PERENCANAAN KEAMANAN INFORMASI BERDASARKAN ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN METODE OCTAVE DAN ISO 27001
(STUDI KASUS BIDANG IT KEPOLISIAN DAERAH BANTEN)

SKRIPSI

Untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun oleh:
Fadzri Ahdi Anshori
145150407111061

PROGRAM STUDI SISTEM INFORMASI
JURUSAN SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2018

PENGESAHAN

PERENCANAAN KEAMANAN INFORMASI BERDASARKAN ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN METODE OCTAVE DAN ISO 27001
(STUDI KASUS BIDANG IT KEPOLISIAN DAERAH BANTEN)

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Fadzri Ahdi Anshori
NIM: 145150407111061

Skripsi ini telah diuji dan dinyatakan lulus pada
12 Desember 2018
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Suprapto, S.T, M.T	Andi Reza Perdanakusuma, S.Kom., M.MT.
NIP. 19710727 199603 1 001	NIK. 2016078611281001

Mengetahui
Ketua Jurusan Sistem Informasi

Rekyan Tolle, Dr. Eng., S.T, M.T
NIP: 19740823200012 1001

ii

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 12 Desember 2018

Fadzri Ahdi Anshori

NIM: 145150407111061

iii

KATA PENGANTAR

Puji Syukur ke hadirat Allah SWT atas segala rahmat yang telah diberikan sehingga memberikan kemudahan dan kelancaran dalam menyelesaikan skripsi yang berjudul "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE Dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)."

Penyusunan dan penulisan skripsi ini tidak terlepas dari bantuan, bimbingan, dukungan, serta motivasi dari berbagai pihak. Namun, penulis dapat melewati hal tersebut karena anugerah dari Allah SWT. Oleh karena itu, dalam kesempatan ini penulis ingin menyampaikan terimakasih kepada:

1. Bapak Suprapto, S.T, M.T dan selaku dosen pembimbing satu yang telah dengan sabar membimbing dan mengarahkan penulis sehingga dapat menyelesaikan skripsi ini.
2. Bapak Andi Reza Perdanakusuma, S.Kom., M.MT. selaku dosen pembimbing dua yang senantiasa membimbing dan memberikan masukan kepada penulis.
3. Bapak Wayan Firdaus Mahmudy, S.Si., M.TI., Ph.D. selaku Dekan Fakultas Ilmu Komputer Universitas Brawijaya.
4. Bapak Dr. Eng., Herman Tolle, S.T., M.T. selaku Ketua Jurusan Sistem Informasi Universitas Brawijaya.
5. Bapak Yusi Tyroni Mursityo, S.Kom., M.AB. selaku Ketua Program Studi Jurusan Sistem Informasi.
6. Bapak Krisdian Yuliono, A.Md dan Bapak Dedi Sutarto, S,Kom selaku narasumber di bidang IT Kepolisian daerah Banten yang telah memberikan data.
7. Kepada bapak Agus Hamdan dan ibu Diana Fauza selaku orang tua yang selalu memberikan nasihat, motivasi dan doa kepada penulis.
8. Alwi Ahdi Fahrozi dan Aldifa Ahdi Raesah selaku kakak dan adik yang selalu membantu dan memberikan semagat kepada penulis.
9. Satrio Dwiartono, Wiratama Ahsani Taqwim, Claudio Canigia Guntara, Jebi Hayi Tamami, dan M. Taufik Dharmawan, Danny Esfarditya, Fandy Adityo selaku grup diskusi yang tidak kenal lelah menemani dan menyemangati penulis.
10. Zanetha Kumara Tunggadewi, Rahmi Maulidya, Annisa Sesyazhade, Intan Camila, Iffa Aulia Ulwani, dan Deafinansia Andiyani yang selalu siap mendorong penulis untuk menyelesaikan skripsi ini.

11. Angga Syahputra, Muhammad Furqan, Muadz Qemal, Francois Africo, Marlisa Maulana, Evan Fardian Sinuhaji yang selalu menghibur penulis dengan berbagai cara.

Malang, 12 Desember 2018

Penulis

fadzriahdi@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*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1 PENDAHULUAN

1.1 Latar belakang

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. Perkembangan teknologi informasi yang sangat pesat menjadi tuntutan bagi organisasi untuk mengikuti perubahan dan melakukan evaluasi dalam penggunaan teknologi informasi yang tepat. Hal ini menjadi aspek yang sangat penting diperhatikan dalam perencanaan strategi untuk mencapai tujuan suatu organisasi termasuk institusi pemerintahan. Dalam bisnis, informasi sering menjadi salah satu aset paling penting yang dimiliki oleh perusahaan. Informasi membedakan perusahaan dan memberikan pengaruh yang membantu satu perusahaan menjadi lebih sukses dari yang lain (Rhodes, 2013).

Keamanan informasi sering kali kurang mendapatkan perhatian dari para pengelola teknologi informasi. Apabila mengganggu peformasi dari sistem, sering kali keamanan dikurangi atau ditiadakan (Raharjo, 2002). 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. Agar penilaian risiko menjadi efektif, perlu dibuat daftar aset informasi yang komprehensif (Watkins, 2008). Artinya, daftar semua yang memiliki nilai bagi organisasi termasuk informasi, pemrosesan informasi dan peralatan penyimpanan. Kerusakan dan kehilangan informasi menjadi hal yang sangat diperhatikan, karena informasi merupakan salah satu aset yang sangat berharga bagi instansi sehingga keutuhan dan kerahasiaannya harus selalu terjaga dengan baik. Dalam menjaga keamanan informasi faktor pendukung, jaringan, dan fasilitas lainnya menjadi hal yang perlu diperhatikan dalam proses pengolahan informasi.

Kantor Kepolisian Daerah Banten adalah sebuah instansi yang memberikan pelayanan kepada publik oleh pemerintah dan bertugas dalam melakukan keamanan negara serta menegakkan hukum yang berlaku. Kantor Kepolisian Daerah Banten didirikan pada tanggal 7 Januari 2004 dengan persetujuan Kapolri. Sebelum terbentuknya provinsi sendiri, Banten merupakan wilayah hukum Kepolisian Jawa Barat. Kantor Kepolisian Daerah Banten melaksanakan upacara pelantikan yang ditandai dengan diserahkannya Pataka Polda Banten “Gawe Kuta Baluarti” dan Lambang Kesatuan Polda Banten “Kepala Harimau Putih".

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 sering terjadi permasalahan terkait dengan kehilangan serta kerusakan

informasi. Hal ini dikarenakan pada instansi tersebut belum memiliki kebijakan terkait dengan keamanan informasi dan manajemen resiko. Dengan demikian kehilangan dan kerusakan informasi pada instansi tersebut akan di pertanggung jawabkan oleh masing-masing pengguna TI.

Dengan tidak ada kebijakan yang jelas, maka organisasi menempatkan diri pada risiko yang mungkin terjadi dan tergagap dalam menanggapi permasalahan dan pelanggaran yang ada (Rhodes, 2013). 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. Dalam mengevaluasi risiko keamanan informasi dapat dilakukan dengan menggunakan pendekatan yang komprehensif yaitu OCTAVE dan memberikan usulan langkah berdasarkan standard ISO27001.

OCTAVE merupakan salah satu pendekatan terhadap evaluasi risiko keamanan informasi yang komprehensif dan sistematis (Alberts dan Dorofee, 2001). Penggunaan metode OCTAVE dalam mengidentifikasi aset dan didukung dengan menggunakan metode FMEA (*Failure Mode and Effect Analysis*) yang merupakan metode untuk mengidentifikasi dan mencegah masalah produk dan proses sebelum terjadi dan untuk menganalisa nilai potensi risiko serta mencegah terjadinya potensi kegagalan (McDermott, 2009). Hal ini dilakukan untuk membantu Kepolisian Daerah Banten untuk mengetahui nilai risiko dan potensi risiko yang memiliki nilai tersbesar pada aset penting yang dimiliki oleh instansi. 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 (Joint Technical Commite, 2013). Standar yang dapat djadikan panduan dalam mengelola keamanan informasi yang baik dan memiliki klausul yang dapat dijadikan kontrol sebagai langkah untuk memitigasi dan pengelolaan pada risiko yang telah teridentifikasi sebelumnya.

Penelitian terdahulu 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. Dengan hasil analis tersebut dapat diberikan penilaian untuk mengetahui tingkat prioritas dari masing-masing risiko. Untuk *framework* ISO 27001 dapat diimplementasikan untuk membatu perbaikan serta meningkatkan keamanan informasi pada instansi.

Peneliti menggunakan metode OCTAVE dan ISO 27001 karena pada metode ini dapat menganalis aset penting, praktik keamanan saat ini, kerentanan organisasi serta mengindentifikasi risiko yang dapat berdampak pada teknologi informasi. pada ISO27001 terdapat kontrol yang dapat dilakukan instansi untuk mengelola dan mengetahui langkah yang harus dilakukan untuk

mengurangi potensi risiko. Dari hasil analisis tersebut dapat dijadikan sebagai usulan manajemen keamanan informasi pada instansi. Atas dasar latar belakang dan permasalahan yang ada, peneliti mengajukan judul penelitian "PERENCANAAN KEAMANAN INFORMASI BERDASARKAN ANALISIS RESIKO TEKNOLOGI INFORMASI MENGGUNAKAN METODE OCTAVE DAN ISO27001".

1.2 Rumusan masalah

Berdasarkan latar belakang yang telah diuraikan, didapatkan rumusan masalah sebagai berikut:

1. Apa aset penting dan risiko yang dapat berdampak pada teknologi informasi pada bidang IT kepolisian daerah banten?
2. Bagaimana potensi risiko yang teridentifikasi terhadap aset yang dimiliki bidang IT kepolisian daerah banten?
3. Bagaimana usulan langkah yang harus dilakukan terhadap risiko yang ada pada bidang IT kepolisian daerah banten?

1.3 Tujuan

Adapun tujuan dilakukannya penelitian ini adalah sebagai berikut :

1. Untuk mengetahui aset penting dan risiko yang dapat berdampak pada teknologi informasi pada bidang IT kepolisian daerah banten.
2. Memberikan penilaian terhadap risiko untuk mengetahui potensi dan prioritas masing-masing risiko.
3. Memberikan rekomendasi untuk langkah pencegahan terhadap risiko pada bidang IT Kantor Kepolisian Daerah Banten.

1.4 Manfaat

Adapun Manfaat dari penelitian ini adalah sebagai berikut :

1. Membantu instansi dalam melakukan peningkatan keamanan informasi yang diterapkan pada instansi.
2. Peneliti dapat menambah pengentahuan dalam melakukan evaluasi keamanan informasi dan analisis resiko.
3. Menambah informasi dalam melakukan perencanaan keamanan informasi pada instansi.

1.5 Batasan masalah

Berdasarkan rumusan masalah yang ada, maka peneliti membatasi masalah yang akan di bahas sebagai berikut :

1. Perencanaan manajemen keamanan informasi dibuat berdasarkan analisis risiko pada instansi.
2. Analisis resiko dilakukan menggunakan metode OCTAVE .
3. Penelitian dilakukan di bidang IT Kepolisian Daerah Banten.

4. Penilaian ini tidak membahas hasil dari penerapan ISO 27001 ke dalam Kepolisian daerah Banten

1.6 Sistematika pembahasan

Adapun sistematika penulisan laporan yang digunakan dalam menyusun laporan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Berisi gambaran singkat tentang latar belakang, tujuan, rumusan masalah, batasan masalah, manfaat, dan sistematika penulisan laporan.

BAB II LANDASAN KEPUSTAKAAN

Berisi uraian mengenai teori-teori yang digunakan sebagai landasan atau acuan penelitian serta literatur-literatur ilmiah yang baik berupa jurnal, buku maupun penelitian terlebih dahulu

BAB III METODOLOGI PENELITIAN

Berisi tentang metodologi atau proses yang digunakan saat melakukan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Berisi tentang uraian hasil pengumpulan data yang dibutuhkan untuk proses analisis risiko dan perencanaan keamanan informasi teknologi informasi.

BAB V ANALISIS

Bab ini menjelaskan tentang proses analisis penilaian menggunakan metode FMEA

BAB VI REKOMENDASI

Berisi tentang hasil rekomendasi yang dapat diberikan untuk memperbaiki tata kelola yang telah diterapkan pada bidang IT Kepolisian Daerah Banten.

BAB VII PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang menjawab rumusan masalah dan saran yang diberikan untuk digunakan dalam penelitian selanjutnya

BAB 2 LANDASAN KEPUSTAKAAN

2.1 Kajian Pustaka

Perencanaan keamanan informasi menggunakan metode OCTAVE dapat membantu perusahaan dalam meningkatkan keamanan informasi. Seperti penelitian yang pernah dilakukan sebelumnya oleh Balqih Lembah pada tahun 2016 yang berjudul "Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE dan Kontrol ISO 27001 Pada Dishubkominfo Kabupaten Tulungagung". Penelitian ini membahas identifikasi aset dan risiko menggunakan metode OCTAVE dan ISO 27001. Tahapan yang digunakan untuk penelitian ini terdiri dari identifikasi masalah, identifikasi aset, identifikasi risiko, penilaian risiko, mitigasi risiko dan pemberian rekomendasi. Metode OCTAVE digunakan pada proses identifikasi aset dan risiko agar memudahkan dalam menemukan kelemahan-kelemahan pada aset. Peneliti menggunaan kerangka kerja ISO 2700 sebagai langkah kontrol atau tindakan yang dapat digunakan oleh organisasi untuk melakukan mitigasi risiko yang sudah diidentifikasi sebelumnya. Berdasarkan hasil analisis dari data yang telah diperoleh, peneliti dapat menyimpulkan dari 31 kejadian risiko didapatkan 13 risiko uang memiiki tingkat risiko dapat terjadi lebih dari satu kali. Dari hasil penilaian risiko terdapat 4 risiko dengan tingkat kejadian *very high*, 2 risiko dengan tingkat kejadian *high*, 7 risiko dengan tingkat kejadian *medium*, 13 risiko dengan tingkat kejadian *low* dan 5 risiko dengan tingkat kejadian *very low*. Hasil identifikasi risiko tersebut, terdapat 12 kontrol pada ISO 27001 yang dapat dijadikan acuan penentuan rekomendasi mitigasi risiko.

