PERANCANGAN MANAJEMEN KEAMANAN INFORMASI MENGGUNKAN METODE ANALISIS RISIKO ISO 27005:2008 PADA DINAS KOMUNIKASI DAN INFORMATIKA JAWA BARAT

DESIGN OF INFORMATION MANAGEMENT SECURITY USING RISK ANALYSIS ISO 27005 IN DINAS KOMUNIKASI DAN INFORMATIKA JAWA BARAT

Erny Nursetyawati[1], Rokhman Fauzi[2], Ryan Adhitya Nugraha[3]
Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]ernynursetyawati@student.telkomuniversity.com, [2]rokhmanfauzi@telkomuniversity.ac.id, [3]ranugraha@telkomuniversity.ac.id

Abstrak

Perkembangan teknologi Informasi saat ini berkembang pesat, sehingga teknologi informasi begitu berperan penting dalam menunjang proses bisnis suatu organisasi dan untuk meningkatkan *value* suatu perusahaan. Semakin berkembanganya teknologi informasi maka menjadikan informasi sebagai salah satu asset yang penting dan perlu untuk dilindungi keamanannya.
Dinas Komunikasi dan Informatika Jawa Barat merupakan organisasi milik pemerintah yang menyediakan layanan bagi pemerintahan daerah Jawa Barat sehingga informasi pada Dinas Komunikasi dan Informatika sangat perlu untuk dilindungi agar pihak – pihak yang tidak memiliki hak akses tidak dapat mengakses dan mengendalikannya, sehingga terlindungi dari potensi ancaman dan risiko dari berbagai jenis dan sumber. Dengan menerapkan manajamen informasi dapat membantu proses untuk menjaga dan melindungi keamanan informasi dari berbagai ancaman Risiko. Pada Penelitian ini bertujuan untuk melakukan perancangan manajemen keamanan informasi pada Dinas Komunikasi dan Informatika Jawa Barat khususnya pada aplikasi yang dikelola oleh Dinas Komunikasi dan Informatika Jawa Barat yaitu aplikasi service desk, penilitian dilakukan dengan cara menganalisis risiko kemudian membuat rancangan yang dapat digunakan sebagai acuan dalam melakukan penerapan keamanan informasi pada aplikasi service desk. Pada penelitian untuk menganalisis risiko menggunakan pendekatan dari Dari hasil analisis risiko menggunakan ISO 27005 pada aplikasi service desk milik Dinas Komunikasi dan Informatika Jawa Barat akan didapat level dari setiap risiko yang telah dianalisis, kemudian dilakukan risk response atau respon pada setiap risiko, setelah diberikan respon terhadap risiko lalu melakukan perancangan keamanan informasi menggunakan ISO 27001 sebagai acuannya, yaitu dengan tahapan memberikan kontrol yang tepat pada setiap risiko, lalu dari semua hasil analisis yang telah dilakukan akan dibuat kebijakan-kebijakan sesuai dengan rekomondasi pada setiap risiko, kebijan yang diusulkan bisa menjadi acuan untuk Dinas Komunikasi dan Informatika Jawa Barat dalam melindungi keamanan informasi pada aplikasi service desk.

Kata kunci : Informasi, Keamanan Informasi, Analisis Risiko, ISO 27005, ISO 27001, Service Desk, Dinas Komunikasi dan Informatika Jawa Barat

Abstract

The development of information technology is currently growing rapidly, so that information technology plays an important role in supporting an organization's business processes and to increase the value of a company. As information technology develops, information becomes one of the most important assets and needs to be protected. The West Java Communication and Informatics Office is a government-owned organization that provides services to the West Java regional government so that information on the Communication and Informatics Office needs to be protected so that those who do not have the access rights cannot access and control it, so they are protected from potential threats and risks of various types and sources. By implementing the information management, it can help the process to maintain and protect the information security from various risk threats
This research aims to design an information security management at the West Java Communication and Informatics Office, especially in an applications managed by the West Java Communication and

Informatics Office, namely the service desk application, the research is carried out by analyzing risk then making a design that can be used as a reference in implementing the information security in the service desk applications. In this research, we analyze the risk using the approach of the ISO 27005 standard as an information technology risk management framework. The initial stages in determining the design of information security consist of risk analysis, namely the identification of assets, identification of threats, weaknesses, probabilities and impacts. The second stage is determining security controls in accordance with the results of the previous risk analysis.

