Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 3, No. 2, Februari 2019, hlm. 1701-1707 http://j-ptiik.ub.ac.id

Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)

Fadzri Ahdi Anshori[1], Suprapto[2], Andi Reza Perdanakusuma[3]

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]fadzriahdi@gmail.com, [2]spttif@ub.ac.id, [3]andireza@gmail.com

Abstrak

Kepolisian daerah Banten merupakan pelayanan publik yang disediakan oleh pemerintah untuk mengamankan dan menegakkan hukum yang berlaku di indonesia khusus nya pada daerah kota Kegiatan operasional pada Kepolisian Daerah Banten telah didukung dengan teknologi informasi, namun penerapan teknologi informasi pada kantor Kepolisian daerah Banten belum memiliki kebijakan terkait dengan keamanan informasi dan manajemen resiko. Tujuan penelitian ini adalah untuk memberikan rencana mitigasi risiko yang tepat untuk bidang IT Kepolisian Daerah Banten. Pemberian rencana mitigasi risiko dapat diperoleh dengan mengidentifikasi dan menilai risiko yang ada pada bidang IT Kepolisian daerah Banten berdasarkan metode OCTAVE. Rekomendasi mitigasi risiko diberikan sesuai dengan standard ISO 27001 dan diprioritaskan berdasarkan cost and benefit dari masing-masing tindakan rekomendasi. Hasil akhir dari penelitian ini terdapat 28 risiko yang mungkin terjadi pada bidang IT Kepolisian daerah Banten dengan nilai RPN tertinggi sebesar 240 hingga nilai RPN terendah sebesar 18. Rekomendasi mitigasi risiko dapat dilakukan dengan 11 kontrol yang terdapat pada ISO27001.

Kata kunci: *Analisis Risiko, Keamanan Informasi, Teknologi informasi, OCTAVE, ISO27001.*

Abstract

Banten Regional Police is a public service provided by the government to secure and enforce the law in force in Indonesia, especially in urban areas. Operational activities at the Banten Regional Police have been supported by information technology, but the application of information technology in Banten Regional Police has not had a policy regarding information security and risk management. The purpose of this study is to provide a risk mitigation plan that is appropriate for the Banten Regional Police. Provisions on risk mitigation plans can be obtained by identifying and assessing the risks in the Banten Regional Police based on the OCTAVE method. Risk mitigation recommendations are provided in accordance with ISO 27001 standards and prioritized based on the costs and benefits of each recommendation action. The final results of this study, there are 28 risks that may occur in Banten Regional Police with the highest RPN value 240 to the lowest RPN value 18. Risk mitigation recommendations can be made with 11 controls contained in ISO27001.

Keywords: *Risk Analysis, Information Security, Teknologi Informasi, OCTAVE, ISO27001*

1. PENDAHULUAN

Saat ini kebutuhan teknologi informasi semakin meningkat dalam menunjang berjalannya proses bisnis secara efektif dan efisien pada suatu organisasi atau institusi. Penerapan teknologi informasi yang tepat dan sesuai kebutuhan pengguna akan mendukung kelancaran pelaksanaan operasional organisasi. Dalam bisnis, informasi sering menjadi salah satu aset paling penting yang dimiliki oleh perusahaan. Menurut Rhodes informasi membedakan perusahaan dan memberikan pengaruh yang membantu satu perusahaan menjadi lebih sukses dari yang lain

Menurut Raharjo keamanan informasi sering kali kurang mendapatkan perhatian dari para pengelola teknologi informasi. Apabila mengganggu peformasi dari sistem, sering kali keamanan dikurangi atau ditiadakan.

Perencanaan keamanan informasi diterapkan untuk mengurangi kerentanan dan menurunkan potensi terhadap resiko yang dapat terjadi pada teknologi informasi. Analisis resiko digunakan untuk mengetahui ancaman yang dapat timbul dan berdampak terhadap informasi yang dimiliki oleh instansi.

