computer pada sebuah organisasi.
6. *Konfigurasi Jaringan Komputer*: Mikrotik Router OS. MikroTik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *router network*, mencakup berbagai fitur yang dibuat untuk *ip network* dan jaringan *wireless*, dapat digunakan oleh ISP dan *provider hotspot*.

Selain itu untuk pengelolaan risiko dan penggunaan control keamanan maka dibutuhkan *Score Card*. *Score card* dibuat dengan menggunakan Ms.Excel yang di dalamnya berisi penilaian, control dan prosedur penanganan keamanan informasi yang dikembangkan dari NIST SP 800-30 Rev1 dan ISO 27002. Dengan menggunakan *Score Card* yang dikembangkan dari control ISO 27002 sangat terlihat sekali bahwa manajemen STMIK Sumedang hanya menerapkan sebagian kontrol atau tidak memiliki kontrol yang mengikuti standar tertentu, karena biasanya kontrol yang ada hanya mengikuti threat/events tanpa adanya petunjuk berupa dokumentasi atau standar untuk melakukan control atau monitoring terhadap *threats/events* tersebut, atau hanya bersifat mendadak tanpa adanya kontrol yang tepat. Hal ini tentunya membuat pihak manajemen tidak efektif tanpa adanya standar. dalam proses penanganannya. Selain itu jika segala yang mengatur hal ini, maka akan mengakibatkan manajemen tidak punya laporan berkala terkait keamanan informasi sesuatunya bersifat mendadak.

Dari hasil manajemen risiko dan penilaian kematangan terdapat banyak risiko, ancaman, dan kejadian yang terkait keamanan informasi yang tidak ditangani dengan baik oleh pihak manajemen. Dengan hasil diatas dapat disimpulkan bahwa organisasi STMIK Sumedang memerlukan standar kebijakan keamanan informasi yang mengatur organisasi/pengguna dalam penggunaan dan pengelolaan Teknologi Informasi. Hal ini diperkuat oleh target Level Maturity yaitu pada Level 3, dimana menjelaskan bahwa pada Level 3 dimana Organisasi membutuhkan Kontrol dan Prosedur dalam menjaga keamanan informasi di STMIK Sumedang. Kebijakan disesuaikan dari hasil mapping

rekomendasi yang ada pada tabel 4.15 berdasarkan hasil kematangan yang ada di organisasi STMIK Sumedang

B. Rekomendasi Peran Organisasi dan Tanggung Jawab

Sebelum merancang dan menetapkan kebijakan keamanan informasi, pihak organisasi harus membentuk tim pelaksana yang memiliki tugas utama membuat, memberi masukan, mengevaluasi dan melakukan perbaikan kebijakan keamanan informasi. Kebijakan keamanan informasi merupakan suatu panduan/aturan keamanan yang penerapannya adalah tanggung jawab semua pihak, dimulai dari pihak manajemen organisasi atas hingga ke *level* yang paling bawah. Tanggung jawab dan aturan fungsional diatas, sangat terkait dengan struktur organisasi yang berlaku di organisasi tersebut. Dalam hal ini tanggung jawab keamanan informasi menjadi tugas UPT.LPSI yang merangkap tugas dan jabatan, yaitu Unit Keamanan Informasi (*Information Security Officer)*.

Dalam rekomendasi peran organisasi dan tanggung jawab, Ka.UPT LPSI atau ketua Unit Keamanan Informasi sebagai pimpinan puncak berperan dalam mengambil keputusan dalam memberikan pertimbangan dalam penetapan kebijakan dan bertanggung jawab terhadap penerapan dan pengelolaan kebijakan keamanan informasi yang didokumentasikan, dimana dokumentasi dibangun benar sesuai dengan standar yang dikembangkan dari NIST SO 800-30 Revision 1 dan ISO 27002.

Dari hasil penilaian *maturity* keamanan informasi di STMIK Sumedang, sesuai Level Kematangan yaitu pada nilai 2.18 dan untuk memenuhi target kematangan yaitu pada nilai 3. Alasan diambil target level 3 karena pada tahapan sebulumnya dilakukan manajemen risiko menggunakan framework *NIST SP 800-30* Rev1 dimana NIST merekomendasikan dan menjelaskan bahwa *Control* dan *Procedures* berada pada level 3 [22].