From the results of the risk analysing using ISO 27005 on the service desk application owned by the Office of Communications and Informatics in West Java, we will get the level of each risk that has been analyzed, then we response to each risk, after that we design the information security using ISO 27001 as a reference, that is, by giving the right control for each risk, then from all the results of the analysis that have been carried out, policies will be made according to the recommendations for each risk, the proposed policy can become a reference for the Office of Communication and Informatics in West Java to protect the information security in the service desk application.

Keywords: : Information, Information Security, Risk Analysis, ISO 27005, ISO 27001, Service Desk, West Java Communication and Informatics Office

1. Pendahuluan

Seiring berkembangannya teknologi, banyak kalangan yang menfaatkan teknologi, baik perorangan maupun kelompok, salah satunya yaitu Instansi Pemerintahan, dalam hal ini secara spesifik yang akan dibahas yaitu Dinas Komunikasi dan Informatika Provinsi Jawa Barat, merupakan salah satu Instansi Pemerintahan di Indonesia yang memanfaatkan keberadaan teknologi dengan membuat sistem informasi berdasarkan instruksi presiden no 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government dan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Regulasi SPBE).

Dinas Komunikasi dan Informatika Provinsi Jawa Barat adalah instansi pemerintahan yang memiliki tanggung jawab atas pengolahan informasi dalam lingkungan Pemerintahan Jawa Barat. Instansi ini mencakup penyediaan sistem informasi daerah dan pemberian solusi untuk pengolahan data Pemerintahan Jawa Barat. Sistem Informasi yang dibangun Dinas Komunikasi dan Informatika digunakan oleh instansi-instansi daerah yang berada di Provinsi Jawa Barat. Salah satunya adalah aplikasi Service Desk yang menjadi fokus penelitian ini, aplikasi service desk merupakan aplikasi milik Dinas Komunikasi dan Informatika Jawa Barat yaitu aplikasi berbasis website yang digunakan untuk memfasilitasi perangkat daerah dalam melakukan permintaan atau keluhan terhadap penerapan layanan teknologi informasi dilingkungan Pemerintah Provinsi Jawa Barat . Sehingga keamanan informasi di instansi ini harus dijaga dikelola dengan baik.

Konsep yang akan diterapkan dalam hal ini yaitu menggunakan metode ISO 27005 sebagai basis untuk menganalisis risiko tentang keamanan informasi yang mengatur tentang manajemen risiko dalam keamanan informasi. ISO 27005 menyediakan pedoman untuk manajemen risiko keamanan informasi, sehingga dapat membantu merancang manajemen keamanan informasi dengan mengetahui terlebih dahulu risikonya. Setelah mengetahui risikonya maka dilakukan analisis dengan metode ini, dengan tujuan dapat mengendalikan risiko yang telah diketahui. Untuk pemelihan kontrol keamanan informasi mengacu pada kerangka kerja standar internasional yaitu ISO 27001 yang menyediakan kerangka kerja dalam ruang lingkup penggunakan teknologi informasi dan pengelolaan asset sehingga dapat membantu organisasi dalam memastikan keamanan informasi yang diterapkan sudah efektif. (Jurnal Teknik ITS Vol. 6, No. 1, 2017). Keamanan informasi begitu penting dalam mendukung kesuksesan Teknologi Informasi pada suatu organisasi atau instansi pemerintahan, oleh karena terdapat beberapa tahapan untuk mengelola keamanan informasi dengan cara mengidentifikasi, menganalisis, memberikan solusi dan melaporkan risiko**.**

Maka dari itu Dinas Komunikasi dan Informatika sebagai instansi pemerintahan memerlukan pedoman atau acuan dalam menjalankan keamananan informasi yang efisien dan efektif sehingga dapat menjaga dan melindungi informasi yang dimiliki. Penelitian ini dilakukan bermaksud untuk membantu dan memberikan solusi dalam penilaian risiko dan memberikan solusi dengan melakukan perancangan kontrol informasi di Dinas Komunikasi dan Informatika Jawa Barat. Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi, dengan membuat kontrol keamanan sesuai dengan hasil dari analisis risiko sebelumnya.

