Analisis Manajemen Risiko Dan Kontrol Pada Seksi Sistem Informasi Berdasarkan Iso 31000 Studi Kasus : Pt.Nusantara Regas

1st Ezra Chrismyralda Sianipar
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
ezrachrismyralda@telkomuniversity.ac.id

2nd Iqbal Santosa.
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
iqbals@telkomuniversity.ac.id

3rd Ryan Adhitya Nugraha
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
ranugraha@telkomuniversity.ac.id

Abstrak

Teknologi informasi diartikan sebagai ilmu pengetahuan dalam bidang informasi yang berbasis komputer dan perkembanganya sangat pesat. Banyak perusahaan sudah menerapkan teknologi informasi untuk mendukung proses bisnis salah satunya PT.Nusantara Regas di Seksi Sistem Informasi. PT Nusantara Regas merupakan perusahaan patungan antara PT Pertamina (Persero) dan PT Perusahaan Gas Negara (Persero) Tbk dengan komposisi kepemilikan 60% dan 40%. Teknologi Informasi sudah berkembang mencakup seluruh aspek dibanyak bidang, tidak terkecuali salah satunya pada perusahaan BUMN. Dalam hal ini menganalisis risiko yang mungkin terjadi dapat dijadikan salah satu solusi untuk dapat meminimalisir risiko teknologi informasi pada perusahaan agar risiko yang mungkin terjadi dapat diminimalisir dan teratasi. Untuk dapat terus melakukan pengembangan terhadap sumber daya manusia dan melakukan peningkatan kualitas pelayanan di PT.Nusantara Regas maka dilakukannya analisi manajemen risiko menggunakan ISO 31000:2018 yang menghasilkan 9 risiko dari 2 proses yang ada di Seksi Sistem Informasi (Proses Operasional Sistem dan Proses Perencanaan dan Integrasi Sistem). Risiko yang teridentifikasi kemudian dilanjutkan dengan tahap analisis risiko yang berpacu dengan level kemungkinan dan level dampak. Risiko tersebut kemudian diberikan kontrol menggunakan standar NIST 800-53 dan DoD 8500.2 yang selanjutnya diberikan rekomendasi dari aspek personil,proses,dan teknologi.

Kata Kunci :Manajemen Risiko, Sistem Informasi, PT.Nusantara Regas, ISO 31000, BUMN, Teknologi Informasi

Abstract

Information technology is defined as science in the field of computer-based information and its development is very rapid. The role of information technology focuses on the regulation of information systems, information technology can meet the needs of organizations very quickly, relevant, and accurate. Many companies have implemented information technology to support business processes, one of which is PT. Nusantara Regas. PT NR is a joint venture between Pertamina and PGN. In this case analyzing the risks that may occur can be used as solution to minimize the risk of information technology in the company so the risks that may occur can be resolved. To develop human resources and improve the quality of service in PT. Nusantara Regas then conducted risk management analysts using ISO 31000 which resulted in 4 risks. The identified risks are then followed by a risk analysis stage that is in a race with the level of likelihood and the level of impact. The identified risks are then followed by a risk analysis stage that is based on level of likelihood and the level of impact. The risk is then given control using NIST 800-53 and DoD 8500.2 which then given recommendations from personnel, process, and technology aspects.

Keywords: Risk Management, Information Systems, PT. Nusantara Regas,ISO 31000,State-owned enterprises,Information Technology

I. PENDAHULUAN

Perkembangan teknologi telah memberikan banyak manfaat dalam dunia industri. Dalam dunia industri penggunaan terhadap teknologi menjadi suatu hal yang sangat penting. Penerapan teknologi dapat membantu untuk meningkatkan produktivitas dan efektifitas bagi suatu perusahaan. Berbagai permasalahan yang muncul pada suatu perusahaan dapat diatasi dengan pemanfaatan teknologi tersebut. Teknologi informasi diartikan sebagai ilmu pengetahuan dalam bidang informasi yang berbasis komputer dan perkembanganya sangat pesat. Teknologi informasi adalah suatu teknologi yang berhubungan dengan pengolahan data menjadi informasi dan proses penyaluran data/informasi tersebut dalam batas-batas ruang dan waktu. Teknologi informasi sudah mempertimbangkan aspek risiko yang mungkin menghambat pencapaian sebuah tujuan atau adanya ancaman terhadap keberjalanan Teknologi Informasi.