Penelitian selanjutnya yang digunakan sebagai acuan dalam mendukung penelitian ini dilakukan oleh Anggi Anugraha Putra dengan judul penelitian "Perencanaan dan Implementasi Informasi Security Menggunakan Framework ISO/IEC 27001" penelitian ini membahas tentang pelaksanaan identifikasi aset dengan menentukan tingkat kritikalitas dan melakukan analisis kecenderungan dampak risiko. Identifikasi aset dan risiko dibantu dengan kerangka kerja ISO 27001 untuk mengetahui kondisi keamanan informasi saat ini dan pemetaan klausul terhadap aset. Penelitian ini dibantu dengan metode penilaian indeks kami untuk mengetahui penerapan yang telah dilakukan oleh organisasi saat ini. Hasil penelitian mengidentifikasi ada 34 aset yang dikategorikan dengan tingkat risiko kritikal dan 8 aset yang dikategorikan dengan tingkat risiko tidak kritikal.

Penelitian lain dilakukan oleh Chanchala Joshi dengan judul "*Information security risks management framework – A step towards mitigating security risks in university network*". Dalam penelitian ini membahas tentang tentang evaluasi terhadap manajemen keamanan informasi pada jaringan universitas Vikram. Penyelesaian masalah dilakukan dengan menggunakan metode kuantitatif dengan mengidentifikasi aset, kebutuhan kemanan, identifikasi kerentanan dan ancaman, analisis kontrol yang dilakukan saat ini, mengukur potensi risiko, mengukur dampak risiko, membuat rencana tindakan pada risiko, membuat

laporan untuk mendukung keputusan, dan membuat usulan yang dapat dilakukan pada universitas tersebut. Berdasarkan hasil identifikasi risiko, Chanchala Joshi menemukan kerentanan terhadap risiko injeksi SQL. Injeksi SQL adalah serangan yang dapat dilakukan oleh para peretas untuk dapat mengubah sifat program sesuai dengan kepentingan peretas (*Hacker).* Selain itu, kerentanan yang teridentifikasi adalah kata sandi (*password*) yang lemah. Ada beberapa langkah yang diusulkan untuk mengatasi kerentanan tersebut, salah satunya adalah membuat kebijakan kata sandi, seperti minimal karakter pada kata sandi dan menggunakan *uppercase* atau angka. Untuk meningkatkan kemanan pada informasi peneliti mengusulkan untuk menggunakan metode OCTAVE. Meotde yang diusulkan berbasis operasional, implementasi praktis dari model yang diusulkan secara signifikan mengklarifikasi informasi apa yang dibutuhkan, bagaimana itu digunakan dan diproses dan apa informasi yang dihasilkan.

2.2 Profil Kepolisian Daerah Banten

2.2.1 Sejarah

Kepolisian Daerah Banten merupakan pelayanan publik yang disediakan oleh pemerintah untuk mengamankan dan menegakkan hukum yang berlaku di indonesia. Kantor Kepolisian Daerah Banten terletak di provinsi banten dengan membawahi kantor kepolisian wilayah Polres Serang, Polres Pandeglang, Polres Lebak, Polres Cilegon dan Polres Tanggerang. Keberadaan Kepolisian Daerah Banten merupakan eksistensi dari Kepolisian Wilayah Banten dibawah naungan Kepolisian Daerah Jawa Barat. Seiring perkembangan Kepolisian Daerah Jawa Barat mengusulkan untuk pembentukan provinsi Banten dikarenakan jumlah penduduk yang terus bertambah yaitu 4,3 juta jiwa pada tahun 2001 sementara jumlah Polisi wilayah Banten hanya 1980 personel. Atas dukungan Markas Besar Kepolisian Negara Republik Indonesia dan Kepolisian Daerah Jawa Barat, pada tanggal 14 Juli 2003 dilaksanakan upacara peletakan batu pertama untuk pembangunan Markas Polisi Daerah Banten oleh Kepala Polisi Daerah Jawa Barat yaitu Irjen Pol Drs. Dadang Garnida. Melalui surat keputusan Kepala Kepolisian Negara Republik Indonesia pada tanggal 7 Januari 2004, Kantor Kepolisian Daerah Banten disetujui oleh Kepala Kepolisian Negara Republik Indonesia pada tanggal 12 Januari 2004 dan melantik Kombes Pol Drs. H. Abdurachman sebagai Kepala Kepolisian Daerah Banten. Upacara pelantikan ditandai dengan diserahkannya Pataka Polda Banten “Gawe Kuta Baluarti” dan Lambang Kesatuan Polda Banten “Kepala Harimau Putih”.

2.2.2 Visi dan Misi

Visi:

Searah dengan penjabaran Visi Polri, maka Visi Polda Banten adalah Tergelarnya Polisi Daerah Banten yang dipercaya masyarakat disemua titik dan lini pelayanan masyarakat disepanjang waktu dalam mewujudkan keamanan dalam negeri dan tegaknya hukum sebagai sinergi pencapaian hasil pembangunan yang berwawasan keamanan.

Misi:

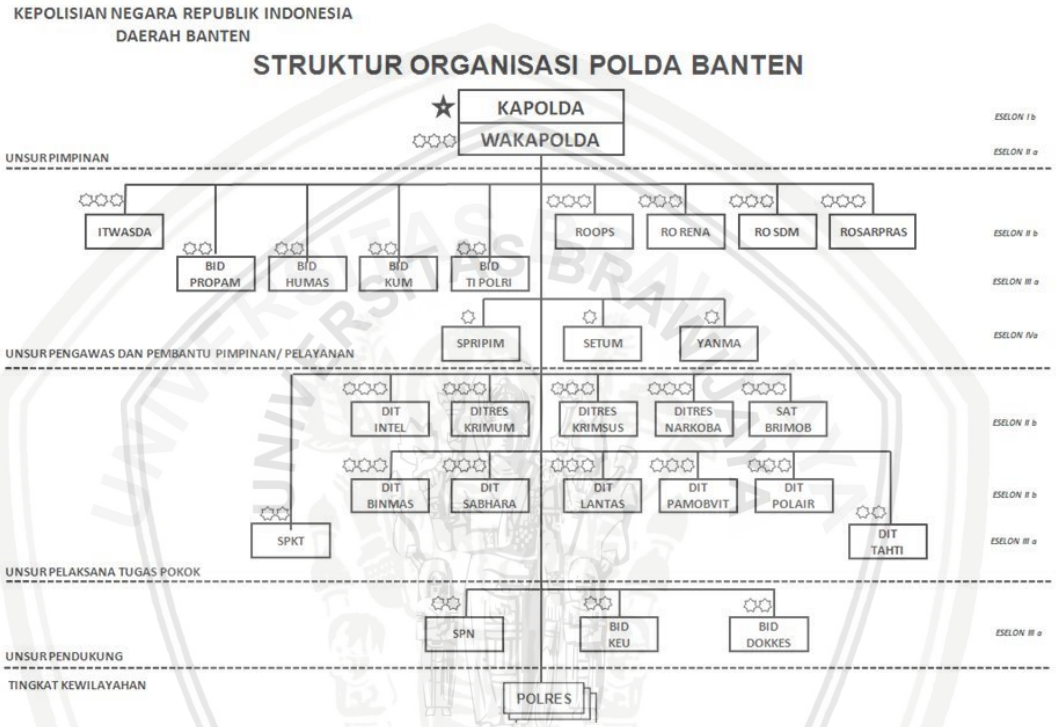
Sebagai penjabaran dari Misi Polri, dalam pelaksanaannya diuraikan dalam Misi Polda Banten sebagai berikut:

1. Pemenuhan hak-hak anggota dan meningkatkan kesejahteraan demi terwujudnya penyelenggaraan pemerintahan yang baik.
2. Melaksanakan deteksi dini dan peringatan dini melalui kegiatan / operasi penyelidikan, pengamanan dan penggalangan.
3. Memberikan perlindungan, pengayoman dan pelayanan secara mudah, responsive dan tidak diskriminatif.
4. Menjaga keamanan, ketertiban dan kelancaran lalu lintas untuk menjamin keselamatan dan kelancaran arus orang dan barang.
5. Menjamin keberhasilan penanggulangan gangguan keamanan di daerah Provinsi Banten.
6. Mengembangkan perpolisian masyarakat yang berbasis pada masyarakat patuh hukum.
7. Menegakkan hukum secara profesional, obyektif, proposional, transparan dan akuntabel untuk menjamin kepastian hukum dan rasa keadilan.
8. Mengelola secara profesional, transparan, akuntabel dan modern seluruh sumber daya Polri baik peronil, sarana dan prasarana serta anggaran guna mendukung operasional tugas Polda Banten (profesionalisme dibidang perencanaan dan anggaran).
9. Meningkatkan kerjasama keamanan dengan Instansi Pemerintah, Swasta, Pam Swakarsa, LSM, TNI dan organisasi-organisasi keagamaan, pemuda dan masyarakat lainnya.
10. Meningkatkan funsi pengawasan dan pemeriksaan dalam mewujudkan kinerja Polda yang bersih berwibawa dan terpercaya.
11. Meningkatkan pembangunan sarana dan prasarana dengan memanfaatkan perkembangan teknologi informasi dan komunikasi.
12. Membangun budaya organisasi Polri pada Polda Banten dalam meningkatkan kinerja.
13. Terwujudnya recruitment personil Polri yang bersih, transparan dan bebas dari intervensi.
14. Tertanggulanginya setiap kontijensi yang terjadi demi terciptanya keamanan masyarakat.
15. Menyelenggarakan pembinaan dan penegakan terhadap profesi kepolisian.
16. Menyelenggarakan pembinaan hukum dalam rangka pelaksanaan tugas pokok Polri.

Dari tugas-tugas Polisi tersebut dapat dikemukakan bahwa pada dasarnya tugas Polisi ada dua yaitu tugas untuk memelihara keamanan, ketertiban, menjamin dan memelihara keselamatan negara, orang, benda dan masyarakat serta mengusahakan ketaatan warga negara dan masyarakat terhadap peraturan negara (Meliyawati, 2014).

2.2.3 Struktur Organisasi

Struktur Kepolisian Daerah Banten dapat dilihat seperti pada Gambar 2.1 berikut.



Gambar 2.1 Struktur Organisasi Kepolisian Daerah Banten

2.3 Aset Informasi

Informasi adalah aset yang sangat penting, semakin banyak informasi yang dimiliki maka semakin baik anda bisa beradaptasi dengan dunia di sekitar anda (Rhodes, 2013). Dalam bisnis, informasi menjadi asset terpenting bagi organisasi karena informasi akan memberikan pengaruh dan membatu organisasi menjadi lebih bagi dari organisasi lainnya. Dalam menjaga keamanan informasi menurut Alberts dan Dorofee (2001) adalah menjaga keamanan informasi merupakan menjaga aset informasi serta aset teknologi informasi yang terkait untuk mengelola informasi tersebut, aset teknologi informasi dapat dikelompokkan menjadi beberapa kategori yaitu

1. Aset Infomasi, merupakan informasi atau data dalam bentuk elektronik atau fisik yang digunakan untuk memenuhi misi suatu organisasi.

2. Aset Perangkat lunak, merupakan aset seperti sistem operasi, aplikasi jaringan, aplikasi office, aplikasi kantor dan lain-lain.
3. Aset Perangkat keras, merupakan aset seperti perangkat komputer, server, dan lain-lain.
4. Aset Sistem, merupakan aset system informasi yang memproses dan menyimpan informasi.
5. Aset Sumber daya manusia, merupakan pegawai yang bekerja pada organisasi yang memiliki pengetahuan, kemampuan dan pengalaman yang sulit untuk digantikan.

2.4 Keamanan Informasi

Keamanan informasi merupakan usaha untuk melindungi aset informasi dalam segala bentuknya, baik tertulis, lisan, elektronik, grafis dan lain-lain (Rhodes, 2013). Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu aspek kerahasiaan, integritas, dan ketersediaan.