Kantor Kepolisian Daerah Banten adalah instansi yang memberikan pelayanan kepada publik yang diberikan oleh pemerintah dan bertugas dalam melakukan keamanan negara dan menegakkan hukum yang berlaku Kantor Kepolisian Daerah Banten telah menerapkan teknologi informasi dan sudah membentuk sebuah departemen untuk mengelola aktivitas IT dengan baik. Penerapan teknologi informasi pada bidang IT Kepolisian Daerah Banten belum memiliki kebijakan terkait dengan keamanan informasi dan manajemen resiko. Hal tersebut dapat meningkatkan kerentanan terhadap keamanan informasi dan tidak ada pihak yang bertanggung jawab atas resiko yang terjadi. Dengan kendala yang telah diuraikan, untuk mengantisipasi resiko keamanan informasi dapat dilakukan perencanaan keamanan informasi dengan mengalisis resiko yang dapat berdampak terdahap teknologi informasi.

Penelitian sebelumnya yang dilakukan oleh Balqis Lembah Mahersmi dengan menggunakan metode OCTAVE dan ISO 27001, dapat disimpulkan bahwa keamanan informasi dapat ditingkatkan dengan menganalisis aset yang digunakan untuk mengelola informasi tersebut serta risiko yang dapat terjadi pada aset tersebut. Metode Untuk menganalisis aset dan risiko dapat dilakukan dengan menggunakan metode OCTAVE. Untuk framework ISO 27001 dapat diimplementasikan untuk membatu perbaikan serta meningkatkan keamanan informasi pada instansi.

Pada penelitian ini peneliti mencoba mengimplementasikan suatu analisis manajemen risiko menggunakan metode OCTAVE dalam mengidentifikasi aset dan risiko yang dapat terjadi serta didukung dengan menggunakan metode FMEA untuk memberikan penilaian terhadap risiko yang telah teridentifikasi sebelumnya. ISO 27001 merupakan salah satu standar Internasional ini yang telah dipersiapkan untuk memberikan persyaratan untuk menetapkan, menerapkan, memelihara dan terus meningkatkan sistem manajemen keamanan informasi.

2. LANDASAN KEPUSTAKAAN

2.1 Keamanan Informasi

Informasi adalah aset yang sangat penting bagi orgnasisasi. Keamanan informasi merupakan usaha untuk melindungi aset informasi dalam segala bentuknya, baik tertulis, lisan, elektronik, grafis dan lain-lain. Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu aspek kerahasiaan, ketersediaan, dan ketersediaan informasi dan mencegah hal-hal yang dapat terjadi seperti kerusakan, kehilangan atau juga informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak bertanggung jawab.

2.2 Manajemen Risiko

Menurut Rhoes pada tahun 2013 mengurangi risiko tidak berarti menghilangkannya, tetapi mengurangi resiko ke tingkat yang dapat diterima oleh organisasi tersebut. Untuk memastikan keamanan informasi, mengendalikan dan mengantisipasi risiko secara efektif diperlukan analisis resiko, definisi ancaman dan dampak dari resiko tersebut. Dengan mengidentifikasi resiko,hal ini dapat memberikan strategi yang tepat untuk keamanan informasi dan mengurangi kemungkinan area risiko berdampak pada aset penting tidak terlindungi. Tujuan utama dari manajemen risiko adalah memberikan gambaran terhadap kemungkinan ancaman yang bisa terjadi sehingga perusahaan dapat menyusun strategi dan langkah untuk mitigasi dan evaluasi risiko.

Stonebumer, Goguen, & Feringa menjelaskan terdadpat 6 perlakuan mitigasi risiko yaitu :

1. Risk Assumption , untuk menerima potensi risiko dan terus mengoperasikan sistem TI atau menerapkan kontrol untuk menurunkan risiko ke tingkat yang dapat diterima
2. Risk Avoidance, untuk menghindari risiko dengan menghilangkan penyebab risiko dan / atau konsekuensi (mis., Melupakan fungsi-fungsi tertentu dari sistem atau mematikan sistem ketika risiko diidentifikasi)
3. Risk Limitation , untuk membatasi risiko dengan menerapkan kontrol yang meminimalkan dampak merugikan dari suatu ancaman yang menggunakan kerentanan (mis., Penggunaan kontrol pendukung, pencegahan, detektif)

4. Risk Planning, untuk mengelola risiko dengan mengembangkan rencana mitigasi risiko yang memprioritaskan, mengimplementasikan, dan mempertahankan kontrol
5. Research and Acknownledge, untuk menurunkan risiko kerugian dengan mengakui kerentanan dan meneliti kontrol untuk memperbaiki kerentanan
6. Pengalihan Risiko, untuk mentransfer risiko dengan menggunakan opsi lain untuk mengkompensasi kerugian, seperti membeli asuransi.

