PERENCANAAN MITIGASI RISIKO PADA LAYANAN KOORDINASI TELE – PRESENCE MENGGUNAKAN METODE OCTAVE –S DI PEMERINTAH KABUPATEN MALANG

SKRIPSI

Oleh

Yuca Akbar Maulana

NIM 132410101066

PROGRAM STUDI SISTEM INFORMASI

UNIVERSITAS JEMBER

2017

PERENCANAAN MITIGASI RISIKO PADA LAYANAN KOORDINASI TELE – PRESENCE MENGGUNAKAN METODE OCTAVE –S DI PEMERINTAH KABUPATEN MALANG

SKRIPSI

Diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan pendidikan di Program Studi Sistem Informasi Universitas Jember dan mendapat gelar Sarjana Sistem Informasi

Oleh

Yuca Akbar Maulana

NIM 132410101066

PROGRAM STUDI SISTEM INFORMASI

UNIVERSITAS JEMBER

2017

PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

1. Allah SWT yang senantiasa memberikan rahmat dan hidayah-Nya untuk mempermudah dan melancarkan dalam mengerjakan skripsi.
2. Ayahanda Tjahjono, S.E dan Ibunda Farida Yulianti, S.Sos tercinta.
3. Saudara Muhammad Bagus Saputro atas doa dan dukungannya
4. Bapak Tri Darmawan atas dukungannya
5. Seluruh keluarga besar Roeslan
6. Bapak dan Ibu Dosen Program Studi Sistem Informasi
7. Teman-teman seperjuangan “d’kontrakan”
8. Almamater Program Studi Sistem Informasi Universitas Jember.

MOTTO

"Be Patient and Just Do Good Things"

("Bersabar dan Lakukan Hal-Hal Baik")

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Yuca Akbar Maulana

NIM : 132410101066

menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul "Perencanaan Mitigasi Risiko Pada Layanan Koordinasi Tele – Presence Menggunakan Metode Octave –S Di Pemerintah Kabupaten Malang", adalah benar-benar hasil karya sendiri, kecuali jika dalam pengutipan substansi disebutkan sumbernya, belum pernah diajukan pada institusi mana pun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika di kemudian hari pernyataan ini tidak benar.

Jember, 14 Juli 2017

Yang menyatakan,

Yuca Akbar Maulana

NIM 132410101066

SKRIPSI

PERENCANAAN MITIGASI RISIKO PADA LAYANAN KOORDINASI TELE – PRESENCE MENGGUNAKAN METODE OCTAVE –S DI PEMERINTAH KABUPATEN MALANG

Oleh :
Yuca Akbar Maulana
NIM 132410101066

Pembimbing

Dosen Pembimbing Utama : Windi Eka Yulia Retnani, S.Kom., M.T

Dosen Pembimbing Pendamping : Oktalia Juwita, S.Kom., M.MT

PENGESAHAN PEMBIMBING

Skripsi berjudul "Perencanaan Mitigasi Risiko Pada Layanan Koordinasi Tele – Presence Menggunakan Metode Octave –S Di Pemerintah Kabupaten Malang", telah diuji dan disahkan pada:

hari, tanggal : Jumat, 21 Juli 2017

tempat : Program Studi Sistem Informasi Universitas Jember

Disetujui oleh:

Pembimbing I,	Pembimbing II,
Windi Eka Yulia Retnani, S.Kom., M.T	Oktalia Juwita, S.Kom., M.MT
NIP. 198403052010122002	NIP. 198110202014042001

PENGESAHAN PENGUJI

Skripsi berjudul "Perencanaan Mitigasi Risiko Pada Layanan Koordinasi Tele – Presence Menggunakan Metode Octave –S Di Pemerintah Kabupaten Malang", telah diuji dan disahkan pada:

hari, tanggal : Jumat, 21 Juli 2017

tempat : Program Studi Sistem Informasi Universitas Jember

Tim Penguji :

Penguji I,	Penguji II,
Prof. Dr. Saiful Bukhori, ST., M.Kom	Nova El Maidah, SSi.,M.Cs
NIP. 196811131994121001	NIP. 198411012015042001

Mengesahkan

Ketua Program Studi

Prof. Drs. Slamin, M.Comp.Sc.,Ph.D

NIP. 19670420 1992011001

RINGKASAN

Perencanaan Mitigasi Risiko Pada Layanan Koordinasi Tele – Presence Menggunakan Metode Octave –S Di Pemerintah Kabupaten Malang; Yuca Akbar Maulana, 132410101066; 2017, 219 HALAMAN; Program Studi Sistem Informasi Universitas Jember.

Layanan atau sistem *Tele-Presemce* adalah salah satu sistem yang dikelola langsung oleh Dinas Komunikasi dan Informatika (DINKOMINFO) Kabupaten Malang yang dibentuk pada tahun 2016. Sistem *Tele-Presence* adalah hasil kerjasama DINKOMINFO dengan pihak ketiga pemilik dan pengembang sistem. Tujuan utama diterapkannya sistem yang telah berjalan sejak Januari 2017 ini adalah menyediakan kemudahan dalam koordinasi antar lembaga pemerintahan Kabupaten Malang. Implementasi teknologi informasi dan komunikasi pada bidang *e-government* ini tentu membawa manfaat disertai risiko yang harus dikelola dengan baik. Risiko yang muncul tidak hanya dari sisi teknis teknologi yang diterapkan, tetapi juga dari sisi praktik keamanan dan strategi organisasi. Permasalahan yang dihadapi oleh DINKOMINFO dengan diterapkannya *Tele-Presence* lebih dominan pada permasalahan praktik dan strategi keamanan organisasi, mengingat usia organisasi yang belum genap satu tahun. Maka perlu dilakukan evaluasi yang ditargetkan pada risiko organisasional dan difokuskan pada strategi dan permasalahan terkait praktik keamanan. Penulis menggunakan metode *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE) –S yang disesuaikan dengan karakter dan kebutuhan organisasi dalam mengidentifikasi risiko dan memberikan rekomendasi pendekatan risiko yang muncul.

Penelitian ini dilaksakan dalam 3 tahap yaitu, tahap pengumpulan data, tahap analisis data dan evaluasi, dan tahap pembangunan sistem. Tahap pengumpulan data dilakukan melalui kuisioner dan wawancara dengan pihak DINKOMINFO. Data yang terkumpul dituliskan dalam *worksheet* metode OCTAVE –S. Tahap analisis dan evaluasi dilakukan dengan membentuk pohon risiko unutk mengidentifikasi risiko aktif

berdasarkan pengamatan dan data yang diperoleh sehingga ditemukan pendekatan risiko. Tahap pembangunan sistem dilakukan dengan membangun sistem untuk membentuk nilai *risk exposure* dari risiko aktif dengan menggunakan kuantifikasi nilai dampak dan kemungkinan yang diolah dengan rumus kuantifikasi risiko. Hasil dari penelitian ini adalah identifikasi ancaman aktif beserta nilai *risk exposure* ancaman pada masing-masing area dampak dan rekomendasi perencanaan mitigasi risiko.

PRAKATA

Puji syukur kehadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul "Perencanaan Mitigasi Risiko Pada Layanan Koordinasi Tele – Presence Menggunakan Metode Octave –S Di Pemerintah Kabupaten Malang". Skripsi ini disusun untuk memenuhi salah satu syarat menyelesaikan pendidikan Strata Satu (S1) pada Program Studi Sistem Informasi Universitas Jember.

Penyusunan skripsi ini tidak lepas dari dukungan berbagai pihak. Oleh karena itu peulis menyampaikan terima kasih kepada :

1. Windi Eka Yulia Retnani, S.Kom., M.T., selaku Dosen Pembimbing Utama dan Otalia Juwita, S.Kom., M.MT selaku Dosen Pembimbing Anggota yang telah meluangkan waktu, pikiran, dan perhatian dalam penulisan skripsi;
2. Windi Eka Yulia Retnani, S.Kom., M.T., sebagai dosen pembimbing akademik, yang telah mendampingi penulis sebagai mahasiswa;
3. Seluruh Bapak dan Ibu dosen beserta staf karyawan di Program Studi Sistem Informasi Universitas Jember;
4. Ayahanda Tjahjono, S.E dan Ibunda Farida Yulianti, S.Sos yang selalu mendukung dan mendoakan;
5. Saudara Muhammad Bagus Saputro atas doa dan dukungannya;
6. Bapak Tri Daramawan atas dukungannya;
7. Dinas Komunikasi dan Informatika Kabupaten Malang, yang telah bersedia menjadi obejek penelitian;
8. Teman-teman d'kontrakan atas motivasi dan dukungannya;
9. Teman-teman seperjuanganku Intention angkatan 2013;
10. Semua pihak yang tidak dapat disebutkan satu persatu.

Penulis menyadari bahwa laporan ini masih jauh dari sempurna, oleh sebab itu penulis mengharapkan adanya masukan yang bersifat membangun dari semua pihak. Penulis berharap skripsi ini dapat bermanfaat bagi semua pihak.

Jember, 14 Juli 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1. PENDAHULUAN

Bab ini merupakan langkah awal dari penulisan tugas akhir. Bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, dan sistematika penulisan.

1.1 Latar Belakang

Penerapan teknologi informasi dalam bidang pemerintahan yang lebih dikenal dengan istilah *e-government* saat ini telah diterapkan di beberapa negara. *United Nation (Department of Economic and Social Affairs)* telah melakukan survei pada tahun 2016 mengenai *e-government* di seluruh dunia. *E-Governement Development Index (EGDI)* adalah index yang dibentuk untuk mengukur seberapa jauh negara-negara di dunia mengembangkan e-government. Jika dibandingkan degan survei pada tahun 2014, pada tahun 2016 terjadi peningkatan. Negara kategori ”*very-high-EGDI*” bertambah dari 25 negara menjadi 29 negara, negara kategori “*high-EGDI*” bertambah dari 62 menjadi 65 negara, sedangkan negara kategori “*medium-EGDI*” mengalami penurunan dari 74 negara menjadi 67 nergara (United Nation, 2016). Indonesia masuk kedalam ketegori “medium-EGDI” dengan nilai index berkisar antara 0.25 hingga 0.50 (United Nation, 2016). Index Indonesia masih kalah dengan nilai index negara tetangganya di sub-regional asia tenggara yaitu Singapura (0.88) yang menempati peringkat ke-2 di seluruh Asia dan peringkat ke-4 di seluruh dunia (United Nation, 2016).

E-government yang diterapkan di Indonesia dan negara-negara lain pada dasarnya memiliki tujuan yang sama, yakni pelayanan dalam bidang pemerintahan yang lebih baik. *E-government* menurut hubungannya dapat dikelompokan kedalam 4 jenis (Hardjaloka, 2014). *Government to citizen* adalah layanan publik dari pemerintah untuk pertukaran informasi dan komunikasi antara pemerintah dengan masyarakat. *Government to bussines* adalah layanan dimana pemerintah menyediakan informasi yang dibutuhkan untuk keperluan bisnis. *Government to government* adalah layanan pemerintahan untuk pertukaran informasi dan komunikasi antar departemen dalam

pemerintahan. *Government to employees* adalah layanan yang digunakan untuk meningkatkan kesejahteraan dan kinerja pegawai negeri.

Seiring dengan semakin berkembangnya teknologi, penerapan teknologi informasi pada *e-government* tentu tidak lepas dari ancaman dan risiko yang semakin tinggi. Berdasarkan survei yang dilakukan oleh ISACA (Information System Audit and Control Association) 75 persen dari 461 responden yang merupakan praktisi dan manajer *cybersecurity*, dapat menjadi korban dari cyberattack pada tahun 2016 (Information System Audit and Control Association, 2016). Survei lain mengenai *cyberattack* yang dilakukan oleh ISACA menyebutkan bahwa 7 persen dari 461 responden yang bekerja di bidang keamanan informasi, mengalami *hacking* setiap minggunya, dan 3 persen responden mengalami kerusakan dari dalam setiap minggunya (Information System Audit and Control Association, 2016). Mengingat bidang penerapan teknologi informasi *e-government* adalah salah satu bidang kritis, yakni pemerintahan negara, maka penerapan ini seharusnya didampingi keamanan yang memadai dengan melihat risiko yang mungkin terjadi.

Salah satu kabupaten di Jawa Timur yang telah menerapkan layanan *e-government* adalah kabupaten Malang. Kabupaten Malang menempati peringkat ke-10 se-Jawa Timur dalam penerepan *e-government* (Kementrian Komunikasi dan Informatika RI, 2016). Sebagai peringkat ke-10, tidak mengherankan jika pemerintah kabupaten Malang melakukan beberapa upaya untuk meningkatkan layanan *e-government* yang dimilikinya. Salah satu upaya peningkatannya adalah dengan menerapkan layanan *government to government* baru sejak Januari 2017.. Layanan yang diberi nama *Tele-Presence* ini adalah sebuah sistem yang memungkinkan adanya koordinasi antar lembaga pemerintahan melaui konferensi virtual. Layanan ini merupakan hasil kerjasama pemerintah Kabupaten Malang, dalam hal ini adalah Dinas Komunikasi dan Informatika dengan pihak pemilik dan pengembang sistem. Layanan ini masih dalam tahap I dan memiliki hak akses untuk bupati beserta jajarannya, dinas, kecamatan dan kelurahan. Untuk rencana tahap II, nantinya hak akses akan sampai ke tingkat desa.

Penggunaan teknologi informasi dalam implementasi layanan *Tele-Presence* ini tidak lepas dari risiko-risiko yang mungkin bisa terjadi. Oleh karena itu, perlu adanya manajemen risiko yang baik untuk meminimalkan dampak risiko-risiko yang muncul, salah satunya dengan metode OCTAVE –S. Metode OCTAVE lebih menekankan pengelolaan risiko berbasis acaman dan kelemahan terhadap aset-aset informasi organisasi meliputi perangkat keras, lunak, sistem, informasi, dan manusia (Supradono, 2009).

Penelitian ini disusun untuk menganalisa penggunaan teknologi informasi pada layanan koordinasi *Tele-Presence* berdasarkan risiko yang ditargetkan pada risiko organisasinal dan berfokus pada strategi keamanan dan permasalahan terkait praktik keamanan organisasi dengan metode OCTAVE –S. Manfaat dari penelitan ini adalah dapat memberikan rekomendasi langkah-langkah pendekatan atau penanganan risiko dengan mengidentifikasi asset-aset teknologi informasi, praktik keamanan organisasi, dan risiko yang muncul.

1.2 Rumusan Masalah

Berdasarkan uraian yang telah disampaikan dalam latar belakang, maka permaslaahan yang diangkat oleh peneliti adalah :

1. Aset-aset apa saja yang berperan dalam layanan *Tele-Presence* yang harus dilindungi keamanannya ?
2. Berapa persentase praktik keamanan organisasi yang dilakukan organisasi?
3. Berapa jumlah ancaman aktif yang teridentifikasi menggunakan metode OCTAVE –S dalam layanan *Tele-Presence* ?
4. Bagaimana pendekatan atau mitigasi risiko yang dapat dilakukan ?
5. Berapa nilai *risk exposure* tertinggi masing-masing area dampak yang ditemukan dalam setiap cabang ancaman aktif penerapan layanan *Tele-Presence* ?
6. Apakah ancaman utama dalam penerapan layanan *Tele-Presence*?

1.3 Tujuan

Tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Menghasilkan identifikasi aset-aset teknologi informasi terkait sistem *Tele-Presence*
2. Menghasilkan identifikasi praktik keamanan dan status praktik keamanan.
3. Menghasilkan profil risiko dalam layanan atau sistem *Tele-Presence.*
4. Menghasilkan rekomendasi langkah-langkah pendekatan atau penanganan risiko dan kelemahan-kelemahan yang muncul.
5. Menghasilkan nilai *risk exposure* masing-masing area dampak yang ditemukan dalam setiap cabang ancaman aktif penerapan layanan *Tele-Presence*.
6. Menghasilkan identifikasi ancaman utama dalam penerapan layanan *Tele-Presence*.

1.4 Manfaat

Manfaat dari penelitian ini adalah :

1. Bagi Akademis

   Hasil penelitian ini diharapkan menjadi salah satu sumber referensi bagi penelitian-penelitian di masa mendatang, yang dapat digunakan untuk pengembangan manajemen risiko.

2. Bagi Peneliti

   Mengetahui bagaimana proses evaluasi risiko dan melatih kemampuan dalam penerapan manajemen risiko dengan mengimplementasikan metode OCTAVE –S.

3. Bagi Objek Penelitian

   Mengetahui profil aset-aset teknologi informasi dalam layanan *Tele-Presence*, profil ancaman berbasis risiko terhadap aset kritis, serta rencana penanganan risiko dalam penerapan layanan

1.5 Batasan Masalah

Batasan masalah berdasarkan perumusan masalah yang akan dikaji dalam penelitian ini adalah :

1. Aset kritis dalam penilitian ini adalah sistem *Tele-Presence.*
2. Penilaian atau pengukuran risiko pada aset kritis dan aset-aset terkait berdasarkan hasil identifikasi permasalahan
3. Pengumpulan data, identifikasi risiko, dan mitigasi risiko menggunakan *worksheet* sesuai metode OCTAVE –S yang disesuaikan dengan kondisi dan kebutuhan oragnisasi.
4. Penentuan responden menggunakan RACI *chart*

1.6 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini adalah sebagai berikut:

1. Pendahuluan

   Bab kesatu ini memuat uraian tentang latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, dan sistematika penulisan skripsi yang masing-masing tertuang secara eksplisit dalam subbab tersendiri.
2. Tinjauan Pustaka

   Bab ini memaparkan tinjauan terhadap hasil-hasil penelitian terdahulu berkaitan dengan masalah yang dibahas, landasan materi, dan kajian teori metode analisis data yang berkaitan dengan masalah dalam penelitian.
3. Metodologi Penelitian

   Bab ini menguraikan tentang tempat dan waktu penelitian, metode penelitian, metode pengumpulan data, metode analisis data, dan teknik pengembangan sistem yang digunakan dalam penelitian.
4. Analisis Risiko

   Bab ini berisi uraian tentang analisis data. Metode analisis data yang digunakan adalah analisis OCTAVE –S, dimulai dari mengidentifikasi infromasi

organisasional kemudian mengidentifikasi profil ancaman kemudian memeriksa infrastruktur komputasi terkait aset kritis.

5. Hasil dan Pembahasan

   Bab ini memaparkan secara rinci pemecahan masalah dengan mengembangkan perencanaan penanganan risiko yang dituliskan dalam bentuk deskripsi dibantu dengan ilustrasi berupa tabel dan gambar untuk memperjelas hasil penelitian.

6. Penutup

   Bab ini terdiri atas kesimpulan atas penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.

BAB 2. TINJAUAN PUSTAKA

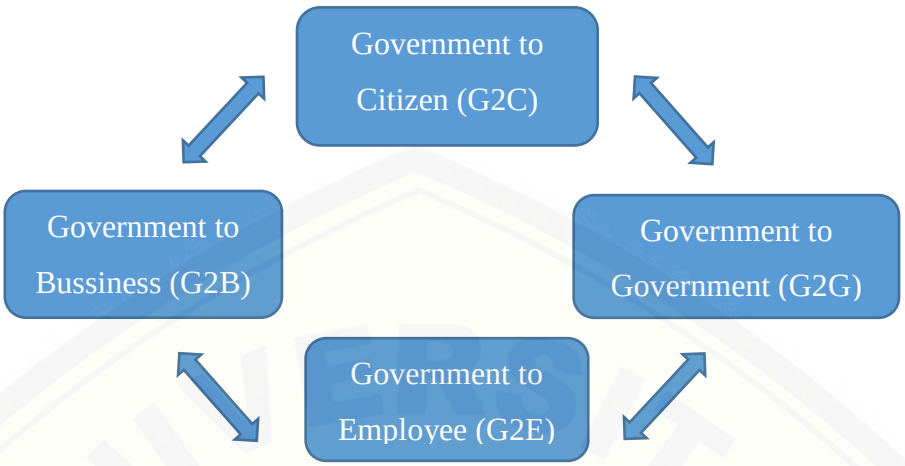
Pada bagian ini dipaparkan tinjauan teori yang digunkan dalam penelitian, kajian teori terkait permaslahan dan kanjian teori berkaitan dengan permasalahan yang dihadapi Teori-teori diambil dari berbagai *literature*, jurnal, dan *website*.

2.1 E-Government

E-government adalah layanan dalam bidang ketatanegaraan atau pemerintahan yang menggunakan teknologi informasi dan komunikasi dengan tujuan agar hubungan anatar badan pemerintahan, pemerintah dengan pelaku bisnis, dan masyarakat menjadi lebih efektif. Jika ditinjau dari bentuk hubungan berdasarkan deskripsi diatas, maka e-govermenet terbagi kedalam 4 model (Hardjaloka, 2014) sebagai berikut :

1. *Goverment to Citizen* (G2C) adalah layanan yang digunakan pemerintah untuk berinteraksi dengan masyarakat.
2. *Government to Bussiness* (G2B) adalah layanan yang digunakan pemerintah untuk berkomunikasi dengan pelaku bisnis.
3. *Government to Government* (G2G) adalah layanan yang memungkinkan komunikasi dan koordinasi antar badan pemerintahan.
4. *Government to Employees* (G2E) adalah layanan yang pemenrintah untuk meningkatkan kesejahteraan pegawai.

Model-model hubungan tersebut ditunjukan pada Gambar 2.1. Penerapan dan pengembangan *e-governement* menggunakan internet secara wajar akan menemui beberapa permaslahan. Permasalahan yang akan dihadapi oleh *e-government* antara lain pemotongan informasi, pengubahan informasi, penolakan layanan, pencurian sumber daya sistem, dan pemalsuan informasi yang dapat menimbulkan ancaman-ancaman terhadap *e-government* yang dapat dikelompokkan ke dalam 3 kelompok berdasarkan sumber ancamannya, yakni ancaman yang disengaja (intentional threats), tidak disengaja (unintentional threats) dan ancaman alam (natural threats) (Zhou dan Hu, 2008).



Gambar 2.1 Model Hubungan *E-Government* (Hardjaloka, 2014)

Penerapan *e-government* akan berdampak pada beberapa elemen antara lain teknologi, proses, sumberdaya manusia, organisasi, finansial, keamanan dan privasi (Ashaye dan Irani, 2014) yang dapat dilihat pada Tabel 2.1-1.

Tabel 2.1 Risiko Implementasi *E-Government* (Ashaye dan Irani, 2014)

Elemen	Risiko penerapan e-government
Teknologi	a. Akses informasi oleh badan lain b. Teknologi baru c. Resiko dari kegagalan d. Ketergantungan pada pihak pengelola teknis
Proses	a. Pengurangan kendali penuh atas informasi b. Rendahnya pelayanan c. Tidak stabilnya sumber daya
Sumber daya manusia	a. Pengurangan tenaga kerja b. Peningkatan pengangguran

Elemen	Risiko penerapan e-government
Organisasi	a. Penyalahgunaan layanan e-government b. Kritikan dari badan pemerintahan lain dan masyarakat
Finansial	a. Kurangnya pendanaan b. Keberlanjutan finansial
Keamanan dan privasi	a. Pencurian informasi

Elemen teknologi yang merupakan risiko penerepan *e-government* adalah satu tantangan besar yang harus dihadapi. Penerapan teknologi, terutama teknologi terbaru selalu menawarkan solusi-solusi yang lebih baik dan kemungkinan perubahan bisnis (Lau, 2003).

