ANALISIS RISIKO KEAMANAN INFORMASI DENGAN METODE OCTAVE ALLEGRO PADA PT. TIRTA INVESTAMA

INFORMATION SECURITY RISK ANALYSIS WITH OCTAVE ALLEGRO METHOD AT TIRTA INVESTAMA

Sulaimanda Isra Hasibuan[1], Tien Fabrianti Kusumasari[2], Rokhman Fauzi[3]
[1]Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University
E-mail: [1]sulaimandaisra@gmail.com, [2]tien.kusumasari@gmail.com, [3]rokhmanfauzi@telkomuniversity.ac.id

Abstrak— Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK), salah satunya Sistem Manajemen Keamanan Informasi (SMKI), sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik. Mengingat peran TIK yang semakin penting dalam upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (Good Corporate Governance). PT. Tirta Investama sebagai salah satu perusahaan swasta di Indonesia memiliki upaya meningkatkan kualitas layanan dengan sejumlah aset yang digunakan untuk mendukung proses bisnis. Standar yang digunakan dalam penelitian ini adalah ISO/IEC 27001:2013. Penelitian ini dilakukan dengan menganalisis profil risiko aset informasi menggunakan metode OCTAVE Allegro. Proses rekomendasi adalah tindak lanjut dari penilaian risiko berupa kontrol pada ISO/IEC 27001:2013. Hasil analisis penelitian akan didapatkan 8 area perhatian yang akan diberikan rekomendasi kontrol berdasarkan ISO/IEC 27001:2013.

Kata kunci: Analisis, Risiko, Manajemen Risiko, Keamanan Informasi, OCTAVE Allegro, ISO 27001, PT. Tirta Investama.

Abstract— *The application of Information and Communication Technology (ICT) governance, the only Information Security Management System (ISMS), has become a necessity and supports every public service provider institution. Consider the role of ICT that is increasingly important in an effort to improve service quality as one of good governance. PT. Tirta Investama as one of the private companies in Indonesia has the support of improving service quality by contributing assets used to support business processes. The standard used in this study is ISO / IEC 27001: 2013. This research was conducted by analyzing asset risk profiles using the OCTAVE Allegro method. The assessment process is a follow-up of the discussion in the form of controls at ISO / IEC 27001: 2013. The results of the research analysis will be obtained 8 areas of attention that will be given control recommendations based on ISO / IEC 27001: 2013.*

Keywords: *Analysis, Risk, Risk Management, Information Security, OCTAVE Allegro, ISO 27001, PT. Tirta Investama.*

1. Pendahuluan

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik, mengingat peran TIK yang semakin penting dalam upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Faktor keamanan informasi merupakan aspek yang sangat penting untung diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama mengalami masalah. Keamanan informasi yang meliputi: kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) [1].

Tata Kelola Teknologi Informasi (TI) telah ditetapkan dalam peraturan Menteri Komunikasi dan Informatika No. 41 tahun 2007 tentang Panduan Umum Tata Kelola TIK Nasional yang bertujuan untuk mewujudkan tata kelola pemerintahan yang baik dan bertanggung jawab *(good governance)*. Melalui penerapan prinsip – prinsip akuntabilitas, transparansi dan supremasi hukum serta merta melibatkan partisipasi masyarakat dalam setiap proses kebijakan publik. Dengan dipublikasikannya regulasi tersebut, institusi pemerintahan pada tingkat kota maupun provinsi harus membuat tata kelola TI sebagai panduan pengelolaan TI.

Sistem Manajemen Keamanan Informasi (SMKI) sendiri merupakan proses untuk menentukan bagimana mengelola, memonitor, dan memperbaiki informasi agar aman. Penerapan SMKI yang baik akan memberikan dampak yang baik terhadap proses bisnis organisasi agar terhindar dari kemungkinan risiko yang mungkin/akan terjadi. ISO/IEC 27001:2013 merupakan standar internasional yang dapat dijadikan pedoman untuk menerapkan SMKI.

Keamanan informasi menjadi hal yang sangat penting saat ini. PT. XYZ sudah menerapkan sistem TI sebagai pendukung proses kegiatan bisnisnya. Salah satu elemen penting dalam tata kelola yang baik adalah tata kelola TI, di dalamnya termasuk tata kelola keamanan informasi. Menurut [2, p. 27] ”Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya memastikan atau menjamin

kelangsungan bisnis *(business continuity)*, meminimalisasi risiko bisnis *(reduce business risk)* dan memaksimalkan pengembalian investasi serta menunjang peluang bisnis".