Dampak dari perkembangan teknologi informasi yang terjadi memacu organisasi-organisasi untuk tetap *exist* serta dapat meningkatkan prestasi yang dijalankannya. Peran teknologi informasi menitik beratkan pada pengaturan sistem informasi, selain itu teknologi informasi dapat memenuhi kebutuhan organisasi dengan sangat cepat, tepat waktu, relevan, dan akurat. Ini sangat diperlukan pengelolaan manajemen risiko di dalam level organisasi atau perusahaan.

Sejumlah fungsi manajemen risiko tradisional merupakan tanggung jawab di hampir semua lembaga termasuk meninjau dan menyetujui kebijakan manajemen risiko secara keseluruhan. Banyak perusahaan sudah menerapkan teknologi informasi untuk mendukung proses bisnis salah satunya PT.Nusantara Regas. PT. Nusantara Regas merupakan perseroan terbatas yang Joint Venture Antar PT Pertamina (Persero) dengan PT Perusahaan Gas Negara Tbk yang bertugas untuk Mensuplai bahan bakar berbentuk gas ke pembangkit listrik milik PLN dengan menerapkan prinsip-prinsip Perseroan Terbatas. Perusahaan Nusantara Regas sudah menerapkan teknologi informasi dalam menjalankan kinerja perusahaan dengan menggunakan SAP berbasis ERP untuk membantu perusahaan dalam menjalankan kegiatan operasionalnya. Oleh karena itu, penelitian yang dilakukan mengenai manajemen risiko dan kontrol PT. Nusantara Regas dengan menggunakan framework ISO 31000. Kerangka kerja ISO 31000 merupakan panduan yang dapat digunakan untuk mengelola manajemen risiko Teknologi Informasi. Hasil dari pengukuran risiko yang dilakukan pengukuran dapat mengetahui besaran dampak dari risiko dan kerentanan dari data aset yang terkait yang dinilai penting oleh instansi yang lalu dapat diterapkan kontrol yang tepat terhadap skala prioritas yang tertinggi.

Pada penelitian ini menggunakan ISO 31000:2018 sebagai acuan dalam menganalisis manajemen risiko, dan identifikasi risiko dengan menggunakan Generic Risk Scenarios Cobit5. Penerapan pengelolaan risiko berbasis ISO 31000:2018 ini sangat penting karena menurut Susilo (2018:22), "proses pengelolaan risiko yang berulang akan membantu organisasi untuk menetapkan strategi, mencapai sasaran, dan mengambil keputusan dengan pertimbangan yang matang." Dengan dilakukannya penelitian ini diharapkan PT.Nusantara Regas dapat mengelola aset dengan lebih baik.

II. KAJIAN TEORI

A. Risiko

Risiko adalah terjadinya sebuah "kemungkinan" terjadinya kejadian risiko dan besarnya " dampak" yang terjadi pada sasaran yang sudah ditetapkan. Setiap risiko akan dinilai berdasarkan "kemungkinan" dan "dampak" sesuai dengan kriteria risiko yang ditetapkan.

B. Manajemen risiko

Manajemen risiko adalah adalah suatu proses yang logis dan sistematis dalam mengidentifikasi, menganalisa, mengevaluasi, mengendalikan, mengawasi, dan mengkomunikasikan risiko yang berhubungan dengan segala aktivitas, fungsi atau proses dengan tujuan perusahaan mampu meminimalisasi kerugian dan memaksimumkan kesempatan.

C. Sistem Informasi

Sistem Informasi adalah sekumpulan komponen yang berhubungan satu sama lain, mengumpulkan, menyimpan, memproses dan menyebarkan informasi yang selanjutnya digunakan untuk membantu manajer dan karyawan proses analisis permasalahan dan penciptaan produk baru.

D. Sistem Informasi Manajemen

Sistem Informasi Manajemen adalah sistem pertama yang mempunyai orientasi pada informasi yang memiliki sasaran untuk membantu para petinggi organisasi.