2.2 Keamanan Informasi

Keamanan informasi memiliki aspek yang perlu diperhatikan. Aspek keamanan informasi tersebut terdiri dari 3 unsur (Supradono, 2009), yaitu :

1 *Confidientiality*, maksudnya adalah informasi hanya bisa diakses oleh orang-orang yang berwenang.

2 *Integrity*, maksudnya adalah data tidak dapat diubah oleh pihak – pihak yang tidak berwenang

3 *Availability*, maksudnya adalah data atau informasi tersedia disaat dibutuhkan dan dapat digunakan oleh pihak yang berwenang.

Menjaga keamanan informasi berarti melakukan praktik-praktik keamanan dan manajemen keamanan pada level tertentu. Untuk melakukan manajemen tingkat keamanan, semua faktor yang terkait dengan pengoperasian sistem informasi harus dipertimbangkan (Kim dan Sakurai, 2008). Mempertimbangkan semua faktor dalam

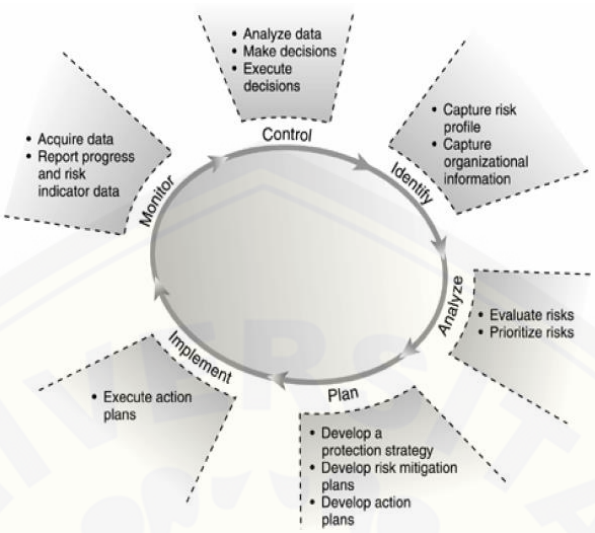
pengorperasian sebuah sistem informasi, memungkinkan menejer untuk melihat seluruh elemen yang digunakan dalam keamanan informasi, sehingga kemanan informasi dapat dikelola dengan baik.

Praktik keamanan informasi dapat diambil dari berbagai standart praktik atau praktik-praktik yang sudah ada. Praktik kemanan yang dipilih oleh sebuah organisasi bisa saja merupakan representasi dari praktik-praktik terbaik yang ada. Namun, praktik keamanan yang terbaik adalah praktik yang dinamis dan dapat dimodifikasi dengan mempertimbangkan lingkungan dan karakteristik dari sistem informasi (Kim dan Sakurai, 2008).

2.3 Manajemen Risiko

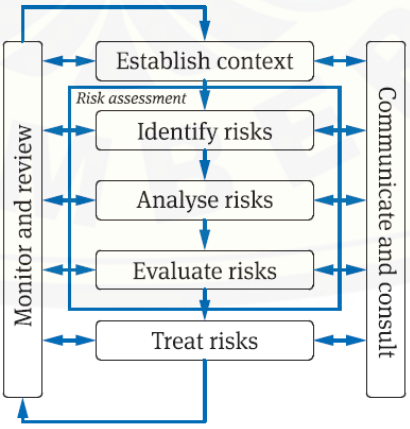
Risiko adalah kemungkinan akibat yang kurang menyenangkan yang dihasilkan dari suatu tindakan. *General Accounting Office* dalam (Supradono, 2009) memberikan gambaran mengenai langkah-langkah dalam manajemen resiko yang dapat dilihat pada Gambar 2.2. Langkah-langkah tersebut adalah:

1. *Identify*
   Mengidentifikasi resiko
2. *Analyze*
   Menganalisa resiko untuk menentukan prioritas resiko
3. *Plan*
   Merencanankan strategi perlindungan dalam penanggulangan resiko dan mitigasi resiko
4. *Implementation*
   Melaksanakan strategi terpilih dalam penanganan resiko
5. *Monitor*
   Pemantauan terhadap data dan proses penanganan resiko
6. *Control*
   Mengendalikan pelaksanaan, apakah sudah sesuai dengan membuat keputusan dan melaksankan keputusan



Gambar 2.2 Model Manajemen Risiko oleh G.A.O (Supradono, 2009)

Panduan lain dalam manajemen risiko adalah ISO 31000:2009. ISO 31000:2009 adalah panduan yang menyediakan prinsip-prinsip, *framework*, dan proses untuk manajemen risiko. Model manajemen risiko ini dikeluarkan oleh *International Organization for Standarization* (ISO). Manajemen risiko pada ISO 31000:2009 adalah sama untuk semua risiko terlepas dari sifat konsekuensinya (International Organization for Standarization, 2015). Manajemen risiko menurut ISO 31000:2009 ditunjukan pada Gambar 2.3.



Gambar 2.3 Model Manajemen Risiko ISO 31000:2009 (Rosyadi, 2013)

Secara garis besar model yang dikeluarkan oleh GAO dan ISO adalah sama, hanya pada model menejemn ISO terdapat proses komunikasi dan konsultasi disetiap proses kecuali pada proses monitor dan review.

Standart manajemen ISO 31000:2009 dalam (Rosyadi, 2013) menyebutkan bahwa terdapat 4 langkah yang dapat dilakukan dalam penanganan risiko, antara lain :

1. Hindari (*avoid*) adalah langkah yang dilakukan unutk menghindari risiko
2. Kurangi (*reduce*) adalah langkah yang dilakukan untuk mengurangi dampak risiko yang terjadi
3. Berbagi (*share*) adalah langkah yang dilakukan untuk membagi risiko dengan pihak ketiga.
4. Terima (*accept*) adalah tindakan menerima dampak risiko dengan tidak melakukan tindakan apapun untuk mempengaruhi dampak risiko.

Dalam peneilitian ini, peneliti menggunakan standart ISO 31000:2009 dalam proses pendekatan risiko (*risk approach*) yang terjadi.

2.4 Metode Octave –S

OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) adalah penilaian strategi berbasis resiko dan teknik perencanaan untuk keamanan (Alberts, dkk., 2005) Metode ini merupakan pendekatan terhadap evaluasi resiko yang komprehensif, sistematik, terarah dan dapat dilakukan sendiri (Supradono, 2009). Metode OCTAVE berfokus permasalahan strategi dan praktik keamanan yang terkait, sementara pada metode lain sebagian besar berfokus pada resiko dari teknologi dan permasalahan teknis.

Metode OCTAVE digunakan untuk orgainasasi yang lebih besar, OCTAVE –S digunakan untuk organisasi yang lebih (Alberts, dkk., 2003) .Pada dasarnya metode-metode ini memiliki hasil akhir yang sama, hanya saja OCTAVE –S adalah penyederhanaan dari metode OCTAVE original. Metode OCTAVE –S memiliki "*look and feel*" yang hampir sama dengan OCTAVE, namun hasil yang dicapai adalah sama.

Karakteristik unik yang menjadi ciri khas metode OCTAVE –S (Alberts, dkk., 2005) adalah :

1. Evaluasi ini dapat dilakukan sendiri (*self-directed evaluation*) dengan membentu tim yang telah menjadi bagian dari organisasi dan mengerti mengenai bisnis dan proses keamanan organisasi. Karena alasan ini OCTAVE –S tidak membutuhkan *data gathering workshop* secara formal untuk memulai evaluasi
2. OCTAVE –S hanya sedikit mengeksplorasi mengenai infrastruktur komputasi mengingat oragnisasi kecil biasanya bekerjasama dengan pihak ketiga untuk layanan TI yang dimiliki dan tidak begitu mengembangkan kemapuan organisasi untuk menjalankan dan mengimplementasikan hasil evaluasi dari perangkat evaluasi.

Metode OCTAVE memiliki 3 fase (Alberts, dkk., 2003).

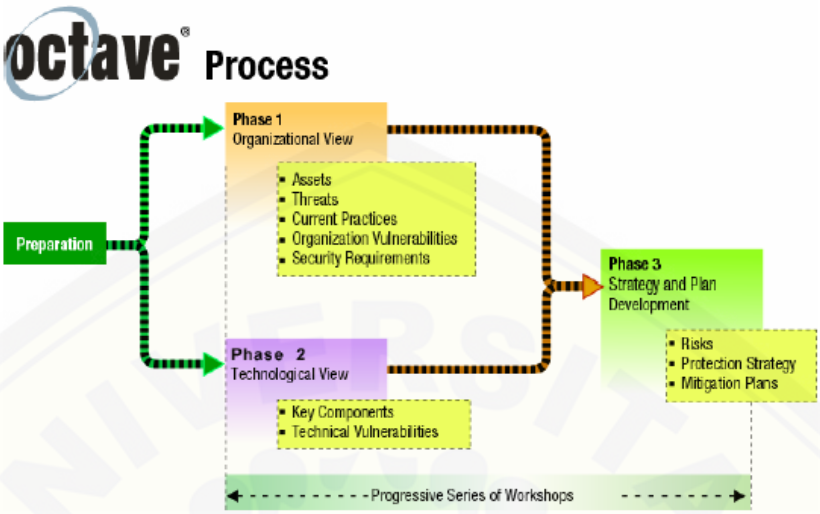
1. Fase1 : Membangun profil ancaman berdasrkan aset

   Tim analis akan menentukan aset-aset yang penting bagi perusahaan dan apasaja yang telah dilakukan untuk keamanan aset. Pada akhirnya tim akan mengidentifikasi ancaman untuk setiap aset dan membentuk prfil ancaman untuk aset tersebut.
2. Fase2 : Mengidentifikasi kelemahan infrastruktur

   Proses ini adalah proses evaluasi dari infrastruktur teknologi informasi. Tim analis akan mengidentifikasi setiap jalur akses dan komponen teknlogi yang terkait dengan aset penting.
3. Fase3 : Mengembangkan strategi dan rencana

   Pada fase ini tim analis akan mengidentifikasi resiko terhadap aset penting organisasi dan memutuskan apa yang harus dilakukan.

   Fase-fase evaluasi OCTAVE dapat dilihat pada Gambar 2.4.



Gambar 2.4 Fase-Fase Evaluasi OCTAVE (Alberts, dkk, 2003)

Sebelum melakukan analisa dengan menggunakan metode OCTAVE –S maka diperlukan tahapan persiapan, antara lain, memperoleh dukungan dari pimpinan organisasi, memilih tim analis, menentukan cakupan penilaian, perencanan, dan persiapan (Alberts, dkk., 2005). Pada Metode OCTAVE –S 3 fase dasar OCTAVE dikelompokkan lagi ke dalam 5 proses (Alberts, dkk., 2005).

1. Proses 1 : Mengidentifikasi informasi organisasi
2. Proses 2 : Membuat profil ancaman
3. Proses 3 : Memeriksa infrastruktur komputasi dalam hubungannya degan aset penting
4. Proses 4 : Mengidentifikasi dan analisa risiko
5. Proses 5 : Mengembangkan strategi perlindungan dan rencana mitigasi resiko.

Penelitian ini menggunakan metode OCTAVE –S untuk mengevaluasi resiko, karena evaluasi yang dilakukan hanya pada satu layanan sistem informasi dan layanan ini dikembangkan oleh pihak diluar pemerintah kabupaten Malang.

2.5 RACI *Chart*

RACI *chart* adalah sah satu bentuk matriks yang digunakan untuk menunjukkan peran dan tanggungjawab seseorang dalam sebuah pekerjaan. RACI sering juga disebut *Responsibility Assignmnet Matrix* (RAM). Bahkan untuk projek kecil, RACI *chart* / RAM dapat meningkatkan pemahaman setiap orang terhadap peran masing-masing partisipan dalam proyek (Nevision, 2013). RACI *chart* sebenarnya adalah tabel dengan dua dimensi, dimensi pertama adalah manusia yang menjadi partisipan dalam projek dan yang kedua adalah pekerjaan yang harus dikerjakan. Pembentukan RACI *chart* dapat dilihat pada Tabel 2.2. Isi dari tabel RACI sendiri adalah penilaian dengan nilai index sebagai berikut :

1. R (*Responsibile*) : adalah partisipan yang dianggap mampu melakukan pekerjaan dan mencapai hasil yang dituju
2. A (*Accountable*) : adalah partisipan yang mampu membawakan sebuah projek, atau suatu prosedur dengan tepat waktu, lebih jauh lagi partisipan ini akan menjadi penentu keputusan
3. C (*Consulted*) : partisipan yang dapat diajak berkonsultasi dan memberikan saran terhadap proyek yang dikerjakan
4. I (*Informed*) : partisipan yang perlu diberi informasi tentang jalannya proyek atau keputusan yang dibuat atau aktifitas yang dilakukan.

Tabel 2.2 RACI *Chart*

Partisipan / Aktivitas	Partisipan 1	Partisipan 2	Partisipan 3	Partisipan 4
Aktivitas 1	INDEX RACI			
Aktivitas 2				
Aktivitas 3				
Aktivitas 4				

Penelitian ini mengguanakan RACI *chart* untuk menentukan responden dengan kriteria-kriteria yang telah ditetapkan dalam penentuan responden dengan metode OCTAVE –S.

2.6 Kuantifikasi Risiko

Teknik kuantifikasi risiko adalah teknik yang digunakan untuk memberikan nilai berupa angka terhadap risiko yang terjadi. Analisi kuantitatif terhadap risiko menyertakan nilai bobot dari dampak risiko dan nilai kemungkinan dari beberapa sumber data (Deloitte dan LPP, 2012). Setelah risiko dinilai secara kualitatif dengan memberikan nilai dampak kualitatif (tinggi, sedang, rendah) maka tahap selanjutnya adalah memberikan nilai-nilai kuantitatif pada risiko untuk membarikan seberapa besar dampak risiko yang terjadi. Kuantifikasi risiko memiliki peran yang cukup signifikan dalam proses pengambilan keputusan (Zhao, 2007). Kuantifikasi risiko dapat dilakukan dengan menghitung nilai *risk eksposure* pada persamaan 1

$$\textit{Risk Eksposure} = \textit{Probability} \times \textit{Impact} \qquad \ldots\ldots (1)$$

BAB 3. METODOLOGI PENELITIAN

Bab ini menggambarkan tentang alur peneilitian yang digunakan sebagai panduan dalam proses pengerjaan tugas akhir agar tahap pengerjaan tugas akhir dapat berjalan terarah dan sistematis. Pada bab ini dijelaskan tentang jenis penelitian, tempat dan waktu pelaksanaan penelitan , teknik pengumpulan data dan alur pelaksanaan penelitian.

3.1 Jenis Penelitian

Jenis penelitian yang akan dilakukan adalah penelitian kualitatif dan kuantitatif. Penelitian kualitatif adalah penelitian yang bersifat deskriptif dan lebih cenderung menggunakan analisis. Penelitian kualitatif dilakukan pada saat melakukan wawancara terkait data yang dibutuhkan dan membentuk rekomendasi langkah-langkah pendekatan atau penanganan risiko yang muncul yang kemudian hasilnya ditunjang dengan penelitian kuantitatif dengan membentuk kuantifikasi risiko yang muncul.

3.2 Tempat dan Waktu Penelitian

Tempat dilaksanakannya penelitan adalah Dinas Komunikasi dan Informatika (DINKOMINFO) Kabupaten Malang. Pelaksanaan penelitian berlangsung selama dua bulan, dimulai bulan April 2017 sampai Mei 2017

3.3 Alat Penelitian

Alat yang digunakan dalam penelitian ini adalah OCTAVE *worksheet* dan laptop atau komputer dengan *software* sebagai berikut :

1. *Windows 8.1*
2. *Microsoft Office Word 2013*
3. *Microsoft Office Excel 2013*
4. *Adobe Acrobat Reader*
5. *XAMPP*

6. *NetBeans IDE*
7. *Mozilla Firefox*

3.4 Metode Tugas Akhir

Metode tugas akhir menjelaskan tahap-tahap peneliti dalam melaksanakan penelitian. Alur penelitian yang digunakan peneliti terdiri dari langkah-langkah pada Gambar 3.1.

Gambar 3.1 Alur Pelaksanaan Tugas Akhir

3.4.1 Tahap Analisa Awal

Tahap analisa awal merupakan tahapan awal dari rangkaian kegiatan penelitian ini. Pada tahap ini terdiri dari dua kegiatan, antara lain :

i. Identifikasi Permasalahan

Pada tahap ini akan dikaji permasalahan-permasalahan mengenai risiko keamanan informasi dan sebab-sebabnya yang timbul dalam penerepan layanan *Tele-Presence* sehingga tujuan utama yang diharapkan dari penelitian ini dapat tercapai. Permasalahan akan dirumuskan lebih terperinci, serta melakukan pengkajian tentang risiko keamanan sistem informasi sehingga permasalahan dapat didentifikasi dengan tepat. Selain itu, juga dilakukan penentuan narasumber terkait permasalahan dan dilakukan pemahaman mengenai tujuan layanan dan pentingnya manajemen risiko.

ii. Studi Literatur

Studi literatur yang dilakukan dalam penelitian ini adalah pengkajian terhadap teori-teori terkait permasalahan-permasalahan yang muncul, seperti keamanan informasi, manajemen risiko, analisis dan penanganan risiko keamanan informasi. Pengkajian dilakukan dengan pencarian bermacam literatur yang relevan dengan permasalahan dan variabel-variabel yang muncul dalam proses identifikasi permaslahan. Literatur yang digunakan bersumber dari buku, jurnal, tugas akhir baik yang berbentuk *hardcopy* maupun *softcopy*.

3.4.2 Pengumpulan Data dan Informasi

Tahap ini bertujuan untuk megumpulkan data yang dibutuhkan untuk melakukan penilaian (*assessment*) manajemen risiko pada layanan *tele-presence*. Data yang dibutuhkan adalah data primer dan data sekunder. Data primer yang dibutuhkan merupakan data-data terkait standart operasi, strategi keamanan, aset-aset yang digunakan dalam layanan *tele-presence* dan sebagainya. Data sekunder yang dibutuhkan merupakan data-data dari penggunaan layanan, seperti *record history* penggunaan layanan, jumlah pengguna, sisi finansial layanan, dan sebagaianya. Hasil pengumpulan data dituliskan dalam beberapa *worksheet* sesuai dengan metode OCTAVE –S. Untuk mendapatkan data-data yang dibutuhkan, maka pada tahap ini terdapat dua aktivitas, yaitu :

i. Survei

Survei dilakukan dengan meminta data dan mengamati data yang telah tercatat selama penggunaan layanan *Tele-Presence*.

ii. Wawancara

Wawancara dilakukan secara langsung kepada narasumber yang telah ditentukan menggunakan RACI *chart* seperti yang telah dijelaskan pada bab sebelumnya, dengan aktifitas pengambilan data pada daftar aktifitas seuai dengan metode OCTAVE –S, pada Tabel 3.1.

Tabel 3.1 Fase, Proses dan Aktifitas OCTAVE –S (Alberts, dkk., 2005)

Fase	Proses	Aktivitas
Fase 1 : Membangun profil ancaman berbasis aset	Proses 1 : Mengidentifikasi informasi organisasi	1. Membentuk evaluasi kriteria dampak
		2. Mengidentifikasi aset organisasi
		3. Mengevaluasi praktik keamanan organisasi
	Proses 2 : Membuat profil ancaman	4. Memilih aset kritis
		5. Mengidentifikasi kebutuhan keamanan untuk aset kritis
		6. Mengidentifikasi ancaman terhadap aset kritis
		7. Menganalisa teknologi terkait proses
Fase 2 : Mengidentifikasi kelemahan infrastruktur	Proses 3 : Memeriksa infrastruktur computer terkait aset kritis	8. Memeriksa jalur akses
		9. Menganalisa teknologi terkait proses

Fase	Proses	Aktivitas
Fase 3 : Mengembangkan rencana dan strategi keamanan	Proses 4 : Identifikasi dan analisa risiko	10. Mengevaluasi dampak dari ancaman
		11. Membentuk evaluasi kriteria kemungkinan
		12. Mengevaluasi kemungkinan ancaman
	Proses 5 : Mengembangkan strategi perlindungan dan rencana mitigasi	13. Mendiskripsikan strategi perlindungan saat ini
		14. Memilih pendekatan mitigasi risiko
		15. Mengembangkan rencana mitigasi risiko
		16. Mengientifikasi perubahan terhadap strategi perlindungan
		17. Identifikasi langkah selanjutnya

Data diperoleh dari angket dengan pertanyaan terbuka dan pertanyaan tertutup dengan memodifikasi poin-poin pertanyaan OCTAVE –S agar dapat mengadaptasi lingkungan organisasi dan karakteristik sistem informasi yang digunakan. Angket dengan pertanyaan terbuka ditunjukan pada Gambar 3.2.

Productivity			Productivity
Impact Type	**Low Impact**	**Medium Impact**	**High Impact**
Staff Hours	Staff work hours are increased by less than _____% for _____ to _____ day(s).	Staff work hours are increased between _____% and _____% for _____ to _____ day(s).	Staff work hours are increased by greater than _____% for _____ to _____ day(s).
Other:			
Other:			
Other:			

Gambar 3.2 Contoh Angket OCTAVE –S Pertanyaan Terbuka (Alberts, dkk., 2005)

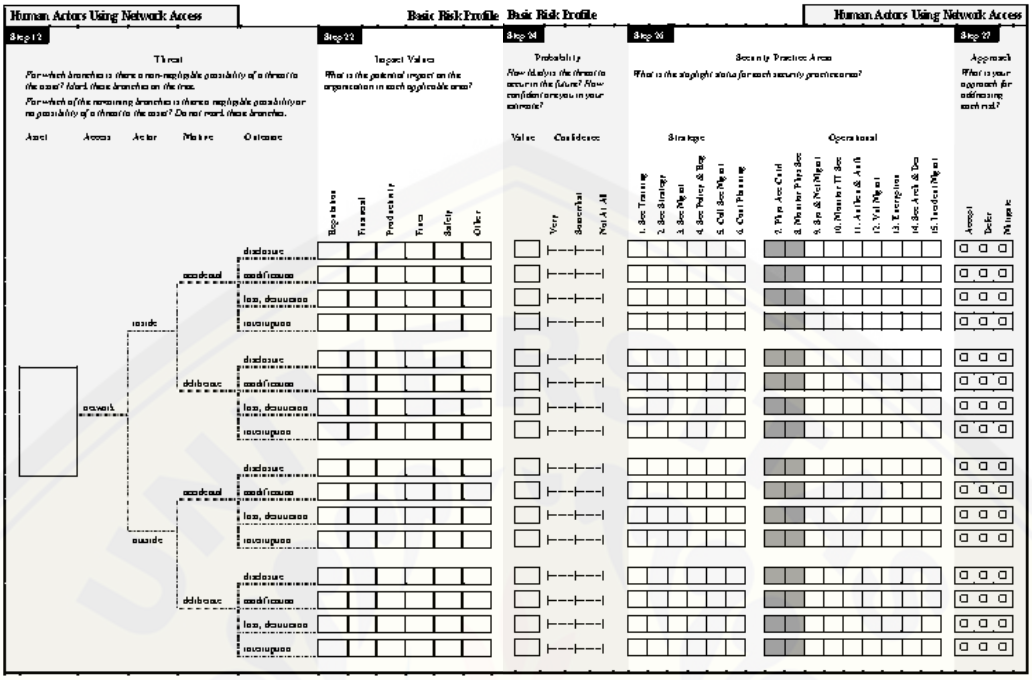
Contoh angket dengan pertanyaan tertutup ditunjukan pada Gambar 3.3. Hasil wawancara akan dirangkum dalam *worksheet* OCTAVE –S. Contoh *worksheet* OCTAVE –S untuk menyajikan informasi ditunjukan pada Gambar 3.4.