PT. XYZ sebagai salah satu perusahaan swasta di Indonesia juga diminta memberikan pelayanan terbaik untuk pihak yang membutuhkan informasi, seperti karyawan ataupun pihak lainnya. Oleh karena itu, PT. XYZ membentuk suatu divisi khusus yang melayani sistem manajemen informasi dan layanan interkoneksi. Dalam hal ini, informasi menjadi aset penting karena selain bersifat rahasia, informasi juga memiliki risiko dari akses tidak sah, modifikasi data, pencurian data, *human error*, kerusakan perangkat keras dan perangkat lunak, maupun risiko dari bencana alam [3, p. 243]. Salah satu standar yang dapat digunakan yaitu ISO/IEC 27001:2013. Sangat diperlukannya pengukuran tingkat keamanan informasi untuk menganalisa organisasi yang telah mengamankan informasi sampai sejauh mana, lalu dapat melakukan evaluasi dan perancangan serta pembaharuan SMKI pada organisasi/perusahaan.

Oleh karena itu dilakukan proses perancangan SMKI yang meliputi: penentuan ruang lingkup, tahap analisis risiko, dan tahap penentuan kontrol keamanan yang sesuai dengan standar ISO/IEC 27001:2013. Kemudian mendapatkan obyektif kontrol dan kontrol keamanan dan mengidentifikasi kontrol sesuai klausul yang ada pada ISO/IEC 27001:2013

Dalam jurnal internasional *Information Security Management System Standards : A Comparative Study of Big Five* [4] menjelaskan bahwa ISO/IEC 27001 telah menjadi *framework* yang paling populer dan banyak digunakan dengan presentase 27% dibanding *framework* lainnya, yaitu COBIT (26%), ITIL (8%), BS7799 (18%), dan PCIDSS (21%). ISO/IEC 27001 dapat digunakan pada semua tipe organisasi, karena standar yang fleksibel, dan dapat disesuaikan dengan kebutuhan dan tujuan dari organisasi. Penggunaan ISO/IEC 27001 juga disebabkan karena fleksibilitas yang tinggi dan dikembangkan karena pemanfaatan standar sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai serta ukuran struktur organisasi. Dan pelaksanaan penelitian ini akan dilakukan dengan laporan berjudul "ANALISIS RISIKO KEAMANAN INFORMASI DENGAN METODE OCTAVE ALLEGRO PADA PT. TIRTA INVESTAMA".

2. Landasan Teori

2.1. Struktur Organisasi ISO 27001:2013

Weber dalam Sarno (2009: 28) mendefinisikan Audit Sistem Informasi sebagai proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif.

Tujuan audit sistem informasi yaitu untuk mengetahui sudah sejauh mana sistem mempertahankan informasi dan integritas data, sudah sejauh mana sistem telah efektif membantu pencapaian organisasi dan sudah sejauh mana optimalisasi penggunaan sumber daya secara optimal [5].

2.2. Struktur Organisasi ISO 27001:2013

Struktur organisasi ISO 27001 terbagi menjadi 2 [6] yaitu:

1. Klausul: *Mandatory Process*

Klausul adalah persyaratan yang harus digunakan, jika perusahaan menerapkan SMKI dengen menggunakan standar ISO 27001:2013 dan terdapat 7 klausul diantaranya sebagai berikut:

A. Konteks Organisasi
B. Kepemimpinan
C. Perencanaan
D. Dukungan
E. Operasional
F. Evaluasi Kinerja
G. Perbaikan

2. Annex A : Security Control

Annex adalah dokumen referensi yang digunakan sebagai rujukan untuk menentukan kontrol keamanan yang perlu diimplementasikan ke dalam SMKI, ISO 27001:2013 diantaranya sebagai berikut:

a) A.5: *Information security policies*
b) A.6: *Organisation of Information Security*
c) A.7: *Human Resource Security*
d) A.8: *Asset Management*
e) A.9: *Access Control*
f) A.10: *Cryptography*
g) A.11: *Physical and Environmental Security*
h) A.12: *Operations Security*
i) A.13: *Communications Security*

j) A.14: *System Acquisition, Development and Maintenance*
k) A.15: *Supplier Relationships*
l) A.16: *Information Security Incident Management*
m) A.17: *Information Security Incident Management*
n) A.18: *Compliance*.

.