2.3 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) merupakan pendekatan untuk mengelola risiko keamanan informasi. Teknik ini memanfaatkan pengetahuan seseorang tentang praktik dan proses keamanan pada organisasi mereka untuk melihat keadaan praktik keamanan saat ini pada organisasi tersebut.

2.4 FMEA

Failure Mode and Effect Analysis (FMEA) merupakan metode yang digunakan untuk mengidentifikasi dan memahami sepenuhnya kemungkinan mode kegagalan dan penyebabnya, dan efek kegagalan pada sistem, produk atau proses tertentu. FMEA memprioritaskan masalah dengan menilai risiko yang terkait dengan mode kegagalan yang teridentifikasi, efek dan penyebab, serta tindakan korektif sesuai dengan tingkat penilaian *severity*, *occurence* dan *detection*.

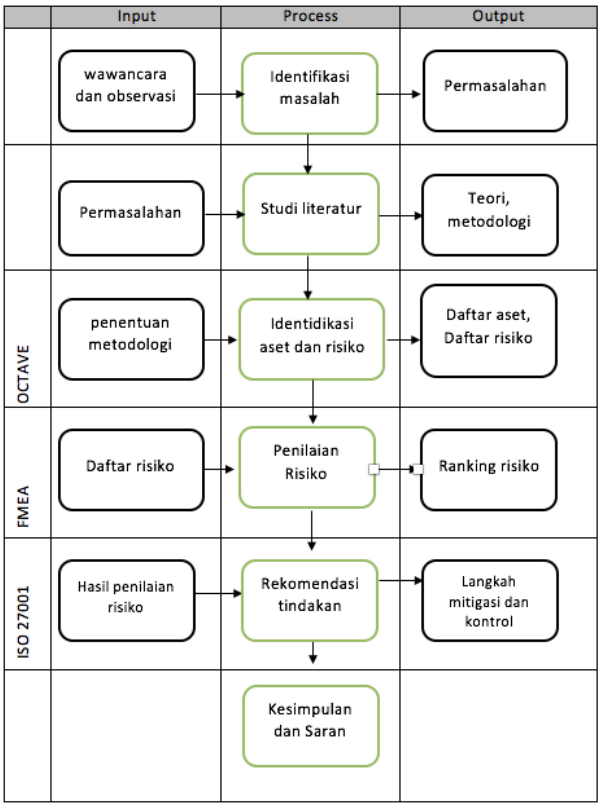
RPN (*Risk Priority* Number) merupakan nilai yang digunakan untuk menentukan prioritas dari risiko/kegagalan. Nilai RPN dapat diperoleh dengan menjumlah kan hasil perkalian nilai *severity*, nilai *occurence* dan nilai *detection*.

RPN = *Severity* x *Occurence* x *Detection*

2.5 ISO 27001

ISO 27001 ini merupakan sebuah standar yang dikeluarkan oleh I*nternational Organization for Standardization*, standar ini ditujukan untuk membantu perusahaan dalam melindungi keamanan aset perusahaan dengan memberikan rekomendasi pengelolaan sistem manajemen keamanan informasi. SMKI merupakan sebuah pendekatan yang bersifat sistematis yang bertujuan untuk mengelola informasi penting maupun informasi perusahaan yang bersifat sensitif agar tetap aman. Pada ISO 27001 terdapat klausul yang dapat digunakan untuk proses mitigasi dan kontrol terhadap risiko yang teridentifikasi.