III. METODE

Terdapat tiga tahapan dalam sistematika penelitian, yaitu tahap pengumpulan data, tahap pengolahan data, dan tahap rekomendasi dan kontrol. Pada tahap pengumpulan data ini mengumpulkan data dengan mengidentifikasi kebutuhan data yang akan dibutuhkan dengan berbagai jenis data yang ada. Untuk penelitian ini terdapat 2 jenis data yaitu primer dan sekunder. Data yang didapatkan dan dikumpulkan dengan cara wawancara langsung dan secara online oleh pihak unit IT PT.Nusantara Regas. Data yang dikumpulkan dan diolah akhirnya dapat dilakukan untuk melakukan penelitian yang sesuai dengan standar dari metode kerja ISO 31000:2018. Proses awal yang dilakukan adalah mengidentifikasi risiko, lalu menganalisis risiko yang sudah teridentifikasi penyebab dan dampak apa yang akan terjadi, setelah itu mengevaluasi risiko tersebut. Selanjutnya akan dilakukan penanganan risiko, pada proses ini risikodiberikan penanganan yang sesuai.

Tahap rekomendasi dan kontrol ini dilakukan ketika risiko sudah diberi penanganan yang sesuai pada tahap sebelumnya. Risiko dilihat berdasarkan rekomendasi kontrol dari standar NIST 800-53 dan DoD 8500 2, kontrol dapat dilihat dan dapat disesuaikan untuk dipakai berdasarkan dengan risiko yang sesuai.

IV. HASIL DAN PEMBAHASAN

A. Kriteria Risiko

Kriteria risiko adalah skala untuk mendefinisikan seberapa besar kemungkinan dan dampak yang menjadi rujukan untuk menilai besaran risiko dan prioritas risiko.

TABEL 1. Kriteria Risiko 1

Level Kemungkinan	Kriteria Kemungkinan
Hampir Tidak Terjadi / Rare (1)	a. Kemungkinan terjadinya sangat jarang (kurang dari 2 kali dalam 5 tahun) b. Persentase kemungkinan terjadinya antara 0% sampai dengan 20% dari volume transaksi dalam 1 periode
Jarang Terjadi / Unlikely (2)	a. Kemungkinan terjadinya jarang (2 kali s.d 10 kali dalam 5 tahun) b. Persentase kemungkinan terjadinya 20% s.d 40% dari volume transaksi dalam 1 periode)

Kadang terjadi Moderate (3)	c. Persentase kemungkinan terjadinya di atas 40% s.d 60% dari volume transaksi dalam 1 periode)
Sering Terjadi / Likely (4)	d. Persentase kemungkinan terjadinya di atas 60% s.d 80% dari volume transaksi dalam 1 periode)
Hampir Pasti Terjadi / Almost Certain (5)	e. Persentase kemungkinan terjadinya di atas 80% s.d 100% dari volume transaksi dalam 1 periode)

B. Kriteria Dampak

Kriteria dampak adalah ukuran seberapa besar dampak risiko tersebut akan mempengaruhi organisasi.