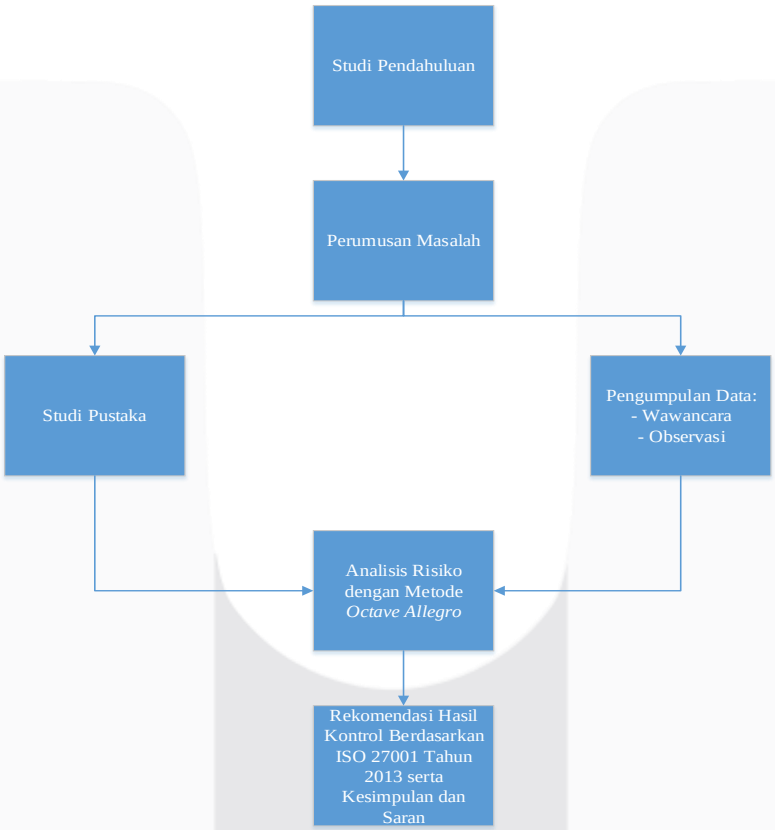
2.3. Metode *OCTAVE Allegro*

OCTAVE Allegro merupakan sebuah framework yang menggunakan pendekata *OCTAVE* dan didesain untuk melakukan penulaian risiko terhadap operasional organisasi atau perusahaan dengan tujuan untuk menghasilkan hasil yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait penilaian risiko [7]. *OCTAVE Allegro* sedikit berbeda dengan pendekatan *OCTAVE* lainnya karena framework ini fokus pada aset informasi yang oleh perusahaan dalam konteks bagaimana aset tersebut digunakan, bagaimana penyimpanan, perpindahan, dan pemrosesannya, serta bagaimana ancaman, kerentanan, dan gangguan dapat terjadi pada aset tersebut. Framework ini terdiri atas delapan tahapan yang diklasifikasikan menjadi empat fase.

3. Metodologi Penelitian

3.1. Sistematika Penulisan

Sistematika penelitian digunakan untuk memberikan arahan yang jelas dan yang akan dilakukan. Berikut adalah sistematika penulisan penelitian yang dapat dilihat pada gambar di bawah.



1. Membangun Kriteria Pengukuran Risiko

Langkah ini memiliki dua aktivitas, yaitu diawali dengan membangun organizational drivers yang digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting. Aktivitas pertama yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas kedua adalah memberikan nilai prioritas impact area menggunakan *Impact Area Ranking Worksheet.*

2. Membangun Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi yang dilanjutkan dengan upaya penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat yaitu mengumpulkan informasi mengenai information asset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset

informasi kritis. Aktivitas lima dan enam adalah membuat deskripsi aset informasi kritis tersebut. Aktifitas tujuh mengisi kebutuhan keamanan sesuai dengan aspek confidentiality, integrity dan availability. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

3. Mengidentifikasi *Container* dari Aset Informasi

Hanya ada satu aktivitas yang merujuk pada tiga poin penting terkait dengan keamanan dan konsep dari *container of information asset* yaitu mengidentifikasi cara aset informasi dilindungi. Tiga poin penting tersebut adalah tingkat perlindungan atau pengamanan aset informasi dan kerentanan serta ancaman terhadap *container* dari aset informasi.