3. METODOLOGI



Gambar 1. Alur penelitian

3.1. Identifikasi Masalah

Identifikasi masalah dilakukan dengan mengidentifikasi permasalahan objek yang terkait dalam penelitian yakni pada kantor Kepolisian Daerah Banten. Identifikasi permasalahan mengenai analisis risiko keamanan teknologi informasi dengan melakukan wawancara serta observasi.

3.2 Studi literatur

Studi literatur dilakukan dengan mencari dan mempelajari teori-teori yang berkaitan terhadap penelitian sejenis yang pernah dilakukan sebelumnya atau teori-teori tersebut berasal dari buku, jurnal, ebook yang mendukung penelitian ini serta untuk mengetahui teknik-teknik dan metode yang akan digunakan dalam pengumpulan data, pengolahan data dan penyelesaian permasalahan yang ada

3.3 Identifikasi Aset dan Risiko

Pada tahap ini dlakukan untuk mengidentifikasi risiko dengan cara menentukan aset penting bagi instansi saat ini serta kerentanan yang ada pada instansi. Pada tahap ini dilakukan melalui 4 proses, yaitu:

1. Melakukan survey dengan senior management
2. Melakukan survey dengan staff IT
3. Melakukan survey dengan operational IT
4. Membuat daftar aset, daftar aset penting bagi instansi, penerapan keamanan yang telah dilakukan oleh instansi dan ancaman yang dapat terjadi pada aset tersebut.

3.4 Penilaian Risiko

Penilaian terhadap risiko yang telah teridentifikasi dengan melakukan penerapan metode FMEA untuk menentukan tingkat *severity*, *occutance*, dan *detection*. Pada proses ini penilaian tingkat potensi risiko akan dihitung menggunakan RPN (*Risk Priority Number*).

3.5 Rekomendasi Tindakan

Rekomendasi diberikan sesuai dengan kebutuhan pada instansi dengan hasil analisis data yang telah dilakukan dan berdasarkan dengan control yang terdapat pada ISO 27001 untuk menawarkan solusi mitigasi dan langkah yang harus dilakukan dalam menyelesaikan permasalahan yang ada.

4. HASIL DAN PEMBAHASAN

4.1 Identifikasi Aset Kritis

Daftar aset kritis yang dimiliki oleh bidang IT Kepolisisan daerah Banten didapatkan dengan melakukan wawancara tatap muk secara langsung dengan kepala bidang IT Kepolisian daerah Banten serta melakukan observasi bahwa aset tersebut benar-benar dimiliki. Berikut merupakan tabel dari hasl identifikasi aset.

Tabel 1. Daftar Aset Kritis

No.	Kategori	Aset
1	Hardware	PC
2		Server
3		AC
4		Perangkat Video Conference
5		Router
6		Kabel Jaringan
7	Software	Aplikasi Hilang temu ranmor
8		Aplikasi Pusiknas
9	Network	Jaringan Internet
10	People	Admin
11	Information	Data Hilang temu ranmor
12		Data Informasi Kriminalitas Nasional

4.2 Identifikasi Ancaman

Identifikasi ancaman ditentukan dengan melakukan *brainstorming* dengan ketua divisi IT serta personil yang bekerja di bidang IT. Proses identifikasi ancaman dilakukan dengan menentukan kejadian yang memiliki probabilitas terjadinya risiko baik disebabkan oleh faktor internal maupun eksternal.Hasil dari identifikasi ancaman dapat dilihat pada tabel 2.

Tabel 2. Identifikasi Ancaman

No	Ancaman
1	Kerusakan fisik aset
2	Power failure
3	Memori penuh
4	Server down
5	Kerusakan sistem pada aset
6	Pencurian perangkat aset
7	Power failure
8	Penyalahgunaan Aplikasi
9	Terserang virus
10	Serangan hacker
11	Penyalahgunaan Hak akses
12	Kehilangan data atau informasi
13	Pencurian data atau informasi
14	Kecepatan internet yang tidak stabil
15	kerusakan Infrastruktur jaringan
16	Kabel terputus
17	Penyalahgunaan teknologi informasi
18	Menggunakan teknologi informasi yang tidak sesuai dengan fungsinya

4.3 Penerapan Keamanan

Pada tahap ini, dilakukan penyebaran survei kepada 7 responden untuk mengetahui penerapan keamanan yang telah dilakukan, yang nantinya akan digunakan untuk mengetahui kerentanan yang ada pada instansi. Hasil survei menunjukkan terdapat 7 poin kerentanan mengenai keamanan pada instansi tersebut.