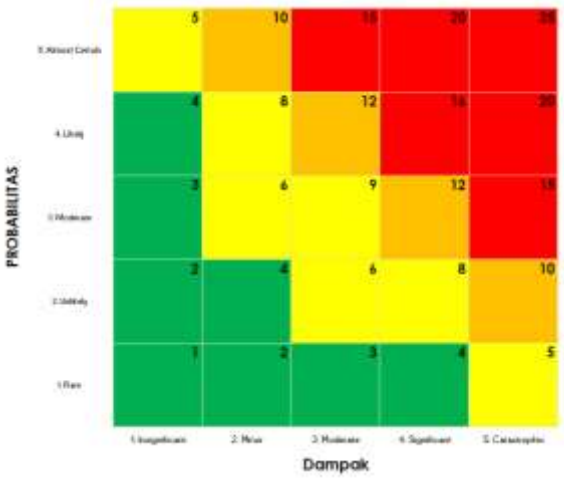
TABEL 2. Kriteria Dampak 1

Level Dampak	Area Dampak				
	Dampak Keuangan	Dampak Reputasi	Dampak kesehatan dan keselamatan	Dampak Lingkungan	Dampak Hukum
Tidak Signifikan (1)	≥ 80% of BTR	Tidak ada dampak reputasi	Tidak ada Dampak kesehatan dan keselamatan	Kerusakan terbatas pada area minimal dengan signifikansi rendah	Pelanggaran terbatas, hanya membutuhkan perhatian manajemen
Minor (2)	80% of BTR >x≥ 60% of BTR	Dampak Internal	Luka Ringan	Efek kecil pada lingkungan biologis atau fisik	Pelanggaran ringan, hanya keterlambatan pelaporan kepada pihak terkait, hukuman administrative
Moderat (3)	60% of BTR >x≥40 % of BTR	Dampak Lokal	Cedera besar pada satu orang	Moderat, efek jangka pendek tetapi tidak mempengaruhi fungsi ekosistem	Pelanggaran besar, sedang diselidiki oleh regulator
Signifikan (4)	40% of BTR >x≥ 20% of BTR	Dampak Regional	Luka besar pada beberapa orang	Efek lingkungan jangka menengah yang serius	Pelanggaran besar, pembatalan dan diselidiki oleh regulator
Sangat Signifikan (5)	≤20% of BTR	Dampak nasional yang luas	Karyawan atau kematian publik	Sangat Serius, kerusakan lingkungan jangka panjang fungsi ekosistem	Pelanggaran fatal, pencabutan oleh regulator

C. Matriks Risiko

Matriks risiko adalah alat yang digunakan untuk mengukur level risiko. Matriks didapat dari level kemungkinan dan level dampak yang lalu menghasilkan skala besaran risiko. Besaran risiko ini yang akan digunakan untuk mengetahui level risiko. Berikut adalah tabel matriks yang menjadi acuan dalam pengukuran risiko.

TABEL 3. Matriks Risiko 1



D. Level Risiko

Level risiko ditentukan berdasarkan atas dua, yaitu level kemungkinan terjadinya risiko dan level dampak risiko. Keduanya harus dikombinasikan dan diperhitungkan secara bersamaan dalam penentuan level risiko. Level kemungkinan terjadinya risiko, level dampak dan level risiko masing-masing menggunakan empat skala tingkatan yang dapat dilihat di tabel berikut:

TABEL 5. Level Risiko 1

Level Resiko		Besaran Risiko	Warna
1.	Extreme	15 s.d 25	Merah
2.	Tinggi	10 s.d 12	Jingga
3.	Moderat	5 s.d 9	Kuning
4.	Rendah	1 s.d 4	Hijau

E. Identifikasi Risiko

Identifikasi risiko dilakukan sebagai tahapan awal dalam penelitian. Untuk menentukan risiko yang mungkin terjadi pada proses yang terjadi di Seksi Sistem Informasi. Identifikasi risiko dijelaskan pada table berikut:

TABEL 6. Dampak Kriteria Risiko 1

No.	Proses	Kategori Resiko	Resiko	Penyebab	Dampak
1.	Operasional Sistem	Operational & Infrastructure Risk	Kerusakan akibat bencana alam seperti kebakaran, gempa bumi, tsunami	1. Bencana alam	1. Adanya kerugian aset fisik secara materil 2. Kerusakan perangkat
2.		Operational & Infrastructure Risk	Adanya kegagalan teknis / utility secara berkala	1. Human Error 2. Arus listrik yang tidak stabil 3. Hardware yang sudah usang 4. Jaringan yang digunakan tidak mendukung	1. Menurunnya performa kerja 2. Kerusakan perangkat 3. Proses terganggu
3.		Operational & Infrastructure Risk	Terjadinya Gagal Recovery Untuk Server Production	1. Perangkat Server Backup Sudah berumur Lebih dari 5 Tahun 2. Kapasitas Server Backup Tidak Memadai	1. Data Sharing dan Semua Sistem Non ERP Tidak Bisa Diakses Yang Berdampak Pada Operasional Perusahaan 2. Kehilangan Data
4.		Operational & Infrastructure Risk	Adanya serangan SPAM pada Mail Server	1) Tidak memiliki izin dari penerima email 2) Konten email terjaring filter spam	Adanya penipuan email,perangkat komputer terserang virus dan malware lainnya
5.		Operational & Infrastructure Risk	Adanya kesalahan input Informasi oleh staff TI	1. Human error 2. Kecerobohan dalam dalam mengelola data 3. Data yang diinputkan tidak tepat dan tidak lengkap	1. Penurunan performa kerja 2. Terganggunya proses dalam mengelola data
6.	Perencanaan dan Integrasi Sistem	Legal & Compliance Risk	Tuntutan Hukum/ penanlti/ denda terkait liisensi software	Pemakaian Software Ilegal atau Tidak Berlisensi	Dapat dikenakan sanksi hukum terkait Hak Cipta
7.		Operational & Infrastructure Risk	Ketidakmampuan untuk Recovery /Pemulihan Sistem Ketika Terjadi Force Major/Kegagalan Sistem	1) Belum Mempunyai Site DRC (Disaster Recovery Center) 2) Belum Mempunyai Dokumen DRP (Disaster Recovery Planning)	1. Kehilangan Data dan Terganggunya Operasional Perusahaan 2. Tidak Mempunyai Panduan Untuk Recovery/Pemulihan
8.		Operational & Infrastructure Risk		1. Koneksi terputus 2. Force down terhadap aplikasi 3. Server mati	1. Sistem down tidak bisa digunakan 2. Data rusak atau hilang
9.		Operational & Infrastructure Risk	Database corrupt, menyebabkan data tidak dapat diakses	1. Koneksi terputus 2.Kegagalan perangkat yang terhubung 3. Force down aplikasi 4. Kurang baiknya kualitas jaringan	1. Database server mati 2. Mengakibatkan putusnya koneksi antar computer cabang dengan server database utama 3. Kerugian untuk perusahaan baik secara material dan non material

