MANAJEMEN RISIKO ASET APLIKASI PADA DISKOMINFO STATISTIK DAN PERSANDIAN KOTA XYZ MENGGUNAKAN STANDAR ISO/IEC 27005: 2008

Dibuat Oleh:

Romualdus Sumbogo Probodi Abiyoga

161708963

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ATMA JAYA YOGYAKARTA

2020

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

MANAJEMEN RISIKO ASET APLIKASI PADA DISKOMINFO STATISTIK DAN PERSANDIAN KOTA XYZ MENGGUNAKAN STANDAR ISO/IEC 27005: 2008

yang disusun oleh

ROMUALDUS SUMBOGO PROBODI ABIYOGA

161708963

dinyatakan telah memenuhi syarat pada tanggal 07 Agustus 2020

		Keterangan
Dosen Pembimbing 1	: Yohanes Priadi Wibisono, S.T.,M.M.	Telah menyetujui
Dosen Pembimbing 2	: Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng.	Telah menyetujui
Tim Penguji		
Penguji 1	: Yohanes Priadi Wibisono, S.T.,M.M.	Telah menyetujui
Penguji 2	: Samiaji Sarosa	Telah menyetujui
Penguji 3	: Clara Hetty Primasari, S.T., M.Cs	Telah menyetujui

Yogyakarta, 07 Agustus 2020

Universitas Atma Jaya Yogyakarta

Fakultas Teknologi Industri

Dekan

ttd

Dr. A. Teguh Siswantoro, M.Sc

KATA PENGANTAR

Puji dan syukur penulis haturkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan pembuatan tugas akhir "Manajemen Risiko Aset Aplikasi Pada Diskominfo Statistik Dan Persandian Kota XYZ Menggunakan Standar ISO/IEC 27005: 2008" ini dengan baik. Penulisan tugas akhir ini bertujuan untuk memenuhi salah satu syarat untuk mencapai derajat sarjana Sistem Informasi dari Program Studi Sistem Informasi, Fakultas Teknologi Industri di Universitas Atma Jaya Yogyakarta. Penulis menyadari bahwa dalam pembuatan tugas akhir ini penulis telah mendapatkan bantuan, bimbingan, dan dorongan dari banyak pihak, untuk itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Bapak Yohannes Priadi Wibisono, S.T., M.M., selaku pembimbing pertama dan pembimbing akademik yang selalu meluangkan waktu di tengah kesibukannya yang luar biasa untuk bimbingannya.
2. Bapak Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng., selaku pembimbing kedua yang yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
3. Seluruh staf Dinas Komunikasi dan Informasi Statistik dan Persandian Kota XYZ yang membantu penulis memperoleh data penelitian.
4. Ibu Enny Susana dan Mba Niken yang telah membantu proses pembelajaran agar dapat mengerjakan skripsi ini dengan baik.
5. Ibu Florensia Sapty Rahayu, S.T., M.Kom. yang telah membantu memberi masukan selama pengerjaan skripsi.
6. Ibu tercinta dan seluruh keluarga untuk semua bentuk dukungan yang tidak pernah putus ketika penulis berkuliah di Universitas Atma Jaya Yogyakarta.

Seluruh pihak yang membantu dan tidak tersebut namanya namun telah menambah keceriaan pada pembuatan skripsi ini. Demikian laporan tugas akhir ini dibuat, dan penulis mengucapkan terima kasih kepada semua pihak. Semoga laporan

ini dapat bermanfaat bagi pembaca.

Yogyakarta, 27 Juli 2020

Romualdus Sumbogo Probodi Abiyoga

161708963

ABSTRAK

Penyelenggaraan TIK tidak akan lepas dari konteks keamanan informasi. Keamanan informasi memainkan peranan penting untuk menjaga keutuhan aset TIK serta aspek kerahasiaan, keutuhan dan ketersediaan sebuah layanan maupun aset pendukung lainnya. Keamanan informasi memiliki sangat banyak proses yang mendukung, salah satu proses yang penting adalah manajemen risiko. Pemerintah menganjurkan agar seluruh proses yang mendukung keamanan informasi seperti manajemen risiko dilakukan di seluruh pemerintahan dari pusat hingga daerah. Tak terkecuali Diskominfo Statistik dan Persandian Kota XYZ, dengan pelayanan publik yang serba online dan banyak layanan yang membutuhkan bantuan teknologi informasi membuat ancaman terhadap penyelenggaraan IT meningkat pesat. Itulah mengapa Diskominfo Statistik dan Persandian XYZ memerlukan proses manajemen risiko pada aset perangkat lunak yang efektif agar mampu menekan risiko inheren pada layanan-layanan tersebut. Manajemen risiko dilakukan agar dapat menentukan ancaman, kerawanan serta evaluasi nilai tingkat ancaman terhadap suatu aset. Standar manajemen risiko keamanan informasi yang dapat digunakan adalah ISO 27005, standar ini digunakan sesuai dengan anjuran dari Kominfo Pusat mengenai manajemen risiko keamanan informasi khususnya pada instansi pemerintahan. Proses manajemen risiko diawali dengan kajian terhadap proses bisnis yang ada di Diskominfo Statistik dan Persandian Kota XYZ dan peraturan yang dimiliki terkait manajemen risiko, selanjutnya dilakukan proses identifikasi aset dan klasifikasi aset menurut ISO 27005: 2008. Kemudian dari aset-aset perangkat lunak yang teridentifikasi dan telah diklasifikasikan, dapat ditentukan ancaman dan kerawanannya. Pada tahap terakhir baru dilakukan evaluasi, yang hasilnya menjadi tolak ukur dalam pembuatan rekomendasi. Dari proses manajemen risiko yang dilakukan ditemukan 22 ancaman, di mana sembilan belas ancaman pada tingkat rendah/*low*, satu ancaman pada tingkat sedang/*medium* dan dua ancaman pada tingkat tinggi/*high*. Dari nilai tingkat ancaman inilah ditentukan beberapa rekomendasi sesuai dengan pengendalian yang telah diterapkan oleh Diskominfo Statistik dan Persandian Kota XYZ.

Kata Kunci: Manajemen Risiko, Keamanan Informasi, ISO 27005: 2008, Evaluasi Risiko.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1. Latar Belakang

Saat ini penggunaan TIK terus meningkat dan memiliki peran penting bagi sebuah organisasi [1], misalnya untuk menjaga kelangsungan proses bisnis atau memaksimalkan layanan produk atau jasa yang ditawarkan[2]. Dalam penyelenggaraan TIK pada sebuah organisasi, aspek keamanan informasi sangatlah penting untuk diperhatikan. Mengingat informasi adalah sebuah aset yang berharga bagi organisasi dan kunci dalam memenangkan persaingan di era global [3]. Oleh karena itu keamanan informasi menjadi kunci di dunia TIK pada abad ke-21, apabila keamanan informasi ini terganggu maka akan dapat mengganggu aspek kerahasiaan, keutuhan dan ketersediaan sebuah informasi atau aset-aset TIK yang ada [4].

Aset-aset TIK ini berperan penting dalam penyelenggaraan TIK pada sebuah organisasi [5] termasuk organisasi pada sektor pemerintahan. Agar pelayanan pemerintah dapat dijalankan secara maksimal serta dapat menggandeng segala sektor baik itu masyarakat, bisnis maupun antar organisasi pemerintahan lainnya, dibutuhkan layanan pemerintah yang mengkolaborasikan TIK yang biasanya disebut sebagai *e-government* [6].

E-government dikenal sebagai layanan pemerintah yang memanfaatkan jaringan internet atau mentransformasi layanannya dalam bentuk digital [7]. Pada praktiknya layanan berbasis internet ini ditujukan agar masyarakat dapat menikmati kemudahan pelayanan pemerintah yang efektif dan efisien. Tidak ada lagi antrian panjang, proses dokumen fisik yang memakan waktu atau akses lokasi kantor yang cukup jauh. Namun di balik kemudahan tersebut banyak risiko yang mungkin muncul, misalnya risiko fisik seperti peretasan, pencurian data, kebakaran, perusakan yang mengancam keamanan fisik aset-aset TIK. Selain itu terdapat risiko kerusakan logik seperti akses yang tidak sah, pemalsuan hak akses atau pengrusakan secara sengaja maupun tidak sengaja aset-aset TIK dan informasi yang terkandung di dalamnya [8].

Berdasarkan uraian risiko-risiko di atas, apabila organisasi mengabaikan atau

memiliki kesadaran yang kurang terhadap risiko yang ada maka berpotensi menimbulkan dampak negatif bagi organisasi. Contoh dampak negatif bagi organisasi misalnya mengganggu kinerja pelayanan pemerintah, menurunkan reputasi pemerintah atau bahkan mengurangi kepercayaan masyarakat [9]. Oleh karena itu dibutuhkan sebuah proses manajemen risiko yang efektif agar risiko serta dampak yang mungkin muncul dapat ditekan atau bahkan dihindari [10].

Pemerintah pusat terus mengupayakan tidak hanya aturan-aturan baru namun juga bimbingan teknis serta pembekalan keamanan informasi kepada pemerintah daerah dan penyelenggara pelayanan publik. Pemerintah mewajibkan agar proses manajemen risiko dilakukan oleh para penyelenggara pemerintah baik itu pusat maupun daerah. Manajemen risiko menjadi instrumen penting dalam menjaga keamanan informasi sebuah organisasi, di mana hal ini sesuai dengan Perpres No.95 Th. 2018 yang menyatakan semua Sistem Berbasis Pemerintahan (SPBE) diharapkan untuk meminimalkan risiko untuk menjaga agar pelayanan publik tetap maksimal [11]. Melalui UU No.23 tahun 2014 [12] tentang pemerintahan daerah pada klausul mengenai Pembagian Urusan Pemerintahan Bidang Persandian, terdapat sub-urusan pertama yaitu mengenai keamanan informasi mulai dari pemerintahan pusat, provinsi hingga kabupaten/daerah. Aturan lain yang dapat dijadikan dasar dalam menerapkan prosedur manajemen risiko pada keamanan informasi adalah Peraturan BSSN No.10 tahun 2019 [13]. Peraturan ini merupakan pembaharuan dari aturan sebelumnya yaitu, Perka Lembaga Sandi No.7 tahun 2017. Peraturan ini menyebutkan mengenai pelaksanaan persandian untuk pengamanan informasi bagi pemerintah daerah. Manajemen risiko juga menjadi upaya dalam pengamanan informasi yang dimaksud. Lewat aturan-aturan tersebut sudah jelas bahwa organisasi pemerintahan wajib mengambil langkah konkrit dalam pemenuhan pengamanan informasi.

Terdapat beberapa standar yang dapat digunakan dalam manajemen risiko antara lain standar ISO/IEC 27001, OCTAVE *(Operationally, Critical, Threat, Asset, Vulnerability Evaluation)*, FAIR *(Factor Analysis of Information Risk),* IRM *(Institute of Risk Management)* dan BS 3110 [14] [15] [16]. Sesuai dengan Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Publik, disarankan menggunakan seri ISO 27000 dalam penerapan keamanan informasi. Termasuk ISO/IEC 27005 dalam

manajemen risiko keamanan informasi sebagai bentuk keseragaman standar manajemen risiko di sektor pemerintahan.