2. Dasar Teori

2.1. Keamanan Informasi

Keamanan informasi merupakan suatu perlindungan terhadap informasi dari berbagai ancaman dan risiko. Setiap informasi harus dijaga keamanannya agar tidak dapat disalahgunakan oleh pihak yang dapat merugikan organisasi, baik pihak eksternal maupun internal perusahaan. Jika terjadi kebocoran informasi atau pencurian informasi dapat mengakibatkan kerugian baik dari sisi finansial maupun produktifitas perusahaan. Tingkat keamanan pada informasi juga bergantung pada tingkat sensitifitas informasi dalam *database*, informasi yang tidak terlalu sensitif sistem keamanannya tidak terlalu ketat sedangkan untuk informasi yang sangat sensitif perlu pengaturan tingkat keamanan yang ketat untuk akses ke informasi tersebut (Nasional, 2013). (Astari Retnowardhani)

2.2. Aspek Kemanan Informasi

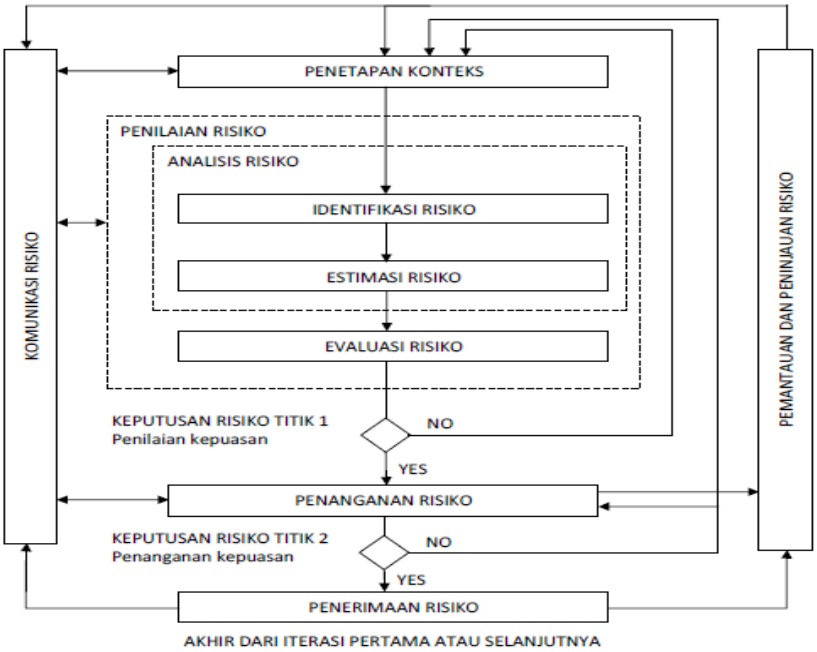
Keamanan Informasi dilakukan untuk memenuhi aspek yang harus diterapkan dan diperhatikan menurut Whitman dan Mattod (2009) menyebutkan beberapa aspek yang terkait dengan keamanan informasi yaitu *Privacy* Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari orang lain, *Identification* Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi umumnya dilakukan dengan penggunaan *username* dan *user* ID, *Authorization* Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia dan komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari informasi. Dan *Accountability* Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu.