4.4 Komponen Kunci

Komponen kunci merupakan jenis perangkat yang berperan penting dalam memproses, menyimpan, atau mentransmisikan informasi penting. Perangkat tersebut mewakili aset yang terkait dengan aset penting.

4.5 Identifikasi Risiko

Pada tahap identifikasi risiko, dapat dilihat dari dua aspek utama yaitu kemungkinan ancaman serta kerentanan yang dimiliki oleh instansi tersebut. Hasil identifikasi risiko dapat dilihat pada tabel 3 berikut.

Tabel 3. Identifikasi Risiko

No	Aset	Ancaman
1	PC	Kerusakan fisik aset
2		Power failure
3		Memori penuh
4	Server	Server down
5		Memori penuh
6		Kerusakan fisik aset
7	AC	Kerusakan fisik aset
8		Power failure
9	Router	Kerusakan fisik aset
10		Power failure
11	Aplikasi Hilang Temu Ranmor	Penyalahgunaan Aplikasi
12		Terserang virus
13		Serangan hacker
14		Penyalahgunaan Hak akses
15	Aplikasi PUSIKNAS	Penyalahgunaan Aplikasi
16		Terserang virus
17		Serangan hacker
18		Penyalahgunaan Hak akses
19	Informasi Hilang Temu Ranmor	Kehilangan data atau informasi
20		Pencurian data atau informasi
21	Informasi Kriminalitas Nasional	Kehilangan data atau informasi
22		Pencurian data atau informasi
23	Jaringan Internet	Kecepatan internet yang tidak stabil
24	Kabel Jaringan	kerusakan Infrastruktur jaringan
25		Kabel terputus
26	Admin	Pencurian data atau informasi
27		Menggunakan teknologi informasi yang tidak sesuai dengan fungsinya
28		Penyalahgunaan hak akses

5. ANALISIS

5.1 Penilaian Risiko

Berdasarkan hasil risiko yang telah teridentifikasi, penilaian risiko dilakukan berdasarkan 3 parameter yaitu keparahan (*severity*), kejadian (*occurrence*), dan deteksi (*detection*). Hasil dari penilaian risiko akan digunakan untuk menentukan prioritas risiko yang akan diberikan perhatian terlebih dahulu.

5.2. Ranking Risiko

Pada tahap ini daftar risiko akan diurutkan berdasarkan hasil perhitungan nilai *Risk Priority Number* yang tertinggi hingga terendah berdasarkan risiko pada masing-masing aset.

6. REKOMENDASI

6.1 TOP IT Risk

Top IT Risk dijabarkan sesuai dengan risiko dari seluruh aset yang memiliki potensi mulai dari level *moderate* hingga *very high* untuk diberikan rekomendasi pengendalian risiko.

6.2 Mitigasi Risiko

Pada tahap ini peneliti memberikan rekomendasi pengendalian risiko pada setiap bentuk risiko yang memili potensi *moderate* hingga *very high*. Hasil rekomendasi pengendalian risiko akan ditunjukkan pada tabel berikut.

Tabel 4. Rekomendasi Pengendalian Risiko

Aset	Risiko	Rekomendasi	Jenis Pengendalian
PC	Kerusakan fisik	A.11.2.1 *Equipment siting and protection*	Risk planning
		A.11.1.1 *Physical security parameter*	Risk limitation
Server	Kerusakan fisik	A.11.2.1 *Equipment siting and protection*	Risk planning