Meskipun pemerintah telah menetapkan serta mengeluarkan alat evaluasi keamanan informasi, dilengkapi dengan bimbingan teknis, namun hingga kini Diskominfo Statistik dan Persandian Kota XYZ belum menerapkan segala bentuk keamanan informasi termasuk manajemen risiko. Dampak dari tidak diterapkannya manajemen risiko ini adalah munculnya beberapa kali kasus peretasan pada situs pemerintahan yang dikelola Diskominfo Statistik dan Persandian Kota XYZ. Pada 14 April 2020 situs pemkot XYZ sempat diserang dan akhirnya tidak dapat beroperasi selama 15 menit [17]. Sebelumnya situs Pemkot XYZ juga terkena serangan sebanyak 3 kali pada akhir tahun 2019. Insiden-insiden ini berpotensi memberikan dampak negatif pada aset TIK maupun reputasi Diskominfo Statistik dan Persandian Kota XYZ serta kerugian secara finansial, sehingga tindakan pencegahan maupun koreksi perlu dilakukan [18]. Salah satu tindakan yang dapat diambil untuk mencegah dampak negatif dan kerugian tersebut adalah dengan menerapkan proses manajemen risiko agar dapat memetakan ancaman dan kerawanan terhadap aset TIK dengan baik [19].

Penelitian ini diawali dari tugas yang diberikan kepada penulis saat melakukan magang. Selama proses magang, penulis diberikan tanggung jawab untuk melakukan identifikasi aset aplikasi dan proses bisnis aplikasi. Oleh karena itu, manajemen risiko ini mengambil konteks aset aplikasi sebagai tindak lanjut dari proses identifikasi sebelumnya.

1.2. Perumusan Masalah

Permasalahan utama yang saat ini sedang dihadapi oleh Diskominfo SP XYZ adalah belum adanya penerapan manajemen risiko yang dimulai dengan proses penilaian risiko secara konkrit yang dilakukan di lapangan. Penerapan manajemen risiko ini dibutuhkan mengingat pentingnya proses keamanan informasi pada lingkup pemerintahan dan didukung dengan anjuran dari Pemerintahan Kota XYZ mengenai Panduan Penyelenggaraan *E-government*. Ketiadaan proses manajemen risiko dapat berakibat pada ketidaksiapan Diskominfo Statistik dan Persandian Kota XYZ untuk menangani risiko-risiko yang mungkin akan muncul. Jika risiko-risiko keamanan tidak

diantisipasi maka dapat mengancam kelangsungan baik proses bisnis maupun aset, serta akan berdampak pada penurunan reputasi baik Diskominfo Statistik dan Persandian Kota XYZ di lingkungan Organisasi Perangkat Daerah (OPD) maupun di mata masyarakat sebagai penyelenggaraan publik yang aman dan terpercaya.

1.3. Pertanyaan Penelitian

1. Bagaimana melakukan penilaian risiko yang merupakan langkah awal dari manajemen risiko pada aset perangkat lunak di Diskominfo Statistik dan Persandian Kota XYZ?

1.4. Batasan Masalah

1. Penelitian ini akan terbatas pada aset aplikasi atau perangkat lunak saja.
2. *Best-practice* yang digunakan sebagai metodologi adalah ISO 27005: 2008, akan tetapi hanya sampai pada tahap evaluasi risiko dan pengendalian yang ada.
3. Parameter yang digunakan pada evaluasi risiko akan menggunakan parameter yang tersedia di Pedoman Bank Indonesia dalam Manajemen Risiko.

1.5. Tujuan Penelitian

1. Melakukan penilaian risiko pada aset aplikasi di Diskominfo Statistik dan Persandian Kota XYZ dimulai dari identifikasi aset, identifikasi ancaman dan kerawanan sampai evaluasi risiko berdasarkan kecenderungan dan dampak.
2. Membuat rekomendasi berdasarkan nilai tingkat risiko yang dihasilkan.

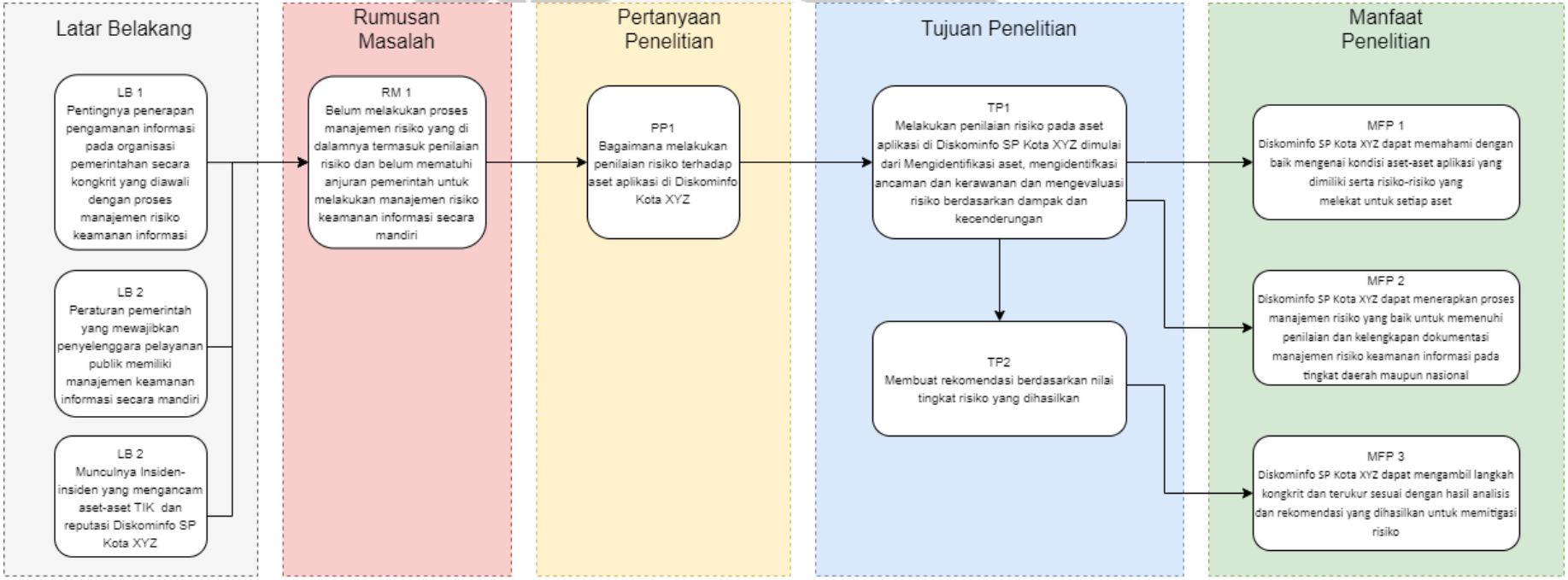
1.6. Manfaat Penelitian

1. Diskominfo Statistik dan Persandian Kota XYZ dapat memahami dengan baik mengenai kondisi aset-aset aplikasi yang dimiliki serta risiko-risiko yang melekat untuk setiap aset.

2. Diskominfo Statistik dan Persandian Kota XYZ dapat menerapkan proses manajemen risiko yang baik untuk memenuhi penilaian dan kelengkapan dokumentasi manajemen risiko keamanan informasi pada tingkat daerah maupun nasional.
3. Diskominfo Statistik dan Persandian Kota XYZ dapat mengambil langkah konkrit dan terukur sesuai dengan hasil analisis dan rekomendasi yang dihasilkan untuk memitigasi risiko.

1.7. Diagram Keterkaitan Antara Latar Belakang, Rumusan Masalah, Pertanyaan Penelitian, Tujuan Penelitian dan Manfaat Penelitian

Berikut adalah diagram keterkaitan antara latar belakang, rumusan masalah, pertanyaan penelitian, tujuan penelitian serta manfaat penelitian pada gambar 1.1.



Gambar 1.1. Diagram Keterkaitan

BAB II

TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Studi sebelumnya mengenai manajemen keamanan informasi pada sistem informasi akademik menggunakan ISO 27005: 2011 pernah dilakukan oleh Asriyanik dan Prajoko. Objek penelitian yang digunakan adalah Sistem Informasi Akademik (SIAK) penelitian dilaksanakan di Universitas Muhammadiyah Sukabumi (UMMI) [15]. Penelitian dilandaskan pada sistem akademik yang digunakan pada jaringan luas agar mempermudah dan mempercepat proses bisnis dari UMMI, khususnya dalam pelayanan akademik. Akan tetapi hal ini memiliki konsekuensi yaitu meningkatkan risiko IT yang harus diterima dan dicegah oleh UMMI.

Pada tahap awal penelitian dilakukan klasifikasi aset pada SIAK kemudian diberikan pengkodean begitu pula risiko serta kerentanan yang ada. Kemudian penilaian risiko dilakukan terhadap aset perangkat lunak utama dan pendukung, perangkat keras serta jaringan tersebut, penilaian dilakukan menggunakan matriks yang terdapat pada ISO 27005: 2011 begitu pula dengan format penelitian dan pengkodean. Setelah melakukan penilaian nilai dampak dan kecenderungan akan dipetakan untuk menentukan tindakan terhadap risiko, ada tiga parameter yaitu *risk modification (rm), risk transfer (rt), dan risk sharing (rs)*. Kesimpulan dari penelitian ini, ditemukan dua level rendah (low), tujuh risiko level tinggi (high), dan 64 risiko level sedang (medium). Rencana penanganan risiko dan pengendalian yang telah dilakukan SIAK UMMI, didapatkan 47 skenario ancaman harus ditangani, sembilan belas skenario ancaman akan dimodifikasi, satu risiko akan ditransfer dan 27 risiko tersisa dapat dihindari.

Penelitian selanjutnya yang dilakukan di Universitas Narotama Surabaya dengan objek penelitian, yaitu eLina [20]. Studi ini dilakukan untuk membantu pihak administrator universitas dapat mendefinisikan faktor risiko secara operasional pada sebuah sistem *e-learning*. Empat risiko utama yang akan dibahas pada studi ini adalah keamanan data, keamanan *password*, risiko proses dan risiko terhadap serangan

peretas. Proses identifikasi risiko akan menggunakan kerangka NIST 800-30 Revisi I dan hasil analisis akan digunakan sebagai rekomendasi untuk mengamankan situs eLina.

Tahapan awal dimulai dengan proses *interview* dalam mengambil data aset yang dibutuhkan [11], kemudian dilakukan juga studi literatur untuk memahami penggunaan NIST 800-30 Revisi I dalam proses analisis manajemen risiko. Studi literatur ini juga digunakan untuk menentukan parameter yang akan digunakan pada dampak dan kecenderungan. Kemudian langkah penelitian yang dilakukan adalah menentukan aset perangkat keras dari eLina, setelah itu melakukan identifikasi peristiwa ancaman yang merupakan hasil wawancara dan observasi berupa sekumpulan risiko yang akan terjadi, dan tahapan terakhir menentukan kerentanan. Penilaian risiko juga dilakukan berdasarkan penentuan dampak dan kecenderungan yang akan menjadi dasar dalam menentukan tingkatan risiko. Hasilnya dari empat belas risiko yang teridentifikasi ditemukan tiga risiko pada level tinggi/*high*, sepuluh risiko pada level sedang/*moderate* dan satu risiko pada level rendah/*low*. Peneliti menyarankan untuk memperbaharui penelitian bahasa pemrograman situs eLina, menggunakan bahasa pemrograman PHP versi 7.0 karena versi PHP yang digunakan saat ini adalah 3.7. Audit aset secara rutin juga disarankan untuk meningkatkan pengamanan aset.