2.3. Manajemen Risiko

Manajemen risiko ialah suatu pendekatan terstruktur yang dilakukan untuk pengawasan risiko dan perlindungan aset yang dimiliki suatu organisasi. Pada teknologi informasi, risiko disebabkan oleh penggunaan teknologi informasi dalam suatu organisai yang terdiri dari semua kejadian yang terkait dengan penggunaan teknologi informasi sehingga memiliki kemungkinan terjadinya risiko

2.4. Proses Manajemen Risiko Keamanan Informasi

Menurut ISO 27005 proses manajemen risiko keamanan informasi terdiri dari penetapan konteks, penilaian risiko, perlakuan terhadap risiko, penerimaan risiko, komunikasi risik dan pemantauan dan pengkajian risiko

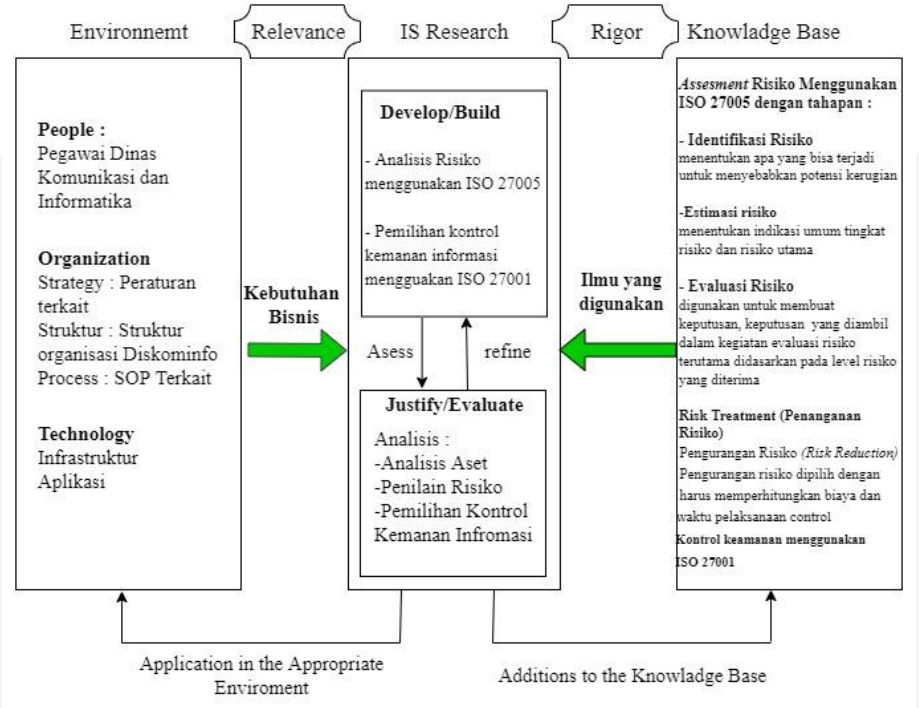


Gambar 1 Proses Manajemen Risiko Keamanan Informasi

Berdasarkan gmabar diatas proses manajemen risiko diawali dengan penetapan konteks, identfikasi risiko dimanan didalamnya dialakukan identifikasi aset, ancaman dan kerentanannya, kemudian estimasi risiko dan yang terakhir merupakan evaluasi risiko yang dibagi menajadi 4 yaitu: mengurangi risiko *(risk reduction)*, mempertahankan Risiko *(Risk Retention)*, menghindari risiko *(risk avoidance)*, dan mentransfer risiko *(Risk Transfer)*

3. Metodologi Penelitian

Model konseptual dalam tugas akhir ini mengacu pada *Hevner's design research* 2004 menyajikan serangkaian desain sebagai pedoman untuk penelitian dalam disiplin Sistem Informasi. Design science research membutuhkan pembutan artefak yang inovatif dan bertujuan untuk mengatai dan menyelesaikan masalah khusus, dan sebagai *knowledge base* atau suatu jenis basis data yang dipergunakan untuk manajemen pengetahuan yaitu dengan menggunakan ISO/IEC 27005:2008 yang digunakan sebagai metode analisis risiko, lalu menggunakan ISO/IEC 27001 sebagai metode untuk pemilihan kontrol keamanan informasi, ISO 27001 merupakan dokumen standar Sistem Keamanan Sistem Informasi yang akan memberikan gambaran secara umum mengenai proses yang harus dilakukan oleh organisasi untuk mengimplementasikan konsep-konsep kemanan informasi. Berikut gambar dan penjelesan model konseptual yang digunakan.