4. Mengidentifikasi Area yang Diperhatikan

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps dan Information Asset Risk Worksheet* maka dapat dicatat area of concern. Berpedoman pada dokumen *Information Asset Risk Worksheet* selanjutnya dilakukan review dari container untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern*.

5. Mengidentifikasi Skenario Ancaman

Aktivitas pertama yang ada pada langkah kelima ini yaitu melakukan identifikasi skenario ancaman tambahan (dapat menggunakan *Threat Scenarios Questionnaries*). Aktivitas kedua adalah melengkapi *Information Asset Risk Worksheets* untuk setiap skenario ancaman yang umum.

6. Mengidentifikasi Risiko

Aktivitas yang ada pada langkah ke-enam adalah menentukan *threat scenario* yang telah didokumentasikan di *Information Asset Risk Worksheets* yang dapat memberikan dampak bagi organisasi.

7. Menganalisa Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheets*. Aktivitas satu dimulai dengan melakukan *review risk measurement criteria* dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko.

8. Memilih Pendekatan Pengurangan Risiko

Aktivitas pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas kedua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

4. Hasil dan Analisis

4.1. Membangun Kriteria Pengukuran Risiko

Pada langkah pertama ini, organizational driver yang akan digunakan untuk mengevaluasi akibat dari sebuah risiko terhadap misi dan tujuan bisnis perusahaan diidentifikasi. Kriteria pengukuran risiko digunakan untuk mengevaluasi akibat dalam masing-masing area dan memprioritaskannya. Di dalamnya terdapat ukuran-ukuran kualitatif yang risikonya dapat dievaluasi dan membentuk dasar dari penilaian risiko sistem informasi.

Tabel 4.1 Kriteria Pengukuran Risiko

***Allegro Worksheet* 6**	**Nilai**	**Dampak Area Prioritas Kerja**
Prioritas		**Area yang Berdampak**
1	**5**	**Produktivitas**
2	**4**	**Reputasi dan Kepercayaan Karyawan**
3	**3**	**Keuangan**
4	**2**	**Keselamatan dan Kesehatan**
5	**1**	**Denda dan Pinalti**

4.2. Membangun Profil Aset Informasi

Langkah kedua adalah membangun profil aset informasi atas aset – aset perusahaan. Profil merupakan representasi dari aset informasi yang menggambarkan fitur, kualitas, karakteristik, dan nilai yang unik. Metode ini berguna untuk meyakinkan bahwa aset tersebut secara jelas dan konsisten digambarkan sehingga dapat

menghindari definisi yang ambigu dari batas-batas aset dan memudahkan dalam menyusun kebutuhan keamanan informasi.

Tabel 4.2 Profil Aset Informasi

***Allegro Worksheet* 7**	**Profil Aset Kritis**
Aset Kritikal	**Rasional Seleksi**
Server Picos *Server Data Warehouse*	Server berfungsi sebagai penggerak/induk dari semua data yang dihasilkan antara lain penyimpan aplikasi dan database yang ada pada komputer klient atau yang terhubung, menyediakan fitur keamanan, melindungi semua komputer yang terhubung dan menyediakan ip address pada mesin komputer yang terhubung
Switch	Digunakan untuk menghubungkan jaringan semua komputer
WLC & Access Point	Digunakan dalam kombinasi dengan *Lightweight Access Point Protocol* (LWAPP) untuk mengatur light-weight access points dalam jumlah yang besar oleh admin jaringan.
Pemilik	
Pemilik dari aset ini adalah Manajer IT	
Persyaratan Keamanan	
Kerahasiaan	Hanya karyawan tertentu yang dapat mengakses aset ini
Integritas	Hanya karyawan tertentu yang dapat memodifikasi aset ini
Ketersediaan	Aset ini harus tersedia untuk semua karyawan selamat 24 jam, 7 hari/ minggu, 52 minggu/ tahun

4.3. Mengidentifikasi Kontainer dari Aset Informasi

Kontainer adalah tempat dimana aset informasi disimpan, dikirim, dan diproses. Dalam langkah ketiga, semua kontainer yang menyimpan, mengirim, dan memproses, baik internal maupun eksternal diidentifikasikan.