Damar Nurcahyono dan Achmad Djunaedi melakukan penelitian tentang manajemen risiko teknologi informasi menggunakan kerangka *IT Risk* dari *COBIT*. Studi kasus Kantor Arsip Daerah Kota Samarinda. Demi mendukung pemerintahan di Kota Samarinda, Kantor Arsip melakukan komputerisasi dalam proses bisnisnya untuk memudahkan kegiatan operasional secara rutin [1]. Selain komputerisasi, Kantor Arsip juga menambahkan dua server agar mempermudah dan mempercepat proses file sharing pada OPD lain. Hal ini selain membantu produktivitas namun sekaligus kontra produktif karena banyak risiko yang akan muncul serta mengganggu proses bisnis yang ada. Oleh karena itu dilakukan studi ini agar dapat memetakan ancaman dan melakukan pencegahan.

Penelitian dimulai dengan studi pendahuluan, perencanaan penelitian, identifikasi responden, pembuatan instrumen pengambilan data, pengolahan data dan

rekomendasi kepada Kantor Arsip [1]. Identifikasi responden dibuat dengan bantuan metode RACI (*Responsible, Accountable, Consulted and/or Informed*). Analisis risiko dilakukan dengan melakukan evaluasi terhadap dua hal, yaitu kuesioner terhadap domain tertentu dan perbedaan tingkat risiko yang diharapkan. Pada penelitian ini digunakan tiga domain, antara lain Domain Tingkat Kematangan Tata Kelola, Domain Tingkat Kematangan Evaluasi Risiko dan Domain Tingkat Kematangan Respon Risiko. Penilaian pada Domain Tata Kelola rerata memiliki nilai dua, Domain Evaluasi Risiko mendapat nilai tiga apabila dibulatkan, dan Domain Respon Risiko juga pada nilai dua. Apabila disimpulkan tingkat kematangan tata kelola risiko pada, Domain Tata Kelola dan Evaluasi Risiko berada pada tingkat repeatable but intuitive dan Domain Evaluasi Risiko berada pada tingkat *defined*. Adapun beberapa saran agar evaluasi manajemen risiko dapat dilakukan secara rutin, hasil analisis juga digunakan sebagai masukan dan referensi perbaikan, perlu dilakukan evaluasi risiko dengan standar lain agar dapat dijadikan tolak ukur dan perbaikan harus terus menerus dipantau agar dapat terlihat perbedaannya.

Sesuai dengan uraian di atas dihasilkan sebuah tabel ringkasan penelitian sebelumnya dan berisi ringkasan penelitian ini untuk menunjukan perbedaan dari penelitian yang telah dilakukan dengan penelitian yang sudah ada. Berikut tabel ringkasan penelitian seperti pada tabel 2.1.

Tabel 2.1. Ringkasan penelitian sebelumnya

No	Penulis	Tahun	Domain	Tujuan	Pendekatan	Alat	Hasil
1	Asriyani, Prajoko	2018	Manajemen risiko aplikasi pada sistem akademik	Menghasilkan rekomendasi yang dapat digunakan UMMI dalam menangani dan memitigasi risiko terhadap aplikasi sistem akademik di Universitas Muhammadiyah Sukabumi	Kuantitatif	ISO 27005: 2011	Didapatkan dua risiko level rendah (low), tujuh risiko level tinggi (high), dan 64 risiko level sedang (medium). 47 skenario ancaman harus ditangani, sembilan belas skenario ancaman akan dimodifikasi, satu risiko akan ditransfer dan 27 risiko tersisa

							dapat dihindari.
2	Riszullah Ramadhan Putra , Eman Setiawan , Awalludiyah Ambarwati	2019	Manajemen risiko perangkat-keras pada sistem akademik	Mengetahui apakah 4 jenis risiko utama mempengaruhi proses operasional eLina atau sistem e-learning di Universitas Narotama	Kuantitatif	NIST SP-800 30 Revisi I	Hasilnya tiga risiko pada level tinggi/high, sepuluh risiko pada level sedang/moderate dan satu risiko pada level rendah/low. Peneliti menyarankan penggantian versi bahasa pemograman menjadi versi 7.0 dan audit IT berkala
3	Damar Nurcahyono , Achmad Djunaedi	2013	Manajemen risiko penggunaan pada sistem manajemen	Mengevaluasi risiko pada sistem informasi kearsipan (SIMPAN) sebagai tindak lanjut dari proses tata kelola teknologi informasi di Kantor Arsip Daerah Samarinda	Kuantitatif	Cobit IT Risk Framework	Penilaian pada Domain Tata Kelola rerata memiliki nilai dua, Domain Evaluasi Risiko mendapat nilai tiga apabila dibulatkan, dan Domain Respon Risiko juga pada nilai dua.
4	Syukron Salahuddin, Awalludiyah Ambarwati, Mohamad Noor Al Azam [18]	2018	Manajemen risiko pada sistem informasi operasional manajemen	Manajemen risiko pada sistem informasi SIM-PTS sesuai dengan ISO 27005: 2008 di Departemen Sistem dan Teknologi Informasi (DSTI)	Kuantitatif	ISO 27005: 2011	Penelitian dilakukan hanya sampai pada tahap *risk assestment.* Penilaian ini dillakukan terhadap aset infrastruktur dan perangkat keras yang ada di DSTI.
5	Fathoni Mahardika [19]	2017	Manajemen risiko keamanan informasi pada seluruh aset TI	Manajemen risiko pada UPT LPSI STMIK Sumedang menggunakan NIST SP 800-30 Rev 1 dan ISO 27002 sebagai penerapan kontrol	Kualitatif	NIST SP 800-30 Rev 1 dan ISO 27002	Penelitian ini menghasilkan tingkat moderat pada risiko keamanan informasi di STMIK Sumedang. Dengan 20 risiko *high*, 46 risiko *moderate,* 10 risiko *low* dan 2 risiko *very low.*

2.2. Dasar Teori

2.2.1. Keamanan Informasi

Dengan peranan informasi yang menjadi krusial, keamanan informasi menjadi suatu usaha sebuah organisasi untuk menjaga aset informasi terhadap risiko-risiko yang berpotensi muncul. Terdapat 3 aspek penting yang harus diperhatikan yaitu: kerahasiaan, ketersediaan serta keutuhan [4]. Kerahasiaan berarti informasi hanya dapat diakses oleh pihak yang berwenang dan aman dari pihak yang tidak berwenang. Ketersediaan dapat diartikan bahwa informasi dapat diakses kapanpun dan dimanapun. Kemudian keutuhan berarti informasi tidak mengalami pengurangan nilai yang disengaja atau utuh secara informasi. Dengan menerapkan prosedur-prosedur serta control dalam mengamankan sebuah informasi maka dapat mereduksi potensial risiko dan mengoptimalkan pengambilan keputusan [21].

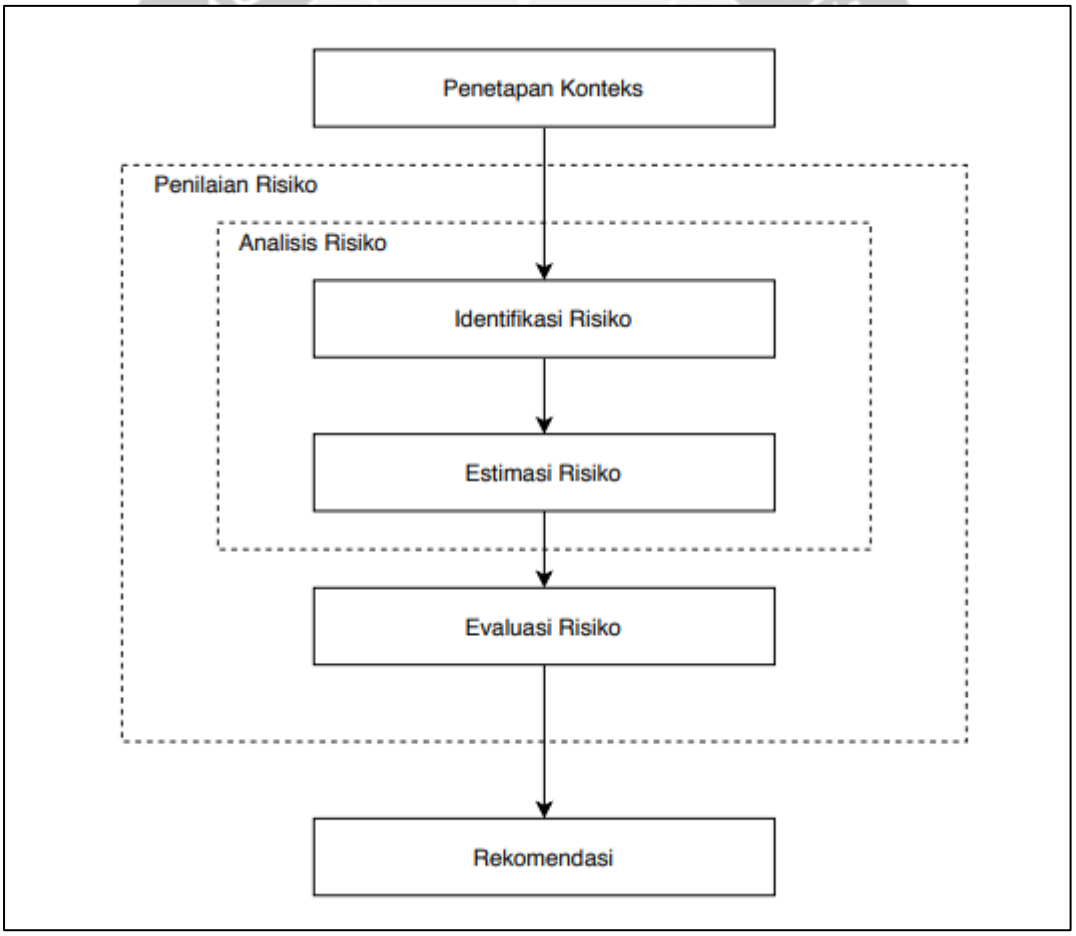
2.2.2. Manajemen Risiko

Pengertian manajemen risiko tidak lepas dari definisi dasar dari risiko apabila merujuk kepada Kamus Besar Bahasa Indonesia, risiko merupakan suatu kata benda yang mengakibatkan suatu kerugian atau membahayakan [22]. The *Institute of Internal Auditor* (IIA) menjelaskan bahwa risiko adalah sebuah ketidakjelasan dari sebuah kejadian yang menghalangi dan berdampak bagi organisasi dalam mencapai tujuan [16]. Menurut NHS risiko selalu berasosiasi dengan sesuatu yang berbahaya, baik dalam tugas dan tempat kerja sampai pada tingkatan yang dapat ditoleransi berkaitan dengan kerugian dari sisi SDM, legal bahkan ekonomi sebuah organisasi [23].

Menurut I. Häring, manajemen risiko merupakan serangkaian aktivitas dalam menganalisis risiko. Risiko tersebut diidentifikasi, dinilai, dan selanjutnya disusun langkah strategis yang dapat digunakan dalam mengatasi risiko tersebut. Tujuan utama dari dilaksanakannya manajemen risiko adalah memberikan pandangan terkait kemungkinan yang bisa terjadi sehingga perusahaan dapat menyusun langkah pencegahan dan penilaian terkait risiko. Terdapat 5 tahapan manajemen risiko berdasarkan [24] :

1. Menetapkan konteks
2. Mengidentifikasikan bahaya/risiko
3. Menganalisis risiko.
4. Mengevaluasi/menilai/memprioritaskan/pemeringkatan risiko.
5. Mencegah risiko.

Standar ISO 27005: 2008 juga memiliki metodologi yang digunakan dalam proses manajemen risiko. Proses ini dikembangkan dalam ruang lingkup keamanan informasi yang tercantum pada klausul dan annex dari ISO 27001, sehingga proses manajemen risiko yang dilakukan dapat melengkapi keseluruhan proses keamanan informasi. Berikut proses manajemen risiko berdasarkan ISO 27005: 2008 yang akan dijadikan pedoman dalam penelitian ini.