Gambar 2 Model Konseptual

4. Hasil dan Pembahasan

A. Identifikasi Risiko

Tujuan dari identifikasi risiko adalah untuk menentukan apa yang bisa terjadi untuk menyebabkan potensi kerugian, dan untuk mendapatkan wawasan tentang bagaimana, di mana dan mengapa kerugian yang mungkin terjadi pada aset teknologi, sumber daya manusia, proses bisnis dan informasi dengan dilakukan identifikasi – identifikasi kerentanan dan ancaman pada setiap aset, kerentanan dan ancaman yang ada dibagi menajadi beberapa faktor antara lain faktor kelalaian manusia, faktor dari dalam aset itu sendiri, dan faktor dari bencana alam tabel berikut menjelaskan risiko terindentifikasi dalam penelitian ini dan penelilain risiko berdasarkan SPBE yang terdiri dari level dampak dan level kemungkinan, tabel berikut menejelaskan aset yang berkaitan dengan aplikasi service desk Dinas Komunikasi dan Informatika Jawa Barat

Tabel 1 Aset

No	Kategori Aset	Nama Aset
1	Teknologi	Aplikasi Service Desk
2		Database
3		Database Server
4		PC
5		Hub
6		Switch
7		Bridge
8		Router
9		Firewall
10		Anti Virus
11	SDM	Kepala seksi layanan infrastruktur
12		Caller
13		Helpdesk
14		Technican
15		Admin / Agen
16	Proses Bisnis	Proses penginputan tiket permintaan layanan baru
17		Proses penginputan insiden baru
18		Proses pemeriksaan tiket yang masuk
19	Informasi	Data Permintaan Layanan
20		Data Insiden
21		Data User
22		Data Tiket Masuk
23		Data Layanan

B. Risiko

Tabel berikut merupakan risiko yang terjadi pada setiap aset yang berkaitan dengan aplikasi service desk

Tabel 2 Risiko

No	Risiko	ID Risiko
1	Gangguan terhadap layanan akibat adanya error dan bug	T1
2	Modifikasi akibat defacing dan SQL Injection oleh pihak yang tidak memiliki akses, penyalahgunaan hak akases	T2
3	Ketidakpuasaan user dengan layanan	T3
4	Penyalahgunaan hak akses pada database	T4
5	Penyebaran data dan Informasi rahasia pada database	T5
6	Data hilang karena tidak melakukan backup data pada database	T6
7	Ruangan database rubuh akibat bencana alam gempa bumi	T7
8	Kebocoran atap ruangan database akibat hujan menyebabkan database terkena air hujan	T8
9	Pencurian,kehilangan database	T9
10	Kebocoran atap ruangan database server akibat hujan menyebabkan database terkena air hujan	T10
11	Server Down	T11
12	Penyalahgunaan hak akses pada database server	T12
13	Penyebaran data dan informasi rahasia pada server	T13
14	Data hilang karena tidak melakukan backup data pada database server	T14
15	Pencurian, kehilangan server	T15
16	PC Error	T16
17	Windows tidak berjalan dengan semestinya jika menggunakan OS bajakan	T17
18	Pencurian, kehilangan PC	T18
19	Hub rusak	T19