Maka setelah meilhat hasil nilai kematangan pihak manajemen yang menangani dan mengelola TI atau SI yaitu Ka UPT LPSI beserta staff merekomendasikan untuk membuat kebijakan keamanan informasi. Hasil Kebijakan merupakan hasil rekomendasi dari penulis dan UPT.LPSI STMIK Sumedang yang dibuat berdasarkan kebutuhan keamanan informasi di STMIK Sumedang. Kebijakan keamanan ditetapkan dan ditanda tangani ketua STMIK Sumedang dalam bentuk standar kebijakan keamanan informasi.

Draft kebijakan keamanan informasi yang dibuat merupakan hasil mapping tabel yang berisikan *control* atau prosedur keamanan informasi yang terdiri dari [21]:

- Manajemen Risiko
- Kebijakan Keamanan Informasi
- Pengorganisasian Keamanan Informasi
- Manajemen Aset
- Keamanan SDM
- Keamanan Fisik dan Lingkungan
- Manajemen Komunikasi dan Operasional
- Akses Kontrol
- Akuisisi Pengembangan dan Pemeliharaan Sistem Informasi
- Manajemen Insiden Keamanan Informasi
- Manajemen Kelangsungan Bisnis
- Kepatuhan

Maksud dan tujuan dibuatnya kebijakan ini yaitu: (1) keputusan ini adalah untuk memberikan referensi kepada seluruh komponen pelaksana keamanan informasi TI STMIK Sumedang dalam menyusun dan menetapkan prosedur operasional agar terjadi keselarasan pada tataran strategis dan operasional: (2) tersedianya panduan untuk mewujudkan standardisasi pelaksanaan keamanan informasi di STMIK Sumedang. Sedangkan ruang lingkup dari standar kebijakan ini meliputi: (1) Kebijakan Keamanan Informasi ini diberlakukan secara menyeluruh di seluruh komponen organisasi STMIK Sumedang; (2) Kebijakan Keamanan Informasi ini mengatur pengelolaan keamanan informasi dan manajemen keamanan informasi.

Demikian penjelasan pembuatan *draft* standar kebijakan keamanan informasi di STMIK Sumedang yang diajukan Ka.UPT LPSI. Draft ini menggambarkan bagaimana system informasi, jaringan, *hardware*, *software* dan pengguna yang di dalamnya dikelola dan diatur secara aman berdasarkan hasil penilaian kematangan yang dikembangkan berdasarkan standar *ISO/IEC 27002*.

V. KESIMPULAN

Berdasarkan hasil penjelasan sebelumnya, penulis dapat menarik kesimpulan diantaranya, sebagai berikut:

- Pada dasarnya STMIK Sumedang belum melakukan penilaian dan manajemen risiko keamanan informasi, setelah dilakukan identifikasi dan manajemen risiko, terdapat beberapa pengendalian yang perlu ditingkatkan sehingga risiko perusahaan dapat diminimalkan. Selain itu, UPT LPSI belum melakukan pencatatan mengenai risiko-risiko yang terjadi setiap tahunnya sehingga tidak diketahui aset-aset apa saja yang risikonya tinggi.
- STMIK Sumedang memiliki level risiko keamanan informasi yang *Moderate*, dimana untuk risiko *adversarial* terdiri dari: 20 *High*, 46 *Moderate*, 10 *Low*, 2 *Very Low*. Sedangkan untuk risiko *non-adversarial* terdiri dari : 2 *Very High*, 5 *High*, 9 *Moderate*, 1 *Low*. Hal diatas ditunjukan berdasarkan analisis kualitatif dan wawancara risiko keamanan informasi.
- Penilaian kematangan (*maturity*) keamanan informasi, Organisasi STMIK Sumedang mempunyai level kematangan pada kisaran nilai 2.18 dimana tingkatan keamanan yang ada hanya direncanakan tanpa adanya dokumentasi dan kontrol penanganan risiko dalam bentuk sebuah prosedur standar kebijakan keamanan.

UCAPAN TERIMA KASIH

Terima Kasih kepada Ketua STMIK Sumedang, Bpk. Dwi Yuniarto, S.Sos., M.Kom yang telah memberikan izin penelitian. Semua pihak terutama UPT.LPSI yang sudah memberikan akses dan izin untuk melakukan uji coba keamanan informasi.

DAFTAR PUSTAKA

[1] Albone, Aan. 2011. Analisis Dan Mitigasi Risiko Teknologi Informasi .Jurusan Teknik Informatika, Universitas Pasundan Bandung.