Gambar 2.1. Proses manajemen risiko yang digunakan peneliti

Setelah menetapkan konteks dari metodologi manajemen risiko berdasarkan

ISO 27005: 2008, metodologi yang dipilih dalam penelitian ini digambarkan di gambar 2.1. Berikut penjelasan dari gambar 2.1.

1. Pada tahapan awal dilakukan penetapan konteks manajemen risiko. Konteks ini ditetapkan dalam ruang lingkup Diskominfo Statistik dan Persandian Kota XYZ yang meliputi kajian kebijakan, standar dan regulasi yang berlaku, kajian proses bisnis yang terdapat di Diskominfo Statistik dan Persandian Kota XYZ.
2. Pada tahap analisis risiko dilakukan proses identifikasi risiko dan estimasi risiko. Identifikasi risiko adalah proses menentukan kerawanan serta ancaman yang dapat merugikan Diskominfo Statistik dan Persandian Kota XYZ. Sedangkan estimasi risiko digunakan untuk menilai kemungkinan dari sebuah konsekuensi risiko terjadi.

Pada tahap penilaian risiko, hasil dari analisis dampak dan kecenderungan yaitu penilaian dampak dan kecenderungan. Dari hasil penilaian ini, nilai risiko ditentukan dengan matriks dampak dan kecenderungan yang akan menghasilkan tingkatan risiko berupa, rendah/*low,* sedang/*medium* dan tinggi/*high.* Penilaian ini dilakukan agar organisasi dapat memetakan secara jelas tingkatan risiko yang terjadi pada aset mereka. Kemudian organisasi dapat mencocokan dengan kriteria nilai risiko yang diinginkan sebelumnya. Tingkatan risiko ini dibagi menjadi tiga tingkat dengan warna sebagai simbol, yaitu : tingkatan rendah / warna hijau, tingkatan sedang / warna kuning, tingkatan tinggi / warna merah. Penilaian ini dibuat dalam matriks (x, y), dengan sumbu x sebagai representasi dampak dan sumbu y sebagai representasi frekuensi atau kecenderungan [25]. Untuk lebih jelasnya dapat disimak pada gambar di bawah ini.

MATRIKS EVALUASI RISIKO

Likelihood					
5	Medium	Medium	High	High	High
4	Low	Medium	Medium	High	High
3	Low	Medium	Medium	Medium	High
2	Low	Low	Medium	Medium	High
1	Low	Low	Low	Medium	Medium
	1	2	3	4	5
	Impact				

Gambar 2.2. Matriks Evaluasi Risiko

Panduan Bank Indonesia (PBI) juga mengeluarkan parameter yang dapat digunakan dalam penilaian risiko yang dilakukan dengan menentukan matriks dampak dan kecenderungan serta parameter tiap matriks. Matriks penilaian dampak yang akan digunakan terdapat pada gambar 2.3.

Gambar 2.3. Matriks Nilai Dampak ISO 27005: 2008 [21]

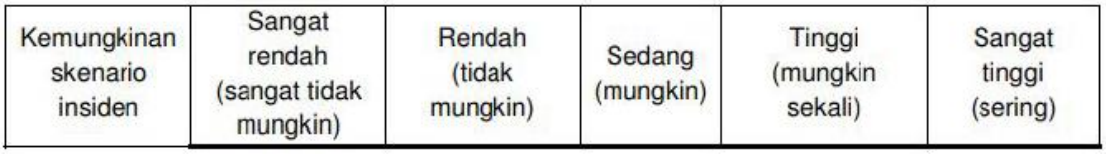
Terdapat lima tingkat pada nilai dampak sesuai ISO 27005: 2008, yaitu mulai dari Sangat Rendah, Rendah, Tinggi, Sedang, Tinggi dan Sangat Tinggi [21]. Dampak bisnis pada Gambar 2.3 dapat dipetakan sesuai dengan konteks aset dan ancaman yang telah ditentukan. Sedangkan parameter dari nilai dampak dapat diuraikan seperti pada Tabel 2.2.

Tabel 2.2. Parameter dampak menurut panduan Bank Indonesia[13]

Nilai	**Potensi gangguan terhadap Proses Bisnis**	**Potensi penurunan Reputasi**
5	Aset Pemrosesan Informasi mengalami kegagalan total sehingga keseluruhan bisnis bank tidak tercapai.	Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan di mata nasabah/stakeholders utama, pasar uang dan masyarakat secara global dan regional.
4	Aset Pemrosesan Informasi	Kerusakan reputasi yang tidak

	mengalami gangguan yang menyebabkan aktivitas bisnis bank mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih	menyeluruh – hanya nasabah atau partner bisnis (counterparties) tertentu.
3	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian bisnis bank mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih	Kerusakan reputasi yang tidak menyeluruh – hanya di divisi/bagian/tim tertentu.
2	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya.	Kerusakan reputasi yang tidak menyeluruh - hanya satuan kerja tertentu.
1	Tidak menyebabkan gangguan terhadap operasional proses bisnis	Tidak berpengaruh pada reputasi.

Pada Tabel 2.2 terdapat parameter dampak terhadap proses bisnis dan penurunan reputasi bagi sebuah organisasi apabila sebuah aset terkena sebuah ancaman/risiko. Parameter ini diambil dari PBI [21]. Dalam hal ini dampak yang ditentukan adalah dampak dari sebuah ancaman terhadap sebuah aset sebelum adanya penerapan pengendalian apapun. Dampak yang melekat pada sebuah aset inilah yang biasa disebut sebagai dampak inheren. Matriks yang akan digunakan pada penilaian kecenderungan akan menggunakan matriks lima nilai seperti pada Gambar 2.4.



Gambar 2.4. Matriks Tingkat Kecenderungan [21]

Tingkat kecenderungan yang ada pada Gambar 2.4. juga diambil dari lampiran ISO 27005: 2008 [21]. Sesuai dengan panduan PBI matriks ini dapat diturunkan menjadi parameter sesuai dengan tabel 2.3. [13]:

Tabel 2.3. Klasifikasi Tingkat Kecenderungan

Level	Frekuensi Kejadian	Potensi Terjadi	Deskripsi
5	Sangat sering terjadi	Potensi terjadi tinggi dalam jangka pendek	Hampir tidak mungkin terjadi atau terjadi kurang dari 10 kali tiap tahun
4	Lebih sering terjadi	Potensi terjadi tinggi dalam jangka panjang	Tidak mungkin terjadi atau terjadi kurang lebih sekali setahun, akan tetapi terjadi lebih dari sekali dalam kurun waktu 10 tahun
3	Cukup sering terjadi	Potensi terjadi sedang	Agak mungkin terjadi, atau terjadi antara 1-10 kali tiap tahunnya
2	Jarang Terjadi	Potensi terjadi kecil	Sangat mungkin terjadi, atau terjadi antara 10-100 kali tiap tahunnya
1	Hampir tidak pernah terjadi	Kemungkinan terjadi sangat kecil	Hampir pasti terjadi, atau terjadi lebih dari 100 kali tiap tahunnya

Kecenderungan ini bersifat kuantitatif, artinya sebuah risiko dapat diukur tingkat terjadinya dalam satuan waktu. Waktu dapat ditetapkan dalam sebuah

frekuensi nilai mulai dari hari, minggu, bulan atau tahunan. Nilai kuantitatif ini akan menyesuaikan dengan deskripsi risiko yang telah didefinisikan dan sifatnya inheren atau melekat terhadap aset [26]. Nilai kecenderungan serta dampak ini yang nanti akan menghasilkan nilai risiko sebuah aset. Berikut matriks nilai risiko pada Gambar 2.5:

	Kemungkinan skenario insiden	Sangat rendah (sangat tidak mungkin)	Rendah (tidak mungkin)	Sedang (mungkin)	Tinggi (mungkin sekali)	Sangat tinggi (sering)
Dampak bisnis	Sangat rendah	0	1	2	3	4
	Rendah	1	2	3	4	5
	Sedang	2	3	4	5	6
	Tinggi	3	4	5	6	7
	Sangat tinggi	4	5	6	7	8

Gambar 2.5. Matriks Nilai Risiko

Nilai risiko ini yang akan digunakan sebagai dasar dalam menentukan prioritas dari penanganan sebuah risiko dengan sumber daya yang ada dan juga menentukan penerimaan terhadap sebuah risiko sesuai dengan kebutuhan organisasi [26]. Semua nilai-nilai, mulai dari dampak, kecenderungan dan nilai risiko akan dikumpulkan bersama dengan identifikasi aset dan risiko yang akan membentuk sebuah risk register. Model *risk register* yang akan digunakan dapat dilihat pada Gambar 2.6.

No	Aset	Deskripsi Risiko	Analisa Kerawanan	Inheren			Pengendalian yg Ada	Residual			Nilai Risiko Akhir Diharapkan
				Kecenderungan	Dampak	Nilai Risiko Dasar		Kecenderungan	Dampak	Nilai Risiko Akhir	
0	1	2	3	4	5	6	7	8	9	10	11

Gambar 2.6. *Risk Register*

Risk Register atau yang biasa disebut Dokumen Hasil Identifikasi dan Pengukuran Risiko inilah yang akan menjadi sebuah keluaran dari proses manajemen risiko. Dalam dokumen ini pendekatan yang digunakan ialah pendekatan aset, sehingga risiko yang diidentifikasi ialah segala potensi risiko yang melekat atau bawaan dari aset itu sendiri, akan tetapi pada tulisan ini tidak akan dibahas mengenai Risiko Residual yaitu, gambar 2.6. tabel nomor delapan sampai sebelas. Model *risk register* ini juga dipilih karena yang paling sesuai dengan *risk register* Diskominfo Statistik dan Persandian Kota XYZ menurut Perwali No. 28 [23].

2.2.3. ISO 27001

ISO 27001 adalah sebuah standar yang dikeluarkan oleh International Organization for Standardization. Standar ISO 27001 ini merupakan standar yang ditujukan dapat membantu perusahaan dalam melindungi keamanan aset perusahaan dan untuk melindungi sistem manajemen keamanan informasi (SMKI). Pada standard ini memuat 114 kontrol dan 35 kontrol objektif dari empat belas area kontrol dalam keamanan informasi [27] [14].

2.2.4. ISO 27005:2008

Standar ini diterbitkan tahun 2008 dalam rangka untuk melengkapi seri Sistem Manajemen Keamanan Informasi (SMKI), baik secara prosedural maupun petunjuk-petunjuk teknis. Standar ISO 27005: 2008 ini memuat pedoman bagi organisasi yang akan melakukan manajemen risiko, khususnya pada keamanan informasi. Standar ini sangat mendukung syarat-syarat dari annex dan clausal berdasarkan ISO 27001 [15] [28]. Pada standar ini terdapat dua belas klausal yaitu klausul lima mengenai latar belakang dari manajemen risiko, deskripsi secara umum mengenai proses manajemen risiko keamanan informasi terletak di klausul enam.

Seluruh aktivitas manajemen risiko keamanan informasi yang dipresentasikan pada klausul enam, akan dijelaskan pada klausul-klausul berikut : penentuan konteks pada klausul tujuh, evaluasi risiko pada klausul delapan, penanganan risiko terletak di klausul sembilan, penerimaan risiko dijelaskan di klausul sepuluh, komunikasi risiko

terletak di klausul sebelas dan pemantauan dan peninjauan risiko pada klausul dua belas. Apabila disimpulkan seluruh aktivitas proses manajemen risiko tercantum mulai dari klausul tujuh sampai dua belas [29].