1. Security Awareness and Training

Step 3a

Statement	**To what extent is this statement reflected in your organization?**			
Staff members understand their security roles and responsibilities. This is documented and verified.	Very Much	Somewhat	Not At All	Don't Know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Very Much	Somewhat	Not At All	Don't Know
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Very Much	Somewhat	Not At All	Don't Know
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Very Much	Somewhat	Not At All	Don't Know

Gambar 3.3 Contoh Angket OCTAVE –S Pertanyaan Tertutup (Alberts, dkk., 2005)



Gambar 3.4 Contoh *Worksheet* OCTAVE –S Untuk Menyajikan Informasi (Alberts, dkk, 2005)

3.4.3 Identifikasi Risiko

Pada tahap ini dilakukan pengolahan data untuk mengidenfikasi risiko yang muncul dalam layana *tele-presence* menggunakan metode OCTAVE –S. Identifikasi risiko dilakukan terhadap aset kritis, aset- aset terkait aset kritis dan infrastruktur yang digunakan. Tahap ini dilakukan dengan menerapkan fase 1 dan fase 2 metode OCTAVE –S. Fase-fase tersebut adalah sebagai berikut :

i. Membangun Profil Ancaman Berdasarkan Aset

Fase pertama adalah membangun profil ancaman berdasarkan aset. Pada tahap ini peneliti akan mengevaluasi kriteria dampak yang nantinya akan digunakan dalam dalam mengevaluasi risiko. Pada tahap ini juga diidentifikasi aset-aset yang digunakan dan mengevaluasi praktik keamanan yang sedang diterapkan dalam organisasi. Data yang digunakan adalah hasil survei dan hasil wawancara pada aktifitas OCTAVE –S

nomor 1 sampai 7. Hasil identifikasi aset, risiko dan ancaman dituliskan dalam *worksheet* OCTAVE –S seperti yang telah dijelaskan sebelumnya.

ii. Mengidentifikasi Kerentanan Infrastruktur

Fase kedua adalah mengidentifikasi kerentanan ifrastruktur teknologi informasi. Pada tahap ini dilakukan analisa mengenai *class component*, infrasturktur dan jalur akses yang digunakan untuk mengakses data atau informasi pada aset kritis. Data yang digunakan adalah hasil survei dan hasil wawancara pada aktifitas OCTAVE –S nomor 8 dan 9. Hasil identifikasi *class component*, infrasturktur dan jalur akses dituliskan dalam *worksheet* OCTAVE –S seperti yang telah dijelaskan sebelumnya.

3.4.4 Penanganan Risiko

Tahap ini adalah tahap yang dilakukan untuk menanggulangi risiko yang telah dievaluasi pada tahap sebelumnya. Pendekatan risiko (*risk approach*) menggunakan pendekatan ISO 31000:2009 antara lain hindari (*avoid*), kurangi (*reduce*), berbagi (*share*), dan terima (*accept*). Untuk menangani risiko yang muncul, maka pada tahap ini terdapat dua aktifitas antara lain :

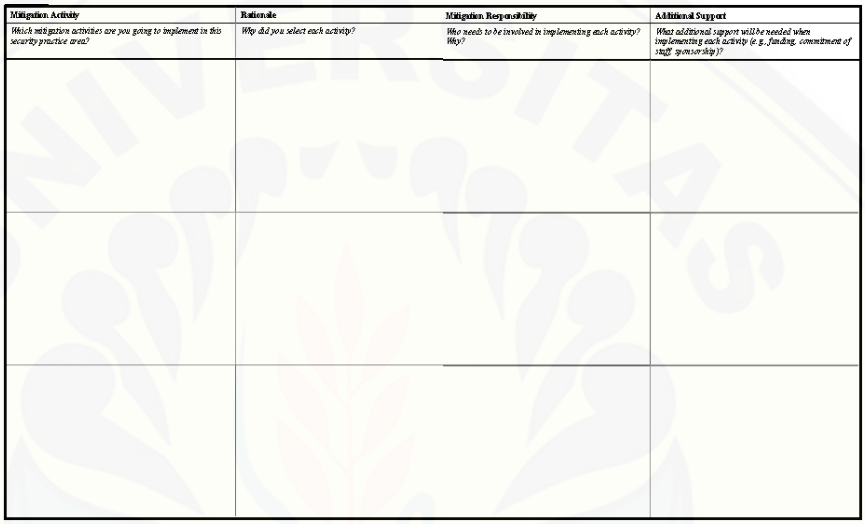
i. Kuantifikasi Risiko

Kuantifikasi risiko dilakukan dengan mengamati dan menganalisa data dampak risiko yang terjadi dan data kemungkinan risiko. Selanjutnya dilakukan pembobotan pada masing-masing data sehingga diperoleh nilai dampak dan nilai kemungkinan. Nilai dampak dan nilai kemungkinan diolah untuk memperoleh nilai *risk exposure* menggunakan persamaan 1.

ii. Mengembangkan Strategi Perlindungan

Aktifitas ini adalah penerapan fase 3 OCTAVE –S. Data yang digunakan adalah hasil survei dan hasil wawancara pada aktifitas OCTAVE –S nomor 13 sampai 17. Tujuan dari aktifitas ini adalah mengevaluasi strategi keamanan orgnisasi dan

membentuk perencanaan mitigasi risko. Evaluasi strategi keamanan berfokus pada perbaikan strategi yang dapat diterapkan oleh DINKOMINFO Kabupaten Malang. Perencanaan mitigasi risiko dilakukan dengan memodifikasi *worksheet* mitigasi risiko OCTAVE –S yang ditujukan pada Gambar 3.5, sesuai dengan kebutuhan Dinas Komunikasi dan Infromatika Kabupaten Malang.

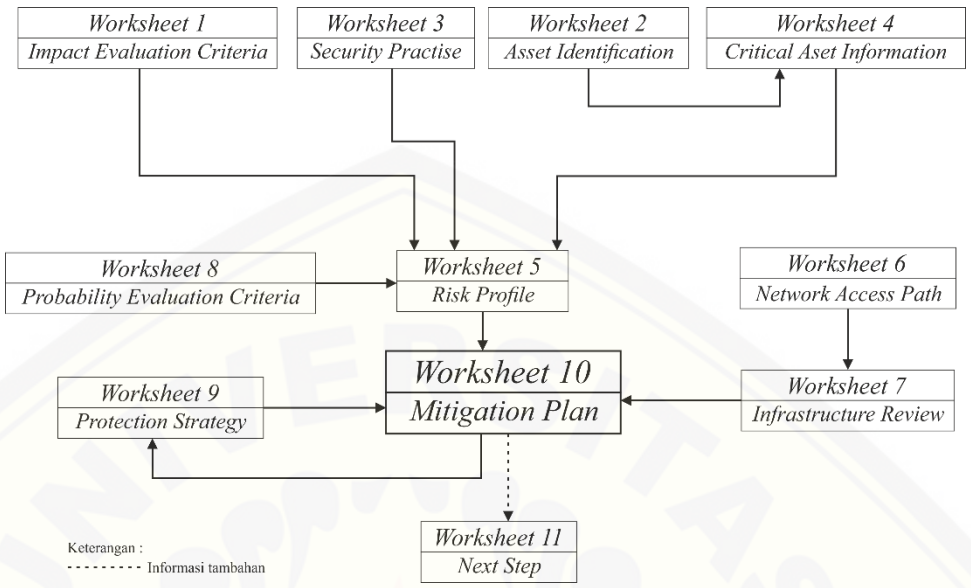


Mitigation Activity	Rationale	Mitigation Responsibility	Additional Support
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*	*Who needs to be involved in implementing each activity? Why?*	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Gambar 3.5 *Worksheet* Mitigasi Risiko OCTAVE –S (Alberts, dkk., 2005)

3.4.5 Pelaksanaan Mitigasi Risiko

Tahap ini adalah tahap penyusunan perencanaan mitigasi risiko. Penyusunan perencanaan mitigasi risiko dilakukan dengan melakukan peninjauan terhadap data yang telah terkumpul dalam *worksheet* metode OCTAVE –S untuk menghasilkan rekomendasi penanganan dari risiko atau ancaman yang muncul. Pada penelitian ini tidak semua *worksheet* OCTAVE –S digunakan. *Worksheet* yang digunakan adalah *worksheet* yang mendukung penelitian sesuai dengan batasan penelitian yang ditetapkan. Proses penyusunan mitigasi risiko menggunakan *worksheet* OCTAVE –S dalam penelitian ini ditunjukan dengan Gambar 3.6.



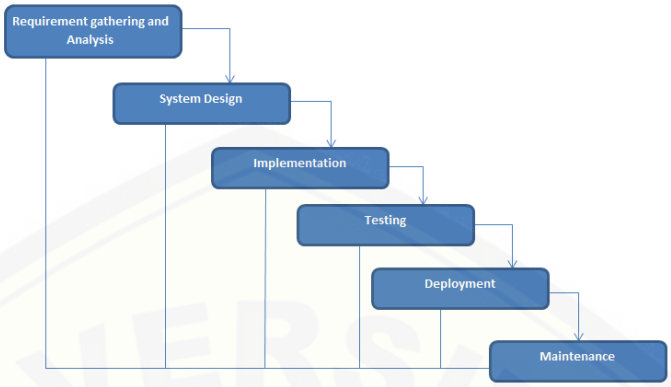
Gambar 3.6 Alur Penyusunan Perencanaan Mitigasi Risiko Menggunakan *Worksheet* OCTAVE –S

3.4.6 Penulisan Tugas Akhir

Tahap ini adalah tahapan terakhir dari penelitian. Semua proses yang telah dilakukan dari awal hingga akhir didokumnetasikan dan ditulis kedalam sebuah laporan dengan format tugas akhir.

3.4.7 Pembuatan Program

Pembuatan program difokuskan pada pembentukan nilai *risk* exposure. Nilai *risk exposure* terdiri tiga index, rendah, sedang dan tinggi. Ketiga index ini akan mengindikasikan seberapa besar dampak yang dapat diterima oleh organisasi terkait risiko yang muncul dalam penerapan layanan *Tele-Presence*. Program yang akan dibangun menggunakan basis desktop, dengan model MVC (*Model View Controller*) sebagai model pembangunan aplikasi. Aplikasi yang dibangun menggunakan *system development life cycle* model *waterfall*. Model *waterfall* ditunjukan dengan Gambar 3.6.



Gambar 3.7 Model SDLC *Waterfall* (Alshamrani dan Bahattab, 2015)

Model *waterfall* dipilih karena model ini adalah model yang dikenal luas dan mudah diimplementasikan (Alshamrani dan Bahattab, 2015). Model ini juga cocok untuk aplikasi yang jarang sekali terjadi perubahan alur program atau fitur, sehingga dapat menghasilkan aplikasi dengan mempertimbangkan kualitas dari aplikasi yang dibangun. Program yang telah dibuat akan diuji dengan pengujian *whitebox testing* dan *black box testing*. *White box testing* dilakukan untuk menguji kecocokan antara desain sistem dengan kode program yang ditulis, sedangkan *black box testing* dilakukan untuk menguji hasil akhir dari aplikasi yang dibangun.

BAB 4. ANALISIS RISIKO

Bab ini membahas analisa data tentang penerapan teknologi informasi baik secara umum yang ditinjau baik dari sisi strategi dan operasional dan secara khusus dalam layanan *Tele-Presence*. Peninjauan dan analisa data menggunakan tahapan proses dalam metode OCTAVE –S sebagai landasan. Data yang digunakan untuk anlisa adalah data hasil wawancara yang dituliskan dalam beberapa *worksheet*. Bab ini juga membahas perancangan sistem untuk menentukan nilai risiko (*Risk Exposure*) dengan menggunakan metode kuantifikasi risiko.

4.1 Deskripsi Dinas Komunikasi dan Informatika

Dinas Komunikasi dan Informatika (DINKOMINFO) Kabupaten Malang merupakan unsur pelaksana urusan pemerintahan bidang komunikasi dan informatika, bidang statistic, dan bidang persandian. Dinas ini dibentuk pada tahun 2016 dengan disahkannya Peraturan Bupati Malang Nomor 31 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Dinas Komunikasi dan Informatika. Dinas ini bertanggungjawab kepada Bupati melalui Sekretaris Dearah.

4.1.1 Tugas Dinas Komunikasi dan Informatika

Dinas Komunikasi dan Informatika Kabupaten Malang mempunyai tugas :

1. Melaksanakan urusan pemerintahan yang menjadi kewenangan Daerah dan tugas pembantuan bidang komunikasi dan informatika, bidang statistic, dan bidang persandian; dan
2. Melaksanakan tugas lain yang diberikan oleh Bupati sesuai dengan bidang tugasnya

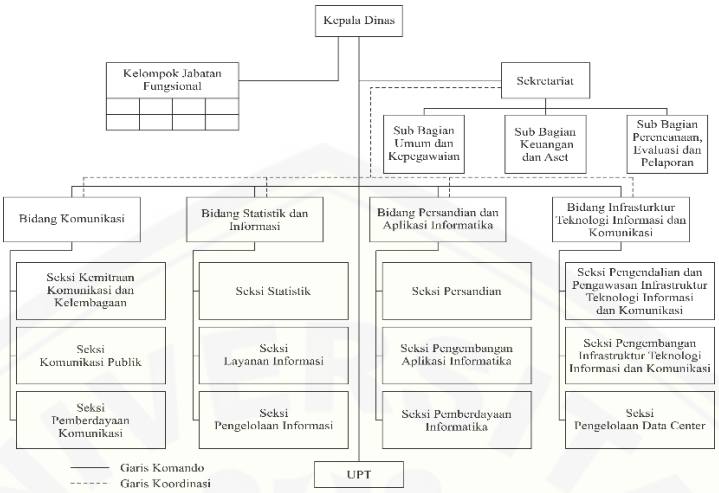
4.1.2 Fungsi Dinas Komunikasi dan Informatika

Dari tugas-tugas Dinas Komunikasi dan Informatika tersebut, maka dapat dijabarkan fungsi-fungsi Dinas Komunikasi dan Informatika antara lain :

1. Pengumpulan, pengelolaan, dan pengendalian data yang berbebtuk *database* serta analaisis data untuk penyusunan program kegiatan;
2. Perancangan strategi pada Dinas;
3. Perumusan kebijakan teknis bidang komunikasi dan informatika, bidang statistik, dan bidang persandian;
4. Penyelenggaraan urusan pemerintahan dan pelayanan umum bidang komunikasi dan informatika, bidang statistik, dan bidang persandian;
5. Pembinaan dan pelaksanaan tugas bidang komunikasi dan informatika, bidang statistik, dan bidang persandian;
6. Pelaksanaan, pengawasan, pengendalian serta evaluasi dan pelaporan penyelenggaraan bidang komunikasi dan informatika, bidang statistik, dan bidang persandian;
7. Pelaksanaan standar pelayanan minimal yang wajib dilaksanakan pada bidang komunikasi dan informatika, bidang statistik, dan bidang persandian;
8. Penyelenggaraan kesekretariatan Dinas;
9. Pembinaan UPT;
10. Pemberian rekomendasi perizinan dan pelaksanaan pelayanan bidang komunikasi dan informatika; dan
11. Pengoordinasian, integritas dan sinkronisasi kegiatan di lingkungan Dinas.

4.1.3 Susunan Organisasi

Dinas Komunikasi dan Informatika Kabupaten Malang memiliki struktur organisasi yang dapat dilihat pada Gambar 4.1.



Gambar 4.1 Struktur Organisasi Dinas Komunikasi dan Informatika (Peraturan Bupati Malang Nomor 31 Tahun 2016)

4.2 Metode Evaluasi

Metode yang digunakan untuk mengevaluasi dan menganalisa data yang didpatkan dalam penelitian ini adalah metode deskriptif. Data yang diperoleh dari hasil wawancara dan survei dievaluasi dan dituliskan dalam *worksheet* dengan metode OCTAVE –S seperti yang sudah dijelskan pada Bab 3. Proses dan aktifitas OCTAVE –S antara lain:

1. Mengidentifikasi informasi organisasi
2. Membuat profil ancaman
3. Memeriksa infrastruktur komputasi terkait aset kritis
4. Identifikasi dan anailisa risiko
5. Mengembangkan strategi perlindungan dan rencana mitigasi

4.2.1 Mengidentifikasi Informasi Organisasi

Proses analisa pada tahap ini difokuskan untuk membentuk kriteria-kriteria dampak yang digunakan dalam evaluasi, mengidentifikasi aset yang dimiliki oleh organisasi beserta praktik keamanan yang dilakukan untuk melindungi aset.

Dalam membetuk kriteria dampak dari enam area dampak yang ditetapkan dalam metode OCTAVE –S, hanya 3 area dampak yang dapat dianalisa atau dievaluasi. Hal ini terjadi karena beberapa area dampak belum sepenuhnya diterapkan atau belum memberikan dampak yang signifikan terhadap kondisi organisasi. Kriteria dampak yang telah dibentuk selanjutnya menjadi dasar penentuan dampak risiko pada tahapan selanjutnya. Kriteria dampak yang dievaluasi dalam penelitan ini antara lain :

1. Dampak reputasi (Tabel 4.1)
2. Dampak produktifitas (Tabel 4.2)
3. Dampak finansial (Tabel 4.3)

Tabel 4.1 Dampak Reputasi

Tipe Dampak	Kategori Dampak		
	Rendah	Sedang	Tinggi
Reputasi	Terdapat keluhan dari pengguna sistem, namun sistem masih bisa dierbaiki kurang dari 24 jam	Pengguna sistem berhenti menggunakan sistem untuk sementara waktu, namun sistem masih bisa diperbaiki	Sistem gagal berjalan dan berhenti digunakan, dibutuhkan install ulang untuk memperbaiki sistem
Kehilangan Pengguna	Departemen tertentu dalam satu dinas berhenti menggunakan	Dinas tertentu berhenti menggunakan	Semua pengguna terkait sistem berhenti menggunakan

Tabel 4.2 Dampak Produktivitas

Tipe Dampak	Kategori Dampak		
	Rendah	Sedang	Tinggi
Jam kerja	Jam kerja bertambah < 2 jam pada hari kerja	Jam kerja bertambah 2 – 5 jam pada hari kerja	Jam kerja bertambah >= 24 jam di luar hari kerja

Tabel 4.3 Dampak Finansial

Tipe Dampak	Kategori Dampak		
	Rendah	Sedang	Tinggi
Biaya Operasional	Rp. 1.000.000 sampai dengan Rp. 3.000.000	Rp. 3.000.000 sampai dengan Rp. 10.000.000	Biaya diatas Rp. 10.000.000
Kerugian Insidental	Rp. 500.000 sampai dengan Rp. 1.000.000	Rp. 1.000.000 sampai dengan Rp. 3.000.000	Rp. 3.000.000 sampai dengan Rp. 10.000.000
Implementasi sistem baru	Rp. 5.000.000 sampai dengan Rp. 50.000.000	Rp. 50.000.000 sampai dengan Rp. 200.000.000	Biaya diatas Rp. 200.000.000

Tipe Dampak	Kategori Dampak		
	Rendah	Sedang	Tinggi
Beban kerja kegiatan (terkait sistem / aplikasi)	Biaya dibawah Rp. 1.000.000.000	Rp. 1.000.000.000 sampai dengan Rp.15.000.000.000	Biaya diatas Rp.15.000.000.000

Tahap analisa selanjutnya untuk mengidentifikasi informasi organisasi adalah membentuk daftar aset yang dimiliki oleh organisasi. Aset yang teridentifikasi pada penelitian ini digolongkan kedalam 2 kriteria, yaitu lain aset sistem, informasi dan aplikasi, dan aset sumber daya manusia. Berdasarkan hasil wawancra teridentifikasi 4 aset organisasi yang berupa sistem, informasi dan aplikasi. Aset-aset tersebut antara lain :

1. SIRUP (Sistem Informasi Rencana Umum Pengadaan)
2. SIMDA (Sistem Informasi Administrasi Daerah)
3. Tele-Presence
4. MailTrack

Aset organisasi berupa sumber daya manusia (SDM) dibagi atas bidang atau departemen dalam organisasi dan perseorangan atau staff organisasi. Pemilihan staff yang menjadi aset kritis organisasi didasarkan pada pengalaman kerja dan sertifikasi yang dimiliki. Hasil analisa aset sumber daya manusia (SDM) menunjukkan dua bidang atau departemen dalam DINKOMINFO yaitu bidang persandian dan aplikasi informatika, dan bidang infrastruktur teknologi informasi dan komunikasi, yang menjadi inti dari pelaksanaan layanan yang menerapkan teknologi informasi (*e-government*), dan tiga staff teknologi informasi yang bekerja sebagai tenaga ahli, yang

mana ketiga staff tersebut tersebar dalam dua departemen yang menangani penerapan teknologi informasi.