F. Analisis Risiko

Analisis risiko dilakukan setelah melakukan identifikasi risiko yang mungkin terjadi. Analisis risiko dilakukan agar dapat mengetahui besar kemungkinan dan besar dampak yang terjadi, berikut dijelaskan pada table dibawah ini.

TABEL 9. Analisis Risiko 1

Proses	Resiko	Level Probabilitas	Level Dampak	Besaran Resiko	Level Resiko
Operasional Sistem	Kerusakan akibat bencana alam seperti kebakaran, gempa bumi, tsunami	Insignificant	Sangat Besar	5	Moderate
	Adanya kegagalan teknis / utility secara berkala	Moderate	Minor	6	Moderate
	Terjadinya Gagal Recovery Untuk Server Production	Likely	Moderate	12	High
	Adanya serangan SPAM pada Mail Server	Likely	Minor	8	Moderate
	Adanya kesalahan input Informasi oleh staff TI	Likely	Minor	8	Moderate
Perencanaan dan Integrasi Sistem	Tuntutan Hukum/ penanlti/ denda terkait liisensi software	Unlikely	Significant	8	Moderate
	Ketidakmampuan untuk Recovery/Pemulihan Sistem Ketika Terjadi Force Major/Kegagalan Sistem	Unlikely	Minor	4	Low
	Adanya masalah software terhadap sistem yang penting secara berkala	Moderate	Minor	6	Moderate
	Database corrupt, menyebabkan data tidak dapat diakses	Minor	Minor	4	Low

G. Evaluasi Risiko

Evaluasi Risiko menentukan skala priotas dari risiko yang sudah ditentukan level risikonya. Skala prioritas ini akan membantu penulis dalam melakukan penanganan risiko, berikut dijelaskan pada table dibawah ini.

Tabel 10. Evaluasi Risiko 1

Proses	Kategori Resiko	Besaran Resiko	Level Resiko	Keputusan Penanganan (Ya/Tidak)
Operasional Sistem	Kerusakan akibat bencana alam seperti kebakaran, gempa bumi, tsunami	5	Moderate	Ya
	Adanya kegagalan teknis / utility secara berkala	6	Moderate	Ya
	Terjadinya Gagal Recovery Untuk Server Production	12	High	Ya
	Adanya serangan SPAM pada Mail Server	8	Moderate	Ya
	Adanya kesalahan input Informasi oleh staff TI	8	Moderate	Ya
Perencanaan dan Integrasi Sistem	Tuntutan Hukum/ penanlti/ denda terkait liisensi software	8	Moderate	Ya
	Ketidakmampuan untuk Recovery/Pemulihan Sistem Ketika Terjadi Force Major/Kegagalan Sistem	4	Low	Tidak
	Adanya masalah software terhadap sistem yang penting secara berkala	6	Moderate	Ya
	Database corrupt, menyebabkan data tidak dapat diakses	4	Low	Tidak