Gambar 2.2 Aspek-aspek Keamanan Informasi

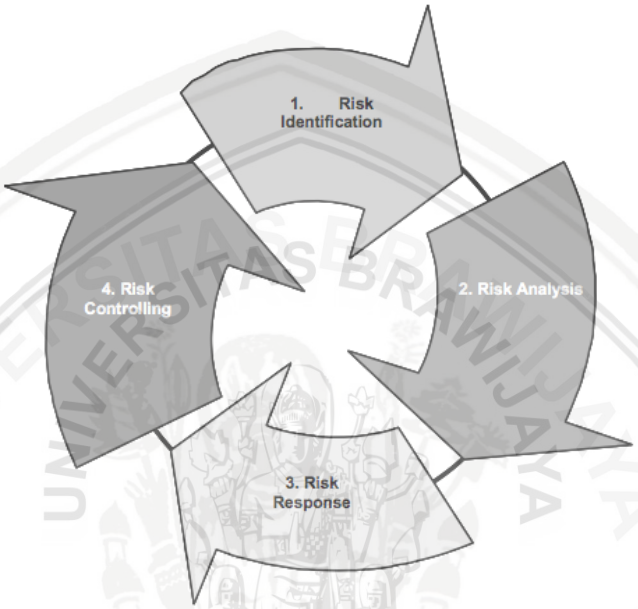
Sumber: Chazar dan Ramadhani (2016)

1. Kerahasiaan : Memastikan informasi hanya dapat digunakan oleh pihak/pemakai yang mempunyai wewenang.
2. Intergritas : Memastikan kelengkapan dan keakuratan informasi tersebut.
3. Ketersediaan : Memastikan informasi tersedia kepada pihak yang memiliki wewenang untuk menggunakannya.

2.5 Manajemen Resiko

Mengurangi risiko tidak berarti menghilangkannya, tetapi mengurangi resiko ke tingkat yang dapat diterima oleh organisasi tersebut (Rhodes, 2013).

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. Tahapan yang perlu dilakukan dalam manajemen resiko berdasarkan (Olaf, 2010) ditunjukkan pada gambar 2.3.



Gambar 2.3 Proses Manajemen Resiko

Sumber : Olaf (2010)

2.5.1 Mitigasi Risiko

Menurut Stonebumer, Goguen, & Feringa (2002) mitigasi risiko adalah tanggung jawab manajemen senior dan manajer fungsional bisnis untuk menggunakan pendekatan biaya-paling rendah dan menerapkan kontrol yang paling tepat untuk mengurangi risiko ke tingkat yang dapat diterima, dengan dampak negatif minimal terhadap sumber daya dan misi organisasi. Terdapat 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

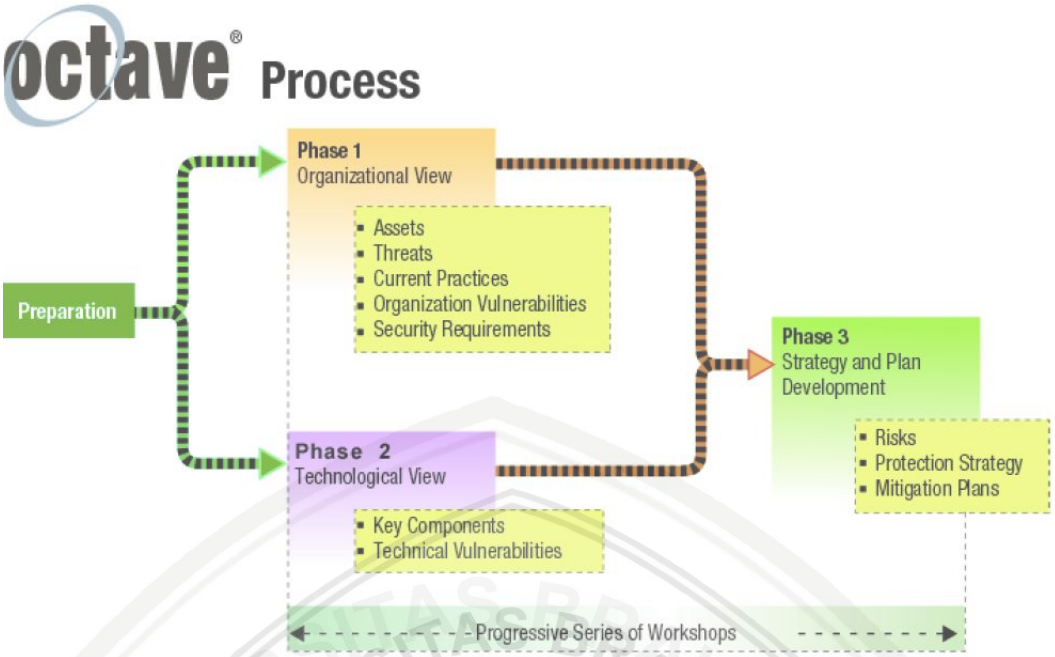
5. *Research and Acknownledge*
   Untuk menurunkan risiko kerugian dengan mengakui kerentanan dan meneliti kontrol untuk memperbaiki kerentanan

6. Pengalihan Risiko.
   Untuk mentransfer risiko dengan menggunakan opsi lain untuk mengkompensasi kerugian, seperti membeli asuransi.

2.6 OCTAVE

2.6.1 Pengertian 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 (Alberts et al, 2003). OCTAVE menggunakan fase dalam memeriksa permasalahan dan memberikan gambaran yang komprehensif tentang kebutuhan keamanan informasi organisasi. Tahapan fase pada metode OCTAVE dapat dilihat pada gambar 2.4 dibawah ini.



Gambar 2.4 Fase Metode OCTAVE

Sumber : Alberts et al (2003)

2.6.2 Fase 1 *Organizational View*

Fase ini adalah melakukan evaluasi dari organisasi. Peneliti menentukan apa yang penting bagi organisasi (informasi terkait aset) dan apa yang sedang dilakukan untuk melindungi aset tersebut. Peneliti kemudian memilih aset yang paling penting bagi organisasi (aset kritis) dan menjelaskan persyaratan keamanan untuk setiap aset penting.

2.6.3 Fase 2 *Technological View*

Pada fase ini adalah evaluasi infrastruktur informasi. Peneliti analisis memeriksa jalur akses jaringan, mengidentifikasi komponen teknologi informasi yang terkait dengan masing-masing aset penting. Peneliti kemudian menentukan sejauh mana masing-masing komponen tahan terhadap serangan jaringan.

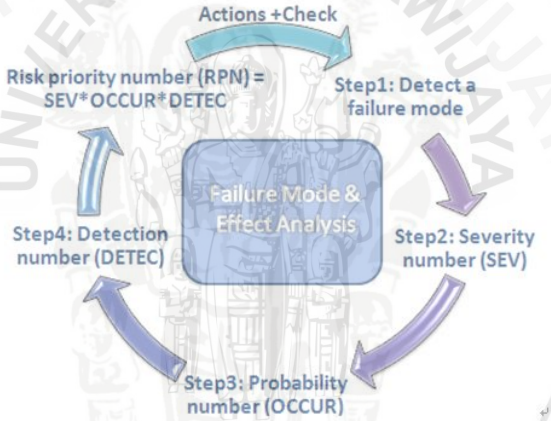
2.6.4 Fase 3 *Strategy and Plan Development*

Pada fase ini, Peneliti analisis mengidentifikasi risiko terhadap aset penting organisasi dan memutuskan apa yang harus dilakukan terhadap risiko tersebut. Peneliti menciptakan strategi perlindungan untuk rencana organisasi dan mitigasi untuk mengatasi risiko terhadap aset penting, berdasarkan analisis informasi yang dikumpulkan.

2.7 FMEA

2.7.1 Pengertian 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* (Carlson, 2014). *Severity* menggambarkan keseriusan konsekuensi kegagalan. *Occurence* menggambarkan seberapa sering kegagalan bisa terjadi. *Detection* mengacu pada tingkat kesulitan dalam mendeteksi kegagalan. FMEA dilakukan untuk mengurangi risiko dengan menghasilkan tindakan yang diprioritaskan pada potensi besarnya risiko sehingga dapat mencegah kegagalan atau setidaknya mengurangi tingkat kemungkinan terjadinya risiko. Pengukuran besarnya potensi yang dapat terjadi pada risiko dihitung untuk menentukan prioritas dari kegagalan.



Gambar 2.5 Proses FMEA

Sumber : Balqis (2016)

2.7.2 *Severity*

Penentuan nilai *Severity* sesuai dengan efek paling serius untuk mode kegagalan yang diberikan, berdasarkan kriteria dari skala keparahan (*severity*). Ketika menerapkan skala keparahan untuk Proses FMEA, tim menilai tingkat keparahan efek pada produk dan proses dan menggunakan kasus terburuk. Penilain *Severity* menggunakan skala dengan 10 tingkatan, yaitu skala 1 sampai dengan 10. Skala 1 merupakan tingkatan risiko yang memiliki dampak yang paling kecil sedangkan skala 10 merupakan tingkatan risiko yang memiliki dampak yang sangat berbahaya. Pada tabel 2.1 akan dijelaskan mengenai tingkatan yang digunakan untuk menilai tingkat *severity*.

Tabel 2.1 Skala *Severity*

No.	Rating	Severity	Deskripsi
1.	1	Tidak ada efek	Tidak memiliki pengaruh pada kinerja
2.	2	Sangat kecil	Risiko memiliki efek yang diabaikan pada kinerja
3.	3	Kecil	Risiko sedikit berpengaruh pada kinerja
4.	4	Sangat rendah	Risiko memiliki efek yang kecil pada kinerja
5.	5	Rendah	Efek risiko mempengaruhi penurunan kinerja secara bertahap
6.	6	Sedang	Sistem beroperasi dan aman tetapi mengalami peforma sehingga mempengaruhi output
7.	7	Tinggi	Sistem beroperasi tetapi tidak dapat dijalankan secara maksimal
8.	8	Sangat Tinggi	Sistem tidak dapat beroperasi
9.	9	Berbahaya	Kegagalan berdampak pada kerugian materil
10.	10	Sangat berbahaya	Kegagalan berdampak pada kerugian materil dan memiliki efek yang berbahaya

2.7.3 *Occurrence*

Penentuan nilai *Occurrence* berdasarkan kemungkinan seringnya terjadi kesalahan pada setiap proses dan didasarkan pada kriteria dari skala kejadian yang sesuai, ditentukan tanpa memperhatikan keparahan atau kemungkinan deteksi. Penilain *occurrence* menggunakan skala dengan 10 tingkatan, yaitu skala 1 sampai dengan 10. Skala 1 merupakan tingkatan risiko yang memiliki tingkat kejadian yang paling kecil sedangkan skala 10 merupakan tingkatan risiko yang memiliki tingkat frekuensi yang paling sering terjadi. Pada tabel 2.2 akan dijelaskan mengenai tingkatan yang digunakan untuk menilai tingkat *occurrence*.

Tabel 2.2 Skala *Occurrence*

No.	Rating	Occurrence	Deskripsi	Kriteria
1.	1	Tidak ada	Tidak pernah terjadi kegagalan	0
2.	2	Sangat rendah	Sangat kecil kemungkinan terjadinya kegagalan	1-2 kejadian dalam jangka waktu 1 bulan
3.	3			3 kejadian dalam jangka waktu 1 bulan
4.	4	Rendah	Kecil kemungkinan terjadinya kegagalan	4 kejadian dalam jangka waktu 1 bulan
5.	5	Sedang	Jarang terjadi kegagalan	5 kejadian dalam jangka waktu 1 bulan
6.	6			6 kejadian dalam jangka waktu 1 bulan
7.	7	Cukup sering	Kegagalan cukup sering terjadi	7 kejadian dalam jangka waktu 1 bulan
8.	8	Sering	Kegagalan sering terjadi	8 kejadian dalam jangka waktu 1 bulan
9.	9			9-10 kejadian dalam jangka waktu 1 bulan
10.	10	Sangat sering	Hampir selalu terjadi kegagalan	lebih dari 10 kejadian dalam jangka waktu 1 bulan

2.7.4 *Detection*

Detection merupakan penilaian atas kemungkinan terdeteksinya penyebab terjadi suatu bentuk kegagalan pada aset. Penilaian *detection* ditentukan tanpa memperhatikan tingkat keparahan atau kemungkinan terjadinya. Penilaian *detection* juga menggunakan skala dengan 10 tingkatan, yaitu skala 1 sampai dengan 10. Skala 1 merupakan tingkatan yang paling mudah terdeteksi dan melakukan kontrol sedangkan skala 10 merupakan tingkatan yang

paling sulit terdeteksi. Pada tabel 4.6 akan dijelaskan mengenai tingkatan yang digunakan untuk menilai tingkat *detection*.

Tabel 2.3 Skala *Detection*

No.	Rating	Detection	Deskripsi
1.	1	Hampir pasti	Pengecekan akan selalu mendeteksi penyebab kegagalan
2.	2	Sangat tinggi	Pengecekan memiliki kemungkinan sangat tinggi untuk mendeteksi penyebab kegagalan
3.	3	Tinggi	Pengecekan memiliki kemungkinan tinggi untuk mendeteksi penyebab kegagalan
4.	4	Sedang	Pengecekan memiliki kemungkinan dengan tingkat rata-rata dapat mendeteksi penyebab kegagalan
5.	5		
6.	6	Sangat Rendah	Pengecekan memiliki kemungkinan rendah untuk mendeteksi penyebab kegagalan
7.	7	Rendah	Pengecekan memiliki kemungkinan sangat rendah untuk mendeksi penyebab kegagalan
8.	8	Kecil	Pengecekan memiliki kemungkinan kecil untuk mendeteksi penyebab kegagalan
9.	9	Sangat Kecil	Pengecekan memiliki kemungkinan sangat kecil untuk mendeteksi penyebab kegagalan
10.	10	Tidak Pasti	Pengecekan tidak mampu untuk mendeteksi penyebab kegagalan

2.7.5 Risk Priority Number

RPN (*Risk Priority* Number) merupakan nilai yang digunakan untuk menentukan prioritas dari risiko/kegagalan (Carlson, 2014). Penentuan nilai *severity* sesuai dengan efek paling serius untuk mode kegagalan yang diberikan, berdasarkan kriteria dari skala *severity*. Ketika menerapkan skala keparahan untuk Proses FMEA, tingkat keparahan efek pada produk atau proses menggunakan kasus terburuk yang terjadi. Penentuan nilai *occurrence* berdasarkan kemungkinan seringnya terjadi kesalahan pada setiap proses dan didasarkan pada kriteria dari skala kejadian yang telah ditentukan, dan penilaian ditentukan tanpa memperhatikan keparahan atau kemungkinan deteksi. *Detection* merupakan penilaian atas kemungkinan terdeteksinya penyebab terjadinya suatu bentuk kegagalan. Penentuan nilai *detection* ditentukan tanpa memperhatikan tingkat keparahan atau kemungkinan terjadinya. RPN ini menunjukkan tingkat prioritas sebuah mode kegagalan yang diperoleh dari hasil analisis pada proses yang dianalisis. Nilai RPN dapat diperoleh dengan menjumlah kan hasil perkalian nilai *severity,* nilai *occurence* dan nilai *detection*.

$$\text{RPN} = \text{Severity x Occurence x Detection} \quad \text{... (2.1)}$$

Hasil nilai RPN akan digunakan untuk mengetahui risiko yang memiliki level yang tinggi dan memerlukan perhatian terlebih dahulu. Tabel 4.4 akan menjelaskan tingkatan yang akan diperoleh dari hasil perhitungan RPN.