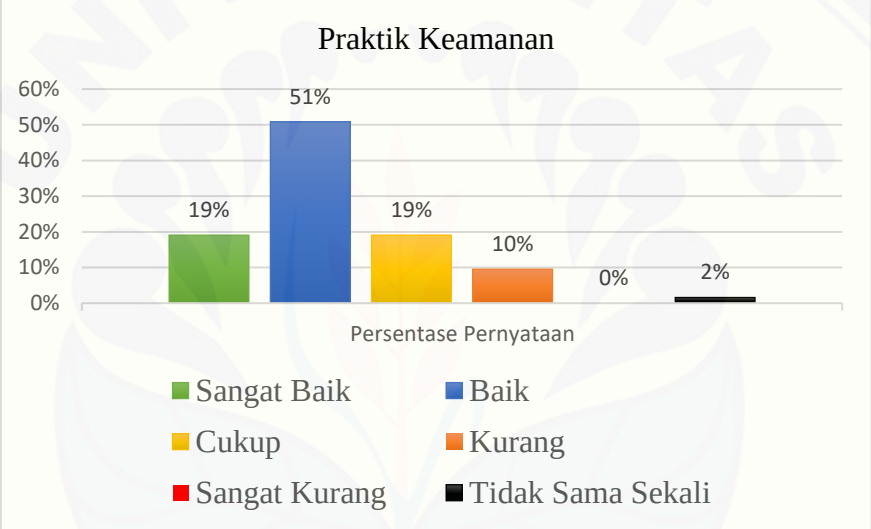
Tahap analisa data terakhir untuk mengidentifikasi informasi organisasi adalah evaluasi terhadap praktik keamanan organisasi dan status *stoplight* masing-masing bidang. Praktik keamanan organisasi terdiri dari lima belas bidang yang digolongkan kedalam 2 area yaitu area strategis dan area operasional yang dapat dilihat pada Tabel 4.4. Skala yang digunakan untuk merespon jawaban dalam evaluasi praktik keamanan adalah sangat baik (SB), baik (B), cukup (C), kurang (K), sangat kurang (SK), tidak sama sekali (TSS)

Tabel 4.4 Bidang Praktik Keamanan Organisasi

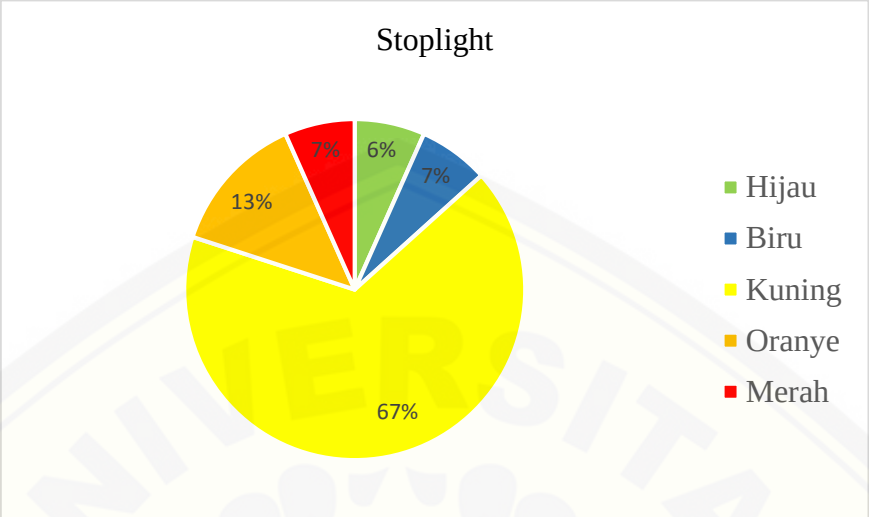
Area Strategis	Area Operasional
1. Kesadaran keamanan dan pelatihan 2. Strategi keamanan 3. Manajemen keamanan 4. Regulasi dan kebijakan keamanan 5. Kolaborasi manajemen keamanan 6. Perencanaan kemungkinan atau pemulihan bencana	7. Kendali akses fisik 8. Monitoring dan audit keamanan fisik 9. Manajemen sistem dan jaringan 10. Monitoring dan audit keamanan TI 11. Autentifikasi dan otoritasi 12. Manajemen kerentanan 13. Enkripsi 14. Arsitektur dan rancangan keamanan 15. Pengelolaan insiden

Skala *stoplight* yang digunakan untuk menggambarkan seberapa baik organisasi melakukan praktik keamanan adalah merah, oranye, kuning, biru dan hijau. Penyesuai atau perubahan skala dilakukan untuk mengadaptasi kebutuhan organisasi. Data dapat dilihat pada *Security Practise Worksheet* pada Lampiran 3. Berdasarkan hasil survei,

19% praktik keamanan masuk dalam kategori sangat baik, 51% praktik keamanan masuk dalam kategori baik, 19% praktik keamanan masuk dalam kategori cukup, 10% praktik keamanan masuk dalam kategori kurang, dan 2% praktik keamanan masuk dalam kategori tidak sama sekali. Persentase praktik kemanan ditunjukan pada Gambar 4.2. Status *stoplight* berdasarkan survei yaitu, 6% *stoplight* dalam kategori hijau, 7% *stoplight* dalam kategori biru, 67% *stoplight* dalam kategori kuning, 13% *stoplight* dalam kategori oranye, dan 7% *stoplight* dalam kategori merah . Persentsae status *stoplight* ditunjukan pada Gambar 4.3.



Gambar 4.2 Persentase Praktik Keamanan Organisasi



Gambar 4.3 Persentase Status *Stoplight*

Keterangan status *stoplight* sebagai berikut :

1. Merah mengindikasikan bahwa praktik keamanan tidak diaplikasikan
2. Oranye mengindikasikan perlu adanya perubahan besar dalam praktik keamanan
3. Kuning mengindikasikan perlu adanya perubahan yang wajar dalam praktik keamanan
4. Biru mengindikasikan perlu adanya perubahan kecil dalam praktik keamanan
5. Hijau mengindikasikan tidak perlu adanya perubahan dalam praktik keamanan

4.2.2 Membuat Profil Ancaman

Pada proses ini analisa data difokuskan untuk memilih aset kritis dari daftar aset yang telah teridentifikasi sebelumnya. Pada proses ini juga dilakukan analisa mengenai aset-aset terkait aset kritis, kebutuhan keamanan, dan ancaman terhadap aset kritis tersebut. Data yang diperoleh dituliskan dalam *Critical Asset Information Worksheet for System* pada Lampiran 4. Pada penelitian ini aset kritis yang dipilih dan menjadi pokok evaluasi adalah layanan atau sistem *Tele-Presence* sehingga aset kritis

ini menjadi batasan dalam penelitian. Aset terkait aset kritis terbagi kedalam tiga kategori antara lain :

1. Informasi

   Aset informasi adalah aset berupa data atau informasi yang tersimpan atau yang digunakan untuk menjalankan sistem

2. Aplikasi

   Aset aplikasi adalah aset berupa program yang dijalankan untuk mengoperasikan sistem.

3. Aset lain

   Aset lain adalah aset berupa perangkat pendukung seperti hardware dan jaringan untuk menjalankan sistem.

Kebutuhan keaman terhadap aset terkait dan aset kritis adalah:

1. *Confidentiality*

   Kerahasiaan informasi yang hanya bisa diakses oleh pihak tertentu

2. *Integrity*

   Keutuhan data atau informasi dimana hanya pihak tertentu yang memiliki akse untuk merubah atau menghapus data

3. *Availability*

   Kebutuhan akan ketersediaan sistem dan informasi didalamnya sehingga sistem atau informasi dapat digunakan saat dibutuhkan.

Ancaman aktif terhadap aset kritis dan aset terkait diidentifikasi dalam *Risk Profile Worksheet for System step* 12,13,14,15 dan 16 dalam metode OCTAVE -S. Dari seluruh cabang pohon ancaman yang dipaparkan dalam metode OCTAVE –S, hasil analisa menunjukkan terdapat 29 cabang yang menunjukkan ancaman aktif. Ancaman-ancaman aktif tersebut digolongkan kedalam 4 kategori antara lain :

1. *Human actor* akses jaringan (Tabel 4.5)
2. *Human actor* akses fisik (Tabel 4.6)
3. *System problem* (Tabel 4.7)
4. *Other problem* (Tabel 4.8)

Tabel 4.5 Ancaman Aktif *Tele-Presence Human Actor* Akses Jaringan

Nomor	Akses	Aktor	Motif	Hasil
1	Jaringan	Internal	Tidak disengaja	Terpapar
2	Jaringan	Internal	Tidak disengaja	Rusak
3	Jaringan	Internal	Tidak disengaja	Terganggu
4	Jaringan	Internal	Disengaja	Modifikasi
5	Jaringan	Internal	Disengaja	Rusak
6	Jaringan	Internal	Disengaja	Terganggu
7	Jaringan	Eksternal	Disengaja	Terpapar
8	Jaringan	Eksternal	Disengaja	Modifikasi
9	Jaringan	Eksternal	Disengaja	Rusak
10	Jaringan	Eksternal	Disengaja	Terganggu

Tabel 4.6Ancaman Aktif *Tele-Presence Human Actor* Akses Fisik.

Nomor	Akses	Aktor	Motif	Hasil
1	Akses fisik	Internal	Tidak disengaja	Terpapar
2	Akses fisik	Internal	Tidak disengaja	Modifikasi
3	Akses fisik	Internal	Tidak disengaja	Rusak
4	Akses fisik	Internal	Tidak disengaja	Terganggu
5	Akses fisik	Internal	Disengaja	Modifikasi
6	Akses fisik	Internal	Disengaja	Rusak
7	Akses fisik	Internal	Disengaja	Terganggu

Tabel 4.7Ancaman Aktif *Tele-Presence System Problem*.

Nomor	Akses	Aktor	Motif	Hasil
1	-	Kegagalan sistem	-	Terganggu

Nomor	Akses	Aktor	Motif	Hasil
2	-	Kecacatan hardware	-	Rusak
3	-	Kecacatan hardware	--	Terganggu
4	-	Kode berbahaya	-	Tepapar
5	-	Kode berbahaya	-	Modifikasi
6	-	Kode berbahaya	-	Rusak
7	-	Kode berbahaya	-	Terganggu

Tabel 4.8Ancaman Aktif *Tele-Presence Other Problem*

Nomor	Akses	Aktor	Motif	Hasil
1	-	Power supply	-	Terganggu
2	-	Telekomunikasi	-	Terganggu
3	-	Konfigurasi fisik	-	Modifikasi
4	-	Konfigurasi fisik	-	Rusak
5	-	Bencana alami	-	Rusak

Masing-masing ancaman aktif memiliki nilai dampak dan karakterisitk tersendiri. Hal ini menyebabkan perlu adanya pengukuran resiko secara kualitatif dengan melihat skenario ancaman untuk menghasilkan penanganan atau pendekatan terhadap risiko yang disesuaikan dengan karakter sistem dan karakter organisasi.

4.2.3 Memeriksa Infrastruktur Komputasi Terkait Aset Kritis

Proses in difokuskan untuk menganalisa infrastruktur dan jalur akses terkait aset kritis, kemudian analisa dilanjutkan untuk mengetahui proses-proses yang terkait dengan penggunaan infrastruktur. Hasil wawancara menujukkan tidak semua kategori yang dipaparkan dalam metode OCTAVE –S digunakan dalam sebagai jalur akses ke aset kritis. Kategori jalur akses yang digunakan dalam sistem *Tele-Presence* antara lain *system of interest*, *intermediate access point*, dan *system access by people*. Data tentang

jalur akses yang digunakan secara detail dapat dilihat dalam *Network Access Path Worksheet* pada Lampiran 6. Analisa proses terkait teknologi yang berhubungan dengan penggunaan aset kritis menghasilkan identifikasi kelas komponen, penanggungjawab, evaluasi perlindungan dan catatan terkait dari kategori jalur akses aktif. Data tentang proses terkait dituliskan dalam *Infrastructure Review Worksheet* pada Lampiran 7 .

4.2.4 Identifikasi dan Analisa Risiko

Proses ini difokuskan untuk menganalisa kemungkinan dan dampak risiko yang ditimbulkan dari setiap cabang risiko yang telah teridentifikasi pada proses sebelumnya. Nilai kemungkinan dibentuk dengan melihat sejarah kejadian kemudian menarik garis batas untuk membentuk kategori rendah, sedang dan tinggi. Frekuensi kejadian yang digunakan dalam analisa kemungkinan adalah frekuensi kejadian selama enam bulan, sehingga frekuensi tahunan yang ditetapkan dalam proses ini adalah satu tahun. Data kriteria kemungkinan secara detail terdapat dalam *Probability Evaluation Criteria Worksheet* pada Lampiran 8.

Analisa dampak risiko dilakukan dengan menetapkan nilai masing-masing area dampak yang telah teridentifikasi pada tahap sebelumnya. Nilai dampak didefinisikan secara kualitatif. Identifikasi dan analisa risiko menghasilkan nilai masing-masing area dampak dan nilai kemungkinan pada 29 ancaman aktif yang telah teridentifikasi pada tahap sebelumnya. Hasil identifikasi dan analisa risiko adalah sebagai berikut:

1. Analisa risiko *human actor* akses jaringan (Tabel 4.9)
2. Analisa risiko *human actor* akses fisik (Tabel 4.10)
3. Analisa risiko *system problem* (Tabel 4.11)
4. Analisa risiko *other problem* (Tabel 4.12)

Tabel 4.9 Analisa Risiko *Human Actor* Akses Jaringan

Nomor	Akses	Aktor	Motif	Hasil	Nilai Dampak			Nilai Kemungkinan
					Reputasi	Finansial	Produktifitas	
1	Jaringan	Internal	Tidak disengaja	Terpapar	R	R	R	R
2	Jaringan	Internal	Tidak disengaja	Rusak	S	R	S	R
3	Jaringan	Internal	Tidak disengaja	Terganggu	S	R	R	R
4	Jaringan	Internal	Disengaja	Modifikasi	S	R	S	R
5	Jaringan	Internal	Disengaja	Rusak	T	S	T	R
6	Jaringan	Internal	Disengaja	Terganggu	S	R	R	S
7	Jaringan	Eksternal	Disengaja	Terpapar	S	R	S	R
8	Jaringan	Eksternal	Disengaja	Modifikasi	T	S	S	S
9	Jaringan	Eksternal	Disengaja	Rusak	T	S	T	S
10	Jaringan	Eksternal	Disengaja	Terganggu	T	S	S	S

Tabel 4.10 Analisis Risiko *Human Actor* akses fisik

Nomor	Akses	Aktor	Motif	Hasil	Nilai Dampak			Nilai Kemungkinan
					Reputasi	Finansial	Produktifitas	
1	Akses fisik	Internal	Tidak disengaja	Terpapar	R	R	R	R

Nomor	Akses	Aktor	Motif	Hasil	Nilai Dampak			Nilai Kemungkinan
					Reputasi	Finansial	Produktifitas	
2	Akses fisik	Internal	Tidak disengaja	Modifikasi	S	R	R	R
3	Akses fisik	Internal	Tidak disengaja	Rusak	S	S	S	R
4	Akses fisik	Internal	Tidak disengaja	Terganggu	S	R	R	R
5	Akses fisik	Internal	Disengaja	Modifikasi	S	S	S	S
6	Akses fisik	Internal	Disengaja	Rusak	T	S	T	R
7	Akses fisik	Internal	Disengaja	Terganggu	R	R	S	S

Tabel 4.11 Analisi Risiko *System Problem*

Nomor	Akses	Aktor	Motif	Hasil	Nilai Dampak			Nilai Kemungkinan
					Reputasi	Finansial	Produktifitas	
1	-	Kegagalan sistem	-	Terganggu	S	R	S	S
2	-	Kecacatan hardware	-	Rusak	T	S	T	R
3	-	Kecacatan hardware	--	Terganggu	R	R	S	S
4	-	Kode berbahaya	-	Tepapar	S	R	S	S

Nomor	Akses	Aktor	Motif	Hasil	Nilai Dampak			Nilai Kemungkinan
					Reputasi	Finansial	Produktifitas	
5	-	Kode berbahaya	-	Modifikasi	T	S	S	S
6	-	Kode berbahaya	-	Rusak	T	S	T	S
7	-	Kode berbahaya	-	Terganggu	T	S	S	S

Tabel 4.12 Analisis Risiko *Other Problem*

Nomor	Akses	Aktor	Motif	Hasil	Nilai Dampak			Nilai Kemungkinan
					Reputasi	Finansial	Produktifitas	
1	-	Power supply	-	Terganggu	S	R	R	S
2	-	Telekomunikasi	-	Terganggu	S	R	R	S
3	-	Konfigurasi fisik	-	Modifikasi	S	R	S	R
4	-	Konfigurasi fisik	-	Rusak	T	S	T	R
5	-	Bencana alami	-	Rusak	T	T	T	R

4.2.5 Mengembangkan Strategi Perlindungan dan Rencana Mitigasi

Proses difokuskan pada strategi dan praktik perlindungan, perencanaan mitigasi risiko dan langkah selanjutnya dalam implemetasi metode OCTAVE –S. Analisa dilakukan untuk mengetahui penerapan dan formalitas strategi perlindungan yang diterapkan dan bagaimana praktik perlindungan yang dilakukan. Langkah selanjutnya dalam implementasi metode OCTAVE –S mendefinisikan kebutuhan lain dalam

mengimplementasikan hasil evaluasi dan merencanakan evaluasi OCTAVE –S periode selanjutnya.

Berdasarkan hasil wawancara, tidak seluruhnya mekanisme atau strategi perlindungan yang diterapkan dalam organisasi adalah strategi yang sepenuhnya formal atau terdokumentasi dengan baik. Strategi perlindungan saat ini masih terbagi kedalam empat kategori antara lain :

1. Formal atau terdokumentasi

   Kategori ini mendefinisikan strategi perlindungan pada suatu bidang yang telah secara penuh berjalan secara formal dan terdokumentasikan

2. Sebagian formal.

   Kategori ini mendefinisikan strategi perlindungan pada suatu bidang dimana beberapa strategi telah berjalan secara formal dan terdokumentasikan

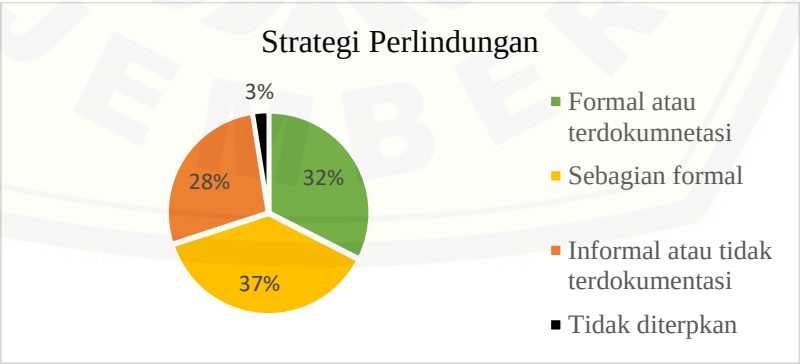
3. Informal atau tidak terdokumentasikan

   Katogeri ini mendefinisikan strategi perlindungan pada suatu bidang yang berjalan secara informal dan belum atau tidak terdokumnetasikan.

4. Tidak diterapkan

   Kategori ini mendefinisikan strategi perlindungan yang belum atau tidak diterpakan.

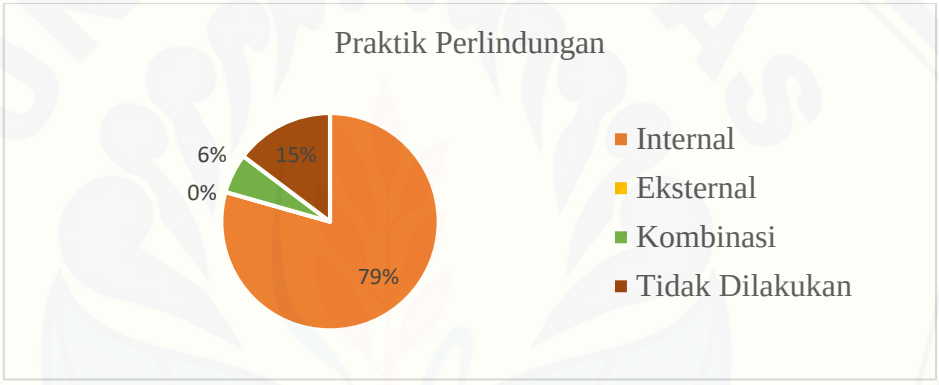
Perbandingan persentase jumlah strategi yang diterapkan dalam organisasi ditunjukan pada Gambar 4.4.



Gambar 4.4 Persentase Strategi Perlindungan

Dari 15 (lima belas) bidang praktik keamanan yang telah dipaparkan pada pembahasan sebelumnya, tidak seluruhnya membahas praktik perlindungan yang dapat dilakukan oleh organisasi. Praktik perlindungan hanya terdapat pada bidang praktik keamanan yang tergolong kedalam area operasional. Pelaksanaan praktik perlindungan dikelompokan menjadi internal, eksternal, kombinasi, dan tidak dilakukan. Sebagian besar praktik perlindungan ini dilakukan oleh internal dan tidak ada praktik perlindungan yang sepenuhnya diserahkan pada pihak eksternal. Persentase praktik perlindungan yang dilakukan organisasi ditunjukan pada Gambar 4.5

.



Gambar 4.5 Persentase Praktik Perlindungan

Data strategi dan praktik perlindungan selengkapnya dapat dilihat pada *Protection Strategy Worksheet* Lampiran 9. Langkah selanjutnya dalam mengimplementasikan hasil evaluasi OCTAVE –S adalah rekomendasi implementasi hasil evaluasi OCTAVE –S tentang kebutuhan-kebutuhan implementasi yang meliputi dukungan pihak menejemen, pengawasan implemtasi, pengembangan evaluasi dan rekomendasi waktu pelaksanaan evaluasi OCTAVE –S selanjutnya (dapat dilihat pada *Next Step Worksheet* Lampiran 11)

4.3 Kuantifikasi Risiko

Kuantifikasi risiko dilakukan dengan menghitung nilai *risk exposure*. Data yang dibutuhkan untuk proses ini adalah data kuantifiakasi nilai dampak dan kuantifikasi nilai kemungkinan. Data kuantifikasi adalah hasil analisa dan kuantifikasi pada *Impact Evaluation Criteria Worksheet* dan *Probablitiy Evaluation Worksheet.* Nilai *risk exposure* yang dihasilkan adalah nilai masing-masing dampak risiko dari ancaman aktif.

BAB 6. PENUTUP

Bab ini berisi simpulan mengenai hasil pengukuran dan mitigasi risiko keamanan informasi yang telah dilakukan, dilengkapi dengan saran penelitian untuk mengembangkan penelitian pengukuran dan mitigasi risiko selanjutnya.

6.1 Simpulan

Kesimpulan yang dapat diambil dalam penelitian ini adalah sebagai berikut :

1. Aset-aset yang berperan dalam layanan *Tele-Presence* antara lain:
   a. Aset informasi yaitu data jadwal konferensi, data dokumen konferensi, data peserta konferensi, dan data user.
   b. Aset aplikasi yaitu aplikasi Vmeet, aplikasi *database*, dan sistem operasi.
   c. Aset lain yaitu server, *personal computer* (PC), jasa *internet provider*, *web camera*, *headphone*, dan *microphone*.
2. Sebesar 19% praktik keamanan yang dilakukan organisasi masuk dalam kategori sangat baik, 51% praktik keamanan masuk dalam kategori baik, 19% masuk dalam kategori cukup, dan 10% praktik keamanan masuk dalam kategori kurang.
3. Identifikasi risiko yang dilakukan menggunakan metode OCTAVE –S menghasilkan 29 cabang ancaman aktif.
4. Pendekatan atau mitigasi risiko dilakukan dengan menerapkan salah satu dar 4 (empat) langkah pendekatan risiko menurut ISO 31000:2009, yang disesuaikan dengan kebutuhan Dinas Komunikasi dan Informatika. Pendekatan risiko adalah sebagai berikut :
   a. Langkah penghidaran dampak risiko dilakukan pada 11 cabang ancaman aktif .
   b. Langkah pengurangan dampak risiko dilakukan pada 12 cabang ancaman aktif.

c. Langkah pembagian damapk risiko dilakukan pada 5 cabang ancaman aktif.
d. Langkah penerimaan dampak risiko dilakukan pada 1 cabang ancaman aktif.

5. Nilai *risk exposure* tertinggi dari risiko yang muncul pada ancaman dikelompokan berdasarkan area dampak adalah sebagai berikut :
   a. Nilai *risk exposure* tertinggi pada dampak reputasi muncul pada 6 cabang ancaman aktif.
   b. Nilai *risk exposure* tertinggi pada dampak finansial muncul pada 7 cabang ancaman aktif.
   c. Nilai *risk exposure* tertinggi pada dampak produktifitas muncul pada 2 cabang ancaman aktif.
6. Berdasarkan nilai tertinggi kuantifikasi risiko pada setiap area dampak, maka dapat disimpulkan bahwa ancaman tertinggi yang saat ini dihadapi adalah tindakan pihak luar (eksternal) yang memasukkan kode-kode berbahaya melalui jaringan dengan tujuan merusak sistem.

6.2 Saran

Saran yang yang dapat disampaikan penulis guna mengembangkan pengukuran risiko penerapan teknologi informasi di pemerintah Kabupaten Malang dengan menggunakan metode OCTAVE –S pada penelitian selanjutnya adalah sebagai berikut:

1. Aset kritis yang dievaluasi tidak hanya aset kritis berupa sistem, melainkan aset kritis kategori lain sesuai dengan metode OCTAVE –S.
2. Pengukuran dampak risiko dapat dilakukan menggunakan metode *multi-risk assessment* untuk mengetahui dampak risiko dari satu cabang ancaman aktif.