H. Penanganan Risiko

Jenis penanganan risiko dilakukan berdasarkan level risiko dan skala prioritas yang sudah dilakukan sebelumnya. Tahap ini menentukan opsi penanganan apa yang akan diberikan. Berikut dijelaskan penanganan risiko pada table berikut:

TABEL 10. Penanganan Risiko 2

No	Proses	Resiko	Besaran Resiko	Skala Prioritas	Penanganan Resiko
1.	Operasional Sistem	Terjadinya Gagal Recovery Untuk Server Production	12	1	Mitigasi
2.		Adanya serangan SPAM pada Mail Server	8	2	Mitigasi
3.		Adanya kesalahan input Informasi oleh staff TI	8	3	Mitigasi
4.		Kerusakan akibat bencana alam seperti kebakara	5	7	Mitigasi

		n, gempa bumi, tsunami			
5.		Adanya kegagalan teknis / utility secara berkala	6	5	Mitigasi
6.	Perencanaan dan Integrasi Sistem	Tuntutan Hukum/ penanlti/ denda terkait liisensi software	8	4	Transfer
7.		Adanya masalah software terhadap sistem yang penting secara berkala	6	6	Mitigasi

I. Rekomendasi dan Kontrol

a. Penetapan Kontrol

Penetapan kontrol dilakukan kepada risiko berdasarkan penanganan yang tepat sesuai dengan batasan selera risiko. Pada penelitian ini menggunakan dua control yaitu, NIST 800-53 dan Department of Defense Instruction 8500.3, kontrol yang diberikan adalah seperti tabel berikut:

TABEL 12. Penetapan Kontrol1

No.	Proses	Resiko	Judul Kontrol	Standar
1.	Operasional Sistem	Terjadinya Gagal Recovery Untuk Server Production	SI-13 |5 Failover Capability	NIST 800-53
2.		Adanya serangan SPAM pada Mail Server	SI-8 Spam Protection	NIST 800-53
3.		Adanya kesalahan input Informasi oleh staff TI	SI-10 Information Input Validation	NIST 800-53
4.		Kerusakan akibat bencana alam seperti kebakaran, gempa bumi, tsunami	CODP-2 Disaster and Recovery Planning	Department of Defense Instruction 8500.3
5.		Adanya kegagalan teknis / utility secara berkala	COPS-1 Power Supply	Department of Defense Instruction 8500.3
6.	Perencanaan dan Integrasi Sistem	Tuntutan Hukum/ penanlti/ denda terkait liisensi software	CM-8 Information System Component Inventory	NIST 800-53
7.		Adanya masalah software terhadap sistem yang penting secara berkala	SA-12 | 7 Supply Chain Protection	NIST 800-53

b. Pengertian Kontrol dan Ketersedian Kontrol

Setelah ditetapkannya kontrok terhadap risiko dibawah ini menjelaskan fungsi dan pengertian dari control yang digunakan pada table dibawah ini:

TABEL 13. Kontrol 1

No.	Judul Kontrol	Deskripsi Kontrol	Ketersediaan Kontrol			Kecukupan Kontrol
			People	Process	Technology	
1.	SI-13.5 Predictable Failure Prevention |Failover Capability	Memindahkan operasional sistem ke sistem cadangan secara otomatis	Tidak Tersedia	Standar Infrastruktur	Recovery dilakukkan secara otomatis pada backup cloud dan backup server	Sudah
2.	SI-8 Spam Protection	Mengelola mekanisme perlindungan spam.	Tidak Tersedia	Standar Infrastruktur	Membatasi kapasitas email pada server	Belum
3.	SI-10 Information Input Validation	Memeriksa validitas saat penginputan informasi.	Tidak Tersedia	Tidak Tersedia	Fungsi validasi pada penginputan informasi	Belum
4.	CODP-2 Disaster and Recovery Planning	Prosedur pemulihan bencana termasuk bisnis rencana pemulihan, rencana kontingensi sistem, rencana pemulihan bencana fasilitas, dan rencana penerimaan.	Tidak Tersedia	Standar Infrastruktur	Sudah Memiliki Disaster Recovery Center (DRC)	Belum
5.	COPS-2 Power Supply	Sistem kelistrikan dikonfigurasi untuk memungkinkan daya	Belum Tersedia	Standar Infrastruktur	Memiliki UPS	Sudah