Tabel 2.4 Nilai RPN

Level	Nilai RPN
Very low (Sangat Rendah)	0 sampai 20
Low (Rendah)	21 sampai 80
Moderate (Sedang)	81 sampai 119
High (Tinggi)	120 sampai 199
Very High (Sangat Tinggi)	lebih dari 200

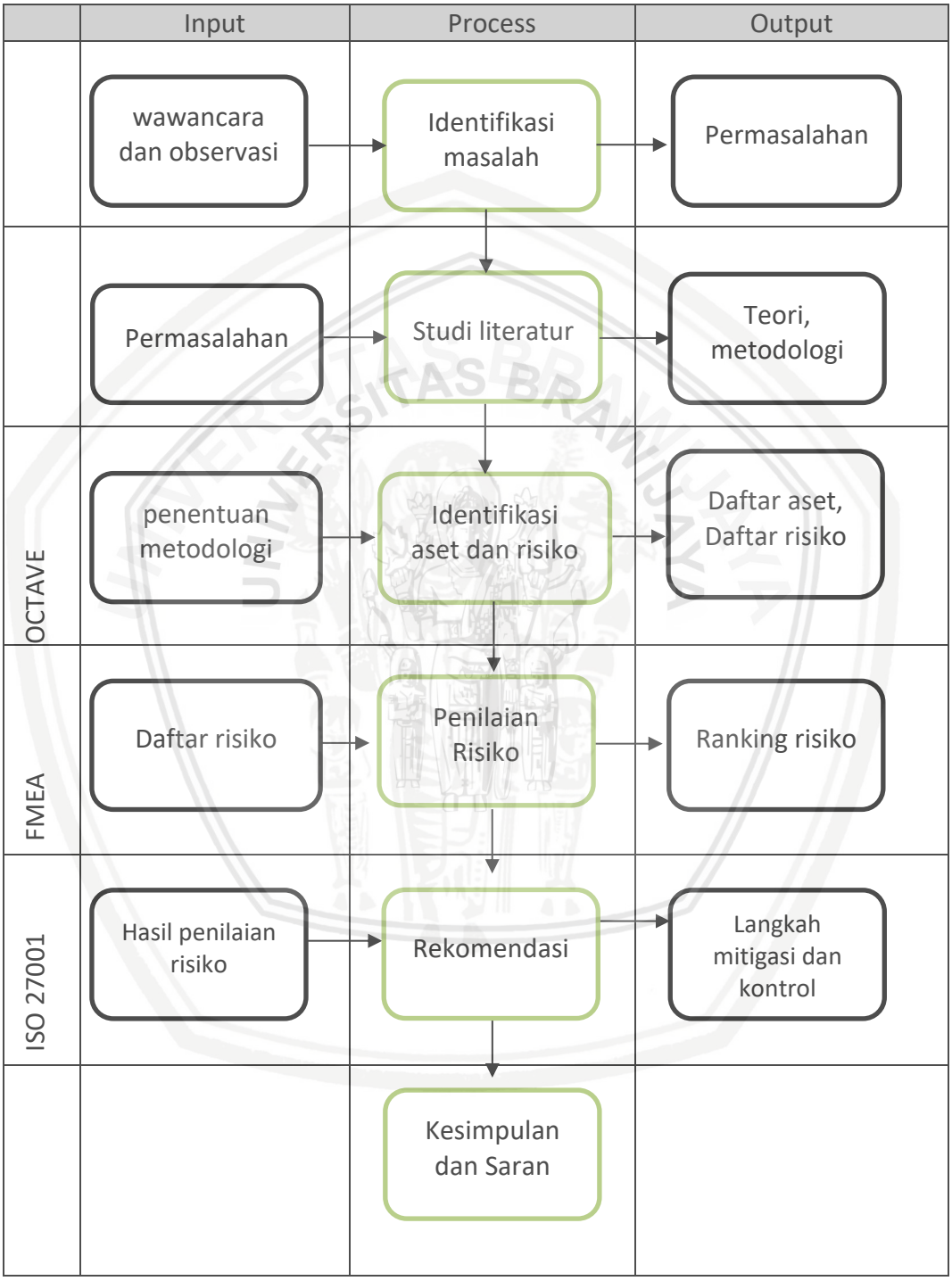
2.8 ISO/IEC 27001

ISO/IEC 27001 merupakan sebuah dokumen standar yang dikeluarkan oleh *International Organization for Standardization*. ISO 27001 ini merupakan standar yang bertujuan untuk membangun, melaksanakan, mengoperasikan, memantau, dan memelihara SMKI (Sistem Manajemen Keamanan Informasi). Sistem manajemen keamanan informasi menjaga kerahasiaan, integritas, dan ketersediaan informasi. Pada ISO 27001 terdapat klausul yang dapat digunakan untuk proses mitigasi dan kontrol terhadap risiko yang telah di identifikasi sebelumnya. ISO/IEC 27001 memiliki 114 kontrol yang dikategorikan menjadi 14 domain dan 35 tujuan (Candiwan, 2014).

BAB 3 METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Penelitian ini akan diselesaikan dengan alur yang tergambar sebagai berikut:



Gambar 3.1 Metodologi Penelitian

3.1.1 Identifikasi Masalah

Identifikasi masalah dilakukan dengan mengidentifikasi permasalahan objek yang terkait dalam penelitian yakni pada bidang IT Kepolisian Daerah Banten. Identifikasi permasalahan mengenai analisis risiko keamanan teknologi informasi didapatkan dengan melakukan wawancara dan observasi bersama ketua bidang IT dan pegawai pada kepolisian daerah banten.

3.1.2 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 .

3.1.3 Identifikasi Aset dan Risiko

Tahap ini merupakan tahap 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.

3.1.4 Penilaian Risiko

Pada tahap ini dilakukan 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*).

3.1.5 Rekomendasi

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

3.1.6 Kesimpulan

Kesimpulan berisi hasil penelitian yang telah dilakukan, mencakup identifikasi aset dan risiko, peringkat risiko, serta rekomendasi mitigasi risiko yang ada di bidang IT Kepolisian daerah Banten yang mana diharapkan dapat

digunakan sebagai acuan perbaikan di masa mendatang, serta pada bagian ini juga akan dijelaskan mengenai saran-saran yang dapat diberikan untuk penelitian selanjutnya.

BAB 4 HASIL DAN PEMBAHASAN

4.1 Identifikasi Aset

4.1.1 Aset Keseluruhan

Wawancara dilakukan untuk mengetahui aset-aset yang terdapat pada Bidang IT Kepolisian Daerah Banten. Setelah melakukan wawancara, jumlah aset yang teridentifikasi dapat diketahui dengan melakukan tinjauan langsung atau observasi terhadap aset-aset tersebut. Hasil wawancara dan observasi dapat dilihati pada lampiran A. Setelah melakukan identifikasi aset dan jumlah aset yang dimiliki oleh bidang IT Kepolisian Daerah Banten, aset-aset dapat digolongkan ke dalam beberapa kategori yaitu perangkat keras, perangkat lunak, jaringan, dan fasilitas pendukung. Berdasarkan hasil wawancara dan observasi didapatkan total 28 jenis aset pada bidang IT kepolisian Daerah Banten. Daftar aset-aset tersebut dapat dilihat pada tabel 4.1.

Tabel 4.1 Daftar Aset

No.	Kategori Aset	Jenis Aset	Jumlah Aset
1	*Hardware*	PC	19
2		Laptop	5
3		*Printer*	10
4		*Scanner*	5
5		Perangkat video conference	3
6		*Server*	3
7		*Tower*	8
8		*Monitor*	19
9		*Router*	20
10		*Repeater*	20
11		Modem	12
12		CCTV	38
13		UPS	15
14		AC	10
15	*Software*	*e-competency*	1
16		Aplikasi Pusiknas	1
17		Aplikasi Tribatanews	1

Tabel 4.1 Daftar Aset (Lanjutan)

No.	Kategori Aset	Jenis Aset	Jumlah Aset
18		Aplikasi LRA (Laporan Rencana Anggaran)	1
19		Aplikasi SIPP (Sistem Informasi Personil Polri)	1
20		*Microsoft Office (Word, Powerpoint, Excel)*	4
21		Windows	5
22	*Network*	Jaringan Internet	37
23		Kabel jaringan (*Fiber optic*)	16
24	*People*	Admin	3
25		Personel IT	22
26	*Information*	Data Hilang temu ranmor	1
27		Data Informasi Kriminalitas Nasional	1
28		Data Personil Polri	1

4.1.2 Aset Kritis

Dalam tahap ini, responden memilih aset yang mereka anggap paling penting. Identifikasi aset penting didapatkan dengan melakukan wawancara. Aset kritis merupakan aset yang dianggap sebagai perangkat penting dalam menjalankan kegiatan operasional instansi. Pada tahap ini direkomendasikan untuk membatasi jumlah aset yang dapat dipilih oleh responden. Jika terlalu banyak aset yang akan dipilih, maka kegiatan analisis selanjutnya dapat membutuhkan waktu yang lebih lama. Hasil dari identifikasi aset penting akan dijelaskan pada tabel 4.2.

Tabel 4.2 Aset Kritis

No.	Kategori	Aset	Deskripsi
1	*Hardware*	PC	Digunakan untuk mengakses aplikasi dan lain-lain.
2		*Server*	Digunakan untuk menyimpan data yang diinputkan pada aplikasi.
3		AC	Digunakan sebagai cooling system pada server.
4		Perangkat *Video Conference*	Digunakan untuk melakukan rapat jarak jauh.

Tabel 4.2 Aset kritis (Lanjutan)

No.	Kategori	Aset	Deskripsi
5		*Router*	Digunakan sebagai pemancar jaringan internet.
6		Kabel Jaringan	Kabel yang digunakan untuk menyambungkan jaringan dengan PC, Server, dan router.
7	*Software*	Aplikasi Hilang temu ranmor	Aplikasi ini digunakan untuk memberikan informasi dari hasil temuan kendaraan untuk kasus pencurian motor.
8		Aplikasi Pusiknas	Aplikasi ini digunakan untuk memberikan informasi untuk kasus kriminalitas nasional.
9	*Network*	Jaringan Internet	Jaringan Internet digunakan untuk mendukung aplikasi yang digunakan pada Polda Banten.
10	*People*	Admin	Personil yang yang melakukan controller terhadap aplikasi.
11	*Information*	Data Hilang temu ranmor	Merupakan informasi untuk hasil temuan kendaraan dari kasus pencurian motor
12		Data Informasi Kriminalitas Nasional	Merupakan informasi yang digunakan untuk mengetahui kasus kriminalitas nasional.

4.2 Identifikasi Ancaman

Berdasarkan hasil identifikasi aset pada bidang IT Kepolisian Daerah Banten, dilakukan brainstorming untuk mengidentifikasi ancaman yang dapat terjadi pada aset tersebut. Proses identifikasi ancaman dilakukan dengan menentukan kejadian yang memiliki probabilitas terjadinya risiko baik disebabkan oleh faktor internal maupun eksternal. Hasil analisis menunjukkan terdapat 18 ancaman yang dapat terjadi pada aset perangkat keras, perangkat lunak, jaringan dan karyawan yang ada di bidang IT Kepolisian Daerah Banten. Hasil identifikasi risiko akan ditunjukkan pada tabel berikut.