DAFTAR PUSTAKA

Alberts, C., Dorofee, A., Steven, J., dan Woody, C. (2005). *OCTAVE -S Implementation Guide, Version 1.0.* Pittsburgh: Carnigie Mellon.

Alberts, C., Dorofee, A., Stevens, J., dan Woody, C. (2003). *Introduction to the OCTAVE Approach.* Pittsburgh: Carnegie Mellon University.

Alshamrani, A., dan Bahattab, A. (2015). A Comparison Between Three SDLC Models Waterfall Model, Spiral Model, and Incremental/Iterative Model. *International Journal of Computer Science Issues*, 1-6.

Ashaye, O. dan Irani, Z. (2014). E-government Implementation Benefits, Risks, and Barriers in Developing Countries: Evidence From Nigeria. *David Publishing*, 13-25.

Deloitte, dan LPP, T. (2012). *Risk Assessment In Practise.* Durham: The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Hardjaloka, L. (2014). Studi Penerapan E-Governmnet di Indonesia dan Negara Lainnya Sebagai Solusi Pemberantasan Korupsi di Sektor Publik. *Rechts Vinding*, 1-18.

Information System Audit and Control Association. (2016). *State of Cybersecurity.* Illinois: Information System Audit and Control Association.

International Organization for Standarization. (2015). *ISO 31000: Risk management – A practical guide for SMEs.* Geneva: International Organization for Standarization.

Kementrian Komunikasi dan Informatika RI. (2016, 1 11). *Tabel Hasil PeGI*. Retrieved from Pemeringkatan e-Government Indonesia (PeGI): http://pegi.layanan.go.id/tabel-hasil-pegi-4/

Kim, T.-H., dan Sakurai, K. (2008). Definition of Security Practices in Security Management Part of Security Level Management Model. *International Journal of Security and Its Applications*, 1-9.

Lau, E. (2003). Challenges For E-Government Development. *5th GLOBAL FORUM ON REINVENTING GOVERNMENT*, 1-18.

Nevision, J. M. (2013). The Responsibility Assignment Matrix (RAM). *New Leaf Project Management*, 1-5.

Pratomo, S. H. (2010). *Analisisi Risiko TI Menggunakan Metode OCTAVE Pada PT. Bank Hana*. Jakarta: Universitas Bina Nusantara.

Rosyadi, M. B. (2013). *Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi Menggunakan Metode OCTAVE di Institut Teknologi Sepuluh Nopember*. Surabaya: Institut Teknologi Sepuluh Nopember.

Supradono, B. (2009). Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). *Media Elektrika*, 4-8.

United Nation. (2016). *United Nation E-Government Survey 2016*. New York: United Nation.

Zhao, G. J. (2007). Significance of Risk Quantification. *RISK Conference*, (pp. 1-11). Palisade.

Zhou, Z., dan Hu, C. (2008). Study on the E-government Security Risk Management. *International Journal of Computer Science and Network Security*, 208-2013.

LAMPIRAN 1

IMPACT EVALUATION CRITERIA WORKSHEET

Catatan	Step
	1
Area dampak yang terdapat dalam panduan metode OCTAVE –S yang meliputi: 1. Reputasi 2. Kesehatan 3. Finansial 4. Produktifitas 5. Denda dan hukum yang berlaku 6. Dampak lain Tidak semua ditemukan dalam observasi di DINKOMINFO kab.Malang. Hal ini terjadi karena beberapa faktor seperti : 1. Usia organisasi (DINKOMINFO) yang masih sangat muda sehingga beberapa area dampak masih belum terdefinisikan dengan baik 2. Area dampak tidak memberikan dampak yang signifikan terhadap organisasi 3. Area dampak yang telah ada dan ditetapkan namun masih belum berlaku Area dampak yang terdapat di DINKOMINFO dan dapat digunakan untuk analisis selanjutnya meliputi : 1. Reputasi 2. Finansial 3. Produktifitas	

DAMPAK REPUTASI

Step 1

Tipe Dampak	Kategori Dampak		
	Rendah	Sedang	Tinggi
Reputasi	Terdapat keluhan dari pengguna sistem, namun sistem masih bisa dierbaiki kurang dari 24 jam	Pengguna sistem berhenti menggunakan sistem untuk sementara waktu, namun sistem masih bisa diperbaiki	Sistem gagal berjalan dan berhenti digunakan, dibutuhkan install ulang untuk memperbaiki sistem
Kehilangan Pengguna	Departemen tertentu dalam satu dinas berhenti menggunakan	Dinas tertentu berhenti menggunakan	Semua pengguna terkait sistem berhenti menggunakan

DAMPAK FINANSIAL

Step 1

Tipe Dampak	Kategori Dampak		
	Rendah	Sedang	Tinggi
Biaya Operasional	Rp. 1.000.000 sampai dengan Rp. 3.000.000	Rp. 3.000.000 sampai dengan Rp. 10.000.000	Biaya diatas Rp. 10.000.000

Kerugian Insidental	Rp. 500.000 sampai dengan Rp. 1.000.000	Rp. 1.000.000 sampai dengan Rp. 3.000.000	Rp. 3.000.000 sampai dengan Rp. 10.000.000
Implementasi sistem baru	Rp. 5.000.000 sampai dengan Rp. 50.000.000	Rp. 50.000.000 sampai dengan Rp. 200.000.000	Biaya diatas Rp. 200.000.000
Beban kerja kegiatan (terkait sistem / aplikasi)	Biaya dibawah Rp. 1.000.000.000	Rp. 1.000.000.000 sampai dengan Rp.15.000.000.000	Biaya diatas Rp.15.000.000.000

DAMPAK PRODUKTIFITAS

Step 1

Tipe Dampak	Kategori Dampak		
	Rendah	Sedang	Tinggi
Jam kerja	Jam kerja bertambah < 2 jam pada hari kerja	Jam kerja bertambah 2 – 5 jam pada hari kerja	Jam kerja bertambah >= 24 jam di luar hari kerja

LAMPIRAN 2

ASSET INDENTIFICATION WORKSHEET

Catatan	Step
	2
Sistem dan aplikasi dalam dunia pemerintahan sering dipandang sebagai satu item, dengan kata lain dalam dunia pemerintahan pemahaman sistem dan aplikasi masih belum sempurna. Beberapa sistem yang sekarang dimiliki / ada pada DINKOMINFO sebenarnya adalah "turunan" dari PDE (Pusat Data Elektronik) Kabupaten Malang Sistem yang sedang ditangani oleh DINKOMINFO saat ini sebenarnya adalah sistem milik pusat pemerintahan Sebagian besar SDM (Sumber Daya Manusia) yang memiliki gelar sarjana computer bekerja pada bidang persandian dan infrastruktur Bidang infrastruktur memiliki lebih banyak SDM bergelar sarjana komputer	

ASET SISTEM, INFORMASI DAN APLIKASI

Step 2

Sistem	Informasi	Aplikasi	Aset Lain
SIRUP (Sistem Informasi Rencana Umum Pengadaan)	Data rencana kegiatan	Aplikasi web SIRUP	1. Layanan internet 2. PC 3. Oracle database

SIMDA (Sistem Informasi Administrasi Daerah)	Data Anggaran Dana pengadaan / kegiatan	SIMDA Aplikasi desktop	1. PC 2. Microsoft Access
Tele-Presence (Sistem Koordinasi)	Data jadwal pertemuan Data pengguna Data file pertemuan	V Meet	1. Layanan internet 2. PC
MailTrack (Sistem persuratan)	Data surat masuk Data surat keluar	Aplikasi website	1. Layanan Internet 2. PC 3. Oracle database

ASET SUMBER DAYA MANUSIA

Step 2

SDM	Keahlian dan Pengetahuan	Sistem Terkait	Aset Lain
Bid. Persandian dan Aplikasi Informatika	1. Pengembangan aplikasi 2. Pelatihan terkait sistem	1. SIMDA 2. Tele – Presence	

Bid. Infrastruktur Teknologi Informasi dan Komunikasi	1. Menejemen penggunaan aplikasi dan sistem 2. Menejemen jaringan 3. Perbaikan jaringan	1. Solar Win 2. Aplikasi monitoring jaringan	
Pak Achmad Zabidi	Tenaga berpengalaman dalam jaringan dan infrastruktur TI		
Pak Linden	Tenaga berpengalaman dalam jaringan dan infrastruktur TI		
Pak Tri Darmawan	Tenaga berpengalman yang memahami secara garis besar jalannya layanan TI		

LAMPIRAN 3

SECURITY PRACTISE WORKSHEET

Catatan	Step
	3a
Skala OCTAVE –S yang digunakan untuk menggambarkan seberapa baik organisasi melakukan praktik keamanan tidak digunakan karena kurang menggambarkan kondisi organisasi saat ini. Skala yang digunakan sebagai skala pengganti adalah skala *Likert* dengan respon jawaban ; sangat baik (SB), baik (B), cukup (C), kurang (K), sangat kurang (SK), tidak sama sekali (TSS)	

Catatan	Step
	4
Skala *stoplight* dirubah menjadi 5 skala karena menyesuaikan dengan keadaan organisasi, skala *stoplight* tersebut adalah; 1. Merah mengindikasikan bahwa praktik keamanan tidak diaplikasikan 2. Oranye mengindikasikan perlu adanya perubahan besar dalam praktik keamanan 3. Kuning mengindikasikan perlu adanya perubahan yang wajar dalam praktik keamanan 4. Biru mengindikasikan perlu adanya perubahan kecil dalam praktik keamanan 5. Hijau mengindikasikan tidak perlu adanya perubahan dalam praktik keamanan	

1. BIDANG KESADARAN KEAMANAN DAN PELATIHAN

Step 3a

Pernyataan	**Sejauh mana pernyataan tersebut tercermin dalam organisasi**					
Staff mengerti peran keamanan dan tanggungjawab mereka. Hal ini terdokumentasi dan terferifikasi.	SB	B	C	K	SK	TSS
Ada tenaga ahli untuk semua layanan mekanisme dan teknologi (misal:monitoring,enkripsi) termasuk operasi aman mereka. Hal ini terdomentasi dan terferifikasi	SB	B	C	K	SK	TSS
Pelatihan, kesadaran keamanan dan pengingatan secara periodik tersedia untuk semua staff. Tingkat pemahaman staff terdokumentasikan dan secara periodik ditinjau.	SB	B	C	K	SK	TSS
Staff mengikuti praktik keamanan yang baik meliputi : a. Mengamankan informasi dimana mereka bertanggung jawab b. Tidak membocorkan informasi c. Memliki kemampuan yang memadai untuk	SB	B	C	K	SK	TSS

menggunakan teknologi (hardware & software) d. Menggunakan praktik password e. Mengerti dan mengikuti kebijakan keamanan f. Mengenali dan melaporkan insiden						

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Penilaian (*assessment*) kemanan informasi diadakan setiap tahunnya dengan menggunakan nilai index KAMI 2. Beberapa tenaga ahli telah memiliki sertifikasi dalam bidang TI 3. Pelatihan selalu diadakan setiap ada pelucuran aplikasi dan sistem baru	1. Staff masih berbagi username dan password 2. Staff sering lupa dengan username dan passwordnya 3. Peserta pelatihan terkait aplikasi atau sistem baru masih sering tidak tepat sasaran, hal ini terjadi karena adanya disposisi perwakilan peserta.

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

2. BIDANG STRATEGI KEAMANAN

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Strategi organisasi secara rutin memasukkan pertimbangan keamanan	SB	B	C	K	SK	TSS
Strategi keamanan dan kebijakan dimasukkan kedalam pertimbangan tujuan dan target organisasi	SB	B	C	K	SK	TSS
Strategi keamanan, tujuan dan target pencapaian terdokmentasi dan secara rutin ditinjuan, diperbaharui dan dikomnikasikan kepada organisasi	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Strategi keamanan yang diterapkan telah mencakup keamanan untuk hardware dan software dan database 2. Strategi keamanan telah didokumentasikan 3. Peninjauan terhadap dokumentasi strategi keamanan	1. Respon *stakeholder* terhadap strategi keamanan masih kurang 2. Ego-sektoral yang masih cukup tinggi menghambat jalannya pelaksanaan strategi keamanan dan kebijakan informasi

dilakukan secara rutin setiap tahun 4. Kebijakan terkait strategi keamanan selalu didukung oleh pemerintah	

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

3. BIDANG MENEJEMEN KEAMANAN

Step 3a

Pernyataan	**Sejauh mana pernyataan tersebut tercermin dalam organisasi**					
Menejer mengalokasikan dana yang memadai untuk aktifitas keamanan informasi	SB	B	C	K	SK	TSS
Peran keamanan dan tanggungjawab terdefinisikan untuk semua staff dalam organisasi	SB	B	C	K	SK	TSS
Seluruh staff pada semua level mengimplementasikan peran dan tanggungjawabnya untuk keamanan informasi	SB	B	C	K	SK	TSS

Perekrutan dan pemberhentian staff mempertimbangkan masalah keamanan informasi	SB	B	C	K	SK	TSS
Organisasi mengelola risiko keamanan informasi termasuk : a. Penilaian risiko terhadap keamanan informasi b. Melakukan langkah untuk memitigasi risiko keamanan informasi	SB	B	C	K	SK	TSS
Menejer menerima dan bertindak atas laporan rutin, merangkum informasi yang berhubungan dengan keamanan	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	**Hah-hal yang tidak dilakukan dengan baik dalam bidang ini**
1. Sebagian staff telah diberi tanggungjawab pada masing-masing level jabatan 2. Menejer telah mengetahui dan mempertimbangkan keamanan informasi	1. Menejemen keamanan belum dicantumkan dalam SOTK 2. Tugas dan tanggungjawab dalam menjaga keamanan informasi masih belum didokumentasikan dan dilegalkan 3. Anggaran untuk menejemen keamanan dalam rangka

	mencapai standart ISO masih minim

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

4. BIDANG REGULASI DAN KEBIJAKAN KEAMANAN

Step 3a

Pernyataan	**Sejauh mana pernyataan tersebut tercermin dalam organisasi**					
Organisasi memiliki satu set kebijakan (yang berlaku) yang didokumentasikan, dan secara periodik ditinjau dan diperbaharui	SB	B	C	K	SK	TSS
Terdapat proses-proses yang terdokumentasi untuk pengelolaan kebijakan keamanan, termasuk : a. Pembentukan	SB	B	C	K	SK	TSS

b. Administrasi (termasuk peninjauan dan pembaharuan periodik) c. komunikasi						
Organisasi memiliki proses yang terdokumentasi untuk evaluasi dan memastikan kepatuhan terhadap kebijakan keamanan informasi dan hukum yang berlaku	SB	B	C	K	SK	TSS
Perekrutan dan pemberhentian staff mempertimbangkan masalah keamanan informasi	SB	B	C	K	SK	TSS
Organisasi secara seragam memberlakukan kebijakan keamanan	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	**Hah-hal yang tidak dilakukan dengan baik dalam bidang ini**
1. SOP untuk pembuatan kebijakan hingga SOP untuk langkah-langkah pelaksanaan kebijakan telah dibuat. 2. Kebijakan keamanan telah ditetapkan untuk semua level menejemen dalam organisasi	1. Masih terdapat perbedaan pendapat mengenai regulasi dan kebijakan mana yang berlaku, disatu sisi jika tidak ada perubahan maka regulasi (SK lama) masih berlaku, disisi lain regulasi harus diperbaharui dan dilegalkan

	2. SOP sudah disusun atua masih dalam proses penyusunan dan legalisasi 3. Regulasi dan kebijakan keamanan baru bisa berjalan secara penuh pada bidang persandian & aplikasi dan bidang infrastruktur TI

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

5. BIDANG KOLABORASI MENEJEMEN KEAMANAN

Step 3a

Pernyataan	**Sejauh mana pernyataan tersebut tercermin dalam organisasi**					
Organisasi memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerjasama dengan organisasi lain termasuk : a. Melindungi informasi milik organisasi lain b. Mengerti kebijakan dan prosedur keamanan dari organisasi lain	SB	B	C	K	SK	TSS

c. Mengakhiri akses ke informasi dengan memutus anggota eksternal						
Organisasi mendokumentasikan kebutuhan perlindungan informasi dan secara jelas mengkomunikasikannya dengan pihak ketiga yang bersangkutan	SB	B	C	K	SK	TSS
Organisasi memiliki mekanisne resmi untuk memferifikasi semua organisasi pihak ketiga, layanan keamanan yang diambil dari luar, mekanisme dan teknologi sesuai keperluan dan kebutuhan	SB	B	C	K	SK	TSS
Organisasi memiliki kebijakan dan prosedur untuk bekerja sama dengan pihak ketiga yang : a. Menyediakan pelatihan dan kesadaran keamanan b. Mengembangkan kebijakan keamanan untuk organisasi c. Mengembangkan rencana-rencana kemungkinan untuk organisasi	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Semua bentuk kerjasama dengan pihak ketiga telah memiliki prosedur sendiri (SOP) dan telah berjalan dengan lancar	

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

6. PERENCANAAN KEMUNGKINAN / PEMULIHAN BENCANA

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Analisa dari operasi, aplikasi data-data kritis telah dilakukan	SB	B	C	K	SK	TSS
Organisasi memiliki hal-hal yang terdokumantasi, telah ditinjau, dan teruji meliputi : a. Keberlanjutan bisnis dan rencana operasi darurat b. Rencana pemulihan dari bencana	SB	B	C	K	SK	TSS

c. Kemungkinan rencana untuk merespon keadaan darurat						
Rencana kemungkinan, pemulihan bencana, keberlanjutan bisnis, mempertimbangkan kebutuhan akses fisik dan elektronik dan kendali	SB	B	C	K	SK	TSS
Semua staff : a. Waspada terhadap kemungkinan-kemungkinan, pemulihan bencana, dan rencana bisnis berkelanjutan b. Mengerti dan mampu tanggungjawab masing-masing	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	**Hah-hal yang tidak dilakukan dengan baik dalam bidang ini**
1. Staff ahli untuk pemulihan bencana telah ditentukan.	2. Terjadi *overlapping* pekerjaan, maksudnya adalah pengambil alihan pekerjaan dalam kegiatan pemulihan bencana. Hal ini terjadi karena kurang tingginya kesadaran dan pemahaman pimpinan.

	3. Kebijakan pemulihan bencana tidak berjalan dengan baik dan bercabang 4. Pelaksanaan aktifitas pemulihan bencana masih tergantung pada otoritas pimpinan

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

7. KENDALI AKSES FISIK

Step 3a

Pernyataan	**Sejauh mana pernyataan tersebut tercermin dalam organisasi**					
Staff dari organisasi bertanggungjawab dalam area ini						
Rencana fasilitas keamanan dan prosedur untuk melindungi tempat, bangunan, dan semua area terlarang terdokumentasi dan teruji	SB	B	C	K	SK	TSS
Terdapat prosedur dan kebijakan yang terdokumentasi untuk mengelola pengunjung	SB	B	C	K	SK	TSS

Terdapat prosedur dan kebijakan yang terdokumentasi untuk mengendalikan akses fisik pada area kerja meliputi hardware dan software	SB	B	C	K	SK	TSS
Area kerja dan komponen lain yang memungkinkan akses ke informasi sensitif secara fisik dijaga untuk mencegah akses yang tidak sah	SB	B	C	K	SK	TSS
Staff dari organisasi pihak ketiga bertanggungjawab pada area ini						
Kebutuhan organisasi untuk kendali akses fisik secara formal dikomunikasikan pada semua kontraktor dan penyedia layanan yang mengendalikan akses fisik ke bangunan dan tempat, area kerja, hardware dan software	SB	B	C	K	SK	TSS
Organisasi secara resmi memverifikasi bahwa semua kontraktor dan penyedia layanan telah memenuhi standart untuk kendali akses fisik	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Penyediaan akses fisik telah sesuai dengan tugas pokok dan fungsi masing - masing departemen	1. Larangan untuk akses fisik tidak dipatuhi 2. Penggunaan hardware terkadang masih belum sesuai dengan otoritas 3. Pelaksanaan untuk kendali akses fisik masih saling berebut, hal ini terjadi karena merasa paling butuh

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

8. BIDANG MONITORING DAN AUDIT KEAMANAN FISIK

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Staff dari organisasi bertanggungjawab dalam area ini						
Record perawatan disimpan untuk mendokumentasikan perbaikan dan	SB	B	C	K	SK	TSS

modifikasi dari komponen fisik fasilitas						
Tindakan perseorangan atau kelompok dengan mempertimbangkan media yang dikendalikan secara fisik, dapat dipertanggungjawabkan	SB	B	C	K	SK	TSS
Record audit dan monitoring secara rutin diperiksa untuk mencari kejanggalan dan aksi pembetulan dilakukan sesuai keperluan	SB	B	C	K	SK	TSS
Staff dari organisasi pihak ketiga bertanggungjawab pada area ini						
Kebutuhan organisasi untuk monitoring keamanan fisik secara formal dikomunikasikan pada semua kontraktor dan penyedia layanan yang mengendalikan akses fisik ke bangunan dan tempat, area kerja, hardware dan software	SB	B	C	K	SK	TSS
Organisasi secara resmi memverifikasi bahwa semua kontraktor dan penyedia layanan telah memenuhi standart untuk memonitoring keamanan fisik	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Semua perbaikan hardware dan akses fisik tercatat dan telah diperiksa	1. Pihak ketiga yang merupakan kerjasama antar dinas terkadang masih bekerja sesuka hati 2. Perbedaan presepi mengenai audit dan monitoring sering terjadi

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

9. BIDANG MENEJEMEN SISTEM DAN JARINGAN

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Staff dari organisasi bertanggungjawab dalam area ini						
Terdapat rencana keamanan yang terdokumentasi dan teruji untuk menjaga sistem dan jaringan	SB	B	C	K	SK	TSS

Informasi sensitif dilindungi dengan penyimpanan yang aman (misal : backup offline)	SB	B	C	K	SK	TSS
Integritas dari software yang terinstal secara teratur diverifikasi	SB	B	C	K	SK	TSS
Semua sistem up-to-date dengan revisi dan rekomendasi dalam saran-saran keamanan	SB	B	C	K	SK	TSS
Terdapat rencana pencadangan data yang terdokumentasi dan teruji untuk mencadangakan baik sistem maupun data. Semua staff paham tanggungjawabnya dalam rencana ini	SB	B	C	K	SK	TSS
Perubahan terhadap hardware dan software TI telah terencana, terkendali, dan terdokumentasi	SB	B	C	K	SK	TSS
Staff TI mengikuti prosedur berikut ketika mengeluarkan, merubah dan mengeksekusi password dan akun pengguna : a. Identifikasi unik untuk user diperlukan untuk semua sistem, termasuk user dari pihak ketiga b. Akun dan password default telah diahapuskan dari sistem	SB	B	C	K	SK	TSS

Hanya layanan yang diperlukan yang berjalan dalam sistem, layanan yang tidak diperlukan telah dihapuskan dari sistem	SB	B	C	K	SK	TSS
Alat dan mekanisme untuk keamanan sistem dan administrasi jaringan telah digunakan, dan secara rutin ditinjau, diperbaharui, atau dihapuskan	SB	B	C	K	SK	TSS
Staff dari organisasi pihak ketiga bertanggungjawab pada area ini						
Kebutuhan organisasi untuk keamanan yang terkait dengan sistem dan pengelolaan jaringan secara formal dikomunikasikan pada semua kontraktor dan penyedia layanan yang menjaga sistem dan jaringan	SB	B	C	K	SK	TSS
Organisasi secara resmi memverifikasi bahwa semua kontraktor dan penyedia layanan telah memenuhi standart untuk untuk keamanan yang terkait dengan sistem dan pengelolaan jaringan	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Backup sistem telah dilakukan untuk melidungi informasi sensitive 2. Fitur – fitur yang tidak relevan dalam suatu sistem tidak langsung begitu saja dibuang, tetapi dianalisa kembali dan dikembangkan menjadi subsistem sendiri	1. Integritas sistem kacau 2. Sering adanya "jalan pintas" dalam aplikasi dan jaringan, yang tidak sesuai dengan prosedur 3. Backup terkadang masih tidak terjadwal