		terus menerus atau tidak terputus untuk kunci TI Aset. Ini mungkin termasuk daya yang tidak terganggu ditambah dengan keadaan darurat generator.				
6.	CM-8 Information System Component Inventory	Memperbarui inventaris komponen sistem informasi sebagai bagian integral dari instalasi komponen, penghapusan, dan pembaruan sistem informasi.	Belum Tersedia	Standar Produk Teknologi sistem Informasi	Aset management ERP	Sudah
7.	SA-12.7 Supply Chain Protection | Assessments Prior To Acceptance	Organisasi melakukan penilaian terhadap sistem informasi, komponen sistem, atau layanan sistem informasi sebelum penerimaan.	Belum Tersedia	Standar Produk Teknologi sistem Informasi	Platform Perangkat Lunak Server	Sudah

c. Perancangan Rekomendasi

Berdasarkan Kontrol yang sudah ditetapkan yang berhubungan dengan risiko yang terjadi, maka penulis memberikan sebuah rekomendasi untuk risiko yang belum adanya kontrol, yaitu ada pada tabel dibawah ini:

TABEL 15. Perancangan Rekomendasi 1

Judul Kontrol	Rekomendasi		
	People	Process	Technology
SI-8 Spam Protection	Peningkatan Keterampilan	-	Peningkatan Tecnology
SI-10 Information Input Validation	-	Standar validasi penginputan data informasi	-
CODP-2 Disaster and Recovery Planning	Peningkatan Keterampilan	-	-
SA-12.7 Supply Chain Protection | Assessments Prior To Acceptance	Peningkatan Keterampilan	-	-

d. Rekomendasi Aspek *People*

Rekomendasi Aspek People yang ditulis penulis ditabel ini sesuai dengan peranacangan rekomendasi yang penulis berikan, berikut tabel perancangan rekomendasi aspek people.

TABEL 16. Rekomendasi Aspek People 1

No.	Judul Kontrol	Judul Pelatihan	Deskripsi
1.	CODP-2 Disaster and Recovery Planning	Pelatihan Tanggap terhadap bencana dan ancaman	Melatih kemampuan staff IT terhadap bencana/ancaman yang terjadi serta menanggulangi pemuihan bencana termasuk fasilitas dan hardware.

e. Rekomendasi Aspek *Process*

TABEL 17. Rekomendasi Aspek Process 1

No.	Judul Kontrol	Rekomendasi	Deskripsi
1.	SI-10 Information Input Validation	Standar validasi penginputan data informasi	Membuat standar untuk mengatasi kesalahan penginputan data informasi

f. Rekomendasi Aspek *Tecchnology*

Rekomendasi pada aspek technology berupa penggunakan technology yang baru dan menerapkannya sebagai rekomendasi. Berikut dijelaskan pada table dibawah ini:

TABEL 18. Rekomendasi Aspek Technology 1

No.	Judul Kontrol	Rekomendasi	Deskripsi
1.	SI-8 Spam Protection	Mail server spam protection	Menggunakan mail server yang sudah termasuk dengan spam protection untuk mengatasi spam mail yang masuk

g. Prioritas Rekomendasi

Prioritas rekomendasi dibuat agar dipakai sebagai acuan penulis dalam membuat roadmap pada implementasi selanjutnya.Besaran risiko diambil penulis untuk menentukan prioritas pelaksanaan rekomendasi, berikut dijelaskan pada table dibawah ini:

TABEL 19. Prioritas Rekomendasi 1

Aspek	Kontrol	Rekomendasi	Besaran Risiko	Prioritas
People	SI-8 Spam Protection	Peningkatan Tecnhnology	8	1
Process	SI-10 Information	Standar validasi	8	2

	Input Validation	penginputan data informasi		
People	CODP-2 Disaster and Recovery Planning	Peningkatan Ketrampilan	6	3
People	SA-12.7 Supply Chain Protection | Assessments Prior To Acceptance	Peningkatan Ketrampilan	5	4

h. *Roadmap* Implementasi

Rekomendasi Penyusunan roadmap dibuat untuk menentukan waktu yang diupayakan untuk melakukan rekomendasi yang diberikan oleh penulis Berikut dijelaskan pada table dibawah ini:

TABEL 19. Roadmap Implementasi 2

No.	Inisiatif	Periode 2022									
		Mar	Apr	Mei	Juni	Juli	Agust	Sept	Okt	Nov	Des
Aspek Technology											
1.											
Aspek People											
1.	Penyusunan Rencana Pelatihan										
2.	Sosialisasi Rencana Pelatihan										
3.	Pelatihan										
Aspek Process											
1.	Pembahasan draft Standar										
2.	Pengesahan seluruh draft Standar baru dan Standar Revisi										
3.	Sosialisasi terhadap Standar baru dan Standar Revisi										

V. KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan, berikut merupakan kesimpulan yang dapat diambil:

A. Pada tahap pengidentifikasian risiko ditemukan 9 risiko dari 2 proses yang ada di Seksi Sistem Informasi (Proses Operasional Sistem dan Proses Perencanaan dan Integrasi Sistem). Risiko yang teridentifikasi Sebagian besar masuk ke dalam Operational & Infrastructure Risk dan Sebagian kecil masuk ke dalam *Legal and Compliance Risk.* Pada tahap analisis, risiko paling tinggi yaitu Terjadinya Gagal Recovery Untuk Server Production dengan nilai risiko 12 (level risiko high), enam risiko dengan nilai risiko 8,6 dan 5 (level risiko moderate) dan dua risiko dengan nilai risiko 4 (level risiko low). Pada tahap evaluasi, diperoleh 7 risko yang ditangani dan 2 risiko yang tidak ditangani.

B. Terdapat dua jenis penanganan yang diberikan yaitu mitigasi dan transfer. Risiko yang diberikan penanganan mitigasi adalah: terjadinya gagal recovery untuk server production, adanya serangan spam pada mail server, adanya kesalahan input informasi oleh staff ti, kerusakan akibat bencana alam seperti kebakaran, gempa bumi, tsunami, adanya kegagalan teknis / utility secara berkala, tuntutan hukum/ penanlti/ denda terkait liisensi software, adanya masalah software terhadap sistem yang penting secara berkala. Risiko diatas diberikan penanganan mitigasi karena mempunyai level dampak yang besar sehingga harus diberikan kontrol untuk mengurangi dampak yang akan terjadi.Selain mitigasi, penanganan lain yang diberikan adalah transfer.

C. Terhadap masing-masing risiko ditentukan kontrol berdasarkan standar NIST 800-53 dan DoD 8500.2. Kontrol yang dipilih dari NIST 800-53 adalah SI-13.5 Failover Capability, SI-8 Spam Protection, SI-10 Information Input Validation, CM-8 Information System Component Inventory dan SA-12.7 Supply Chain Protection. Sedangkan kontrol yang dipilih dari DoD 8500.2 adalah CODP-2 Disaster and Recovery Planning dan COPS-1 Power Supply. Rekomendasi yang dihasilkan yaitu Penggunaan *Mail server spam protection*, Penerapan Standar validasi penginputan informasi, Pelatihan Tanggap terhadap bencana dan ancaman, dan Penggunaan *Software acceptance checklist*.

D. Tahapan yang dilakukan yang pertama Penyusunan dan Sosialisasi Agenda Pelatihan, dilanjutkan dengan yang kedua Pembahasan dan Pengeasahan draft Standar validasi penginputan informasi, Sosialisasi terhadap Standar baru dan Standar Revisi Penyusunan software acceptance checklist dan yang ketiga Pendefinisian kebutuhan fitur spam protection dan Konfigurasi fitur spam protection.

REFERENSI

[1] ISACA. (2013). COBIT 5 for Risk. ISACA.
[2] Santosa, I., & R., Y. (2019). *Analisis Risiko dan Kontrol Perlindungan Data Pribadi pada Sistem Informasi Administrasi Kependudukan. Jurnal RESTI*. Rekayasa Sistem dan Teknologi Informasi.
[3] ISO 31000, ISO 31000:2018. (2018). Risk management — Guidelines, Switzerland: ISO Organization.