Tabel 4.3 Kontainer Aset Informasi

***Allegro Worksheet* 8a**	**Identifikasi (Pemetaan) Risiko Lingkungan Aset Kritis (Teknikal)**
Internal	
Deskripsi Kontainer	**Pemilik**
Jaringan internal. Semua transaksi berjalan dalam jaringan.	Manajer IT
Workstation	Manajer IT
Modul SAP	Manajer IT
WLC & Access Point	Manajer IT
Firewall	Manajer IT

4.4. Mengidentifikasi Area yang Diperhatikan

Langkah keempat Identifikasi *area of concern* dengan meninjau kembali setiap kontainer untuk melihat dan menentukan *area of concern* yang potensial dilanjutkan dengan melakukan dokumentasi setiap *areas of concern* yang telah diidentifikasi. *Area of concern* diperluas untuk mendapatkan *threat scenarios* kemudian didokumentasikan untuk melihat apakah mempengaruhi *security requirements*.

Tabel 4.4 Area Perhatian

No	Area Perhatian	Aset Terkait
1	Perubahan data master dan data transaksi	Aplikasi
2	*Network failure*	Infrastruktur
3	Pencurian media atau informasi penting	Aplikasi
4	*Hardware failure*	*Hardware*
5	Serangan *Hacker*	Infrastruktur
6	Penyalahgunaan hak akses	Aplikasi
7	Kebakaran	Infrastruktur
8	*Human* atau *technician error*	*People*

4.5. Mengidentifikasi Skenario Ancaman

Dalam langkah kelima ini, area – area yang telah diidentifikasi pada langkah sebelumnya diperluas menjadi skenario ancaman yang lebih jauh mendetailkan properti dari sebuah ancaman dengan menggunakan sebuah *threat tree*. Langkah ini berguna untuk memberikan pertimbangan atas kemungkinan dalam skenario ancaman. Kemungkinan ini kemudian dibagi ke dalam *high*, *medium*, atau *low*.

Tabel 4.5 Skenario Ancaman

No	Area Perhatian	Skenario Ancaman	
1	Perubahan data master dan data transaksi	***Actor***	Staff IT
		Mean	Kehilangan atau penimpaan data dalam memback-up data yang secara rutin (data transaksi) dan atau sesekali (data master) dilakukan
		Motive	*Human error*
		Outcome	*Destruction, Modification*
		Security Requirement	Perencanaan jadwal back up berkala yang matang dengan bantuan setting dari sistem dengan penolakan jadwal yang sama dengan sebelumnya
2	*Network failure*	***Actor***	Staff IT
		Mean	Kesalahan dalam melakukan konfigurasi
		Motive	*Accidental*
		Outcome	*Interruption*
		Security Requirement	Perlu dilakukan tindakan control jaringan dengan cara dimonitoring dan dipelihara keamanan sistemnya yang ditinjau secara berkala.

4.6. Mengidentifikasi Risiko

Pada langkah keenam, konsekuensi bagi organisasi jika sebuah ancaman terjadi dicatat, dalam mendapatkan gambaran risiko secara lengkap. Sebuah ancaman dapat mempunyai akibat – akibat yang potensial bagi organisasi.

Tabel 4.6 Nilai Area Dampak

Area Dampak	Prioritas	Nilai Dampak		
		Rendah (1)	Sedang (2)	Tinggi (3)
Produktivitas	1	5	10	15
Reputasi dan Kepercayaan Karyawan	2	4	8	12
Keuangan	3	3	6	9
Keselamatan dan Kesehatan	4	2	4	6
Denda dan Pinalti	5	1	2	3

4.7. Menganalisis Risiko

Pada langkah ketujuh, pengukuran kuantitatif dari sejauh mana organisasi terkena dampak dari *threat* dihitung. Nilai risiko relatif didapatkan dengan cara mempertimbangkan sejauh mana konsekuensi atas dampak risiko terhadap berbagai *impact area*, dan memperkirakan kemungkinannya.

Tabel 4.7 Nilai Risiko Relatif

No	Area Perhatian	Risiko			
1	Perubahan data master dan data transaksi setelah back-up data	***Consequences***	Diperlukan kecakapan khusus dan perhatian detail dalam mengerjakan back-up data		
		Severity	**Area Terdampak**	**Nilai**	**Skor**
			Produktivitas	Tinggi	15

No	Area Perhatian	Risiko			
			Reputasi dan Kepercayaan Karyawan	Sedang	8
			Keuangan	Sedang	6
			Keselamatan dan Kesehatan	Rendah	2
			Denda dan Pinalti	Rendah	1
		Relative Risk Score			32
2	*Network failure*	***Consequences***	Perlu dilakukan tindakan kontrol jaringan dengan cara dimonitoring dan dipelihara keamanan sistemnya yang ditinjau secara berkala.		
		Severity	**Area Terdampak**	**Nilai**	**Skor**
			Produktivitas	Tinggi	15
			Reputasi dan Kepercayaan Karyawan	Sedang	8
			Keuangan	Sedang	6
			Keselamatan dan Kesehatan	Sedang	4
			Denda dan Pinalti	Rendah	1
		Relative Risk Score			34