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

10. BIDANG MONITORING DAN AUDIT KEAMANAN TI

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Staff dari organisasi bertanggungjawab dalam area ini						
Perangkat auditing dan monitoring sistem dan jaringan secara rutin digunakan oleh organisasi.	SB	B	C	K	SK	TSS

Aktifitas tidak normal ditangani dengan kebijakan dan prosedur yang sesuai						
Firewall dan komponen keamanan yang lain secara periodik diaudit untuk pemenuhan kebijakan keamanan	SB	B	C	K	SK	TSS
Staff dari organisasi pihak ketiga bertanggungjawab pada area ini						
Kebutuhan organisasi untuk monitoring keamanan TI secara formal dikomunikasikan pada semua kontraktor dan penyedia layanan yang memonitor sistem dan jaringan	SB	B	C	K	SK	TSS
Organisasi secara resmi memverifikasi bahwa semua kontraktor dan penyedia layanan telah memenuhi standart untuk monitoring keamanan TI	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Penggunaan perangkat untuk audit TI telah sesuai dengan standart yaitu dengan menggunakan index KAMI 2. Pemilahan permasalahan teknis yang terjadi sudah sangat baik sehingga kategori permaslahan internal dan external sudah jelas	1. Perbaikan yang ditangani oleh pihak ketiga cukup memakan waktu

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

11. BIDANG AUTENTIFIKASI DAN OTORITASI

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Staff dari organisasi bertanggungjawab dalam area ini						
Kendali akses dan autentifikasi user (misal : konfigurasi jaringan, perijinan akses file) yang konsisten	SB	B	C	K	SK	TSS

dengan kebijakan digunakan membatasi akses pengguna ke informasi, sistem yang sensitif, aplikasi dan layanan tertentu, dan koneksi jaringan						
Terdapat kebijakan dan prosedur yang terdokumentasi untuk membuat dan mengakhiri akses ke informasi untuk perseorangan maupun kelompok	SB	B	C	K	SK	TSS
Metode atau mekanisme disediakan untuk memastikan bahwa informasi sensitif tidak pernah diakses, diubah atau dihancurkan oleh pihak tidak berwenang. Metode dan mekanisme secara periodik ditinjau dan diverifikasi	SB	B	C	K	SK	TSS
Staff dari organisasi pihak ketiga bertanggungjawab pada area ini						
Kebutuhan organisasi pengendalian akses ke sistem dan informasi secara formal dikomunikasikan pada semua kontraktor dan penyedia layanan yang menyediakan layanan autentifikasi dan otoritasi	SB	B	C	K	SK	TSS
Organisasi secara resmi memverifikasi bahwa semua	SB	B	C	K	SK	TSS

kontraktor dan penyedia layanan telah memenuhi standart untuk autentifikasi dan otoritasi						

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Beberapa aplikasi telah mengikuti prosedur pengamanan yang umum	1. Autentifikasi perlu ditegaskan lagi 2. Pemahaman otoritas masih kurang

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

12. BIDANG MENEJEMEN KERENTANAN

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Staff dari organisasi bertanggungjawab dalam area ini						
Terdapat satu set prosedur yang terdokumentasi untuk mengelola kerentan termasuk :	SB	B	C	K	SK	TSS

a. Memilih alat evaluasi kerentanan b. Tetap up-to-date dengan tipe kerentanan yang telah diketahui dan metode serangan c. Peninjauan sumber dari informasi pada pengumuman kerentanan, peringatan keamanan, dan notifikasi d. Mengidentifikasi komponen infrastruktur untuk dievaluasi e. Menterjemahkan dan menanggapi hasil f. Menjaga penyimpanan yang aman dan disposisi data rawan						
Prosedur menejemen kerentanan diikuti dan secara periodik ditinjau dan diperbaharui	SB	B	C	K	SK	TSS
Penilaian kerentanan teknologi dilakukan secara periodik, dan kerentanan ditangani ketika teridentifikasi	SB	B	C	K	SK	TSS
Staff dari organisasi pihak ketiga bertanggungjawab pada area ini						

Kebutuhan organisasi untuk pengelolaan kerentanan secara formal dikomunikasikan pada semua kontraktor dan penyedia layanan yang mengelola kerentanan teknologi	SB	B	C	K	SK	TSS
Organisasi secara resmi memverifikasi bahwa semua kontraktor dan penyedia layanan telah memenuhi standart untuk pengelolaan kerentanan	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	**Hah-hal yang tidak dilakukan dengan baik dalam bidang ini**
1. Dokumentasi telah lengkap mengenai menejemen	1. Pelaksanaan dengan pihak ketiga butuh pengawasan dari pihak internal 2. Kekurangan dalam hal ini berasal dari vendor (pihak ketiga) yag tidak kompeten 3. Beberapa sistem yang belum layak dipaksakan berjalan, sehingga kerentanan pada sistem lebih besar

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

13. BIDANG ENKRIPSI

Step 3a

Pernyataan	**Sejauh mana pernyataan tersebut tercermin dalam organisasi**					
Staff dari organisasi bertanggungjawab dalam area ini						
Kendali keamanan yang sesuai digunakan untuk melindungi informasi senstif selama dalam penyimpanan dan selama masa transmisi (misal : enkripsi data, infrastruktur public key)	SB	B	C	K	SK	TSS
Protokol enkripsi diguanakan dalam mengelola sistem, router, dan firewall	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Praktik enkripsi sudah pernah diterapkan 2. Permasalahan mengenai enkripsi tidak pernah diserahkan kepada pihak ketiga	1. Kondisi yang dulu terlindungi enkripsi sekarang beberapa terlepas dari perlindungan enkripsi 2. Kebijakan yang masih kurang mengenai enkripsi 3. Banyak sistem atau aplikasi masih banyak yang belum dienkripsi

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

14. BIDANG ARSITEKTUR DAN RANCANGAN KEAMANAN

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Staff dari organisasi bertanggungjawab dalam area ini						
Rancangan dan arsitektur sistem untuk sistem baru atau revisi mempertimbangkan :	SB	B	C	K	SK	TSS

a. Strategi keamanan, kebijkan dan prosedur b. Sejarah kerusakan (compromises) c. Hasil dari pengukuran risiko						
Organisasi memiliki diagram up-to-date yang menunjukkan arsitektur dan topologi jaringan keamanan organisasi secara keseluruhan	SB	B	C	K	SK	TSS
Staff dari organisasi pihak ketiga bertanggungjawab pada area ini						
Kebutuhan organisasi terkait keamanan secara formal dikomunikasikan pada semua kontraktor dan penyedia layanan yang menyediakan rancangan sistem dan topologi	SB	B	C	K	SK	TSS
Organisasi secara resmi memverifikasi bahwa semua kontraktor dan penyedia layanan telah memenuhi standart untuk rancangan dan arsitektur keamanan	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
1. Arsitektur sistem selalu direvisi atau ditinjau 2. Jaringan selalu diawasi	1. Tidak semua pihak ketiga yang terlibat dalam bidang arsitektur terikat oleh kontrak

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

15. BIDANG PENGELOLAAN INSIDEN

Step 3a

Pernyataan	Sejauh mana pernyataan tersebut tercermin dalam organisasi					
Staff dari organisasi bertanggungjawab dalam area ini						
Prosedur terdokumentasi tersedia untuk mengidentifikasi, melaporkan, dan menanggapi insiden dan pelanggaran keamanan yang dicurigai	SB	B	C	K	SK	TSS

Prosedur pengelolaan insiden secara periodik diuji, diverifikasi, dan diperbaharui	SB	B	C	K	SK	TSS
Terdapat prosedur dan kebijakan yang terdokumentasi untuk bekerja dengan pihak-pihak penegak hukum	SB	B	C	K	SK	TSS
Staff dari organisasi pihak ketiga bertanggungjawab pada area ini						
Kebutuhan organisasi untuk mengelola insiden secara formal dikomunikasikan pada semua kontraktor dan penyedia layanan yang menyediakan layanan pengelolaan insiden	SB	B	C	K	SK	TSS
Organisasi secara resmi memverifikasi bahwa semua kontraktor dan penyedia layanan telah memenuhi standart untuk mengelola insiden	SB	B	C	K	SK	TSS

Step 3b

Hal-hal yang dilakukan secara baik dalam bidang ini	Hah-hal yang tidak dilakukan dengan baik dalam bidang ini
	1. Laporan yang tidak akurat karena tidak ada dokumen yang disertakan untuk pelaporan insiden 2. Tingkat "sok tahu" dalam identifikasi insiden masih tinggi 3. Hubungan dengan pihak ketiga perlu dipebaiki 4. Pemahaman pimpinan perlu ditingkatkan

Step 4

Seberapa baik organisasi mengimplemantasikan praktik dalam bidang ini					
Merah	Oranye	Kuning	Biru	Hijau	Tidak Teraplikasi

LAMPIRAN 4

CRITICAL ASSET INFORMATION WORKSHEET FOR SYSTEM

Catatan	**Step**
	5
Aset kritis yang dinilai diutamakan aset yang dikelola pribadi oleh DINKOMIFO dan sudah berjalan atau dalam tahap pembaharuan, bukan dalam tahap pembangunan. Dalam penelitian ini peneliti berfokus pada aset sistem TELE-PRESENCE sehingga CRITICAL ASSET SELECTION WORKSHEET tidak digunakan	

Catatan	**Step**
	10
Kebutuhan keamanan difokuskan oada kebutuhan yang ingin dicapai bukan kebutuhan yang telah terpenuhi.	

Step 5

Aset Kritis	**Catatan**
Tele - Presence	Sistem koordinasi antar lembaga pemerintahan dibawah menejemen DINKOMINFO yang sudah berjalan 80 %

Step 6 **Step 7**

Aset Kritis	Rasionalisasi
Tele – Presence	Sistem yang telah berjalan 80% dibawah menejemen DINKOMINFO dan dengan sistem ini DINKOMINFO mampu menghemat waktu dan juga biaya hingga jutaan rupiah dalam mengadakan koordinasi antar lembaga pemerintahan

Step 9

Aset Terkait	
Informasi : 1. Data jadwal konferensi 2. Data dokumen konferensi (dokumen, pdf, dll) 3. Data peserta konferensi 4. Data user	**Aplikasi :** 1. Vmeet application 2. Database 3. Sistem operasi (min Win. 7)
Aset Lain: 1. Server 2. Personal computer (PC) 3. Internet provider (termasuk hardware) 4. Web camera 5. Headphone dan microphone	

Step 8

Diskripsi
Sistem *Tele – Presence* dimenejemen oleh DINKOMINFO dengan user dari lembaga pemerintahan hingga sampai level kecamatan. Perawatan dan pengoperasian sistem ada dalam pengawasan bidang Persandian dan Aplikasi Informatika Dinas Komunikasi dan Informasi Kabupaten Malang

Step 10 **Step 11**

Kebutuhan Keamanan		**Kebutuhan Keamanan Paling Penting**
Confidentiality **X**	Hanya pihak yang berwenang yang dapat mengakses : **Tele – Presence**	[ ] Confidentiality
	Diskripsi : Informasi mengenai konferensi seharusnya tersedia dan hanya bisa diakses oleh peserta konferensi	**X** Integrity
Integrity **X**	Hanya pihak yang berwenang yang dapat mengubah informasi pada: **Tele – Presence**	**X** Availability
	Diskripsi : Penjadwalan rapat koordinasi harus tersistemkan dan informasi jadwal harus terjaga dengan baik. Hasil rapat koordinasi dengan sistem ini seharusnya terintegrasi	

	dengan sistem e-notulen yang saat ini dikembangkan	
Availability **X**	Sistem **: Tele – Presence** Harus tersedia bagi staff untuk melakukan pekerjaannya	
	Diskripsi : Sistem dan aplikasi harus mampu berjalan pada jadwal konferensi yang telah ditentukan secara tepat waktu	

LAMPIRAN 5

RISK PROFILE WORKSHEET

Catatan	Step
	13
Aktor yang dimaksud dalam Tele-Presence adalah : 1. Chairman adalah pihak yang berkuasa menyelenggarakan konferensi. Chairman juga mempunyai hak untuk menjadikan peserta konferensi lain sebagai pembicara dalam konferensi 2. Sytem admin adalah perseorangan yang mengelola atau merawat sistem dan database nya	

Catatan	Step
	14
Kekuatan motif terbagi kedalam 3 ketegori : 1. Tinggi Aktor menyerang dengan tujuan yang sangat jelas dengan target khusus atau sangat spesifik, serangan akan dipastikan untuk berhasil 2. Sedang Aktor menyerang dengan tujuan yang umum dengan target serangan ada dalam jangkauan tertentu, aktor memiliki strategi tertentu untuk menghentikan dan meninggalkan serangan 3. Rendah Aktor menyerang tanpa tujuan khusus dengan target yang termudah untuk diserang, serangan akan cepat berhenti jika tidak sukses Estimasi kekuatan motif terbagi kedalam 3 kategori : 1. Sangat	

Terdapat data yang memadai terkait kekuatan motif. Pihak lain yang meninjau data akan menghasilkan kesimpulan yang sama.

2. Kira-kira

Terdapat data dalam jumlah yang terbatas untuk mendukung kekuatan motif. Pihak lain akan dibutuhkan untuk berasumsi sehingga dapat menghasilkan kesimpulan yang sama

3. Tidak

Tidak terdapat data yang mendukung. Pihak lain dapat memberikan kesimpulan yang berbeda karena ketidaktersediaan data.

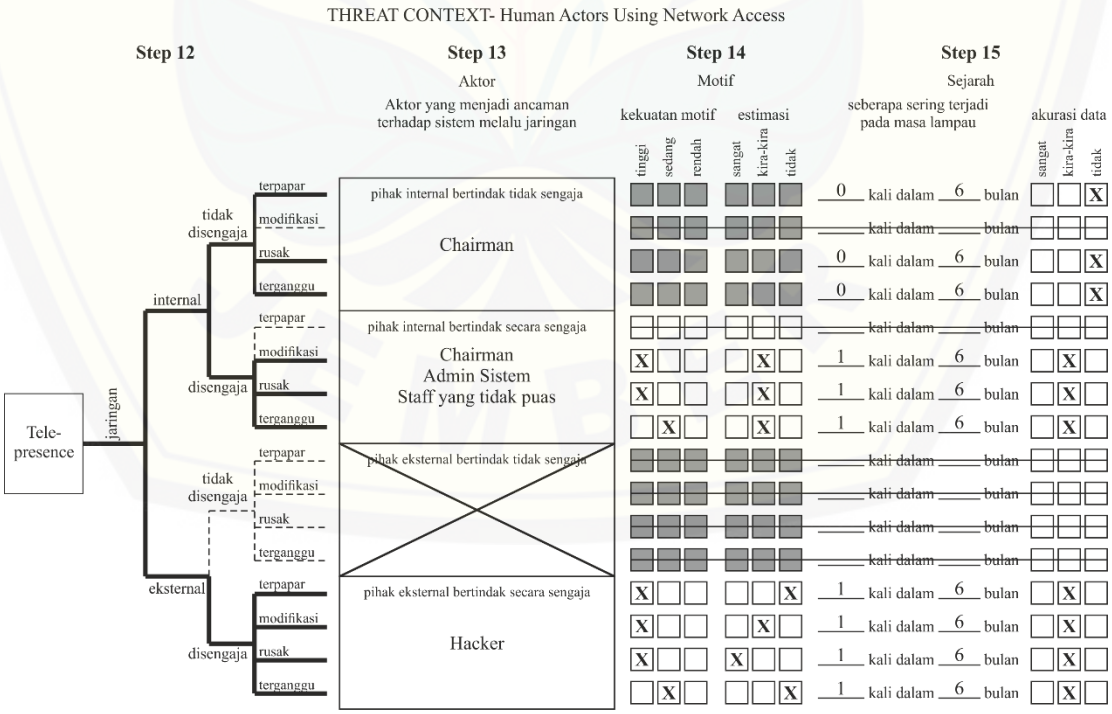
Catatan	**Step**
	15
Rentang waktu yang telah ditetapkan untuk sejarah insiden adalah 6 bulan.	

Catatan	**Step**
	26
Praktik kemanan organisasi (step 26) yang dilingkari bukan dengan maksud menjadi *mitigation area* dari cabang pohon risiko yang terbentuk. Praktik keamanan organisasi dilingkari untuk menandakan bidang yang perlu diperhatikan atau ditinjau terkait risiko yang muncul. Peninjauan dapt dilakukan dengan menggunakan *Security Practise Worksheet* (step 3 dan 4) dan *Protection Strategy Worksheet* (step 25 dan 29) Pada tahap ini penyesuaian dilakukan untuk memenuhi kebutuhan evaluasi DINKOMINFO yang dijelaskan lebih lanjut pada *Mitigation Plan Worksheet* (step 28)	

Catatan	Step
	27

Pendekatan risiko dalam penelitian ini menggunakan pendekatan risiko yang mengacu pada ISO 31000:2009, antara lain :

1. Hindari (*avoid*) adalah langkah yang dilakukan unutk menghindari risiko
2. Kurangi (*reduce*) adalah langkah yang dilakukan untuk mengurangi dampak risiko yang terjadi
3. Berbagi (*share*) adalah langkah yang dilakukan untuk membagi dampak risiko dengan pihak ketiga.
4. Terima (*accept*) adalah tindakan menerima dampak risiko dengan tidak melakukan apa apa.

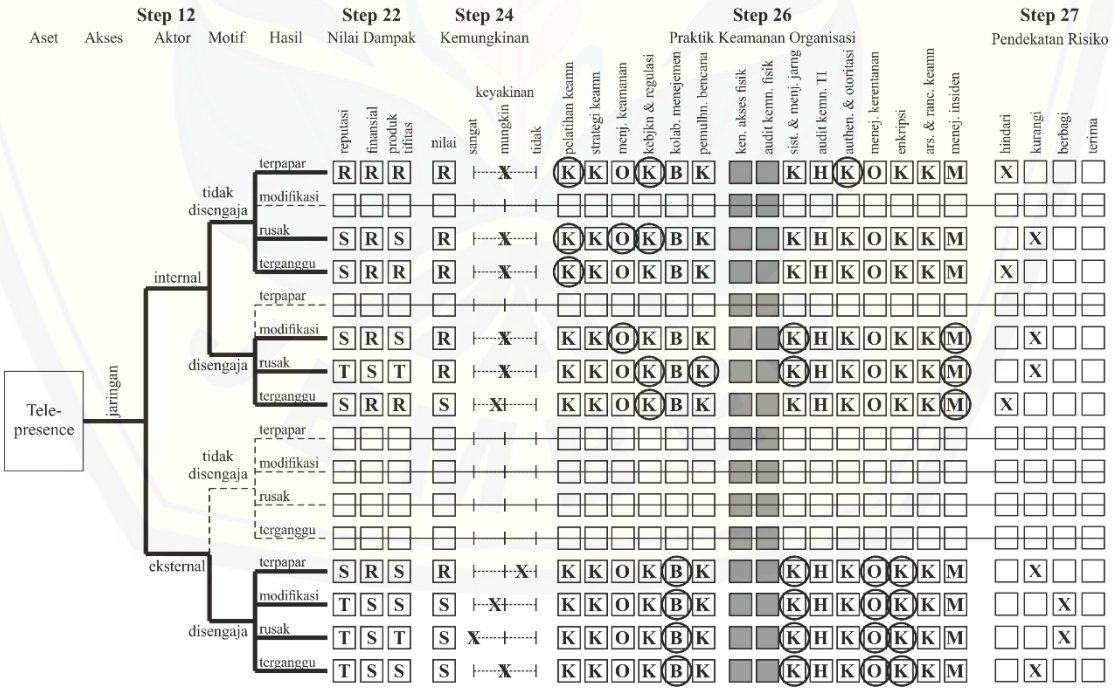


AREAS OF CONCERN - Human Actors Using Network Access

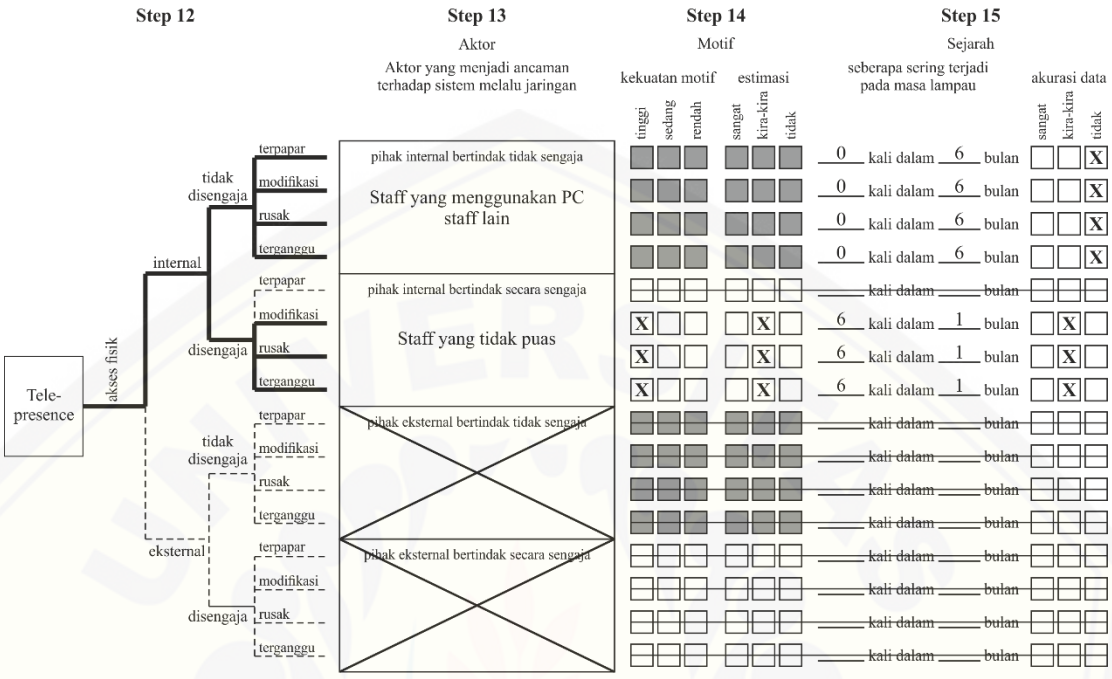
Step 16

pihak internal menggunakan akses jaringan	contoh bagaimana pihak internal bertindak **tidak sengaja** dapat menggunakan akses jaringan untuk mengancam sistem	1. Chairman bisa saja membocorkan dokumen pada level konferensi yang berbeda atau bahkan tidak sengaja menghancurkan dokumen-dokumen terkait konferensi atau menghancurkan log konferensi. 2. Chairman bisa saja lupa memberikan hak akses pada satu atau beberapa user dalam mengadakan konferensi sehingga akses user terganggu.
	contoh bagaimana pihak internal bertindak **secara sengaja** dapat menggunakan akses jaringan untuk mengancam sistem	1. Chairman bisa mengganti file atau dokumen yang terkait dengan konferensi 2. Chairman bisa saja memutus akses salah satu user selama konferensi, karena suatu alasan 3. Admin sistem dapat memodifikasi atau merusak data user atau mengganti akses user sehinga akses ke sistem terganggu. 4. Staff yang tidak puas bisa saja merusak aset dan atau data pribadinya kemudian melaporkannya sebagai kecacatan atau kegagalan sistem dengan maksud atau tujuan tertentu
pihak eksternal menggunakan akses jaringan	contoh bagaimana pihak eksternal bertindak **tidak sengaja** dapat menggunakan akses jaringan untuk mengancam sistem	
	contoh bagaimana pihak eksternal bertindak **secara sengaja** dapat menggunakan akses jaringan untuk mengancam sistem	1. Hacker bisa masuk atau meretas level administrator pada sistem dan hal ini mengacam keamanan data pada server atau database.