Tabel 4.3 Identifikasi Ancaman Aset Kritis

No	Kategori	Ancaman
1	*Hardware*	Kerusakan fisik aset
2		*Power failure*

Tabel 4.3 Identifikasi Ancaman Aset Kritis (Lanjutan)

No	Kategori	Ancaman
3		Memori penuh
4		*Server down*
5		Pencurian perangkat aset
6	*Software*	Penyalahgunaan Aplikasi
7		Terserang virus
8		Serangan *hacker*
9		Penyalahgunaan Hak akses
10	*Information*	Kehilangan data atau informasi
11		Pencurian data atau informasi
12	*Network*	Kecepatan internet yang tidak stabil
13		kerusakan Infrastruktur jaringan
14		Kabel terputus
15	*People*	Penyalahgunaan teknologi informasi
16		Menggunakan teknologi informasi yang tidak sesuai dengan fungsinya

4.3 Penerapan Keamanan

Untuk mengetahui penerapan keamanan saat ini, dilakukan survei kepada pegawai dan ketua bidang IT Kepolisian Daerah Banten. Survei dilakukan dengan menggunakan kuesioner, dengan menggunakan skala Guttman untuk menjawab kuesioner tersebut. Berdasarkan hasil survei yang dilakukan, Penentuan penerapan keamanan yang telah diterapkan dapat dilihat dari jumlah jawaban yang melebihi rasio 75%. Dengan demikian dapat ditemukan upaya yang telah dilakukan untuk kegiatan keamanan informasi yang saat ini sudah diterapkan. Diantaranya adalah :

1. Instansi melakukan pelatihan terhadap karyawan dalam penggunaan teknologi informasi.
2. Instansi melakukan perencanaan strategi untuk keamanan dan sesuai dengan strategi bisnis.
3. Instansi memiliki manajemen untuk tindakan terhdap risiko dan keamanan.
4. Instansi memiliki manajemen terhadap kerja sama dengan pihak ketiga.

5. Instansi memiliki perencanaan dan menguji fasilitas dalam menanggapi keadaan darurat.
6. Menerapkan keamanan hak akses terhadap aset perangkat keras dan perangkat lunak.
7. Menetapkan tanggung jawab aset kepada setiap personil untuk mengamankan informasi yang dimiliki.

dapat dikatakan bahwa adanya beberapa kerentanan yang teridentifikasi sesuai dengan hasil survey yang telah dilakukan. Diantaranya adalah :

1. Instansi tidak melakukan proses dokumentasi untuk manajemen kebijakan keamanan informasi
2. Instansi tidak memiliki proses yang terdokumentasi untuk memastikan kepatuhan dengan kebijakan keamanan informasi, hukum dan peraturan yang berlaku.
3. Instansi tidak memberlakukan kebijakan keamanan secara seragam.
4. Instansi tidak memiliki rencana dan prosedur yang terdokumentasikan mengenai keamanan fasilitas untuk menjaga tempat, bangunan dan area terlarang.
5. Instansi tidak memiliki rencana backup data yang terdokumentasi dan teruji.
6. Instansi tidak memiliki prosedur manajemen insiden yang diuji, diverifikasi dan diperbarui secara berkala.

4.4 Komponen Kunci

Pada tahap ini dijelaskan mengenai jenis perangkat yang berperan penting dalam memproses, menyimpan, atau mentransmisikan informasi penting. Perangkat tersebut mewakili aset yang terkait dengan aset penting. Berdasarkan aset perangkat lunak yang dimiliki bidang IT Kepolisian Daerah Banten, terdapat dua aset perangkat lunak yang digunakan untuk mengelola informasi penting. Aset perangkat lunak tersebut ialah Aplikasi Hilang Temu Ranmor dan Aplikasi Pusat Informasi Kriminalitas Nasional. Hasil wawancara yang telah dilakukan kepada salah satu pegawai di Bidang IT Kepolisian Daerah Banten terdapat beberapa perangkat yang berperan penting dan dibutuhkan untuk mengelola informasi.

4.4.1 Komponen Kunci Informasi Hilang Temu Ranmor

Pada pengelolaan informasi Data Hilang Temu Ranmor terdapat 5 komponen kunci yang digunakan untuk mengelola informasi tersebut. Berikut merupakan komponen kunci yang digunakan untuk menjalankan aplikasi Hilang Temu Ranmor serta menyimpan informasi yang ada di dalamnya. Tabel 4.4 akan menjelaskan mengenai 5 komponen kunci tersebut.

Tabel 4.4 Komponen Kunci Aplikasi Hilang Temu Ranmor

No	Kategori	Key Component	Penjelasan
1	*Hardware*	PC	Digunakan untuk menjalankan aplikasi serta mengontrol aplikaasi yang digunakan.
2		*Server*	Digunakan untuk menyimpan data.
3	*Software*	Aplikasi	Digunakan untuk mengelola data atau informasi hilang temu ranmor
4	*Network*	Jaringan internet	Digunakan sebagai alat pendukung aplikasi dan komunikasi.
5	*People*	Admin	Pegawai yang memiliki wewenang dalam melakukan pengelolaan teknologi informasi untuk tujuan bisnis instansi.

4.4.2 Komponen Kunci Informasi Kriminalitas Nasional

Pada informasi data Kriminalitas Nasional, didapatkan 6 komponen kunci yang digunakan sebagai perangkat untuk mengelola informasi tersebut. Komponen tersebut digunakan untuk memproses serta menyimpan informasi penting yang ada di dalamnya. Tabel berikut akan menjelaskan mengenai komponen kunci dan penjelasan komponen kunci yang digunakan untuk pegelolaan informasi Kiriminalitas Nasional.

Tabel 4.5 Komponen Kunci Aplikasi Pusat Informasi Kriminalitas Nasional

No	Kategori	Key Component	Penjelasan
1	*Hardware*	PC	Digunakan untuk menjalankan aplikasi serta mengontrol aplikasi yang digunakan.
2		*Server*	Digunakan untuk menyimpan data.
3	*Software*	Aplikasi	Digunakan untuk mengelola data atau informasi kriminalitas nasional
4	*Network*	Jaringan internet	Digunakan sebagai alat pendukung aplikasi dan komunikasi.

Tabel 4.5 Komponen Kunci Aplikasi Pusat Informasi Kriminalitas Nasional Lanjutan

No	Kategori	Key Component	Penjelasan
5		*Firewall*	Digunakan untuk melindungi informasi dari ancaman yang dapat terjadi melaui koneksi internet.
6	*People*	Admin	Pegawai yang memiliki wewenang dalam melakukan pengelolaan teknologi informasi untuk tujuan bisnis instansi.

4.5 Identifikasi Risiko

Identifikasi risiko dilakukan dengan melihat dua aspek yaitu kemungkinan ancaman serta kerentanan yang dimiliki oleh instansi tersebut. Dengan demikian dapat dilihat daftar ancaman yang menjadi risiko bagi instansi. Tabel berikut akan menjelaskan mengenai risiko yang ada pada masing-masing aset di bidang IT Kepolisian daerah Banten.

Tabel 4.6 Identifikasi Risiko

No	Aset	Risiko
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

Tabel 4.6 Identifikasi Risiko (Lanjutan)

No	Aset	Risiko
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

BAB 5 ANALISIS

5.1 Penilaian Risiko

5.1.1 Risk Priority Number

Berdasarkan hasil risiko yang telah teridentifikasi, penilaian risiko dilakukan berdasarkan 3 faktor yaitu keparahan (*severity*), kejadian (*occurrence*), dan deteksi (*detection*). Penilaian dilakukan dengan melakukan wawancara dan *brainstorming* dengan ketua bidang IT dan personil yang bertugas pada bidang IT Kepolisian daerah Banten. Hasil wawancara dapat dilihat pada lampiran E. Penilaian *severity* dilakukan untuk menganalisa risiko dengan menghitung seberapa besar dampak kejadian mempengaruhi proses. Setelah melakukan penilaian terhadap tingkat keparahan risiko, dapat dilakukan penilaian terhadap tingkat kejadian atau frekuensi risiko. hal ini dapat dilakukan dengan melihat keseringan terjadinya risiko. Setelah melakukan penilaian tingkat kejadian, selanjutnya menilai risiko yang dilihat dari faktor pendeteksian terhadap risiko tersebut. Penilaian ini dilakukan dengan melihat kemungkinan terdeteksinya penyebab terjadinya suatu bentuk risiko. Setelah mendapatkan nilai dari 3 faktor tersebut, perhitungan tingkat prioritas dapat dilakukan dengan menggunakan perhitungan RPN. Perhitungan RPN berdasarkan hasil dari perkalian nilai *Severity* , *Occurrence* , dan *Detection* . Hasil nilai RPN akan digunakan untuk mengetahui risiko yang memiliki *level* yang tinggi dan memerlukan perhatian terlebih dahulu.

Hasil perhitungan RPN pada aset perangkat keras menunjukan pada aset PC terdapat 1 risiko yang termasuk pada level *Very Low,* 2 risiko yang termasuk pada level *Low*, dan 1 risiko yang termasuk pada level *High*. Pada aset server terdapat terdapat 2 risiko yang termasuk pada level *Low*, dan 2 risiko yang termasuk pada level *High*. Pada aset *router* terdapat 1 risiko yang termasuk pada level *Very Low* dan 1 risiko yang termasuk pada level *Low.* Perhitungan nilai RPN pada aset perangkat keras akan dijelaskan pada tabel 5.1 berikut ini.

Tabel 5.1 *Risk Priority Number* Aset Perangkat Keras

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
1	PC	*Maintenance* tidak teratur	Kerusakan fisik pada aset	5	Kurangnya prosedur pemeliharaan pada aset	3	5	75	*Low*

Tabel 5.*1 Risk Priority Number* Aset Perangkat Keras (Lanjutan)

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
2		Tidak ada perlindungan perangkat terhadap lingkungan	Kerusakan fisik pada aset	8	Kurang memperhatikan penempatan perangkat	5	4	160	*High*
3		Pemadaman listrik	*Power failure*	3	Pasokan listrik yang tidak stabil	3	2	18	*Very Low*
4		Kapasitas memori kecil	Memori penuh	5	Tidak memperbarui kapasitas memori	5	1	25	*Low*
5	*Server*	*Server overheat*	*Server down*	8	Kurang fasilitas *cooling system*	3	6	120	*High*
7		*Maintenance* tidak teratur	Kerusakan fisik pada aset	5	Kurangnya prosedur pemeliharaan pada aset	2	5	50	*Low*

Tabel 5.1 *Risk Priority Number* Aset Perangkat Keras (Lanjutan)

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
6		Tidak ada perlindungan perangkat terhadap lingkungan	Kerusakan fisik pada aset	8	Kurang memperhatikan penempatan perangkat	5	4	160	*High*
8		Kapasitas memori kecil	Memori penuh	5	Tidak memperbarui kapasitas memori	5	1	25	*Low*
9	AC	Maintenence tidak teratur	Kerusakan fisik pada aset	5	Kurangnya prosedur pemeliharaan pada aset	3	5	75	*Low*
10		Pemadaman listrik	*Power failure*	3	Pasokan listrik yang tidak stabil	3	2	18	*Very Low*
14	*Router*	*Maintenence* tidak teratur	Kerusakan fisik pada aset	5	Kurangnya prosedur pemeliharaan pada aset	3	5	75	*Low*
15		Pemadaman listrik	*Power failure*	3	Pasokan listrik yang tidak stabil	3	2	18	*Very Low*

Perhitungan RPN pada aset perangkat lunak menunjukan pada aset aplikasi hilang temu ranmor terdapat 3 risiko yang termasuk pada level *Low* dan 1 risiko yang termasuk pada level *Very High*. Pada aset aplikasi pusat informasi

kriminalitas nasional terdapat 3 risiko yang termasuk pada level *Low* dan 1 risiko yang termasuk pada level *Very High*. Hasil perhitungan nilai RPN pada aset perangkat lunak akan dijelaskan pada tabel 5.2 berikut ini.

Tabel 5.2 *Risk Priority Number* Aset Perangkat Lunak

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
1	Aplikasi Hilang temu ranmor	Kurangnya dokumentasi penggunaan aplikasi	Penyalahgunaan Aplikasi	5	Tidak memiliki prosedur penggunaan aplikasi yang terdokumentasi	4	3	60	*Low*
2		Kurangnya kesadaran terhadap keamanan	Terserang virus	6	Tidak menggunakan antivirus	8	5	240	*Very High*
3			Serangan *hacker*	9	Kurangnya pemahaman terhadap keamanan	1	8	72	*Low*
4		Kurangnya mekanisme otentifikasi	Penyalahgunaan Hak akses	7	Tidak menggunakan kata sandi pada PC	1	8	56	*Low*
5	Aplikasi Pusat informasi kriminal nasional	Kurangnya dokumentasi penggunaan aplikasi	Penyalahgunaan Aplikasi	5	Tidak memiliki prosedur penggunaan aplikasi yang terdokumentasi	2	3	30	*Low*

Tabel 5.2 *Risk Priority Number* Aset Perangkat Lunak (Lanjutan)

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
6		Kurangnya kesadaran terhadap keamanan	Terserang virus	6	Tidak menggunakan antivirus	8	5	240	*Very High*
7			Serangan *hacker*	9	Kurangnya pemahaman terhadap keamanan	1	8	72	*Low*
8		Menggunakan kata sandi yang umum	Penyalahgunaan hak akses	5	Tidak melakukan penggantian kata sandi secara berkala	3	5	75	*Low*

Perhitungan nilai RPN pada aset informasi menunjukkan pada informasi hilang temu ranmor terdapat 1 risiko yang termasuk pada level *Moderate* yaitu kehilangan data atau informasi yang disebabkan karena tidak melakukan backup data atau informasi dan 1 risiko yang termasuk pada level *Low* yaitu pencurian data atau informasi yang disebabkan oleh kurangnya mekanisme keamanan yang dilakukan. Pada informasi pusat kriminalitas nasional terdapat 2 risiko yang termasuk pada level *Low*. Penjelasan mengenai perhitungan nilai RPN akan ditunjukkan pada tabel berikut.