2.2.5. Aset Teknologi Informasi

Aset teknologi informasi adalah semua aset yang digunakan untuk melakukan pemrosesan informasi bagi sebuah organisasi. Segala aspek yang mendukung proses bisnis utama dapat dianggap sebagai aset teknologi informasi, aset-aset ini dapat digolongkan menjadi dua jenis aset, meliputi [14]:

a. Aset utama biasanya didefinisikan sebagai proses atau informasi yang digunakan organisasi dalam konteks penyusunan keamanan informasi atau rencana kelangsungan bisnis.
   - Proses bisnis, sub-proses bisnis dan kegiatan
   - Informasi
b. Aset pendukung adalah seluruh aset yang mendukung kinerja aset utama agar dapat berjalan dengan semaksimal mungkin. Apabila aset pendukung ini dieksploitasi maka akan berdampak secara langsung ke aset utama.
   - Perangkat keras;
   - Perangkat lunak;
   - Jaringan;
   - Personel;
   - Tempat; dan
   - Struktur Organisasi.

BAB III

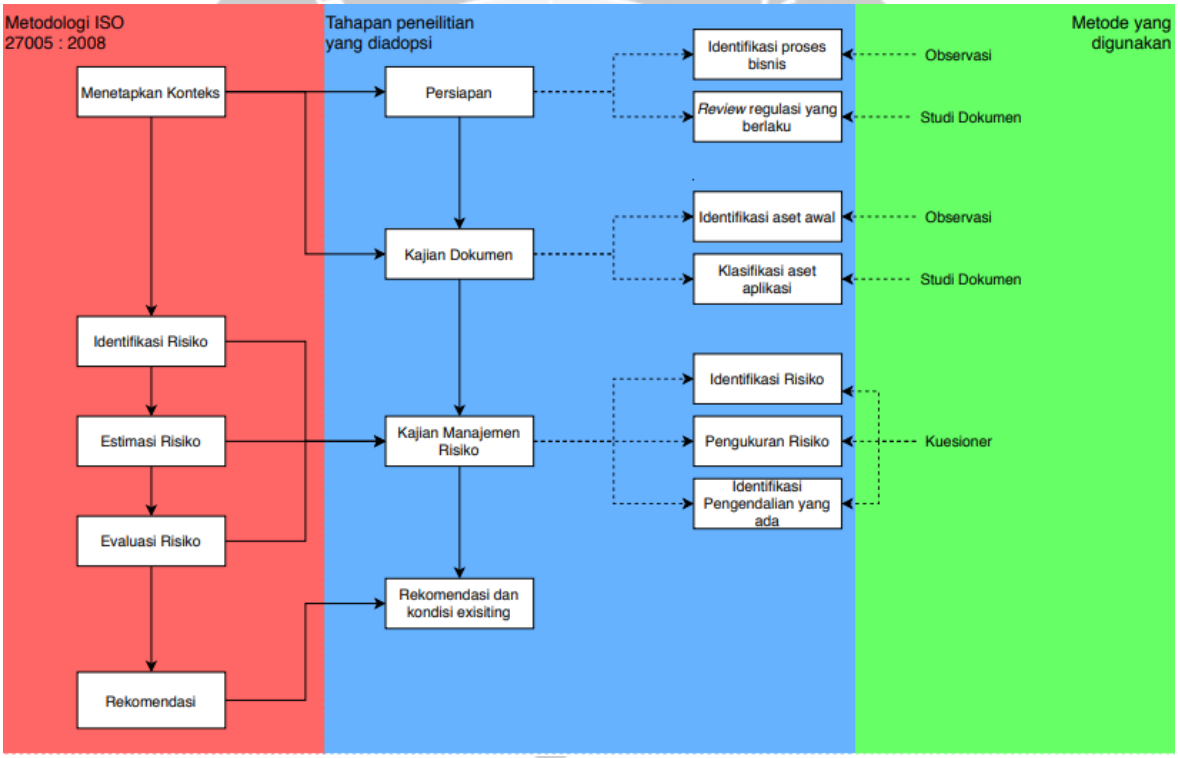
METODOLOGI PENELITIAN

3.1. Waktu Penelitian

Penelitian akan dilaksanakan mulai dari bulan Mei hingga Juli 2020.

3.2. Tahapan Penelitian

Tahapan penelitian yang memuat manajemen risiko sesuai ISO 27005: 2008 ditunjukkan pada gambar 3.1.



Gambar 3.1. Tahapan Penelitian

Pada gambar 3.1. terdapat tahapan penelitian yang dilengkapi dengan metode yang digunakan. Secara garis besar terdapat empat tahapan utama mulai dari persiapan, kajian dokumen, kajian manajemen risiko serta rekomendasi berdasarkan kajian manajemen risiko. Tahapan ini sesuai dengan batasan masalah yang telah ditentukan dan menyesuaikan ruang lingkup metodologi manajemen risiko menurut

ISO 27005: 2008 dan disesuaikan dengan kondisi Diskominfo Statistik dan Persandian Kota XYZ saat ini. Tahapan penelitian ini dijabarkan dalam tahapan, metode dan luaran, seperti pada tabel 3.1 di bawah ini.

Tabel 3.1. Tabel Tahapan Penelitian

No	Tahapan	Deskripsi Tahapan	Metode	Luaran
I	**Persiapan**			
I.1	Identifikasi Proses Bisnis	• Melakukan observasi terhadap proses bisnis yang dilakukan di lapangan.	Observasi	• Proses Bisnis Organisasi
I.2	*Review* Regulasi yang berlaku	• Kajian peraturan, kebijakan, standar instansi.	Studi Dokumen	
II	**Kajian Dokumen**			
II.1	Identifikasi Aset Awal	• Melakukan identifikasi terhadap aset-aset yang akan dinilai risikonya secara langsung.	Observasi	• Daftar Aset Perangkat Lunak
II.2	Klasifikasi Aset Aplikasi	• Melakukan klasifikasi aset sesuai dengan standar ISO 27005: 2008. Aset Aplikasi akan mengikuti klasifikasi Aset	Studi Dokumen	• Klasifikasi Aset Perangkat Lunak

		Perangkat Lunak sesuai dengan yang tertera pada lampiran ISO 27005: 2008.		
III	**Kajian Manajemen Risiko**			
III.1	Identifikasi Risiko	• Evaluasi pengguna dan penyelenggara TI terhadap potensi ancaman dan dampak dari kerentanan atau kelemahan proses pengamanan yang ada/diterapkan Diskominfo Statistik dan Persandian Kota XYZ atas aset yang telah didefinisikan	Kuesioner	• *Risk Register* Perangkat Lunak yang memuat Identifikasi ancaman, analisa kerawanan, dampak dan kecenderungan.
III.2	Pengukuran Risiko	• Menilai risiko berdasarkan nilai dampak dan kecenderungan yang telah ditentukan sebelumnya. Nilai risiko akan diklasifikasikan berdasarkan	Kuesioner	• Penilaian Risiko Perangkat Lunak

		tingkatan risiko (*high, medium dan low*).		
III.3	Identifikasi Pengendalian yang Ada	• Menetapkan pengendalian yang telah diterapkan dan digunakan dalam organisasi, sebagai Langkah pencegahan terjadinya sebuah risiko pada sebuah aset.	Kuesioner	• *Risk Register* Perangkat Lunak yang memuat pengendalian yang telah diimplemetasikan
IV	**Rekomendasi dan Kondisi Saat ini**			
IV.1	Analisis Kondisi Aset Aplikasi saat ini dan Rekomendasi Perbaikan	• Mengumpulkan hasil klasifikasi aset, identifikasi risiko dan kerawanan, kemudian evaluasi nilai risiko berdasarkan dampak dan kecenderungan, untuk menggambarkan kondisi aset saat ini dan menentukan rekomendasi perubahan untuk menurunkan nilai		• Rekomendasi

		risiko yang diinginkan.		

Pada tabel di atas terdapat empat tahapan utama yaitu persiapan yang sebenarnya dapat diringkas menjadi penetapan konteks, kemudian dari hasil tersebut akan dilanjutkan ke dalam proses manajemen risiko tahap awal yaitu mendaftarkan aset dalam bentuk luaran dokumen identifikasi risiko. Tahapan selanjutnya dilanjutkan dengan proses manajemen risiko menggunakan ISO 27005: 2008, yaitu mengklasifikasikan aset sesuai dengan standar tersebut dalam bentuk dokumen klasifikasi aset. Klasifikasi aset ini akan dijadikan dasar dalam menentukan risiko dan ancaman serta penilaian risikonya akan dituangkan dalam bentuk kuesioner. Setelah penilaian selesai dilakukan baru dapat diberikan rekomendasi perbaikan terhadap risiko.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Proses penilaian risiko diawali dengan identifikasi aset aplikasi di Diskominfo Statistik dan Persandian Kota XYZ, dilanjutkan dengan klasifikasi aset perangkat lunak, identifikasi menggunakan standar ISO 27005: 2008 dan tahapan akhir yaitu rekomendasi. Dari proses identifikasi risiko dihasilkan enam belas aset aplikasi yang tersedia di Diskominfo Statistik dan Persandian Kota XYZ. Hasil identifikasi aset aplikasi ini diklasifikasikan lagi sesuai dengan klasifikasi aset perangkat lunak menurut ISO 27005: 2008, yang menghasilkan lima jenis aset. Identifikasi risiko dan kerawanan dilakukan sesuai klasifikasi aset yang ditentukan. Dari proses identifikasi risiko dihasilkan 22 risiko yang dikategorikan dalam tiga tingkat risiko yaitu sembilan belas risiko pada tingkat rendah/*low*, satu risiko pada tingkat sedang/*medium* dan dua risiko pada tingkat tinggi/*high*. Sedangkan penilaian risiko ini memuat nilai kecenderungan dan dampak menggunakan parameter yang tercantum pada parameter penilaian dari Pedoman Manajemen Risiko Bank Indonesia.

Adapun rekomendasi peneliti berdasarkan tingkat risiko dan implementasi yang telah diterapkan. Pada sisi teknis perlu ditambahkan fitur *session login* dan logout agar *user* dapat logout secara otomatis, melakukan konfigurasi pada server secara berkala, menambahkan enkripsi pada kata sandi semua *user.* Dari sisi infrastruktur dapat menambahkan stabilizer untuk menjaga tegangan listrik khususnya bagi aset pendukung perangkat lunak. Dari segi prosedural dapat melakukan pelatihan setiap ada pengubahan antarmuka perangkat lunak, pelatihan mengenai keamanan informasi agar meningkatkan kesadaran hingga tingkat *staff*, membuat kerangka pelaporan yang sesuai dengan standar internal, menambah prosedur teknis seperti pencatatan log server, menyebar data ke beberapa server untuk menekan risiko kehilangan data, menghapus hak akses bagi para pegawai yang sudah non-aktif, meletakan aset-aset kritikal di tempat yang lebih tinggi, membuat skenario bencana dan membuat *IT master plan* 5-10 tahun ke depan. Rekomendasi dibuat dengan melakukan studi

literatur pada standar-standar, aturan atau prosedur yang bisa diterapkan dan relevan bagi perbaikan pengendalian yang ada serta kondisi aset terkini.

5.2. Saran

Berdasarkan keterbatasan yang dilakukan pada penelitian ini, berikut beberapa saran yang dapat dilakukan untuk penelitian selanjutnya. Berikut saran yang dapat dilakukan:

1. Melakukan penilaian manajemen risiko lanjutan untuk menentukan nilai risiko residual setelah penerapan pengendalian yang merupakan hasil manajemen risiko sebelumnya.
2. Melakukan proses *risk treatment* setelah proses penilaian risiko dilakukan.