BASIC RISK PROFILE - Human Actors Using Network Access



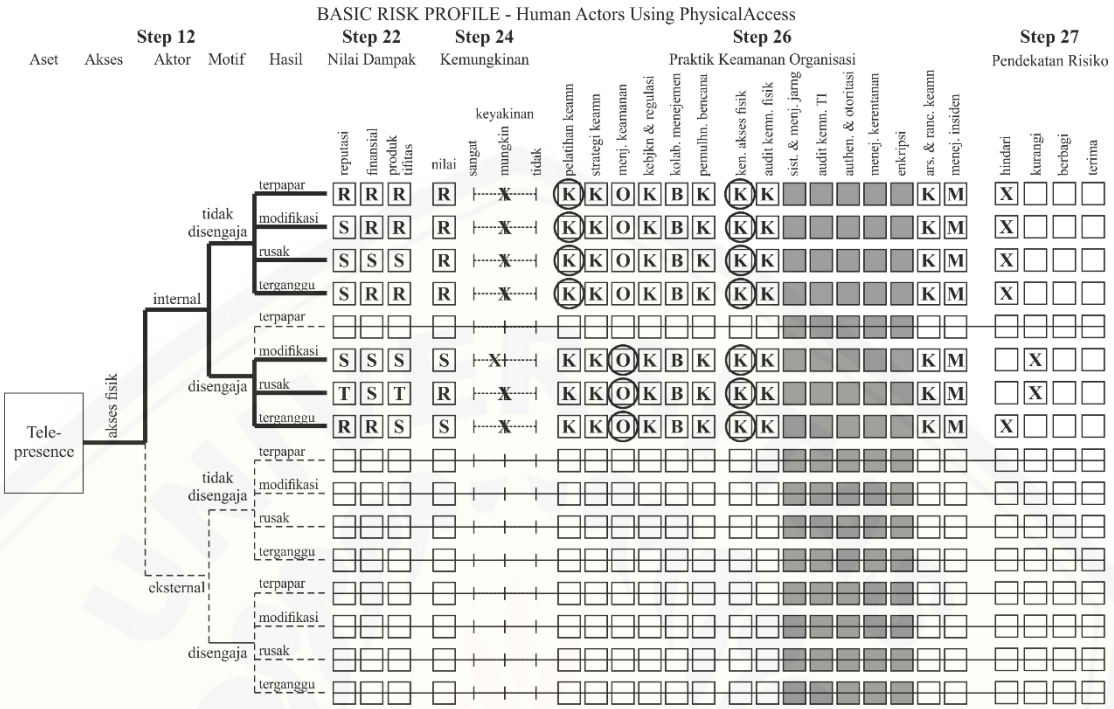
THREAT CONTEXT- Human Actors Using Physical Access

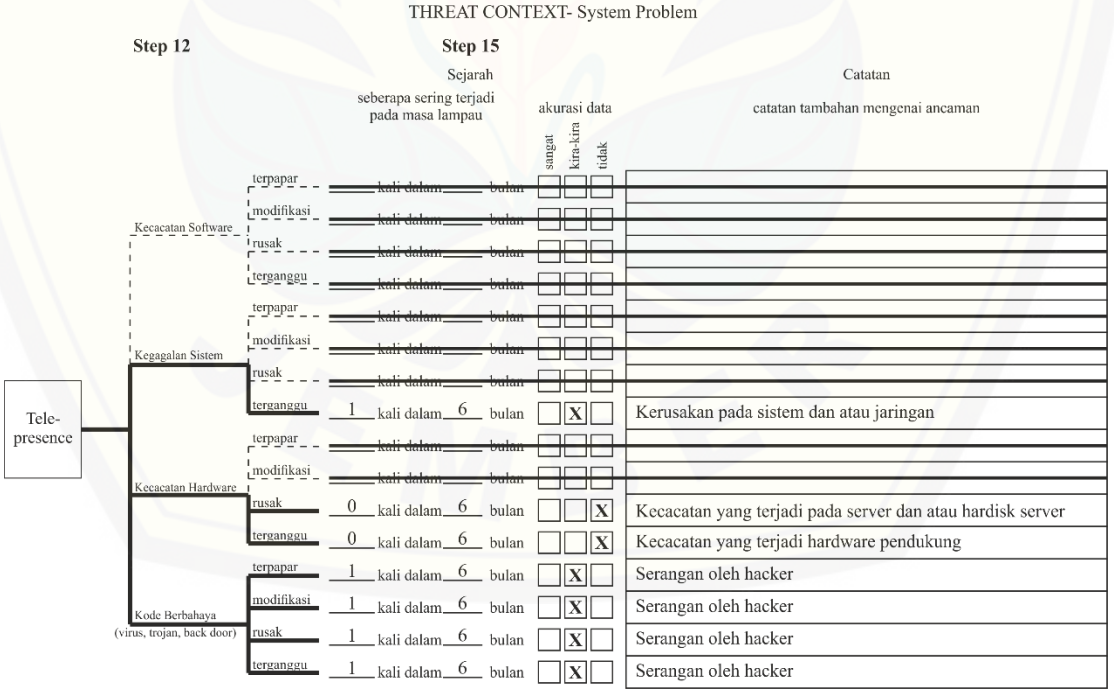


AREAS OF CONCERN - Human Actors Using Physical Access

Step 16

pihak internal menggunakan akses fisik	contoh bagaimana pihak internal bertindak **tidak sengaja** dapat menggunakan akses fisik untuk mengancam sistem	1. Staff menggunakan komputer staff lain yang belum atau tidak *logout* dari sistem
	contoh bagaimana pihak internal bertindak **secara sengaja** dapat menggunakan akses fisik untuk mengancam sistem	1. Staff yang tidak puas dan memiliki akses fisik ke server bisa memasukkan program-program tertentu yang dapat menghambat kerja server 2. Staff yang tidak puas dapat merusak satu atau beberapa aset terkait sistem dan melaporkannya sebagai kerusakan dengan tujuan tertentu.
pihak eksternal menggunakan akses fisik	contoh bagaimana pihak eksternal bertindak **tidak sengaja** dapat menggunakan akses fisik untuk mengancam sistem	
	contoh bagaimana pihak eksternal bertindak **secara sengaja** dapat menggunakan akses fisik untuk mengancam sistem	



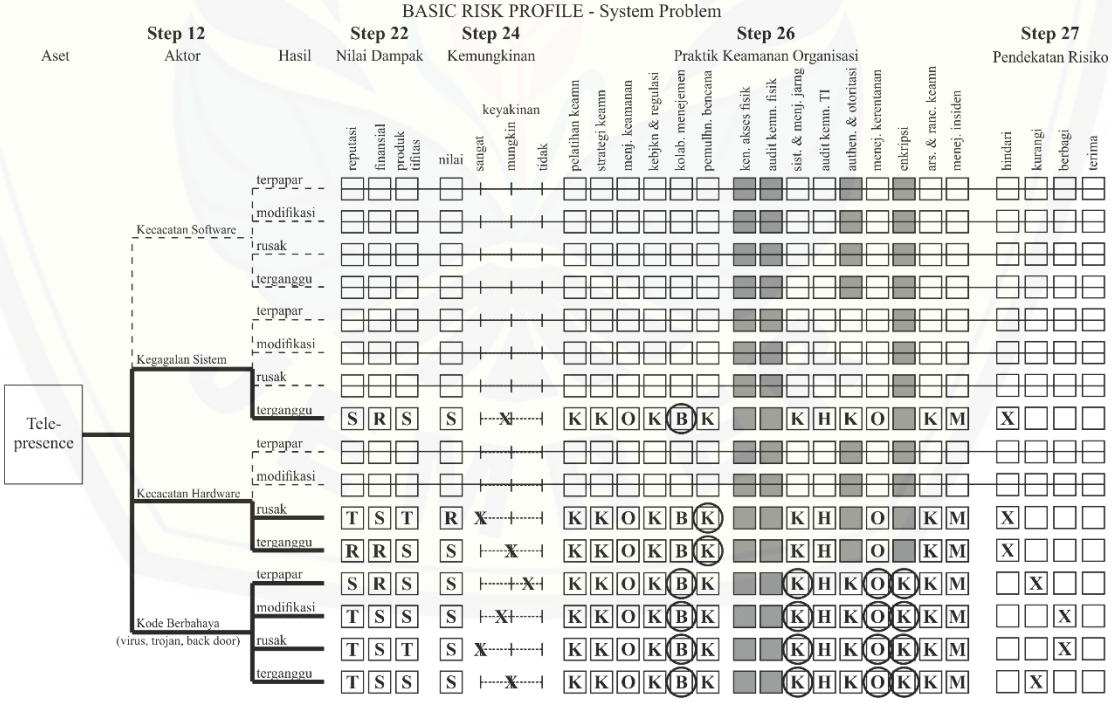


AREAS OF CONCERN - System Problem

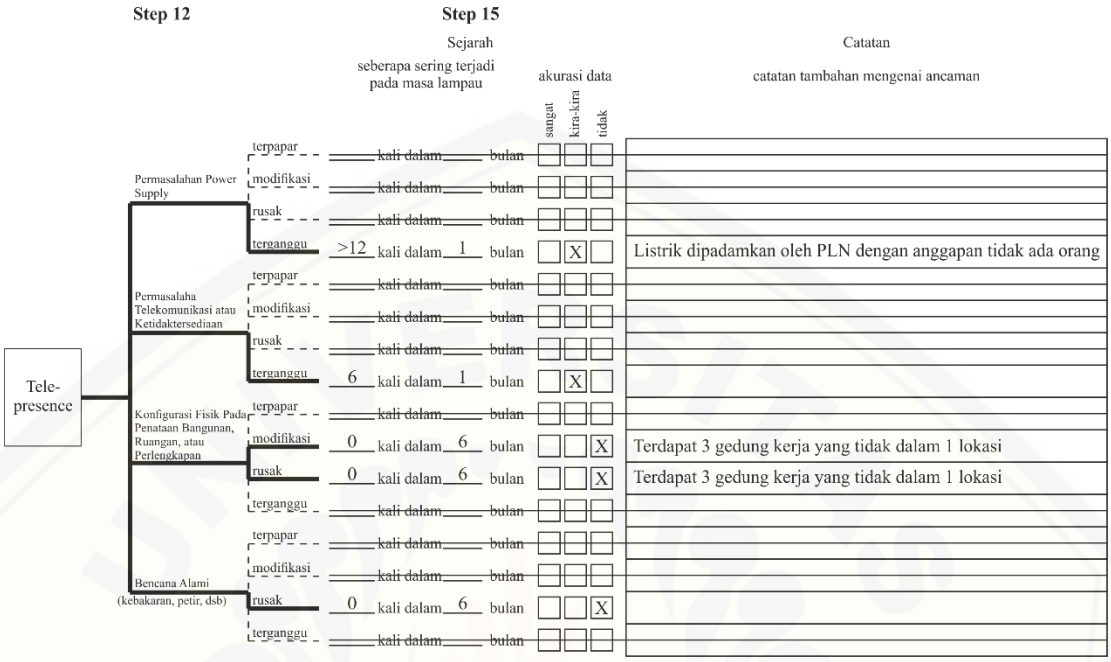
Step 16

Kecacatan Software	contoh bagaimana kecacatan software dapat mengancam sistem ini	
Kegagalan Sistem	contoh bagaimana kegagalan sistem dapat mengancam sistem ini	1. Sistem tidak bisa berjalan atau berjalan lambat karena terdapat satu atau beberapa program dalam server Tele-Presence yang mana seharusnya program-program tersebut tidak terinstal dalam server.
Kecacatan Hardware	contoh bagaimana kecacatan hardware dapat mengancam sistem ini	1. Ketidak sesuaian spesifikasi hardware dengan spesifikasi yang dibutuhkan dapat mengganggu penggunaan dan atau perawatan sistem
Kode Berbahaya	contoh bagaimana kode-kode berbahaya dapat mengancam sistem ini (dengan mempertimbangkan virus, back door, dsb)	1. Setiap back door yang terdapat dalam sistem dapat digunakan untuk masuk dan mengambil informasi, memasukkan virus, atau merusak data.

BASIC RISK PROFILE - System Problem



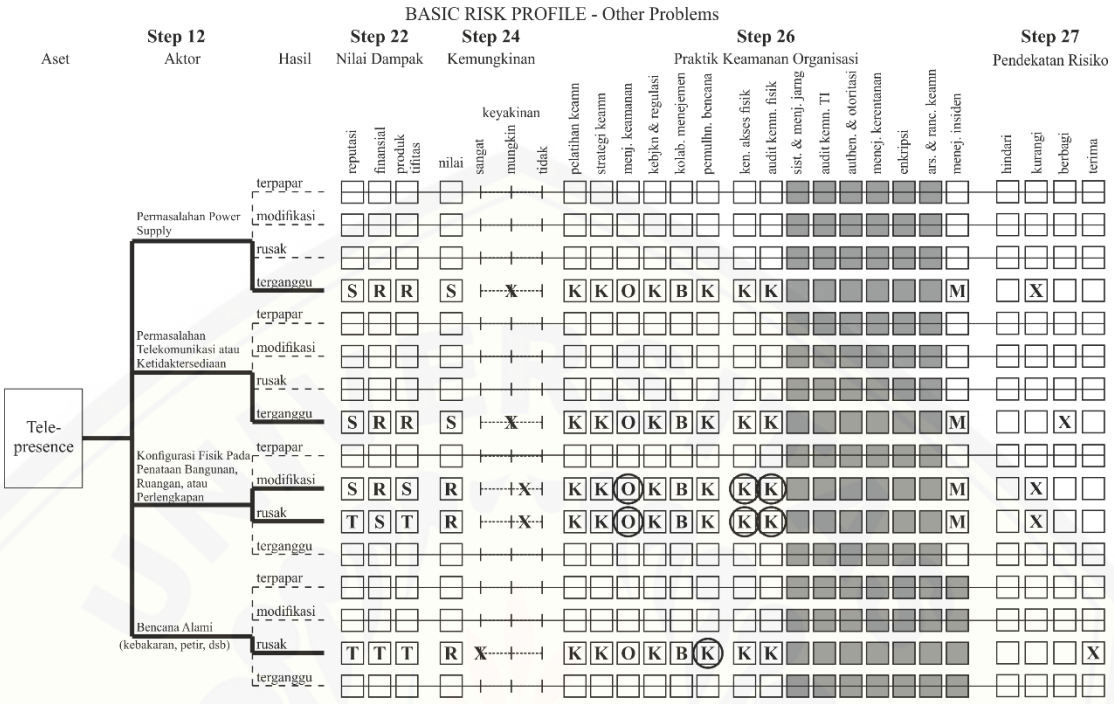
THREAT CONTEXT- Other Problems



AREAS OF CONCERN - Other Problems

Step 16

Permasalahan Power Supply	contoh bagaimana permasalahan power supply dapat mengancam sistem ini	1. Padamnya listrik tanpa adanya sumber listrik alternatif dapat menghentikan kerja server 2. Tidak tersedianya sumber listrik darurat dapat menghentikan akses pada saat sistem sedang digunakan
Permasalahan Telekomunikasi	contoh bagaimana permasalahan telekomunikasi dapat mengancam sistem ini	1. Gangguan yang terjadi pada jaringan yang disediakan oleh pihak *Internet Service Provide* menyebabkan sistem tidak dapat diakses
Permasalah Pihak Ketiga	contoh bagaimana permasalahan konfigurasi fisik dari bangunan, ruangan atau perlengkapan dapat mengancam sistem ini	1. Lokasi gedung kerja DINKOMINFO yang terletak pada 3 dearah yang berbeda di kabupaten Malang, memberikan potensi adanya tindakan modifikasi server yang sulit dideteksi 2. Lokasi gedung yang berjauhan juga menghambat dalam proses pengawasan dan monitoring
Bencana Alami	contoh bagaimanapermasalahan pihak ketiga dapat mengancam sistem ini	1. Petir, arus pendek aliran listrik kebakaran, dan bencana lain memberikan kerusakan baik fisik maupun data yang tidak dapat dipulihkan, tanpa adanya menejemen indsiden yang baik



LAMPIRAN 6

NETWORK ACCESS PATH WORKSHEET

Catatan	Step
	17
System of Interest adalah sistem yang paling dekat dengan aset kritis, sebagai contoh : 1. Dimana sistem itu "hidup" 2. Sistem mana yang dituju untuk mendapatkan salinan asli aset kritis 3. Sistem yang memberikan akses sah ke aset kritis 4. Sistem yang memberikan akses kepada aktor yang mengancam aset kritis Pada penelitian ini berfokus pada sistem Tele-Presence, maka *system of interest* dari sistem ini adalah sistem Tele-Presence ini sendiri.	

Catatan	Step
	18 (a-e)
Component class yang digunakan dalam analisis antara lain : 1. Server *Host* yang menyediakan teknologi layanan informasi kepada organisasi 2. Internal network Jaringan dalam organisasi yang menghubungkan komputer dan sistem yang dirawat oleh staff 3. On-Site workstation *Host* pada jaringan yang digunakan staff untuk melakukan pekerjaannya 4. Laptops Laptop yang digunakan staff untuk mengakses informasi dari jarak jauh 5. PDA / wireless components	

Perangkat yang mungkin digunakan staff untuk mengakses informasi

6. Other system

Sistem, atau aplikasi lain yang mengakses informasi kritis dari *system of interest*

7. Storage device

Perangkat dimana informasi disimpan untuk tujuan pencadangan data

8. External networks

Jaringan yang menghubungkan komputer dengan sistem yang bukan merupakan bagian dari jaringan organisasi

9. Home / external workstation

Perangkat yang digunakan staff atau individual untuk mengakses informasi dari jarak jauh melalui jaringan organisasi

10. Other

Perangkat jenis lain yang mungkin menjadi skenario ancaman sendiri, yang tidak termasuk dalam golongan yang disebutkan sebelumnya.

Catatan	**Step**
	18d
Data Storage Location tidak diisi dan diberi warna merah karena sistem Tele-Presence belum memiliki perangkat penyimpanan untuk tujuan pencadangan data.	

Step 17

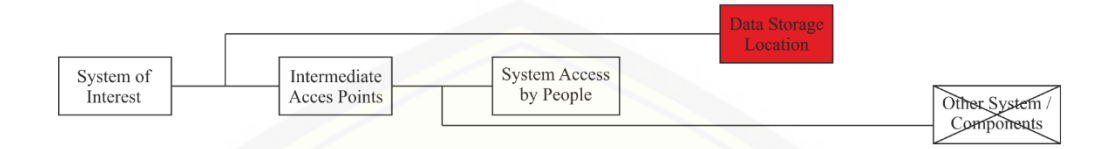
System of Interest

System yang paling terkait dengan aset kritis

Tele-Presence (sistem itu sendiri)

Access Point

Access Point



Step 18a	Step 18b	Step 18c	Step 18d	Step 18e
System of Interest	Intermediate Acces Points	System Access by People	Data Storage Location	Other System / Components
classes of components yang merupakan bagian dari system of interest	classes of components yang digunakan untuk mentransfer informasi dari system of interest kepada perseorangan classes of components yang dapat bertindak sebagai intermediate acces point	classes of components yang dapat digunakan perseorangan (misal : user, hacker) mengakses system of interest	classes of componentsyang menyimpan informasi dari system of interest untuk tujan backup	system lain yang mengakses informasi dari system of interest classes of components yang dapat digunakan untuk mengakses informasi dari aset kritis atau aplikasi dari system of interest
[X] Server Vmeet Server - Kepanjen	[X] Internal Network Local Area Network	[X] On-Site Workstation	[ ] Storage Devices	[ ] _____
[-] ~~Internal Network~~	[X] External Network Internet Sevice Provider	[X] Laptops Staff dinas lapangan	[ ] Other :	[ ] _____
[X] On-Site Workstation PC	[-] ~~Other :~~	[-] ~~PDAs/Wireless Components~~		[ ] _____
[-] ~~Other :~~		[X] Home/External Workstation Staff tertentu		[ ] _____
		[-] ~~Other :~~		

LAMPIRAN 7

INFRASTRUCTURE REVIEW WORKSHEET

Catatan	**Step**
	19b
Aset kritis yang terkait dengan *class components* (step 19b) tidak digunakan (dihapuskan) karena aset kritis dalam penelitain ini hanya ada satu yaitu sistem Tele-Presence	

Catatan	**Step**
	21
Teknik pengamatan terbagi atas 3 kriteria : 1. Teknik formal Staff melakukan *data gathering* dengan teliti dan menjalankan teknik analisis tertentu untuk mendapatkan kesimpulan 2. Sarana informal Analis melakukan evaluasi singkat terhadap situasi saat ini dalam organisasi untuk mendapatkan kesimpulan 3. Lain-lain Kategori ini digunakan untuk mengidentifikasi teknik lain yang digunakan untuk mendapatkan kesimpulan	

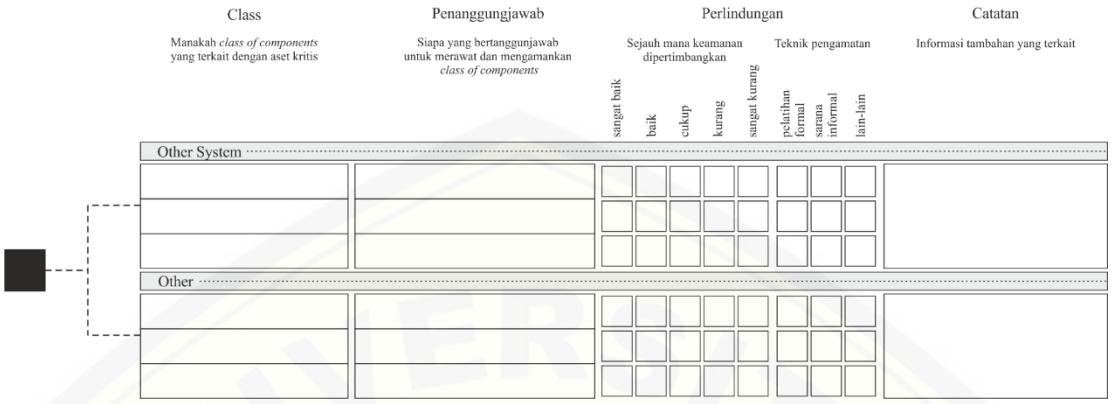
INFRASTURCTURE REVIEW

Step 19 Class Manakah *class of components* yang terkait dengan aset kritis	Step 20 Penanggungjawab Siapa yang bertanggunjawab untuk merawat dan mengamankan *class of components*	Step 21 Perlindungan Sejauh mana keamanan dipertimbangkan					Teknik pengamatan			Catatan Informasi tambahan yang terkait
		sangat baik	baik	cukup	kurang	sangat kurang	teknik formal	sarana informal	lain-lain	
Server										
Vmeet server	Bid. Infrastruktur Teknologi Informasi & Komunikasi seksi Pengelolaan Data Center				X			X		
Internal Networks										
LAN	Bid. Infrastruktur Teknologi Informasi & Komunikasi seksi Pengendalian & Pengawasan Inf. TI		X					X		Jaringan internal perlu diperbaiki atau ditata ulang
On-Site Workstation										
Staff jaringan	Staff		X					X		
Staff	Staff			X				X		
Menejer (pimpinan)	Menejer (pimpinan)			X				X		
Laptops										
Staff dinas lapangan	Staff yang bertugas		X					X		

INFRASTURCTURE REVIEW

Class Manakah *class of components* yang terkait dengan aset kritis	Penanggungjawab Siapa yang bertanggunjawab untuk merawat dan mengamankan *class of components*	Perlindungan Sejauh mana keamanan dipertimbangkan					Teknik pengamatan			Catatan Informasi tambahan yang terkait
		sangat baik	baik	cukup	kurang	sangat kurang	pelatihan formal	sarana informal	lain-lain	
PDA / Wireless Components										
Storage Device										
External Networks										
Jaringan internet	Pihak ISP (third party)		X					X		
Home / External Workstation										
Staff tertentu	Staff yang bersangkutan			X				X		

INFRASTURCTURE REVIEW



LAMPIRAN 8

PROBABILITY EVALUATION CRITERIA WORKSHEET

Catatan	**Step**
	23
Nilai kemungkinan didefinisikan dari satu set evaluasi pada kriteria yang telah dikategorikan menurut frekuensi kejadian. *Worksheet* ini mendefinisikan standart definisi – definisi untuk nilai kemungkinan. Rentang waktu frekuensi tahunan kejadian ditetapkan 1 tahun, sesuai dengan usia DINKOMINFO dan usia penggunaan sistem Tele-Presence yang baru berjalan 6 bulan. Kriteria yang terbentuk mendefinisikan pengukuran tinggi, sedang, dan rendah dari kemungkinan ancaman.	