		A11.1.4 Protecting against external and environmental threats	Risk planning
	Server down	A.11.2.2 *Supporting Utilities*	Risk avoidance
Aplikasi hilang temu ranmor	Terserang virus	A.12.2.1 *Control against Malware*	Risk planning
		A.12.5.1 *Restriction on software installation*	Risk limitation
Aplikasi pusat informasi kriminalitas nasional	Terserang virus	A.12.2.1 *Control against Malware*	Risk planning
		A.12.5.1 *Restriction on software installation*	Risk limitation
Informasi hilang temu ranmor	hilang data atau informasi	A.12.3.1 *Information Backup*	Risk planning
Kabel jaringan	Kabel jaringan terputus	A.11.2.3 *Cabling Security*	Risk assumption
Sumber daya manusia	Menggunakan teknologi informasi yang tidak sesuai dengan fungsinya	A.7.2.3 *Disciplinary process*	Risk planning
		A.12.1.1 Documented operating procedures	Risk planning

6.3. Rekomendasi Pengendalian Risiko

Pada tahap ini akan memberikan rekomendasi pengendalian risiko yang tepat pada masing-masing risiko dengan menentukan rincian biaya serta keuntungan yang akan diperoleh dari setiap pilihan pengendalian risiko. Hal sering dikatakan sebagai *cost and benefit analysis* yaitu menganalisa dampak apabila digunakan rekomendasi pengendalian serta apabila tidak digunakan rekomendasi pengendalian risiko.

7. KESIMPULAN DAN SARAN

7.1 Kesimpulan

Berdasarkan hasil penelitian yang telah telah dilakukan, maka dapat disimpulkan :

1. Terdapat 12 aset kritis yang digunakan pada bidang IT Kepolisian daerah Banten dan dikelompokkan menjadi 5 kategori aset serta 28 risiko ditemukan yang dapat terjadi pada aset kritis.
2. Hasil penilaian yang dilakukan terdapat sebanyak 2 risiko yang termasuk pada tingkat *very high*, 3 risiko yang termasuk pada tingkat *high*, 3 risiko yang termasuk pada tingkat *moderate*, 21 risiko yang termasuk pada tingak *low* dan 5 risiko yang termasuk pada level *very low*.
3. Berdasarkan hasil Identifikasi risiko dan penilaian risiko terdapat 11 kontrol pada ISO 27001 yang terdiri dari beberapa dapat digunakan untuk mencegah atau meminimalisir potensi terjadinya risiko pada bidang IT Kepolisian Daerah Banten.

7.1 Saran

Berikut ini adalah saran yang dapat berikan pada penelitian berikutnya :

1. Penelitian ini dilakukan dengan ruang lingkup pada bidang IT. Diharapkan untuk melakukan perencanaan keamanan informasi dan analisa risiko dengan ruang lingkup yang lebih besar.
2. Mengimplementasikan hasil rekomendasi yang diberikan untuk mengetahui tingkat efektifitas hasil analisa risiko dengan rekomendasi yang diberikan.

DAFTAR PUSTAKA

Alberts, C. J., Dorofee, A. J., Allen, J. H,. 2001. *OCTAVE Catalog Of Practice Version* 2.0. [ebook].

ISO/IEC 27001. 2013. *Information Technology – Security Techniques – Information Security Management Systems – Requirements*. [ebook]

Mahersmi, B. L. 2016. Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode Octave dan Kontrol ISO 27001 Pada Dishubkominfo Kabupaten Tulungagung. Institute Teknologi Sepuluh Nopember.

McDermott, Robin E., Raymond J.Mikulak & Michael R. Beauregard. 2009. The Basic Of FMEA 2nd Edition. New York : Taylor & Francis Group.

Putra, A.N. 2016. Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 27001. Universitas Diponegoro. Jurnal Teknologi dan Sistem Komputer, 4(1). 60-66.

Raharjo, B., 2002 Keamanan Informasi Berbasis Internet. Jakarta. [Ebook]

Rhodes, M., 2013. *Information Security: The Complete Reference* (2nd Edition). [Online] Tersedia di <http://www.ebook777.com/information-security-complete-reference-2nd-edition/> [diakses 14 Februari 2018].

Sadowsky, G., Dempsey, J.X., Greenberg, A., Mack, B.J., Schwartz, A., 2003. Information Technology Security Handbook. Washington, DC : The International Bank.

Tipton, H.F., Krause, M., 2006. Information Security Management Handbook. Auerbach Publication.

Watkins, S. G., 2008. An Introduction to Information Security ang ISO27001.