DAFTAR PUSTAKA

[1] D. Nurcahyono and A. Djunaedi, "Evaluasi Pelaksanaan Manajemen Risiko Teknologi Informasi pada K antor Arsip Daerah Kota Samarinda dengan Menggunakan The Risk IT Framework," *Jnteti*, vol. 2, no. 3, pp. 3–6, 2013.

[2] H. Nugroho, "Analisis Manajemen Resiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 4.1," *Konf. Nas. ICT-M Politek. Telkom*, 2012.

[3] S. Kaushik, M. Singh, and A. Chugh, "Information Security," *J. J. Reasearch Appl. Sci. Eng. Technol.*, vol. 8, no. 5, pp. 2779–2738, 2020, doi: 10.1017/CBO9781107415324.004.

[4] T. D. K. Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013, doi: 10.1017/CBO9781107415324.004.

[5] T. Informatika, U. Sam, R. Manado, J. Kampus, and U. Bahu, "Implementasi Indeks Kami Di Universitas Sam Ratulangi," *J. Tek. Inform. Univ. Sam Ratulangi*, vol. 12, no. 1, 2017, doi: 10.35793/jti.12.1.2017.17869.

[6] I. Muallidin, "Konsep, Kerangka Pikir & Nilai E-Government & E-Service," *Researchgate*, no. January 2015, 2015, doi: 10.13140/RG.2.2.26828.92801.

[7] L. Salsabila and E. P. Purnomo, "Establishing and Implementing Good Practices E-Government (A Case Study : e-Government Implementation between Korea and Indonesia)," *Asean/ Asia Acad. Soc. Int. Conf.*, vol. 5, pp. 221–229, 2017.

[8] J. Sleeman, T. Finin, and M. Halem, "Temporal Understanding of Cybersecurity Threats," no. May, pp. 115–121, 2020, doi: 10.1109/bigdatasecurity-hpsc-ids49724.2020.00030.

[9] V. Gaftea, "Socio-economic Major Risks Related to the Information Technology," *Procedia Econ. Financ.*, vol. 8, no. 14, pp. 336–345, 2014, doi: 10.1016/s2212-5671(14)00099-9.

[10] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan*

Ilmu Komput., vol. 2, no. 11, pp. 4991–4998, 2018.

[11] Pemerintah Republik Indonesia, "Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik," *Media Huk.*, p. 110, 2018.

[12] Permenkes. 2014., "UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 23 TAHUN 2014 TENTANG PEMERINTAHAN DAERAH," no. Peraturan Menteri Kesehatan Republik Indonesia Nomor 75 Tahun 2014 tentang Pusat Kesehatan Masyarakat., 2014, doi: 10.1038/132817a0.

[13] B. S. dan S. N. R. Indonesia, "PERATURAN BADAN SIBER DAN SANDI NEGARA," *J. Chem. Inf. Model.*, vol. 1, no. 9, p. 20, 2019, doi: 10.1017/CBO9781107415324.004.

[14] International Organization for Standardization, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements," *Inf. Technol. — Secur. Tech. — Inf. Secur. Manag. Syst. — Requir.*, vol. 2014, no. ISO/IEC 27001:2013, p. 38, 2013.

[15] A. Asriyanik and Prajoko, "Manajemen Keamanan Informasi pada Sistem Informasi Akademik Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 315–325, 2018, doi: 10.28932/jutisi.v4i2.792.

[16] P. Hopkin and I. of R. Management, *Fundamentals of Risk Management*, vol. 2nd Editio. 2010.

[17] B. A. Isnanto, "Situs Pemkot Solo Diretas, Hacker Sebutkan Kata Tak Senonoh," 2020. [Online]. Available: https://news.detik.com/berita-jawa-tengah/d-4977110/situs-pemkot-solo-diretas-hacker-sebutkan-kata-tak-senonoh.

[18] S. Salahuddin, A. Ambarwati, and M. N. Al Azam, "Identifikasi Risiko Keamanan Informasi Menggunakan ISO 27005 pada Sebuah Serguruan Tinggi Swasta di Surabaya," *Semin. Nas. Sist. Inf.*, pp. 990–996, 2018.

[19] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," vol. 02, no. 02, pp. 1–8, 2017.

[20] R. R. Putra, "ANALISIS MANAJEMEN RISIKO TI PADA KEAMANAN DATA E -

LEARNING DAN ASET IT MENGGUNAKAN NIST SP 800 – 30 Revisi 1," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 6, no. 1, pp. 96–105, 2019, doi: 10.35957/jatisi.v6i1.154.

[21] O. B. Umum, "Direktorat Penelitian dan Pengaturan Perbankan," no. November, p. 2009, 2007.

[22] KBBI, "Definisi Risiko menurut Kamus Besar Bahasa Indonesia." [Online]. Available: https://kbbi.web.id/risiko.

[23] Cardiff and Vale University Health Board, "Risk Assessment and Risk Register Procedure," no. January 2013, pp. 1–22, 2017.

[24] I. Häring, "Risk analysis and management: Engineering resilience," *Risk Anal. Manag. Eng. Resil.*, pp. 1–365, 2016, doi: 10.1007/978-981-10-0015-7.

[25] G. Mochammad Husein and R. V. Imbar, "Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL)," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, no. 2, pp. 75–87, 2015, doi: 10.28932/jutisi.v1i2.368.

[26] NIST, "NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments," *NIST Spec. Publ.*, no. September, p. 95, 2012, doi: 10.6028/NIST.SP.800-30r1.

[27] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, 2018.

[28] International Standard Organization, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Application security —," vol. 2011, 2011.

[29] The British Standards Institution, "Information technology - Security techniques - Code of practice for information security controls (BS ISO/IEC 27002:2013)," *BSI Stand. Publ.*, pp. 1–94, 2013, doi: 10.1016/j.emj.2004.09.025.

[30] M. R. M. Dangi, A. Nawawi, and A. S. A. P. Salin, "Application of COSO framework in whistle-blowing activities of public higher-learning institutions,"

Int. J. Law Manag., vol. 62, no. 2, pp. 193–211, 2020, doi: 10.1108/IJLMA-06-2017-0145.

DAFTAR REVISI

Tabel Revisi

No.	Tugas Revisi	Halaman Revisi
1.	Detail OS dan Lisensi	- Halaman 30 - Halaman 32 - Halaman 39 - Lampiran Telah ditambahkan versi-versi pada sistem operasi yang berdasarkan hasil observasi serta *interview* sebelumnya. Untuk aset Linux ditiadakan karena terletak pada komputer server.
2.	*Flowchart* pengambilan keputusan atau kesepakatan	- Halaman 27 Telah ditambahkan penjelasan singkat mengenai proses pengambilan keputusan atau kesepakatan selama proses manajemen risiko berlangsung.
3.	Nilai kuantitatif diperjelas	- Halaman 16 dan 17 Sudah ditambahkan kuantitatif tiap-tiap kecenderungan dan sitasi terkait sumber.
4.	Justifikasi bahwa *project* ini benar-benar diimplementasi oleh *client*	- Halaman 43 Telah ditambahkan justifikasi mengenai implementasi penelitian ini yang diacu dari peta jalan keamanan informasi yang diberikan.
5.	Latar belakang ditambahkan penelitian ini hasil dari magang dan konteksnya mendapat tugas manajemen aset *software*	- Halaman 3 Pada paragraf terakhir mengenai tindak lanjut dari proses magang sebelumnya.

LAMPIRAN

Contoh Kuesioner

TATA CARA PENGISIAN KUISIONER:
1. Kuisioner terbagi menjadi 5 kategori (hardware, software, data & informasi, personel)
2. Bapak/Ibu cukup mengisi kuning KOLOM 5 yaitu KECENDERUNGAN , KOLOM 6 yaitu DAMPAK dan KOLOM 7 yaitu PENGENDALIAN YANG ADA.
3. KOLOM 5 berisi pilihan (pilih salah satu), urut dari atas mulai dengan frekuensi PALING SERING
4. KOLOM 6 berisi pilihan (pilih salah satu), urut dari atas mulai DAMPAK TERBURUK
5. KOLOM 7 mohon diisi dengan uraian (kegiatan/kebijakan) yang dilakukan untuk memperkecil dampak
6. Mohon diisi sesuai kondisi eksisting di dalam organisasi Bapak/Ibu

CONTOH PENGISIAN KUISIONER, sebagai berikut:

KUISIONER PENILAIAN RISIKO ASET

PERANGKAT KERAS

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada	Nilai Risiko
					Kecenderungan	Dampak		
0	1	2	3	4	5	6	7	8

Paramerter Penilaian Kecenderungan

Inheren		
Kecenderungan		
	Keterangan	
Frekuensi Kejadian	Potensi Terjadi	
Sangat Sering Terjadi	Potensi Terjadinya Tinggi dalam jangka pendek	Sangat Sering Terjadi | Potensi Terjadinya Tinggi
Lebih Sering Terjadi	Potensi Terjadi tinggi dalam jangka panjang	Lebih Sering Terjadi | Potensi Terjadi tinggi dalam
Cukup Sering Terjadi	Potensi Terjadi Sedang	Cukup Sering Terjadi | Potensi Terjadi Sedang
Jarang Terjadi	Potensi Terjadi Kecil	Jarang Terjadi | Potensi Terjadi Kecil
Hampir Tidak pernah terjadi	Kemungkinan Terjadi Sangat Kecil	Hampir Tidak pernah terjadi | Kemungkinan Terjadi

Paramerter Penilaian Dampak

Pengukuran Dampak		
Keterangan		
Potensi Gangguan terhadap proses layanan	Potensi Penurunan Reputasi	
Aset Pemrosesan Informasi mengalami kegagalan total sehingga keseluruhan layanan instansi tidak tercapai	Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan dimata masyarakat/stakeholders utama dan masyarakat	Aset Pemrosesan Informasi mengalami kegagalan total sehingga keseluruhan layanan instansi tidak tercapai | Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan dimata masyarakat/stakeholders utama dan
Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan aktivitas layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih	Kerusakan reputasi yang tidak menyeluruh – hanya masyarakat atau partner bisnis (counterparties) tertentu	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan aktivitas layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya masyarakat atau partner bisnis
Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih	Kerusakan reputasi yang tidak menyeluruh – hanya di divisi/bagian/tim tertentu	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya di divisi/bagian/tim tertentu
Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya	Kerusakan reputasi yang tidak menyeluruh - hanya satuan kerja tertentu	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya | Kerusakan reputasi yang tidak menyeluruh - hanya satuan kerja tertentu
Tidak menyebabkan gangguan terhadap operasional proses bisnis	Tidak berpengaruh pada reputasi	Tidak menyebabkan gangguan terhadap operasional proses bisnis | Tidak berpengaruh pada reputasi

Paramerter Penilaian Risiko

Nilai Risiko Dasar	
Kecenderungan-Dampak	Score
11	Low
12	Low
13	Medium
14	Medium
15	High
21	Low
22	Low
23	Medium
24	Medium
25	High
31	Low
32	Low
33	Medium
34	High
35	High
41	Low
42	Medium
43	High
44	High
45	High
51	Medium
52	Medium
53	High
54	High
55	High