No	Risiko	ID Risiko
20	Gangguan terhadap hub karena tidak ada aliran listrik	T20
21	Penyalahgunaan hak akses pada switch	T21
22	Error / hang pada switch	T22
23	Pencurian, kehilangan switch	T23
24	Gangguan pada bridge akibat arus listrik terputus	T24
25	Pencurian, kehilangan bridge	T25
26	Kerusakan router akibat DoS Attack	T26
27	Penyalahgunaan hak akses, mengubah konfigurasi tidak sesuai standar oleh pihak yang tidak berwenang pada router	T27
28	Pencurian kehilangan router	T28
29	Penyalahgunaan hak akses, mengubah konfigurasi tidak sesuai standar oleh pihak yang tidak berwenang pada firewall	T29
30	Gangguan terhadap layanan akibat serangan virus yang tidak terdeteksi oleh anti virus yang tidak up to date	T30
31	Penyalahgunaan otoritas	S1
32	Kepala seksi layanan infrastruktur kurang melakukan monitoring pekerjaan	S2
33	Kepala seksi layanan infrastruktur lupa password sehingga tidak dapat menindaklajuti pekerjaan yang melalui aplikasi	S3
34	Kesalahan input data sehingga data tidak sesuai dan Tindak lanjut akan tidak sesuai dengan masalah	S4
35	Melakukan pelaporan insiden dan permintaan layanan tidak disampaikan secara detail sehingga penanganan insiden dan layanan menjadi lama seperti tidak melampirkan file surat atau foto case yg terjadi hardware maupun software.	S5
36	Caller lupa password sehingga tidak dapat menindaklajuti pekerjaan yang melalui aplikasi	S6
37	Helpdesk tidak memberikan penjelasan secara detail kepada caller	S7
38	Helpdesk Lupa password sehingga tidak dapat menindaklajuti pekerjaan yang melalui aplikasi	S8
39	Aplikasi yang dibuat tidak sesuai dengan kebutuhan dan ketentuan	S9
40	Aplikasi yang dibuat selesai dalam waktu yang lebih lama	S10
41	Technician tidak dapat mengembangkan aplikasi	S11
42	Technican kurang berkompeten	S12
43	Technician lupa password sehingga tidak dapat menindaklajuti pekerjaan yang melalui aplikasi	S13
44	Kebocoran data akibat tidak mengikuti standar / prosedur terkait pengembangan aplikasi	S14
45	Lupa melakukan *assign ticket* sehingga tiket tidak dapat diproses	S15
46	Laporan permintaan layanan dan pengaduan insiden tidak tercatat sehingga laporan hilang dan tidak ada arsip	S16
47	Kualitas layanan tidak sesuai akibat tidak mengikuti standar / prosedur terkait	S17
48	Kinerja admin yang tidak konsisten	S18
49	Admin lupa password sehingga tidak dapat menindaklajuti pekerjaan yang melalui aplikasi	S19
50	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan	S20
51	Tidak lengkapnya data yang dimasukan saat penginputan menyebabkan layanan yang akan diproses akan tidak sesuai dengan kebutuhan	P1
52	Proses assign ticket menjadi lama karena data ticket tidak detail	P2
53	Tidak menjelaskan secara detail insiden yang terjadi mengakibtkan penaganan insiden menjadi lama	P3
54	Tiket masuk tidak semua terdata, proses penanganan permintaan layanan yang diajukan tidak dapat dilakukan	P4
55	Hardware dan Software yang dibutuhkan untuk membuat aplikasi tidak support	P5
56	Data yang dibutuhkan tidak lengkap	P6
57	Aplikasi yang diproses tidak sesuai dengan kebutuhan	P7
58	Kerusakan data permintaan layanan, data sudah ada tetapi tidak terbaca	I1
59	Data permintaan layanan hilang	I2
60	Kerusakan data insiden, data sudah ada tetapi tidak terbaca	I3

No	Risiko	ID Risiko
61	Data insiden hilang	I4
62	Kerusakan data user, data sudah ada tetapi tidak terbaca	I5
63	Data user hilang	I6
64	Data user diperjual belikan	I7
65	Kerusakan data tiket masuk, data sudah ada tetapi tidak terbaca	I8
66	Data tiket masuk hilang	I9
67	Kerusakan data layanan, data sudah ada tetapi tidak terbaca	I10
68	Data layanan Hilang	I11

Selah dianalisis aset yang dimiliki maka tabel dibawah ini mengelompokan level risiko dari setiap aset yang telah dianalisis, risiko yang didapat sebanyak 68 risiko dari jumlah asetnya 25