[2] Gunawan, Bambang. Merry, Nelly. 2011. *Information Technology Risk Assessment: Octave-S Approach*. Fakultas Ilmu Komputer Universitas Bina Nusantara. Mei

[3] Sumantri, Iwan,. 2013. ID-SIRTII/CC Founder JABAR-CSIRT. Seminar Indonesia Security Incident Response Team On Internet Infrastructure.
[4] Maryuni, Bekti Susanto,. 2013. Mengukur Keamanan Informasi : Studi Komparasi ISO 27002 dan NIST SP 800-55. Program Studi Manajemen Informatika, AMIK BSI YOGYAKARTA. Seminar Nasional Teknologi Informasi dan Komunikasi 2013. Yogyakarta.
[5] Rudy M. Harahap, Marisa Caroline Subita, Shinta Octavia. 2009. Pengukuran Risiko Aset Teknologi Informasi Berbasis Pbi Pada Sektor Perbankan Di Indonesia. Fakultas Ilmu Komputer Universitas Bina Nusantara.
[6] Supradono, Bambang. 2009. Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metoda Octave (*Operationally Critical Threat, Asset, And Vulnerability Evaluation*). Jurnal Unimus Vol 2 2009.
[7] Susanto, B. M., & Wahyudi, M. (2012). Sistem Manajemen Keamanan Informasi Pada Organisasi Kesehatan Berdasarkan ISO 27799. *Seminar Nasional Ilmu Komputer* (ss. 65-72). Semarang: Graha Ilmu.
[8] Hendra Sandi Firmansyah. 2010. Implementasi Framework Manajemen Risiko terhadap penggunaan teknologi perbankan. STMIK Jabar Bandung.
http://www.educause.edu/library/resources/information-security-program-assessment-tool, diakses pada tanggal 30 Juni 2014 Pukul 09.00 WIB.
[9] Joint Task Force Transformation Initiative, 2011. SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View.
[10] *National Institute of Standards and Technology Special Publication 800-30, Revision 1,*. 2011. *Guide for Conducting Risk Assessments, (Projected Publication Spring 2011).*
[11] Ross, R.S., 2009. Recommended Security Controls for Federal Information Systems and Organizations [includes updates through 9/14/2009]. *Special Publication (NIST SP)-800-53 Rev 3*.
[12] Chew, E., Swanson, M.M., Stine, K.M., Bartol, N., Brown, A. and Robinson, W., 2008. Performance measurement guide for information security. *Special Publication (NIST SP)-800-55 Rev 1*.
[13] NIST. 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.
[14] Ross, R.S. and Johnson, L.A., 2010. Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans. *Special Publication (NIST SP)-800-53A Rev 1*.
[15] NIST. (2012). *Security And Privacy Control For Federal Information Systems And Organizations.* Gaithersburg: National Institute Standard And Technology US. Department Of Commerce
[16] Deni Ahmad, R Teduh Dirgahayu, Hendrik. 2013. Manajemen Risiko Sistem Informasi Akademik pada perguruan tinggi Menggunakan Octave Allegro. Seminar Nasional Aplikasi Teknologi Informasi (SNATI). Yogyakarta.
[17] R Werlinger, K Muldner, K Hawkey, K Beznosov. 2010. Preparation, detection, and analysis : 2010. the diagnostic work of IT security incident response. Information Management & Computer Security 18 (1), 26-42
[18] Djohanputro, Bramantyo. 2008. Manajemen Risiko Korporat. Penerbit PPM. Jakarta.
[19] Fahmi, Irfan. 2010. MANAJEMEN RISIKO Teori, Kasus dan Solusi. Alfabeta : Bandung.
[20] Jill Slay, Andy Koronios. 2006. *Information Technolog Security & Risk Management. John Wiley & Sons*.
[21] O'Hanley, Richard., Tiller, James S. 2014. *Information Security Management Handbook Sixth Edition Volume 7*.. *Taylor & Francis Group, LLCCRC Press is an imprint of Taylor & Francis Group, an Informa business*.
[22] Peltier, Thomas R. 2010. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Aurbach Publication.*
[23] Sugiyono, 2009, Metode Penelitian Kuantitatif, Kualitatif dan R&D, Bandung : Alfabeta.
[24] Wheeler, Evan. 2011. *Security Risk Management Building an Information Security Risk Management Program from the Ground Up.* Syngress is an imprint of Elsevier 225 Wyman Street, Waltham, MA 02451, USA.
[25] Rizkie, Caroline Putri. 2011. Penerapan Manajemen Risiko Untuk Meningkatkan Keamanan Informasi (Studi Kasus: Divisi IT Security PT.XYZ).Thesis Magister Ilmu Komputer . Universitas Binus. Jakarta.
[26] Lane, Tim. 2007. Information Security Management in Australian University – An Exploratory Analysis, *Thesis*