Lampiran Daftar Aset Perangkat Lunak

No	Nama Aplikasi	Bidang/ Bagian / UPTD	Penanggung Jawab teknis	Alamat Aplikasi	Lokasi Hosting	Jenis Aplikasi	Deskripsi Aplikasi
1	Website XYZ	DISKOMINFO STATISTIK DAN PERSANDIAN – Bidang Informatika	DISKOMINFO STATISTIK DAN PERSANDIAN	XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	WEB PROFIL	Website *official* Pemerintah Kota XYZ yang memuat konten fokus Kota XYZ atau berasal dari OPD (Organisasi Perangkat Daerah
2	Website Diskominfo Statistik dan Persandian Kota XYZ	DISKOMINFO STATISTIK DAN PERSANDIAN – Bidang Informatika		diskominfosp.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	WEB PROFIL	Website *official* Diskominfo Statistik dan Persandian Kota XYZ yang memuat konten di seluruh bidangnya
3	E-Office	DISKOMINFO STATISTIK DAN PERSANDIAN – Bidang Informatika dan Sekretariat		e-office.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	SISTEM INFORMASI	Sistem informasi untuk pengelolaan surat masuk dan surat keluar, yang diimplementasikan kepada seluruh OPD dan BUMD Kota XYZ
4	Surat Elektronik XYZ	DISKOMINFO STATISTIK DAN PERSANDIAN – Bidang Informatika		webmail.XYZ.go.id		E-MAIL	E-mail khusus untuk OPD Kota XYZ

No	Nama Aplikasi	Bidang/ Bagian / UPTD	Penanggung Jawab teknis	Alamat Aplikasi	Lokasi Hosting	Jenis Aplikasi	Deskripsi Aplikasi
5	Aplikasi Penyimpanan Data	DISKOMINFO STATISTIK DAN PERSANDIAN – Bidang Informatika		download.XYZ.go.id (Link Tidak Tersedia)	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	PENYIMPANAN CLOUD	Aplikasi untuk penyimpanan berbagai data guna dipublikasikan ke masyarakat
6	Aplikasi Penyimpanan Data	DISKOMINFO STATISTIK DAN PERSANDIAN – Bidang Informatika		dropbox.XYZ.go. id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	PENYIMPANAN CLOUD	Aplikasi untuk penyimpanan berbagai data
7	XIBO BSTV	DISKOMINFO STATISTIK DAN PERSANDIAN -Bidang Informatika		digitalinfo.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	SISTEM INFORMASI	Sistem guna memantau video Batik XYZ TV yang ada di seluruh kelurahan di Kota XYZ
8	E-Kelurahan	Kelurahan dan Kecamatan di Kota XYZ	DISKOMINFO STATISTIK DAN PERSANDIAN	kelurahan.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	SISTEM INFORMASI	Sistem yang digunakan untuk pelayanan kependudukan di lingkungan kelurahan dan kecamatan
9	Open Data	DISKOMINFO STATISTIK DAN PERSANDIAN – BIDANG STATISTIK	DISKOMINFO STATISTIK DAN PERSANDIAN	data.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	SISTEM INFORMASI	Open Data Kota XYZ merupakan sistem yang menyajikan seluruh data Pemerintah Kota XYZ yang bersifat publik.

No	Nama Aplikasi	Bidang/ Bagian / UPTD	Penanggung Jawab teknis	Alamat Aplikasi	Lokasi Hosting	Jenis Aplikasi	Deskripsi Aplikasi
10	Dashboard Kota XYZ	DISKOMINFO STATISTIK DAN PERSANDIAN – BIDANG INFORMATIKA	DISKOMINFO STATISTIK DAN PERSANDIAN	Dashboard.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	SISTEM INFORMASI	Sistem yang digunakan untuk memantau perkembangan visi misi Walikota XYZ (3 WMP)
11	Aset Diskominfo Statistik dan Persandian	DISKOMINFO STATISTIK DAN PERSANDIAN – BIDANG INFORMATIKA	DISKOMINFO STATISTIK DAN PERSANDIAN	aset.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	SISTEM INFORMASI	Sistem yang dapat menyimpan seluruh infrastruktur jaringan yang dimiliki DISKOMINFO STATISTIK DAN PERSANDIAN
12	SIBAHENOL	DISKOMINFO STATISTIK DAN PERSANDIAN – BIDANG INFORMATIKA, BIDANG KOMUNIKASI DAN PERSANDIAN	DISKOMINFO STATISTIK DAN PERSANDIAN	baliho.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	SISTEM INFORMASI	SIBAHENOL (Sistem Informasi Baliho Pesan Online) merupakan Sistem yang dapat digunakan untuk pengelolaan baliho secara online mulai dari pemesanan hingga pelaporan penggunaan baliho
13	SDS	DISKOMINFO STATISTIK DAN PERSANDIAN -BIDANG STATISTIK	DISKOMINFO STATISTIK DAN PERSANDIAN	sds.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	SISTEM INFORMASI	SDS (Single Data System) merupakan sistem yang menyediakan keterbukaan data publik di tingkat Provinsi Jawa Tengah

No	Nama Aplikasi	Bidang/ Bagian / UPTD	Penanggung Jawab teknis	Alamat Aplikasi	Lokasi Hosting	Jenis Aplikasi	Deskripsi Aplikasi
14	FORUS	DISKOMINFO STATISTIK DAN PERSANDIAN	DISKOMINFO STATISTIK DAN PERSANDIAN	forus.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	APLIKASI	FORUS (Forum untuk Semua) merupakan aplikais yang digunakan untuk ajang diskusi dan pustaka Pemerintah Kota XYZ, informasi publik
15	WEBSITE PPID	DISKOMINFO STATISTIK DAN PERSANDIAN – BIDANG STATISTIK	DISKOMINFO STATISTIK DAN PERSANDIAN	ppid.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	WEB PROFIL	Web PPID (Pejabat Pengelola Informasi Daerah) merupakan website yang memuat seluruh informasi publik dari berbagai OPD dan konten yang ada kaitannya dengan pejabat di Pemkot XYZ
16	WEBSITE SPEEDTEST	DISKOMINFO STATISTIK DAN PERSANDIAN – BIDANG INFORMATIKA	DISKOMINFO STATISTIK DAN PERSANDIAN	speedtest.XYZ.go.id	SERVER DISKOMINFO STATISTIK DAN PERSANDIAN	APLIKASI	Aplikasi berbasis web yang digunakan untuk mengetahui tingkat kecepatan penggunaan internet

Lampiran *Risk Register* Perangkat Lunak

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
1	Sistem Operasi di Clients	Sistem Operasi: - Ms. Windows (Windows 10 Pro 64bit) - macOS versi 10.14 dan 10.15	Penyalahgunaan hak	Tidak logout ketika meninggalkan komputer	Cukup Sering Terjadi | Potensi Terjadi Sedang	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya | Kerusakan reputasi yang tidak menyeluruh - hanya satuan kerja tertentu	1. Mengingatkan untuk logout dan mematikan komputer apabila tidak dipakai 2. Memanfaatkan fitur *auto logout*

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
			Kesalahan penggunaan	Antar muka yang rumit	Cukup Sering Terjadi | Potensi Terjadi Sedang	Tidak menyebabkan gangguan terhadap operasional proses bisnis | Tidak berpengaruh pada reputasi	1. Pelatihan dasar penggunaan sistem operasi 2. Assisting terhadap permasalahan yang muncul (tidak bisa printing, tidak bisa scanning, dsb) 3. Menyiapkan panduan untuk permasalahan yang sering terjadi

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
			Pemalsuan hak	Kurangnya mekanisme identifikasi dan otentikasi, contoh : - Manajemen pengguna - Manajemen *Password*	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya di divisi/bagian/tim tertentu	1. Penggantian *password* berkala 2. Melakukan pendataan *user* (siapa bertanggungjawab atas komputer mana)
			Pengolahan data ilegal	Layanan-layanan krusial yang tidak diaktifkan, contoh :	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset	1. Pengecekan kondisi antivirus 2. Sosialisasi berinternet yang baik dan sehat

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
				- Antivirus - Firewall		pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya | Kerusakan reputasi yang tidak menyeluruh - hanya satuan kerja tertentu	
			Perusakan dengan perangkat lunak lainnya	Unduhan / penggunaan perangkat lunak / aplikasi yang tidak terkontrol	Cukup Sering Terjadi | Potensi Terjadi Sedang	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak	1. Melakukan instal ulang program tertentu atau bahkan sistem operasi yang digunakan 2. Melakukan pembatasan

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						menyeluruh – hanya di divisi/bagian/tim tertentu	terhadap situs-situs ilegal dari jaringan kantor
2	Situs	Situs resmi : - Website XYZ - Website Diskominfo Statistik dan Persandian Kota XYZ	Perusakan Peralatan atau Media	Penggunaan yang tidak memadai atau ceroboh atas kontrol akses fisik ke bangunan dan ruangan-ruangan	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya | Kerusakan reputasi yang tidak menyeluruh - hanya	1. Terdapat pembatasan akses masuk ke ruangan-ruangan tertentu 2. Keamanan menggunakan sidik jari 3. Terdapat kamera keamanan

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						satuan kerja tertentu	
			Banjir	Lokasi pada daerah yang rentan banjir	Hampir Tidak pernah terjadi | Kemungkinan Terjadi Sangat Kecil	Aset Pemrosesan Informasi mengalami kegagalan total sehingga keseluruhan layanan instansi tidak tercapai | Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan di mata masyarakat/stakeholders utama dan masyarakat	1. Simulasi terhadap kebencanaan yang mungkin terjadi (gempa bumi, kebakaran, dsb) 2. Membuat backup terhadap data/aset penting di daerah lain 3. SOP untuk

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
							recovery dari bencana
			Hilangnya pasokan listrik	Jaringan listrik yang tidak stabil	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami kegagalan total sehingga keseluruhan layanan instansi tidak tercapai | Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan di mata masyarakat/stakeholders utama dan masyarakat	1. Menyiapkan cadangan listrik (genset/generator listrik cadangan) 2. Menyiapkan alur kerja cadangan apabila listrik mati 3. Menggunakan perangkat dengan tenaga baterai (laptop,

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
							smartphone, tablet, dsb)
			Pencurian peralatan	Kurangnya perlindungan fisik terhadap gedung, pintu, dan jendela	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami kegagalan total sehingga keseluruhan layanan instansi tidak tercapai | Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan di mata masyarakat/stakeholders utama dan masyarakat	1. Terdapat pembatasan akses masuk ke ruangan-ruangan tertentu 2. Keamanan menggunakan sidik jari 3. Terdapat kamera keamanan

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
3	Layanan, pemeliharaan, atau perangkat lunak administrasi	Sistem Informasi : - E-Office - XIBO BSTV - E-Kelurahan - Dashboard Kota XYZ - Aset DISKOMINFO STATISTIK DAN PERSANDIAN - SIBAHENOL - SDS - PPID	Penyalahgunaan hak	- Tidak ada atau tidak cukup pengujian perangkat lunak - Tidak 'logout' ketika meninggalkan komputer - Pembuangan atau pemakaian ulang media penyimpanan tanpa penghapusan	Cukup Sering Terjadi | Potensi Terjadi Sedang	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan aktivitas layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya masyarakat atau partner bisnis (counterparties) tertentu	1. Sosialisasi sistem informasi 2. Uji coba dan pelaporan bug terhadap sistem informasi yang dipakai 3. Penyediaan grup whatsapp untuk penanganan permasalahan-permasalahan yang muncul 4. Membiasakan mematikan

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
				yang tepat - Kesalahan penempatan hak akses			komputer ketika ditinggal/tidak dipakai 5. Pembaruan media penyimpanan (DVD/flashdisk)
			Pemalsuan hak	- Kurangnya mekanisme identifikasi dan otentikasi seperti otentikasi pengguna - Tabel	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak	1. Pendataan identitas pengguna 2. Menggunakan enkripsi dengan tambahan salt 3. Penggantian *password* berkala