Tabel 5.3 *Risk Priority Number* Aset Informasi

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurre*	*Detectio*	RPN	Level
1	Informasi Hilang temu ranmor	Tidak melakukan backup data	Kehilangan data atau informasi	9	Tidak memiliki perangkat untuk melakukan backup data	5	2	90	*Moderate*

Tabel 5.3 *Risk Priority Number* Aset Informasi (Lanjutan)

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurre*	*Detectio*	RPN	Level
2		Kurangnya mekanisme keamanan	Pencurian data atau informasi	7	Tidak menggunakan kata sandi pada PC	1	8	56	*Low*
3	Informasi pusat krimnalitas nasional	Tidak melakukan backup data	Kehilangan data atau informasi	9	Tidak memiliki perangkat untuk melakukan backup data	1	2	18	*Low*
4		Kurangnya mekanisme keamanan	Pencurian data atau informasi	7	Tidak menggunakan kata sandi pada PC	1	8	56	*Low*

Perhitungan RPN pada aset jaringan internet menunjukkan hanya terdapat 1 risiko dan risiko tersebut termasuk pada level *low*. Sedangkan pada aset kabel jarigan menunjukan terdapat 2 risiko yang termasuk pada level *Low*, dan 1 risiko yang termasuk pada level *High*. Hasil perhitungan nilai RPN pada aset jaringan akan dijelaskan pada tabel berikut ini.

Tabel 5.4 *Risk Priority Number* Aset Jaringan

No	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
1	Jaringan internet	Jaringan internet tidak optimal	Kecepatan internet yang tidak stabil	5	Menggunakan layanan internet yang tidak berkualitas	7	2	70	*Low*

Tabel 5.4 *Risk Priority Number* Aset Jaringan Lanjutan

No	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
2	Kabel Jaringan (Fiber Optik)	Pindah ruangan	Kerusakan infrastuktur jaringan IT	4	Ketidak pastian penempatan infrastuktur IT	5	2	40	*Low*
3		Tidak menggunakan pelindung kabel	Kabel jaringan terputus	8	Kabel digigit oleh hewan	3	6	144	*High*

Perhitungan RPN pada aset tenaga kerja atau personil menunjukan terdapat 3 risiko yang termasuk pada level *Low* yaitu penyalahgunaan teknologi infomasi dikarenakan kurangnya pelatihan penggunaan teknologi informasi, pencuran data atau informasi dikarenakan karyawan mengetahui kelemahan pada kemanan serta penyalahgunaan hak akses teknologi informasi dikarenakan karyawan tidak *logout* setelah meninggalkan komputer dan 1 risiko yang termasuk pada level *Moderate* yaitu personil menggunaakan teknologi informasi tidak sesuai dengan fungsinya disebabkan karena karyawan tidak memiliki pemaham mengenai regulasi dan sanksi yang berlaku pada bidang IT Kepolisian daerah Banten. Hasil perhitungan nilai RPN pada aset jaringan akan dijelaskan pada tabel berikut ini.

Tabel 5.5 *Risk Priority Number* Aset Sumber Daya Manusia

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
1	Karyawan	Kurangnya pelatihan penggunaan teknologi informasi	Penyalahgunaan teknologi informasi	6	Kurangnya pemahaman pengguna an teknologi informasi	3	3	54	*Low*

Tabel 5.5 *Risk Priority Number* Aset Sumber Daya Manusia Lanjutan

No.	Aset	Potensi Kesalahan	Efek Kesalahan	*Severity*	Penyebab Kesalahan	*Occurrence*	*Detection*	RPN	Level
2		Karyawan mengetahui kelemahan pada keamanan aplikasi	Pencurian data atau informasi	7	Kurangnya pemantauan terhadap keamanan informasi	1	8	56	*Low*
3		Kurangnya pemahaman tentang regulasi dan sanksi	Menggunakan teknologi informasi yang tidak sesuai dengan fungsinya	5	Kurangnya melakukan sosialisasi tentang penggunaan teknologi informasi	3	6	90	*Moderate*
4		Karyawan tidak logout ketika meninggalkan komputer	Penyalahgunaan hak akses teknologi informasi	4	Kurangnya pemahaman atau kesadaran terhadap keamanan	3	2	24	*Low*

5.1.2 Ranking Risiko

Pada tahap ini daftar risiko akan diurutkan berdasarkan hasil perhitungan nilai RPN yang tertinggi hingga terendah berdasarkan risiko pada masing-masing aset. Hal ini dilakukan untuk mempermudah dalam melihat risiko yang harus mendapatkan perhatian terlebih dahulu. Ranking risiko pada peringkat PC akan ditunjukkan pada tabel berikut.

Tabel 5.6 Ranking Risiko aset PC

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	PC	Tidak ada perlindungan perangkat terhadap lingkungan	Kerusakan fisik pada aset	160	*High*
2		Maintenence tidak teratur	Kerusakan fisik pada aset	75	*Low*
3		Kapasitas memori kecil	Memori penuh	50	*Low*
4		Pemadaman listrik	*Power failure*	18	*Very Low*

Dalam table 5.6 ini dapat dilihat bahwa pada aset PC, pada peringkat pertama risiko kerusakan fisik pada aset yang disebabkan oleh tidak adanya perlindungakn perangkat terhadap lingkungan mempunyai RPN sebesar 160 dengan level *high* sehingga membutuhkan perhatian agar instansi dapat mencegah terjadinya risiko tersebut. Pada peringkat kedua terdapat risiko kerusakan fisik pada aset yang disebabkan oleh maintenance yang tidak teratur dengan nilai RPN sebesar 75 dan termasuk level *Low*. Pada peringkat ketiga terdapat risiko memori penuh yang disebabkan oleh kapasitas memori kecil dengan nilai RPN 50 dan termasuk pada level *Low*. Para peringkat keempat terdapat risiko power failure yang mempunyai nilai RPN sebesar 18 dan termasuk pada level *Very Low*.

Tabel 5.7 Ranking Risiko aset Server

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	*Server*	Tidak ada perlindungan perangkat terhadap lingkungan	Kerusakan fisik pada aset	160	*High*
2		*Server overheat*	*Server down*	120	*Moderate*

Tabel 5.7 *Ranking Risiko* aset Server Lanjutan

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
3		*Maintenence* tidak teratur	Kerusakan fisik pada aset	50	*Low*
4		Kapasitas memori kecil	Memori penuh	50	*Low*

Pada tabel 5.7 dapat dilihat bahwa dalam aset server terdapat 4 potensi risiko yang mungkin terjadi dan diurutkan sesuai nilai RPN dan levelnya. Peringkat pertama yaitu risiko kerusakan fisik pada aset yang disebabkan oleh tidak adanya perlindungan perangkat terhadap lingkungan mempunyai nilai RPN sebesar 160 dengan level *high* sehingga membutuhkan perhatian agar instansi dapat mencegah terjadinya risiko tersebut. Pada peringkat kedua terdapat risiko server down dengan nilai RPN sebesar 120 dan termasuk pada level *moderate*. Pada peringkat ketiga terdapat risiko kerusakan fisik pada aset yang disebabkan oleh maintenance yang tidak teratur dengan nilai RPN sebesar 50 dan termasuk pada level *low*. Pada peringkat keempat terdapat risiko memori penuh dengan nilai RPN sebesar 50 dan termasuk pada level *low*.

Tabel 5.8 Ranking Risiko Aset AC

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	AC	*Maintenence* tidak teratur	Kerusakan fisik pada aset	75	*Low*
2		Pemadaman listrik	*Power failure*	18	*Very Low*

Pada tabel 5.8 dapat dilihat bahwa dalam aset AC terdapat 2 potensi risiko yang mungkin terjadi. Peringkat pertama yaitu risiko kerusakan fisik aset yang disebabkan oleh maintenance yang tidak teratur dengan nilai RPN sebesar 75 dan termasuk pada level *low*. Pada peringkat kedua terdapat risiko power failure dengan nilai RPN sebesar 18 dan termasuk pada level *very low*.

Tabel 5.9 Ranking Risiko Aset Router

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	AC	*Maintenence* tidak teratur	Kerusakan fisik pada aset	75	*Low*
2		Pemadaman listrik	*Power failure*	18	*Very Low*

Pada tabel 5.9 dapat dilihat bahwa dalam aset Router terdapat 2 potensi risiko yang mungkin terjadi. Peringkat pertama yaitu risiko kerusakan fisik aset

yang disebabkan oleh maintenance yang tidak teratur dengan nilai RPN sebesar 75 dan termasuk pada level *low*. Pada peringkat kedua terdapat risiko power failure dengan nilai RPN sebesar 18 dan termasuk pada level *very low*.

Tabel 5.10 Ranking Risiko Aset Aplikasi Hilang Temu Ranmor

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	Aplikasi hilang temu ranmor	Kurangnya kesadaran terhadap keamanan	Terserang virus	240	*Very High*
2		Kurangnya kesadaran terhadap keamanan	Serangan *hacker*	72	*Low*
3		Kurangnya dokumentasi penggunaan aplikasi	Penyalahgunaan Aplikasi	60	*Low*
4		Kurangnya mekanisme otentifikasi	Penyalahgunaan Hak akses	56	*Low*

Pada tabel 5.10 dapat dilihat bahwa dalam aset aplikasi hilang temu ranmor terdapat 4 potensi risiko. Peringkat pertama yaitu potensi risiko kurangnya kesadaran terhadap keamanan yang disebabkan oleh aplikasi terserang virus mempunyai nilai RPN sebesar 240 sehingga menempatkan risiko ini dalam level *very high*, peringkat kedua dengan potensi risiko kurangnya kesadaran terhadap keamanan disebabkan oleh serangan dari *hacker* mempunyai nilai RPN 72 dalam level *low*, peringkat ketiga yaitu kurangnya dokumentasi penggunaan aplikasi disebabkan oleh penyalahgunaan aplikasi RPN 60 dengan level *low*, peringkat keempat yaitu kurangnya mekanisme otentifikasi disebabkan oleh penyalahgunaan hak akses dengan nilai RPN 56 dan level *low.*

Tabel 5.11 Ranking Risiko Aset Aplikasi Pusat Informasi Kriminal Nasional

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	Aplikasi pusat informasi kriminalitas nasional	Kurangnya kesadaran terhadap keamanan	Terserang virus	240	*Very High*
2		Menggunakan kata	Penyalahgunaan	75	*Low*

Tabel 5.11 Ranking Risiko Aset Aplikasi Pusat Informasi Kriminal Nasional

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
		sandi yang umum	hak akses		
3		Kurangnya kesadaran terhadap keamanan	Serangan *hacker*	72	*Low*
4		Kurangnya dokumentasi penggunaan aplikasi	Penyalahgunaan Aplikasi	30	*Low*

Pada tabel 5.11 dapat dilihat bahwa dalam aset aplikasi pusat informasi kriminal nasional terdapat 4 potensi risiko yang mungkin terjadi. Peringkat pertama yaitu potensi risiko kurangnya kesadaran terhadap keamanan yang disebabkan oleh aplikasi terserang virus mempunyai nilai RPN sebesar 240 sehingga menempatkan risiko ini dalam level *very high*, peringkat kedua dengan potensi risiko kurangnya kesadaran terhadap keamanan disebabkan oleh serangan dari *hacker* mempunyai nilai RPN 72 dalam level *low*, peringkat ketiga yaitu kurangnya mekanisme otentifikasi disebabkan oleh penyalahgunaan hak akses dengan nilai RPN 56 dan level *low,* peringkat keempat yaitu kurangnya dokumentasi penggunaan aplikasi disebabkan oleh penyalahgunaan aplikasi RPN 30 dengan level *low.*

Tabel 5.12 Ranking Risiko Aset Informasi Hilang Temu Ranmor

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	Informasi Hilang temu ranmor	Tidak melakukan backup data	Kehilangan data atau informasi	90	*Moderate*
2		Kurangnya mekanisme keamanan	Pencurian data atau informasi	56	*Low*

Pada tabel 5.12 dapat dilihat bahwa dalam aset informasi hilang temu ranmor terdapat 2 risiko yang mungkin terjadi. Peringakt pertama yaitu kehilangan data atau informasi yang disebabkan oleh tidak melakukan backup data atau informasi dengan nilai RPN 90 dan termasuk pada level *moderate*. Para peringkat kedua terdapat risiko pencurian data atau informasi yang disebabkan oleh kurangnya mekanisme keamanan dengan nilai RPN sebesar 56 dan termasuk pada level *low*.

Tabel 5.13 Ranking Risiko Aset Informasi PUSIKNAS

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	Informasi pusat krimnalitas nasional	Kurangnya mekanisme keamanan	Pencurian data atau informasi	56	*Low*
2		Tidak melakukan backup data	Kehilangan data atau informasi	54	*Low*

Pada tabel 5.13 dapat dilihat bahwa dalam aset informasi pusat kriminalitas nasional terdapat 2 risiko yang mungkin terjadi. Peringkat pertama terdapat risiko pencurian data atau informasi yang disebabkan oleh kurangnya mekanisme kemanan dengan nilai RPN sebesar 56 dan termasuk pada level *low*. Sedangkan risiko kehilangan data atau informasi yang disebabkan oleh tidak melakukan backup data berada di peringkat kedua dengan nilai RPN sebesar 54 dan termasuk pada level *low*.

Tabel 5.14 Ranking Risiko Aset Kabel Jaringan

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	Kabel Jaringan	Tidak menggunakan pelindung kabel	Kabel jaringan terputus	144	*High*
2		Pindah ruangan	Kerusakan infrastuktur jaringan IT	40	*Low*

Pada tabel 5.14 dapat dilihat bahwa dalam aset kabel jaringan terdapat 2 potensi risiko yang mungkin terjadi. Peringkat pertama yaitu potensi risiko tidak menggunakan pelindung kabel yang dapat menyebabkan kabel jaringan terputus mempunyai nilai RPN sebesar 144 sehingga menempatkan risiko ini dalam level *high*, peringkat kedua dengan potensi risiko pindah ruangan menyebakan kerusakan dalam infrastruktur jaringan dengan nilai RPN 40 dalam level *low*.