4.8. Memilih Pendekatan Pengurangan Risiko

Dalam langkah terakhir dari proses *OCTAVE Allegro* ini, penulis dan organisasi menentukan risiko yang memerlukan mitigasi dan mengembangkan strategi untuk mengurangi risiko tersebut. Hal ini dilakukan dengan cara memprioritaskan risiko-risiko berdasarkan nilai risiko relatif, kemudian mengembangkan strategi mitigasi dengan mempertimbangkan nilai dari aset dan kebutuhan keamanan, kontainer atas aset, serta lingkungan operasional yang unik dari organisasi.

Pool	Area Perhatian	Pendekatan Mitigasi
30 – 45	1. Perubahan data master dan data transaksi 2. Network failure	Mitigasi
16 – 29	Tidak ada	Mitigasi atau Ditangguhkan
0 – 15	Tidak ada	Diterima

5. Rekomendasi Kontrol, Kesimpulan, Dan Saran

5.1. Rekomendasi Kontrol

Dari hasil identifikasi dan penilaian risiko maka berikut beberapa kontrol objektif dari standar ISO 27001 yang direkomendasikan untuk penanganan potensi risiko-risiko yang telah diidentifikasi.

Tabel 5.1 Rekomendasi Kontrol

No	Area Perhatian	Identifikasi Potensi Solusi			Referensi
		People	***Process***	***Technology***	
1	Perubahan data master dan data transaksi		Penambahan Kebijakan pembatasan hak akses terhadap *database*		Menerapkan Kontrol A.9 Kendali Akses
2	*Network failure*		Penambahan kebijakan dan prosedur untuk memantau, menganalisis, dan mengevaluasi perangkat		Menerapkan Kontrol 9.1 Pemantauan, Pengukuran, Analisis Dan Evaluasi

No	Area Perhatian	Identifikasi Potensi Solusi			Referensi
		People	*Process*	*Technology*	
			infrastruktur jaringan		

5.2. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan bahwa:

a. Dari hasil analisis potensi risiko pada PT Tirta Investama diperoleh profil risiko dengan 8 area perhatian yang akan diberi rekomendasi kontrol dari ISO 27001 yaitu:
   1. Perubahan data master dan data transaksi
   2. *Network failure*
   3. Pencurian media atau informasi penting
   4. *Hardware failure*
   5. Serangan *Hacker*
   6. Penyalahgunaan hak akses
   7. Kebakaran
   8. *Human* atau *technician error*

b. Dalam rekomendasi analisis risiko adanya usulan untuk melakukan perbaikan kontrol. Berikut rekomendasi dari ISO 27001:
   1. *People*: Penambahan deskripsi kerja, kewenangan, dan kompetensi terhadap divisi Project & Asset.
   2. *Process*: Dilakukan usulan berupa kebijakan dan prosedur berdasarkan temuan yang didapatkan pada PT. Tirta Investama

5.3. Saran

Adapun saran dari penelitian yang dilakukan adalah sebagai berikut:

1. Menerapkan rekomendasi perbaikan kontrol berdasarkan analisis risiko.

2. Dengan adanya rekomendasi yang telah diberikan, diharapkan PT. Tirta Investama dapat menerapkan sistem manajemen keamanan informasi dengan lebih baik.

DAFTAR PUSTAKA

[1] KOMINFO, Panduan Penerapan Tata Kelola Keamanan Informasi, 2011.

[2] R. Sarno, Sistem Manajemen Keamanan Informasi Berbasis ISO 27001, 2009.

[3] K. N. F. Deni Darmawan, Sistem Informasi Manajemen, Bandung: Remaja Rosdakarya, 2013.

[4] M. N. A. Y. C. T. Heru Susanto, "Information Security Management System Standards: A Comparative Study of the Big Five," 2011.

[5] I. Swastika and I. Putra, "Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus," 2016.

[6] B. ISO, "ISO/IEC 27001," 2013.

[7] R. Caralli, J. Stevens, L. Young and W. Wilson, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Pittsburgh, Pennsylvania: Carnegie Mellon University, 2007.