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
				password yang tidak dilindungi - Manajemen *password* yang buruk		menyeluruh – hanya di divisi/bagian/tim tertentu	
			Kegagalan perangkat	- Spesifikasi pengembangan yang tidak jelas atau tidak lengkap - Kurangnya kontrol perubahan yang efektif	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan aktivitas layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya masyarakat atau partner	1. Evaluasi terhadap spesifikasi dan fitur yang ada serta perbaikannya 2. Manajemen perubahan disertai dokumentasi / buku petunjuk pelaksanaan

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						bisnis (counterparties) tertentu	
			Perusakan dengan perangkat lunak	Kurangnya salinan back-up	Cukup Sering Terjadi | Potensi Terjadi Sedang	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan aktivitas layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya masyarakat atau partner bisnis (counterparties)	1. Backup berkala 2. Pelaksanaan SOP apabila terjadi kerusakan 3. Penyediaan alternatif sistem apabila terjadi kerusakan

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						tertentu	
			Pencurian media atau dokumen	Kurangnya perlindungan fisik pada gedung, dan jendela	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan aktivitas layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya masyarakat atau partner bisnis (counterparties)	1. Terdapat pembatasan akses masuk ke ruangan-ruangan tertentu 2. Keamanan menggunakan sidik jari 3. Terdapat kamera keamanan

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						tertentu	
			Penggunaan peralatan yang tidak sah	Kesalahan pembuatan laporan manajemen	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya | Kerusakan reputasi yang tidak menyeluruh - hanya	1. Monev terhadap laporan 2. Pendataan terhadap perangkat dan penggunanya

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						satuan kerja tertentu	
4	Perangkat lunak paket atau perangkat lunak standar	Surat Elektronik XYZ	Penyalahgunaan hak	- Tidak 'logout' ketika meninggalkan komputer - Pembuangan atau pemakaian ulang media penyimpanan tanpa penghapusan	Cukup Sering Terjadi | Potensi Terjadi Sedang	Tidak menyebabkan gangguan terhadap operasional proses bisnis | Tidak berpengaruh pada reputasi	1. Penggantian *password* berkala 2. Menggunakan fitur log-out for all *user* secara berkala 3. Penyediaan media penyimpanan baru 4. Dokumen pembagian hak akses

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
				yang tepat - Kesalahan penempatan hak akses			
			Kesalahan penggunaan	- Kurangnya dokumentasi - Kesalahan tanggal	Cukup Sering Terjadi | Potensi Terjadi Sedang	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya | Kerusakan reputasi yang	1. Penomoran dan penanggalan surat secara teratur/tercatat pada agenda 2. Dokumentasi surat secara otomatis menggunakan E-Office

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						tidak menyeluruh - hanya satuan kerja tertentu	3. Backup agenda secara manual
			Pemalsuan hak	Manajemen *Password* yang buruk	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya | Kerusakan reputasi yang tidak menyeluruh - hanya	1. Penggantian *password* berkala 2. Monev dokumen hak akses

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						satuan kerja tertentu	
			Perusakan dengan perangkat lunak	Kurangnya salinan back-up	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya di divisi/bagian/tim tertentu	1. Backup berkala 2. Penyediaan sistem/alur kerja secara manual 3. Pelaksanaan tahapan recovery

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
5	Aplikasi bisnis	Aplikasi : - Aplikasi Penyimpanan Data (Dropbox) - Web Speedtest	Penyalahgunaan hak	- Tidak 'logout' ketika meninggalkan komputer - Pembuangan atau pemakaian ulang media penyimpanan tanpa penghapusan yang tepat -Kesalahan penempatan hak akses	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya di divisi/bagian/tim tertentu	1. Penggantian *password* berkala 2. Membudayakan log out dan mematikan komputer jika tidak dipakai 3. Penyediaan media penyimpanan baru 4. Dokumentasi terhadap hak akses

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
			Pemalsuan hak	Manajemen *Password* yang buruk	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian layanan instansi mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya di divisi/bagian/tim tertentu	1. Penggantian *password* berkala 2. Sosialisasi keamanan informasi bagi end *user* 3. Dokumentasi hak akses
			Perusakan dengan perangkat lunak	Kurangnya salinan back-up	Jarang Terjadi | Potensi Terjadi Kecil	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan aktivitas layanan instansi mengalami penundaan sampai Aset	1. Backup berkala 2. Melakukan tahapan recovery 3. Penyediaan data secara manual/fisik

No	Klasifikasi Aset	Aset	Risiko	Analisa Kerawanan	Inheren		Pengendalian yg Ada
					Kecenderungan	Dampak	
0	1	2	3	4	5	6	7
						Pemrosesan Informasi yang terkait pulih | Kerusakan reputasi yang tidak menyeluruh – hanya masyarakat atau partner bisnis (counterparties) tertentu	

Lampiran Penilaian Risiko

No	Klasifikasi Aset	Aset	Risiko	Nilai Risiko (Kecenderungan, Dampak)
0	1	2	3	4
1	Sistem Operasi di Clients	Sistem Operasi : - Linux - Ms. Windows	Penyalahgunaan hak	*3,2 (Low)*
			Kesalahan penggunaan	*3,1 (Low)*
			Pemalsuan hak	*2,3 (Low)*
			Pengolahan data illegal	*2,2 (Low)*
			Perusakan dengan perangkat lunak lainnya	*3,3 (Medium)*
2	Situs	Situs resmi : - Website XYZ - Website Diskominfo Statistik dan Persandian Kota XYZ	Perusakan Peralatan atau Media	*2,2 (Low)*
			Banjir	*1,5 (Low)*
			Hilangnya pasokan listrik	*2,5 (Low)*
			Pencurian peralatan	*2,5 (Low)*
3	Layanan, pemeliharaan, atau perangkat lunak administrasi	Sistem Informasi : - E-Office - XIBO BSTV - E-Kelurahan - Dashboard Kota	Penyalahgunaan hak	*3,4 (High)*
			Pemalsuan hak	*2,3 (Low)*
			Kegagalan perangkat	*2,4 (Low)*

No	Klasifikasi Aset	Aset	Risiko	Nilai Risiko (Kecenderungan, Dampak)
0	1	2	3	4
		XYZ - Aset DISKOMINFO STATISTIK DAN PERSANDIAN - SIBAHENOL - SDS - PPID	Perusakan dengan perangkat lunak	*3,4 (High)*
			Pencurian media atau dokumen	*2,4 (Low)*
			Penggunaan peralatan yang tidak sah	*2,2 (Low)*
4	Perangkat lunak paket atau perangkat lunak standar	Surat Elektronik XYZ	Penyalahgunaan hak	*3,1 (Low)*
			Kesalahan penggunaan	*3,2 (Low)*
			Pemalsuan hak	*2,2 (Low)*
			Perusakan dengan perangkat lunak	*2,3 (Low)*
5	Aplikasi bisnis	Aplikasi : - Aplikasi Penyimpanan Data (Dropbox) - Web Speedtest	Penyalahgunaan hak	*2,3 (Low)*
			Pemalsuan hak	*2,3 (Low)*
			Perusakan dengan perangkat lunak	*2,4 (Low)*

Lampiran Rekomendasi

No	Klasifikasi Aset	Aset	Risiko	Nilai Risiko (Kecenderungan, Dampak)	Rekomendasi
0	1	2	3	4	5
1	Sistem Operasi di Clients	Sistem Operasi : - Linux - Ms. Windows	Penyalahgunaan hak	*3,2 (Low)*	Membuat *session* untuk *user* dan fitur *auto logout* apabila beberapa saat *user* dalam kondisi *idle*.
			Kesalahan penggunaan	*3,1 (Low)*	Melakukan pelatihan pada *user* setiap ada pembaharuan antar muka aplikasi.
			Pemalsuan hak	*2,3 (Low)*	Melakukan penghapusan akses pada *user* yang sudah tidak aktif/bekerja lagi, Menambahkan enkripsi pada table *password*, Menerapkan prosedur untuk penggantian *password* berkala.
			Pengolahan data ilegal	*2,2 (Low)*	Memblokir layanan-layanan dan situs yang berbahaya.
			Perusakan dengan perangkat lunak lainnya	*3,3 (Medium)*	Menyediakan lisensi perangkat lunak yang asli dan aman kepada *user*.

2	Situs	Situs resmi : - Website XYZ - Website Diskominfo Statistik dan Persandian Kota XYZ	Perusakan Peralatan atau Media	*2,2 (Low)*	Melakukan penyuluhan berkala mengenai pemeliharaan aset agar aset terjaga dalam jangka panjang.
			Banjir	*1,5 (Low)*	Membuat skenario bencana, Meletakan aset-aset kritikal di tempat yang lebih tinggi.
			Hilangnya pasokan listrik	*2,5 (Low)*	Menambahkan *stabilizer* tegangan listrik.
			Pencurian peralatan	*2,5 (Low)*	Membuat catatan log akses pengunjung pada lokasi aset bertempat.
3	Layanan, pemeliharaan, atau perangkat lunak administrasi	Sistem Informasi : - E-Office - XIBO BSTV - E-Kelurahan - Dashboard Kota XYZ	Penyalahgunaan hak	*3,4 (High)*	Membuat *session* untuk *user* dan fitur *auto logout* apabila beberapa saat *user* dalam kondisi *idle,* Melakukan penghapusan akses pada *user* yang sudah tidak aktif/bekerja, Menerapkan pemeliharaan aset berkala pada media penyimpanan.

		- Aset DISKOMINFO STATISTIK DAN PERSANDIAN - SIBAHENOL - SDS - PPID	Pemalsuan hak	*2,3 (Low)*	Melakukan penghapusan akses pada *user* yang sudah tidak aktif/bekerja lagi, Menerapkan prosedur untuk penggantian *password* berkala, Membuat fitur 2 kali verifikasi pada *login user.*
			Kegagalan perangkat	*2,4 (Low)*	Membuat IT master plan 5-10 tahun ke depan, Menggali kebutuhan *user* pada setiap calon *user* yang akan menggunakan.
			Perusakan dengan perangkat lunak	*3,4 (High)*	Menyebar data di beberapa server untuk mengurangi risiko kehilangan, Menggunakan layanan server yang terbaik
			Pencurian media atau dokumen	*2,4 (Low)*	Menerapkan prosedur pencatatan log pada setiap peminjaman dokumen dan media.
			Penggunaan peralatan yang tidak sah	*2,2 (Low)*	Membuat *template* pelaporan yang sudah menerapkan standar internal.
4	Perangkat lunak paket	Surat Elektronik XYZ	Penyalahgunaan hak	*3,1 (Low)*	Membuat *session* untuk *user* dan fitur *auto logout* apabila beberapa saat *user* dalam kondisi *idle*.

	atau perangkat lunak standar		Kesalahan penggunaan	*3,2 (Low)*	Melakukan konfigurasi tanggal pada server secara berkala.
			Pemalsuan hak	*2,2 (Low)*	Menghapus hak akses bagi pekerja yang sudah tidak aktif atau bekerja lagi.
			Perusakan dengan perangkat lunak	*2,3 (Low)*	Membagi data ke beberapa server untuk mengurangi potensi kehilangan data.
5	Aplikasi bisnis	Aplikasi : - Aplikasi Penyimpanan Data (Dropbox) - Web Speedtest	Penyalahgunaan hak	*2,3 (Low)*	Membuat *session* untuk *user* dan fitur *auto logout* apabila beberapa saat *user* dalam kondisi *idle.*
			Pemalsuan hak	*2,3 (Low)*	Menghapus hak akses bagi pekerja yang sudah tidak aktif atau bekerja lagi.
			Perusakan dengan perangkat lunak	*2,4 (Low)*	Membagi data ke beberapa server untuk mengurangi potensi kehilangan data.