Tabel 5.15 Ranking Risiko Aset Jaringan Internet

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	Jaringan Internet	Jaringan internet tidak optimal	Kecepatan internet yang tidak stabil	70	*Low*

Pada tabel 5.15 dapat dilihat bahwa pada aset jaringan internet hanya terdapat 1 potensi risiko yaitu kecepatan internet yang tidak stabil disebabkan oleh jaringan internet yang tidak optimal mempunya nilai RPN 70 dengan level *low.*

Tabel 5.16 Ranking Risiko Aset Sumber Daya Manusia

Rank	Aset	Kerentanan dan Potensi	Risiko	RPN	Level
1	Karyawan	Kurangnya pemahaman tentang regulasi dan sanksi	Menggunakan teknologi informasi yang tidak sesuai dengan fungsinya	90	*Moderate*
2		Karyawan mengetahui kelemahan pada keamanan aplikasi	Pencurian data atau informasi	56	*Low*
3		Kurangnya pelatihan penggunaan teknologi informasi	Penyalahgunaan teknologi informasi	54	*Low*
4		Karyawan tidak logout ketika meninggalkan komputer	Penyalahgunaan hak akses teknologi informasi	24	*Low*

Pada tabel 5.16 dapat dilihat bahwa pada aset sumber daya manusia terdapat 4 risiko yang mungkin terjadi. Peringkat pertama yaitu risiko bertindak seenaknya pada teknologi informasi. Risiko tersebut memiliki nilai RPN 90 dan termasuk pada level *moderate*. Pada peringkat kedua terdapat risiko pencurian data atau informasi yang disebabkan karena karyawan mengetahui kelemahan pada keamanan aplikasi dengan nilai RPN sebesar 56 dan termasuk pada level *low*. Peringkat ketiga terdapat risiko penyalahgunaan teknologi informasi yang disebabkan oleh kurangnya pelatihan penggunaan teknologi informsai dan memiliki nilan RPN 54 dan termasuk pada level *low*. Peringkat keempat terdapat risiko penyalahgunaan hak akses TI disebabkan oleh karyawan yang tidak logout saat meninggalkan komputer dengan nilai RPN sebesar 24 dan termasuk pada level *low*.

BAB 6 REKOMENDASI

Pada ISO 27001 terdapat panduan yang dapat digunakan sebagai acuan dalam pembentukan kontrol keamanan informasi terhadap masing-masing potensi risiko pada aset teknologi informasi yang telah diidentifikasi pada bidang IT Kepolisian Daerah Banten. Langkah rekomendasi diberikan pada risiko yang memiliki potensi mulai dari level *moderate* hingga *very high*. Tabel berikut akan menjelaskan penerapan kontrol yang dapat dilakukan oleh instansi sesuai dengan standar ISO 27001.

6.1 *Top IT Risk*

Dari 28 risiko yang telah teridentifikasi dan telah diberikan penilaian. Top IT Risk dijabarkan sesuai dengan risiko dari seluruh aset yang memiliki potensi mulai dari level *moderate* hingga *very high*. Risiko pertama dari kategori aset PC dengan risiko kerusakan fisik yang disebabkan oleh tidak ada perlindungan aset terhadap lingkungan. Pada kategori aset server dengan risiko kerusakan fisik disebabkan oleh tidak ada perlindungan aset terhadap lingkungan dan risiko server down. Pada kategori aset perangkat lunak yaitu aplikasi hilang temu ranmor dan aplikasi pusat informasi kriminalitas nasional dengan risiko terserang virus. Pada kategori aset informasi hilang temu ranmor dengan risiko kehilangan data atau informasi. Pada kategori aset kabel jaringan dengan risiko kabel jaringan terputus, serta pada aset sumber daya manusia dengan risiko bertindak seenaknya pada teknologi informasi yang digunakan.

6.2 Mitigasi Risiko

Pada tahap ini peneliti memberikan rekomendasi pengendalian risiko pada setiap bentuk risiko yang memiliki tingkat potensi *moderate* hingga *very high*. Rekomendasi yang diberikan bedasarkan dari beberapa literatur disajikan pada tabel berikut.

Tabel 6.1 Rekomendasi Pengendalian Risiko

No	Aset	Risiko	Rekomendasi Pengendalian	Jenis Pengendalian
1	PC	Kerusakan fisik	A.11.2.1 *Equipment siting and protection*	*Risk planning*
2			A.11.1.1 *Physical security paramenter*	*Risk limitation*
3	*Server*	Kerusakan fisik	A.11.2.1 *Equipment siting and protection*	*Risk planning*

Tabel 6.1 Rekomendasi Pengendalian Risiko (Lanjutan)

No	Aset	Risiko	Rekomendasi Pengendalian	Jenis Pengendalian
4			A11.1.4 Protecting against external and environmental threats	*Risk planning*
5		*Server down*	A.11.2.2 *Supporting Utilities*	*Risk avoidance*
6	Aplikasi hilang temu ranmor	Terserang virus	A.12.2.1 *Control against Malware*	*Risk planning*
7			A.12.5.1 *Restriction on software installation*	*Risk limitation*
8	Aplikasi pusat informasi kriminalitas nasional	Terserang virus	A.12.2.1 *Control against Malware*	*Risk planning*
9			A.12.5.1 *Restriction on software installation*	*Risk limitation*
10	Informasi hilang temu ranmor	Kehilangan data atau informasi	A.12.3.1 *Information Backup*	*Risk planning*
11	Kabel jaringan	Kabel jaringan terputus	A.11.2.3 *Cabling Security*	*Risk assumption*
12	Sumber daya manusia	Menggunakan teknologi informasi yang tidak sesuai dengan fungsinya	A.7.2.3 *Disciplinary process*	*Risk planning*
13			A.12.1.1 Documented operating procedures	*Risk planning*

6.3 Rekomendasi Pengendalian Risiko

Pada tahap mitigasi risiko akan diberikan rekomendasi pengendalian risiko yang tepat pada masing-masing risiko yang telah diprioritaskan sebelumnya. Sebelum menentukan pengendalian risiko yang tepat, rincian biaya serta keuntungan yang akan diperoleh dari setiap pilihan perlu dilakukan. Maka dilakukan *cost and benefit analysis* dengan menganalisa dampak apabila digunakan rekomendasi pengendalian serta apabila tidak digunakan rekomendasi pengendalian.

6.3.1 Rekomendasi Pengendalian Risiko Aset PC

Untuk menentukan pilihan mitigasi risiko yang tepat pada aset PC, maka akan dilakukan *cost benefit analysis* untuk setiap opsi rekomendasi pengendalian untuk menentukan prioritas mitigasi risiko.

1. *Equipment sitting and protection*

   Risiko kerusakan fisik pada aset dapat disebabkan oleh penempatan aset yang tidak terencana serta kurang memperhatikan perlindungan yang diberikan terhadap aset tersebut. Maka salah satu pegendalian risiko yang dapat dilakukan yaitu dengan membuat perencanaan untuk penempatan aset serta perlindungan aset

   Dampak apabila dibuat perencanaan untuk penempatan aset yang tepat dan sesuai adalah terhindar dari ancaman mungkin terjadi oleh lingkungan. Sehingga aset dapat digunakan lebih lama dan mengurangi biaya dan waktu yang dibutuhkan untuk memperbaiki kerusakan aset.

   Sedangkan apabila tidak dilakukan perencanaan penempatan dan perlindungan aset yang tepat maka pemulihan dari risiko yang terjadi akan mengeluarkan biaya dan waktu yang lebih besar dibandingkan dengan melakukan perencanaan dan perlindungan aset yang tepat dari awal.

   Cost

   -

   Benefit

   Mengurangi tingkat kejadian risiko pada aset.

   Mengurangi biaya dan waktu yang dibutukan untuk memperbaiki aset.

2. *Physichal security parameter*

   Selain melakukan perencanaan penempatan dan perlindungan yang tepat untuk sebuah aset, batasan untuk keamanan aset dapat dilakukan untuk melindungi aset.

   Dampak apabila dibuat batasan keamanan aset adalah membatasi jumlah hak akses yang yang bertanggung jawab serta mengurangi tingkat kerusakan aset yang ditimbulkan oleh orang yang tidak bertanggung jawab. Sehingga mengurangi kemungkinan risiko terjadi yang ditimbulkan oleh pihak yang tidak bertangguna jawab atau orang tidak memiliki wewenang.

   Dampak apabila tidak membuat batasan untuk keamanan aset adalah banyak kerusakan yang timbulkan karena akses yang diberikan oleh yang yang tidak memiliki tanggung jawab terhadap aset tersebut sehingga menambah biaya dan waktu untuk memperbaiki aset tersebut.

   Cost

-

Benefit

Mengurangi jumlah kerusakan aset oleh pihak yang tidak bertanggung jawab.

Mengingkatkan batasan keamanan setiap aset.

Mengurangi biaya dan waktu yang dibutuhkan untuk memperbaiki kerusakan aset.

Dari hasil *cost – benefit analysis* tersebut maka instansi dapat melaksanakan pengendalian risiko secara bersamaan yaitu dengan membuat perencanaan penempatan perangkat teknologi informasi serta membuat kebijakan mengenai batasan untuk melindungi aset teknologi informasi tersebut.

6.3.2 Rekomendasi Pengendalian risiko aset Server

Untuk menentukan pilihan mitigasi risiko yang tepat pada aset server, maka akan dilakukan *cost benefit analysis* untuk setiap opsi rekomendasi pengendalian untuk menentukan prioritas mitigasi risiko.

1. *Equipment sitting and protection*

   Risiko kerusakan fisik pada aset dapat disebabkan oleh penempatan aset yang tidak terencana serta kurang memperhatikan perlindungan yang diberikan terhadap aset tersebut. Maka salah satu pegendalian risiko yang dapat dilakukan yaitu dengan membuat perencanaan untuk penempatan aset serta perlindungan aset.

   Dampak apabila dibuat perencanaan untuk penempatan aset yang tepat dan sesuai adalah terhindar dari ancaman mungkin terjadi oleh lingkungan. Sehingga aset dapat digunakan lebih lama dan mengurangi biaya dan waktu yang dibutuhkan untuk memperbaiki kerusakan aset.

   Sedangkan apabila tidak dilakukan perencanaan penempatan dan perlindungan aset yang tepat maka pemulihan dari risiko yang terjadi akan mengeluarkan biaya dan waktu yang lebih besar dibandingkan dengan melakukan perencanaan dan perlindungan aset yang tepat dari awal.

   Cost

   -

   Benefit

   Mengurangi peluang tingkat kejadian risiko pada aset..

   Mengurangi biaya dan waktu yang dibutukan untuk memperbaiki aset.

2. *Protecting against external and environmental*

Salah satu rekomendasi yang dapat dilakukan untuk mengurangi risiko kerusakan fisik dapat dilakukan dengan cara memperhatikan dan memberikan perlindungan terhadap ancaman yang ditimbulkan oleh bencana yang tidak dapat diprediksi sebelumnya.

Dampak apabila memberikan perlindungan pada aset terhadap bencana yang tidak dapat diprediksi adalah mengurangi tingkat keparahan atau kerusakan yang mungkin terjadi. Sehingga menghindari tingkat keparahan yang terjadi karena bencana alam.

Dampak apabila tidak memberikan perlindungan aset terhadap ancaman external atau bencana alam maka tingkat keparahan risiko yang terjadi akan meningkat sehingga aset tidak dapat digunakan kembali.

Contoh alat yang dapat digunakan untuk mengurangi potensi risiko melindungi aset yang disebabkan oleh lingkungan, yaitu dengan menggunaan produk yang dibuat oleh perusahaan fire indo.

Tabel 6.2 Perhitungan Cost Untuk Perlindungan Ancaman External

	Jumlah Individu	Harga per individu	Total
APAR	3	Rp. 600.000	Rp. 1.800.000
Total			RP. 1.800.000

Benefit

Mengurangi tingkat keparahan risiko pada aset.

3. *Supporting Utilities*

Pada risiko yang kedua yaitu server overheat, menurut (Sadowsky, 2003) perangkat komputer beroperasi paling baik dalam rentang suhu tertentu. Sebagian besar sistem komputer harus dijaga antara 10 hingga 32 derajat celcius. Jika suhu disekitar komputer terlalu tinggi, komputer tidak dapat mendinginkan dirinya sendiri, dan komponen internal dapat rusak. Setelah instansi menentukan rentang suhu yang yang ideal untuk kinerja perangkat komputer, pertahankan suhu tersebut dengan menggunakan alat *cooling system* yang tepat dan utilitas pendukung harus diinspeksi dan diuji secara teratur untuk memastikan fungsinya tepat dan untuk mengurangi risiko dari kerusakan atau kegagalannya.

Dampak apabila instansi memberikan perangkat pendukung untuk aset server adalah menjaga suhu yang dibutuhkan oleh perangkat server sehingga kinerja perangkat tidak mengalami kerusakan serta kegagalan sistem.

Dampak apabila tidak memberikan utilitas pendukung maka suhu perangkat server yang digunakan akan terlalu tinggi sehingga komponen internal akan mengalami kerusakan.

Cost

-

Benefit

Menjaga kestabilan suhu dan kinerja perangkat.

Mengurangi tingkat kejadian risiko.