Tabel 3 Pengelompokan hasil penilaian

Kategori	Level Risiko				
	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Teknologi	8	11	9	2	-
Sumber Daya Manusia	-	11	6	3	-
Proses Bisnis	-	3	2	2	-
Informasi	6	-	5	-	-

C. Risk Response

Setelah dikelompokan dan diketahui jumlah level risiko yaitu sangat rendah, rendah, sedang, tinggi dan sangat tinggi disetiap kategori aset, selanjutnya akan dilakukan analisis untuk *Risk Response* yaitu memilih respon atau tanggapan untuk mengatasi risiko yang dimiliki oleh setiap aset. Berikut merupakan tabel untuk untuk pengelompokan *risk response*

Tabel 4 Risk Response

ID Risiko	Risk Response	Jumlah
T2.T4,T5,T7,T8,T9,T10,T12,T13,T15,T16 T18,T21,T23,T25,T26,T27,T28,T29,S1,S8 S9,S11,S12,S13,S15,S16,S18,S19,S20,P5 P6,P7,I2,I4,I6,I7,I9,I11	Menerima Risiko	39
T11,S10	Mentransfer Risiko	2
T1,T3,T6,T14,T17,T19,T20,T22,T24,T30 S2,S3,S5,S6,S7,S14,S17,P1,P2,P3,P4,I1,I3 I5,I8,I10	Mengurangi Risiko	27

D. Rekomendasi Kontrol

Tabel dibawah ini menjelaskan rekomendasi kontrol yang diambil berdasarkan keaadan risiko, untuk pemeilihan kontrol diambil dari ISO 27001

Tabel 5 Rekomendasi Kontrol

ID Risiko	**ISO 27001**
T1	*Controls against malware A.12.2.1* dan *Separation of development, testing and operational environments A.12.1.4*
T3	Berkaitan dengan manajemen layanan
T3,T6,T14,I1,I3,I5,I8,I10,P4	*Information backup A.12.3.1* dan *Management responsibilities A.7.2.1*
T11	*Information security in supplier relationships A.15.1*
T17	*Installation of software on operational systems A.12.5.1*
T19,T22	*Equipment maintenance A.11.2.4*
T20,T24	*Supporting utilities A.11.2.2*

ID Risiko	ISO 27001
T30	*Controls against malware A.12.2.1* Dan *Installation of software on operational systems A.12.5.1*
S2, S7	*Information security awareness, education and training A.7.2.2* *Management responsibilities A.7.2.1*
S3,S6	*Password management System A.9.4.3*
S4	*Handling of assetsA.8.2.3*
S5,P1,P2,P3	*Collection of evidence A.16.1.7*
S10	*Outsourced development A.14.2.7*
S14,S17	*Handling of assets A.8.2.3* *Compliance with security policies and standards A.18.2.2*

5. Kesimpulan

Aplikasi service desk memiliki 24 aset yang dibagi menjadi aset utama dan aset pendukung, aset utama terdiri dari proses bisnis, kegiatan, informasi (data) dan aset pendukung terdiri dari hardware, software dan sumber daya manusia. Aset yang yang berkaitan dengan aplikasi service desk dibagi menjadi 4 kategori yaitu kategori teknologi yang berisi hardware dan software, kategori sumber daya manusia yang berisi stakeholder yang berkaitan dengan dengan aplikasi service desk, kategori proses bisnis yang berisi proses-proses yang dapat dilakukan oleh aplikasi service desk dan yang terkhir adalah kategori informasi yang berisi data-data yang berada pada aplikasi service desk.