6.3.3 Rekomendasi Pengendalian Risiko Aset Perangkat Lunak

Pada kedua aset kritis kategori perangkat lunak terdapat 1 risiko yang memiliki potensi dengan level *very high*, dengan demikian rekomendasi pengendalian diberikan kepada kedua aset perangkat lunak dan menentukan opsi pengendalian risiko dengan melakukan *cost and benefit analysis* dari masing-masing opsi pengendalian risiko tersebut.

1. *Control Against Malware*

   Perlindungan terhadap malware harus didasarkan pada deteksi malware dan perangkat lunak perbaikan, kesadaran keamanan informasi dan akses sistem yang tepat dan mengontrol manajemen perubahan. Dengan memberikan antivirus akan memudahkan untuk mendeteksi *malware* serta memberikan perlindungan terhadap aplikasi yang digunakan instansi dan dilakukan pengecekkan antivirus secara berkala.

   Dampak apabila memberikan antivirus akan memudahkan untuk mendeteksi *malware* dan mengurangi tingkat kejadian risiko, mencegah kehilangan informasi serta mencegah virus yang timbul karena menggunakan software yang tidak sah. Sehingga perangkat lunak akan terlindungi dari virus-virus yang dapat merusak aplikasi atau informasi.

   Dampak apabila tidak memberikan antivirus adalah tingkat kejadian terserang *malware* akan meningkat dan peluang kehilangan data atau informasi akan sulit untuk dihindari.

   Contoh *anti virus* yang dapat digunakan untuk mengurangi potensi risiko, yaitu dengan menggunakan produk yang dibuat oleh perusahaan Kaspersky lab.

Tabel 6.3 Perhitungan Cost Untuk Anti Virus

	Jumlah Individu	Harga per individu	Total
Anti virus	19	Rp. 535.668	Rp. 10.177.692
Total			RP. 10.177.692

Benefit

Mengurangi tingkat kejadian risiko

Mengurangi peluang kehilangan data dan informasi

2. *Restriction on Software Installation*

   Aturan yang mengatur instalasi perangkat lunak oleh pengguna harus ditetapkan dan diimplementasikan. organisasi harus menetapkan dan menegakkan kebijakan yang ketat mengenai jenis perangkat lunak yang dapat dipasang oleh pengguna. Pada sistem operaso windows, administrator dapat mengatur kebijakan sistem untuk mencegah pemasangan aplikasi baru dan juga memiliki fitur yang disebut kebijakan pembatasan perangkat lunak yang memungkinkan administrator untuk menunjuk perangkat lunak apa yang diizinkan untuk dijalankan pada komputer tertentu.

   Dampa apabila memberikan pembatasan instalasi perangkat lunak yaitu mengurangi tingkat kejadian risiko terserang virus yang timbuk karena pengguna melakukan instalasi perangkat lunak yang tidak sah sehingga mengurangi waktu yang dibutuhkan untuk mendeteksi dan melakukan instal ulang ketika terkena serangan virus.

   Dampak apabila tidak memberikan pembatasan instalasi perangkat lunak adalah pengguna akan menghiraukan pentingnya keamanan informasi yang dilakukan, serta melakukan instalasi perangkat lunak yang tidak sah semakin meninggat sehingga peluang terjadinya risiko terserang virus akan sangat besar.

   Cost

   -

   Benefit

   Mengurangi peluang terjadinya risiko terserang virus.

Dari hasil *cost – benefit analysis* tersebut maka instansi dapat melaksanakan pengendalian risiko secara bersamaan yaitu dengan memberikan anti virus serta membuat kebijakan mengenai pembatasan aplikasi yang dapat diinstalasi.

6.3.4 Rekomendasi Pengendalian Risiko Aset Informasi Hilang Temu Ranmor

Dalam mengendalikan risiko kehilangan data atau informasi dapat diatasi dengan mengontrol *backup* informasi atau data penting dan dilakukan secara berkala. Dengan demikian berikut ini dijelakan mengenai *cost and benefit* dari pengendalian risiko *information backup*.

1. *Information Backup*

Salinan informasi cadangan, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan *backup* yang disepakati. Salinan *backup* informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati. Kebijakan mengenai *backup* harus dibuat untuk menentukan persyaratan organisasi dalam melakukan *backup* informasi, perangkat lunak, dan sistem. Fasilitas *backup* yang memadai harus disediakan untuk memastikan bahwa semua informasi penting dan perangkat lunak dapat dipulihkan setelah bencana atau kegagalan media.

Dampak apabila melakukan *backup* secara rutin adalah instansi dapat melindungi aset informasi dari risiko kehilangan atau kerusakan yang disebabkan oleh bencana maupun kesalahan pengguna.

Dampak apabila tidak melakukan *backup* informasi adalah akan menurunkan kesadaran mengenai informasi penting serta mengalami kehilangan dan kerusakan informasi penting bagi instansi.

Cost

-

Benefit

Mengurangi peluang risiko kerusakan dan kehilangan informasi.

Memiliki informasi cadangan apabila risiko terjadi.

6.3.5 Rekomendasi Pengendalian Risiko Aset Jaringan

Dalam mengendalikan risiko kabel terputus dapat diatasi dengan memberikan perlindungan kepada kabel yang digunakan. Dengan demikian berikut ini dijelakan mengenai *cost and benefit* dari pengendalian risiko *cabling security*.

1. *Cabling Security*

   Salah satu metode sederhana untuk melindungi kabel jaringan adalah dengan menentukan lokasi yang aman secara fisik serta menggunakan pelindung kabel. Periksa secara rutin semua kabel jenis kabel dan kabel jaringan yang digunakan untuk menghindari kerusakan fisik atau modifikasi aset, dan pertimbangkan untuk menggunakan pelindung kabel pada semua jenis kabel yang digunakan agar kinerja keamanan informasi pada aset kabel berjalan maksimal (Sadowsky, 2003).

   Dampak apabila menggunakan pelindung kabel adalah kabel jaringan akan terhindar dari risiko kerusakan fisik sehingga kabel jaringan dapat digunakan untuk jangka waktu yang cukup panjang.

   Dampak apabila tidak menggunakan pelindung kabel adalah tingkat kejadian risiko kerusaka fisik pada aset kabel jaringan akan meninggkat sehingga mengganggu operasional instansi.

Cost

-

Benefit

Melindungi aset jaringan dari gangguan dan kerusakan.

Mengurangi tingkat keparahan apabila terjadi risiko.

6.3.6 Rekomendasi Pengendalian Risiko Aset Sumber Daya Manusia

Untuk dapat mengendalikan risiko personil yang menggunakan teknologi informasi yang tidak sesuai dengan fungsinya dapat diatasi dengan dua opsi pengendalian risiko diantaranya yaitu membuat prosedur untuk penggunaan aset teknlogi informasi dengan baik dan melakukan *disciplinary process* bagi personil yang melanggar aturan penggunaan teknologi informasi. Untuk memprioritaskan pengendalian risiko yang dipilih maka dibantu dengan pemaparan menggunakan cost benefit analysis sebagai berikut.

1. *Documented Operation Procedures*

   Prosedur yang terdokumentasi harus disiapkan untuk kegiatan operasional yang terkait dengan pemrosesan informasi, fasilitas komunikasi, penggunaan komputer dan prosedur meninggalkan kmputer, pemeliharaan peralatan, penanganan media, ruang komputer dan manajemen penanganan surat dan keselamatan.

   Dampak apabila memberlakukan prosedur yang tertulis untuk menggunakan perangkat teknologi informasi adalah memastikan bahwa penggunaan teknologi informasi sesuai dengan fungsi dan tujuannya mengurangi penggunaan komputer yang digunakan secara berlebihan atau tidak sesuai dengan fungsinya.

   Dampak apabila tidak memberlakukan prosedur yang tertulis untuk penggunaan perangkat teknologi informasi adalah akan meningkatkan tingkat kejadian risiko penggunaan teknologi yang tidak sesuai dengan fungsinya sehingga aset teknologi informasi dapat mengalami kerusakan.

   Cost

   -

   Benefit

   Memastikan penggunaan teknologi informasi sesuai dengan fungsinya.

   Mengurangi tingkat tingkat kejadian risiko

2. *Disciplinary Process*

   Kebijakan keamanan yang jelas dan terdokumentasi dengan baik akan menentukan tindakan apa yang diperlukan organisasi ketika pelanggaran keamanan terjadi. contoh salah satu kebijakan yang dapat diberlakukan kepada seluruh personil yaitu kebijakan keamanan yang menjelaskan

bagaimana mereka harus berperilaku ketika menggunakan sistem komputer, email, telepon, dan surat suara (Rhodes, 2013). Membuat kebijakan yang terdokumentasi dengan baik akan menentukan tindakan yang akan dilakukan terhadap karyawan yang melakukan pelanggaran keamanan informasi. Penegakan kebijakan keamanan perusahaan untuk karyawan biasanya merupakan tanggung jawab bidang sumber daya manusia. Kebijakan tersebut dibuat untuk menerapkan tindakan hukuman dan penghentian pekerja untuk pelangaran serius terhadap kebijakan keamanan, dan juga pekerja akan mendapatkan peringatan untuk memperbaiki perilaku dan evaluasi etika. Kebijakan tersebut sebaiknya diberlakukan untuk semua karyawan tanpa pengecualian. Hal ini sangat penting untuk tidak mendiskriminasikan atau membedakan antara karyawan saat menegakkan kebijakan.

Dampak apabila memberlakukan *disciplinary process* kepada seluruh personil adalah memberikan informasi mengenai regulasi dan sanki yang akan diterima apabila melakukan pelanggaran yang ada sehingga mencegah risiko personil dalam melakukan pelanggaran

Dampak apabila tidak memberlakukan *disciplinary process* kepada seluruh personil adalah jumlah personil yang melakukan pelanggaran akan meningkat sehingga menurunkan kinerja operasional organisasi.

Cost

-

Benefit

Mengurangi peluang risiko personil dalam melakukan pelanggaran pada peraturan yang telah ditetapkan instansi.

Dari hasil *cost – benefit analysis* tersebut maka instansi dapat melaksanakan pengendalian risiko secara bersamaan yaitu dengan membuat prosedur penggunaan perangkat teknologi informasi serta embuat kebijakan mengenai sanksi bagi personil yang melanggar aturan yang ada.

BAB 7 PENUTUP

7.1 Kesimpulan

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

1. Hasil identifikasi aset menggunakan metode OCTAVE diperoleh 12 aset kritis yang digunakan pada bidang IT Kepolisian Daerah Banten. Aset kritis pada kategori perangkat keras yaitu PC, *server*, AC, perangkat *video confrence, router*, dan kabel jaringan. Pada aset perangkat lunak memiliki 2 aset kritis yaitu aplikasi hilang temu ranmor dan aplikasi pusat informasi kriminalitas nasional. Pada aset jaringan terdapat 1 aset kritis yaitu jaringan internet. Pada aset informasi terdapat 2 aset kritis yaitu informasi hilang temu ranmor dan informasi kriminalitas nasional. Setelah mendapatkan daftar aset kritis dilakukan identifikasi risiko pada masing-masing aset, dan ditemukan sebanyak 28 risiko.
2. Penilaian risiko dilakukan menggunakan metode FMEA dengan menentukan nilai keparahan, tingkat kejadian dan tingkat deteksi risiko. Ketiga aspek tersebut digunakan untuk menghitng tingkat nilai prioritas serta membuat *ranking* risiko sesuai dengan nilai prioritas risiko yang tertinggi pada masing-masing aset. Dari 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 penilaian risiko, dapat dilihat risiko yang memiliki potensi paling tinggi dan membutuhkan perencanaan yang tepat untuk mencegah dan meminimalisir potensi risiko tersebut. Pada ISO 27001 terdapat kontrol yang dapat digunakan sebagai acuan untuk memberikan tindakan terhadap risiko yang memiliki nilai prioritas tertinggi. 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.

7.2 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*. Carnegie Mellon Software Engineering Institute. [Ebook]

Alberts, C. J., Dorofee, A. J. 2002. *Managing Information Security Risks: The OCTAVE Approach*. Addison Wesley. [Ebook]

Candiwan. 2014. *Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia*. Faculty of Economic & Business, Telkom University. Bandung

Chazar, C. 2016. *Model Perencanaan Keamanan Sistem Informasi Menggunakan Pendekatan Metode OCTAVE dan ISO27001:2005*. STMIK Indonesia Mandiri.

Carlson, C. S. 2014. *Understanding and Applying the Fundamentals of FMEAs*. Arizona, USA.

Firdaus, H., Widianti, T., 2015. *Failure Mode And Effect Analysis (FMEA) Sebagai Tindakan Pencegahan Pada Kegagalan Pengujian*. Lembaga Ilmu Pengetahuan Indonesia.

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

Josi, C. dan Singh, U. K. 2017. *Information Security Risk Management Framework — A Step Towards Mitigating Security Risk In University Network.* Journal of Information Security and Applications. 35 (2017). 128–137.

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, R. E., Raymond, J. M. & Michael, R. B. 2009. *The Basic Of FMEA 2nd Edition*. New York : Taylor & Francis Group.

Passenheim, O., 2010. *Enterprise Risk Management*. [Ebook].

Polda Banten. 2016. Sejarah Kepolisian Daerah Banten [Online] tersedia di : < http://banten.polri.go.id/polda-banten/> [Diakses 12 Februari 2018]

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].

Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Gaithersburg: National Systems*. Institute of

Standards and Technology.

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*. United Kingdom. [ebook]