Aset yang berkaitan dengan aplikasi service desk dianalisis keretanan dan ancamannya serta sumber dari ancaman dan kerentanan tersebut, maka didapat 68 risiko, lalu dilakukan penilaian disetiap risiko yang dilihat dari level dampak dan level kemungkinan lalu didapat level risiko dan keterangannya yaitu pada kategori teknologi didapat 8 risiko yang sangat rendah, 11 risiko rendah,, 9 risiko sedang, dan 2 risiko tinggi, pada kategori Sumber Daya Manusia didapat 11 risiko rendah, 6 risiko sedang dan 3 risiko tinggi, untuk kategori proses bisnis didapt 3 risiko rendah, 2 risikp sedang dan 2 risiko tinggi, dan pada kategori informasi didapat 6 kategori sangat rendah dan 5 kategori sedang. Hasil penilain maka ditentukan risk response atau respon pada risiko yaitu didapat 27 risiko dihindari atau risk reduction, 2 risiko ditransfer atau risk transfer dan 39 risiko dikurangi atau risk reduction

Rekomendasi kontrol risiko diambil berdasarkan referensi dari ISO 27001. Risiko diberikan kontrol berdasarkan hasil dari analisis risk response, hasil akhir dari rekomendasi kontrol yaitu berupa kebijakan yang disesuaikan dengan kondisi risiko tersebut

Daftar Pustaka

[1] Y. R. Eryanto, Perancangan Manajemen Keamanan Risiko Teknologi Informasi Berdasarkan Kerangka Kerja ISO/IEC 27005 di PT. Z, Jakarta , 2015.

[2] W. Yustanti, A. Qoiriah, R. Bisma and A. Prihanto, "Strategi Identifikasi Resiko Keamanan Informasi Dengan Kerangka Kerja ISO 27005:2018," *Journal Information Engineering and Educational Technology Volume 03 Nomor 02.*

[3] F. I. S. Yudha and R. E. Gunadhi, "RISK ASSESSMENT PADA MANAJEMEN RESIKO KEAMANAN INFORMASI MENGACU PADA BRITISH STANDARD ISO/IEC 27005 RISK MANAGEMENT," *ISSN: 2302-7339 Vol. 13 No. 1* , 2016.

[4] D. Setiawan, "Kebijakan Sistem Informasi Manajemen Keamanan Standar ISO 17799:27002," 2009.

[5] S. Salahuddin, A. Ambarwati and M. N. A. Azam, "IDENTIFIKASI RISIKO KEAMANAN INFORMASI MENGGUNAKAN ISO 27005 PADA SEBUAH PERGURUAN TINGGI SWASTA DI SURABAYA".

[6] A. N. Rilyani, Y. Firdaus and D. D. Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 Studi Kasus : i-Gracias Telkom University," *e-Proceeding of Engineering : Vol.2, No.2 Agustus,* 2015.

[7] V. Reni, Marwata and S. Irwan, "ANALISIS KEAMANAN SIKAPEG IVET BERBASIS ISO 27001:2013," *Journal for Informatics Education,* 2018.

[8] K. H. Dewantara, Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi Berdasarkan Standar ISO 27001:2005 dan ISO 27002:2013, Surabaya , 2016.

[9] Asriyanik and Prajoko, "Manajemen Risiko Keamanan Informasi Menggunakan ISO:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," *Jurnal Teknik Informatika dan Sistem Informasi Volume 4 Nomor 2,* 2018.

[10] Kementrian Hukum dan HAM, Keputusan Menteri Hukum da Ham Nomor: M.HH-01.06.02 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Kementrian Hukum dan HAM, 2017.

[11] Badan Siber dan Sandi Negara , CYBER INCIDENT MANAGEMENT & RESPONSE.

[12] Badan Pengkajian dan Penerapakan Teknologi, Goverment Computer Security Incident Response Team, 2014.

[13] International Organization for Standarizaritaion, ISO 27005, Switzerland, 2011.

[14] Menteri Komunikasi dan Informatika Republik Indonesia, Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tentang Sistem Manajemen Pengamanan Informasi, Indonesia , 2016.

[15] W. Apriandari and A. Sasongko, "ANALISIS SISTEM MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN SNI ISO/IEC 27001:2013 PADA PEMERINTAHAN," *Jurnal Ilmiah SANTIKA Volume 8 No. 1 ,* 2018.

[16] D. Dewannanta, "IlmuKomputer.com," [Online]. Available: https://ilmukomputer.org/2013/02/02/ancaman-keamanan-jaringan-komputer/.