Frequency – Based Criteria

Waktu Antar Kejadian	Harian	<5 kali Per minggu	>2 kali per minggu	Mingguan	Bulanan	3 kali per 6	2 kali per 6	1 kali per 6	1 kali per 12
Annualized Frequency	182	<=96	>=72	26	6	3	2	1	0.5
Kategori	**TINGGI**	**SEDANG**		**RENDAH**					

LAMPIRAN 9

PROTECTION STRATEGY WORKSHEET

Catatan	Step
	25
Stop light status (step 4) direvisi dengan mempertimbangkan hasil dari step 25 dan peninjauan kembali hasil step 3a yang telah dilakukan. Kondisi yang dipilih adalah kondisi paling dominan terjadi dalam organisasi. Pilihan kondisi saat ini dalam area pertanggungjawaban pada bidang 7 hingga 15 berubah menjadi 4 pilihan : 1. Internal 2. External 3. Kombinasi 4. Belum Pihak ketiga yang dimaksud pada bidang 7 hingga bidang 15 hanya disebutkan sebagai perseorangan atau perusahaan, hal ini menyesuaikan dengan privasi data yang dimiliki DINKOMINFO	

Catatan	Step
	29
Analisis perubahan strategi perlindungan bukan didasarkan pada pohon risiko yang terbentuk (step 12). Analisis perubahan dilakukan dengan mempertimbangkan kondisi saat ini dari *protection strategy* (step 25), *security practise* (step 3a dan step 3b), dan *stop light status* (step 4). Hal ini disesuaikan dengan kebutuhan DINKOMINFO kab. Malang yang meminta adanya analisis dari hasil angket yang telah diisi.	

1. KESADARAN KEAMANAN DAN PELATIHAN

Stop Light Status : KUNING

	Step 25	**Step 29**
Strategi Pelatihan	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki **strategi pelatihan yang terdokumentasi** termasuk pelatihan kesadaran dan pelatihan terkait keamanan untuk teknologi yang digunakan		**X**
Organisasi memiliki **strategi pelatihan yang informal** atau tidak terdokumentasikan	**X**	

	Step 25	**Step 29**
Pelatihan Kesadaran Keamanan	**Kondisi saat ini**	**Perlu Perubahan**
Pelatihan kesadaran keamanan secara periodik tersedia bagi semua staff …….. kali dalam ……		**X**
Pelatihan kesadaran keamanan **tersedia** bagi staff baru sebagai bagian dari masa orientasi	**X**	
Organisasi **tidak menyediakan** pelatihan kesadaran keamanan. Staff mempelajari permasalahan atas inisiatif sendiri		

	Step 25	Step 29
Pelatihan Terkait Keamanan untuk Teknologi yang Digunakan	**Kondisi saat ini**	**Perlu Perubahan**
Staff TI **perlu menghadiri pelatihan** terkait keamanan untuk segala jenis teknologi yang mereka gunakan	**X**	
Staff TI **dapat menghadiri pelatihan** terkait keamanan untuk segala jenis teknologi yang mereka gunakan **jika mereka memintanya**		
Organisasi secara umum **tidak menyediakan peluang** bagi staff TI **untuk menghadiri pelatihan** terkait keamanan untuk teknologi yang mereka gunakan. Staff TI mempelajari permasalahan keamanan berdasarkan inisiatif sendiri		

	Step 25	Step 29
Pembaharuan Keamanan Secara Periodik	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki mekanisme** formal untuk menyediakan pembaharuan atau bulletin untuk para staff secara periodik atau permasalahan keamanan yang penting		**X**
Organisasi **tidak memiliki mekanisme** untuk menyediakan pembaharuan atau bulletin untuk para staff secara periodik atau permasalahan keamanan yang penting	**X**	

Verifikasi Pelatihan	Step 25 Kondisi saat ini	Step 29 Perlu Perubahan
Organisasi memiliki **mekanisme formal** untuk melacak dan memferivikasi bahwa staff menerima pelatihan terkait keamanan yang memadai		**X**
Organisasi memiliki **mekanisme informal** untuk melacak dan memferivikasi bahwa staff menerima pelatihan terkait keamanan yang memadai	**X**	
Organisasi **tidak memiliki mekanisme** untuk melacak dan memferivikasi bahwa staff menerima pelatihan terkait keamanan yang memadai		

2. STRATEGI KEAMANAN

Stop Light Status : KUNING

Bisnis dan Itegrasi Strategi Keamanan	Step 25 Kondisi saat ini	Step 29 Perlu Perubahan
Organisasi **memiliki mekanisme formal** untuk mengintegrasikan : - Pertimbangan keamanan kedalam strategi bisnis - Tujuan dan strategi bisnis kedalam kebijakan dan strategi keamanan	**X**	

Organisasi **memiliki mekanisme informal** untuk mengintegrasikan : - Pertimbangan keamanan kedalam strategi bisnis - Tujuan dan strategi bisnis kedalam kebijakan dan strategi keamanan		
Organisasi **tidak memiliki mekanisme** untuk mengintegrasikan : - Pertimbangan keamanan kedalam strategi bisnis - Tujuan dan strategi bisnis kedalam kebijakan dan strategi keamanan		

	Step 25	**Step 29**
Strategi yang Terdokumentasi	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki** strategi keamanan, sasaran dan tujuan yang terdokumentasi		**X**
Organisasi **memiliki sebagian** strategi keamanan, sasaran dan tujuan yang **terdokumentasi** . Beberapa aspek dari strategi keamanan, sasaran, dan tujuan masih informal dan belum sepenuhnya didukung	**X**	
Organisasi **memiliki** strategi keamanan, sasaran dan tujuan yang **informal dan tidak terdokumentasi**		

3. MENEJEMEN KEAMANAN

Stop Light Status : ORANYE

	Step 25	**Step 29**
Peran dan Tanggungjawab	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki dokumentasi secara formal mengenai peran dan tanggungjawab keamanan informasi **untuk semua staff** dalam organisasi		**X**
Organisasi memiliki dokumentasi secara formal mengenai peran dan tanggungjawab keamanan informasi **untuk beberapa staff terpilih** dalam organisasi	**X**	
Organisasi memiliki peran dan tanggungjawab keamanan informasi yang **informal dan tidak terdokumentasi**		

	Step 25	**Step 29**
Pendanaan	**Kondisi saat ini**	**Perlu Perubahan**
Anggaran organisasi memiliki garis batasan yang jelas untuk kegiatan keamanan informasi. **Level pendanaan ditentukan berdasarkan penilaian secara formal dari risiko keamanan informasi organisasi.**	**X**	
Anggaran organisasi memiliki garis batasan yang jelas untuk kegiatan keamanan informasi.		

Level pendanaan ditentukan berdasarkan proses informal		
Angaran orgnisasi secara jelas memasukkan aktifitas keamanan informasi dibawah garis batas untuk teknologi informasi. **Level pendanaan ditentukan berdasarkan penilaian formal dari risiko keamanan informasi organisasi**		X
Angaran orgnisasi secara jelas memasukkan aktifitas keamanan informasi dibawah garis batas untuk teknologi informasi. **Level pendanaan ditentukan berdasarkan proses penilaian informal**	**X**	
Tidak satupun baik dana organisasi maupun dana departemen TI secara jelas memasukkan pendanaan untuk kegiatan keamanan informasi		

	Step 25	**Step 29**
Prosedur Sumber Daya Manusia	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki prosedur** yang didefinisikan secara **formal** untuk memasukan pertimbangan keamanan dalam proses penyewaan atau pemutusan sewa oleh organisasi	**X**	
Organisasi **memiliki beberapa prosedur** yang didefinisikan secara **formal** untuk memasukan pertimbangan keamanan dalam proses		

penyewaan atau pemutusan sewa oleh organisasi. Beberapa prosedur pada area ini masih informal dan tidak terdokumentasi		
Organisasi **memiliki prosedur informal dan tidak terdokmentasi** untuk memasukan pertimbangan keamanan dalam proses penyewaan atau pemutusan sewa oleh organisasi		

	Step 25	**Step 29**
Menejemen Risiko	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki **proses yang terdefnisi secara formal** untuk penilaian dan pengelolaan risiko keamanan informasinya.		**X**
Organisasi memiliki **proses yang terdefnisi secara formal** untuk penilaian. Proses pengelolaan risiko keamanannya masih **informal dan tidak terdokumentasi**	**X**	
Organisasi memiliki **pendekatan informal dan tidak terdokumentasi** untuk penilaian dan pengelolaan risiko keamanan informasinya		

	Step 25	Step 29
Kesadaran Staff	**Kondisi saat ini**	**Perlu Perubahan**
Program pelatihan kesadaran keamanan organisasi menyertakan informasi mengenai proses menejemen keamanan organisasi. Pelatihan disediakan untuk semua staff 1 kali setiap 1 tahun	**X**	
Program pelatihan kesadaran keamanan organisasi **menyertakan** informasi mengenai proses menejemen keamanan organisasi. **Pelatihan disediakan untuk staff baru sebagai bagian dari masa orientasi**		
Program pelatihan kesadaran keamanan organisasi **tidak menyertakan** informasi mengenai proses menejemen keamanan organisasi. **Staff mempelajari menejemen keamanan atas inisiatif pribadi**		

	Step 25	Step 29
Menejemen Kesadaran	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki mekanisme formal** untuk menyediakan para menejer kumpulan kesimpulan dari informasi penting terkait keamanan	**X**	

Organisasi **memiliki mekanisme informal dan tidak terdokumentasi** untuk menyediakan para menejer kumpulan kesimpulan dari informasi penting terkait keamanan		
Organisasi **tidak memiliki mekanisme** untuk menyediakan para menejer kumpulan kesimpulan dari informasi penting terkait keamanan		

4. REGULASI DAN KEBIJAKAN KEAMANAN

Status Stop Light : KUNING

	Step 25	**Step 29**
Kebijkan Terdokumentasi	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki **set dokumentasi secara formal** mengenai kebijakan terkait keamanan		**X**
Organisasi memiliki **beberapa dokumentasi secara formal** mengenai kebijakan terkait keamanan. Beberapa kebijakan terkait keamanan masih informal dan tidak terdokumentasi	**X**	
Kebijkan organisasi terkait keamanan masih informal dan tidak terdokumentasi		

	Step 25	Step 29
Menejemen Kebijakan	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki **mekanisme formal untuk membuat dan memperbaharui** kebijakan terkait keamanan	**X**	
Organisasi memiliki mekanisme **formal untuk membuat kebijakan** terkait keamanan. Organisasi memiliki **mekanisme informal dan tidak terdokumentasi untuk memperbaharui** kebijakan terkait keamanan		
Organisasi memiliki mekanisme informal dan tidak terdokumentasi utnuk membuat dan memperbaharui kebijakan terkait keamanan		

	Step 25	Step 29
Penegakan Kebijakan	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki prosedur formal untuk menegakkan kebijakan terkait keamanan. Prosedur penegakan **diikuti secara konsisten**	**X**	
Organisasi memiliki prosedur formal untuk menegakkan kebijakan terkait keamanan. Prosedur penegakan **diikuti secara tidak konsisten**		
Organisasi **memiliki prosedur informal dan tidak terdokumentasi** untuk mengakkan kebijakan keamanan		

	Step 25	Step 29
Kesadaran Staff	**Kondisi saat ini**	**Perlu Perubahan**
Program pelatihan kesadaran keamanan oleh organisasi **menyertakan** informasi mengenai regulasi dan kebijakan keamanan. Pelatihan disediakan untuk **semua staff sebanyak 1kali dalam 1 tahun**	**X**	
Program pelatihan kesadaran keamanan oleh organisasi **menyertakan** informasi mengenai regulasi dan kebijakan keamanan. Pelatihan disediakan untuk **staff baru sebagai bagian dari masa orientasi**		
Program pelatihan kesadraan keamanan oleh organisasi **tidak menyertakan** informasi mengenai regulasi dan kebijakan keamanan. Staff mempelajari regulasi dan kebijakan keamanan atas inisiatif sendiri		

	Step 25	Step 29
Kepatuhan Kebijakan dan Regulasi	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki prosedur formal untuk **pemenuhan** kebijakan keamanan informasi, hukum dan regualsi yang berlaku dan kebutuhan asuransi		**X**

Organisasi memiliki prosedur formal untuk **pemenuhan beberapa** kebijakan keamanan informasi, hukum dan regualsi yang berlaku dan kebutuhan asuransi. Beberapa prosedur dalam area ini masih informal dan tidak terdokumentasi	**X**	
Organisasi memiliki prosedur **informal dan tidak terdokumentasi** untuk pemenuhan kebijakan keamanan informasi, hukum dan regualsi yang berlaku dan kebutuhan asuransi		

5. KOLABORASI MENEJEMEN KEAMANAN

Status Stop Light : BIRU

	Step 25	**Step 29**
Kolaborator dan Mitra	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki prosedur dan kebijakan yang **terdokumentasi untuk melindungi informasi** ketika berkerja dengan kolaborator dan mitra		**X**
Organisasi memiliki prosedur dan kebijakan yang terdokumentasi **untuk melindungi informasi khusus** ketika berkerja dengan kolaborator dan mitra. Organisasi memiliki prosedur dan kebijakan informal untuk melindung jenis informasi lain keitka bekerja dengan kolaborator dan mitra.	**X**	

Organisasi memiliki prosedur dan kebijakan yang **informal dan tidak terdokumentasi untuk melindungi informasi** ketika berkerja dengan kolaborator dan mitra		

	Step 25	**Step 29**
Kontraktor dan Subkontraktor	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki prosedur dan kebijakan yang **terdokumentasi untuk melindungi informasi** ketika berkerja dengan kontraktor dan subkontraktor		**X**
Organisasi memiliki prosedur dan kebijakan yang terdokumentasi **untuk melindungi informasi khusus** ketika berkerja dengan kontraktor dan subkontraktor. Organisasi memiliki prosedur dan kebijakan informal untuk melindung jenis informasi lain keitka bekerja dengan kontraktor dan subkontraktor	**X**	
Organisasi memiliki prosedur dan kebijakan yang **informal dan tidak terdokumentasi untuk melindungi informasi** ketika berkerja dengan kontraktor dan subkontraktor		

	Step 25	Step 29
Penyedia layanan	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki prosedur dan kebijakan yang **terdokumentasi untuk melindungi informasi** ketika berkerja dengan penyedia layanan		**X**
Organisasi memiliki prosedur dan kebijakan yang terdokumentasi **untuk melindungi informasi khusus** ketika berkerja dengan penyedia layanan. Organisasi memiliki prosedur dan kebijakan informal untuk melindung jenis informasi lain keitka bekerja dengan penyedia layanan	**X**	
Organisasi memiliki prosedur dan kebijakan yang **informal dan tidak terdokumentasi untuk melindungi informasi** ketika berkerja dengan penyedia layanan.		

	Step 25	Step 29
Persyaratan	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **mendokumentasikan** persyaratan perlindungan informasi dan secara tegas mengkomunikasikannya kepada pihak ketiga	**X**	

Organisasi **secara informal** mengkomunikasikan persyaratan perlindungan informasi kepada semua pihak ketiga.		
Organisasi **tidak mengkomunikasikan** persyaratan perlindungan informasi kepada pihak ketiga		

	Step 25	**Step 29**
Verifikasi	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki mekanisme formal** untuk memverfikasi semua organisasi pihak ketiga, layanan keamanan (outsourced), mekanisme dan teknologi yang memenuhi kebutuhan dan persyaratan organisasi	**X**	
Organisasi **memiliki mekanisme informal** untuk memverfikasi semua organisasi pihak ketiga, layanan keamanan (outsourced), mekanisme dan teknologi yang memenuhi kebutuhan dan persyaratan organisasi		
Organisasi **tidak memiliki mekanisme** untuk memverfikasi semua organisasi pihak ketiga, layanan keamanan (outsourced), mekanisme dan teknologi yang memenuhi kebutuhan dan persyaratan organisasi		

	Step 25	Step 29
Kesadaran Staff	**Kondisi saat ini**	**Perlu Perubahan**
Program pelatihan kesadaran keamanan oleh organisasi **menyertakan** informasi mengenai kebijakan dan prosedur kolaborasi menejemen keamanan yang dimiliki organisasi. **Pelatihan tersedia untuk semua staff sebanyak 1kali dalam 1 tahun**	**X**	
Program pelatihan kesadaran keamanan oleh organisasi **menyertakan** informasi mengenai kebijakan dan prosedur kolaborasi menejemen keamanan yang dimiliki organisasi. **Pelatihan tersedia untuk staff baru sebagai bagian dari masa orientasi**		
Program pelatihan kesadaran keamanan oleh organisasi **tidak menyertakan** informasi mengenai kebijakan dan prosedur kolaborasi menejemen keamanan yang dimiliki organisasi. Staff mempelajari kebijakan dan prosedur kolaborasi menejemen keamanan atas inisiatif sendiri		

6. PERENCANAAN KEMUNGKINAN / PEMULIHAN BENCANA

Status Stop Light : KUNING

	Step 25	**Step 29**
Analisi Operasi Bisnis	**Kondisi saat ini**	**Perlu Perubahan**
Analisis operasi, aplikasi dan data kritis **telah dilakukan**		**X**
Analisis operasi, aplikasi dan data kritis **telah sebagian dilakukan**	**X**	
Analisis operasi, aplikasi dan data kritis **belum dilakukan**		

	Step 25	**Step 29**
Rencana Terdokumentasi	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki perencanaan keberlanjutan bisnis atau operasi darurat, perencanaan pemulihan bencana, perencanaan kemungkinan untuk merespon keadaan darurat yang **terdokumentasi**		**X**
Organisasi memiliki perencanaan keberlanjutan bisnis atau operasi darurat, perencanaan pemulihan bencana, perencanaan kemungkinan untuk merespon keadaan darurat yang **sebagian terdokumentasi.** Beberapa aspek dari perencanaan masih informal dan tidak terdokumentasi	**X**	

Organisasi memiliki perencanaan keberlanjutan bisnis atau operasi darurat, perencanaan pemulihan bencana, perencanaan kemungkinan untuk merespon keadaan darurat yang **informal dan tidak terdokumentasi**		

	Step 25	**Step 29**
Rencana yang Telah Teruji	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **telah secara formal** menguji perencanaan keberlanjutan bisnis atau operasi darurat, perencanaan pemulihan bencana, perencanaan kemungkinan untuk merespon keadaan darurat		**X**
Organisasi **telah secara informal** menguji perencanaan keberlanjutan bisnis atau operasi darurat, perencanaan pemulihan bencana, perencanaan kemungkinan untuk merespon keadaan darurat	**X**	
Organisasi **belum pernah** menguji perencanaan keberlanjutan bisnis atau operasi darurat, perencanaan pemulihan bencana, perencanaan kemungkinan untuk merespon keadaan darurat		

	Step 25	Step 29
Akses Informasi	**Kondisi saat ini**	**Perlu Perubahan**
Akses fisik dan elektronik **ke informasi** kritis **secara formal** diperhitungkan kedalam perencanaan kemungkinan organisasi, pemulihan bencana dan rencan keberlanjutan bisnis	**X**	
Akses fisik dan elektronik **ke beberapa informasi** kritis **secara formal** diperhitungkan kedalam perencanaan kemungkinan organisasi, pemulihan bencana dan rencan keberlanjutan bisnis. Jenis lain dari informasi kritis tidak secara formal diperhitungkan.		
Akses fisik dan elektronik **ke informasi** kritis **secara tidak formal** diperhitungkan kedalam perencanaan kemungkinan organisasi, pemulihan bencana dan rencan keberlanjutan bisnis		

	Step 25	Step 29
Kesadaran Staff	**Kondisi saat ini**	**Perlu Perubahan**
Program pelatihan kesadaran keamanan oleh organisasi **menyertakan** perencanaan kemungkinan organisasi, pemulihan bencana, dan keberlanjutan bisnis. **Pelatihan tersedia**	**X**	

untuk semua staff sebanyak <u>1 kali</u> dalam <u>1 tahun</u>		
Program pelatihan kesadaran keamanan oleh organisasi **menyertakan** perencanaan kemungkinan organisasi, pemulihan bencana, dan keberlanjutan bisnis. **Pelatihan tersedia untuk staff baru sebagai bagian dari masa orientasi.**		
Program pelatihan kesadaran keamanan oleh organisasi **tidak menyertakan** perencanaan kemungkinan organisasi, pemulihan bencana, dan keberlanjutan bisnis. Staff mempelajari hal hal tersebut atas inisiatif sendiri.		

7. KENDALI AKSES FISIK

Status Stop Light : KUNING

	Step 25				**Step 29**		
Pertanggungjawaban *Tugas :*	**Kondisi saat ini**				**Perlu Perubahan**		
	Internal	**External**	**Kombinasi**	**Belum**	**Internal**	**External**	**Kombinasi**
Mengendalikan akses fisik ke dalam bangunan atau tempat tertentu (misal: pengendalian pengujung)	**X**						

Mengendalikan akses fisik ke area kerja (misal: pengendalian staff dan akses pengunjung)	**X**						
Mengendalikan akses fisik terhadap hardware TI	**X**						

	Step 25	**Step 29**
Prosedur *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki **perencanaan dan prosedur** yang secara **formal terdokumentasi** untuk mengendalikan akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI		**X**
Organisasi memiliki **sebagian perencanaan dan prosedur** yang secara **formal terdokumentasi** untuk mengendalikan akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI. Sebagian kebijakan dalam area ini masih informal dan tidak terdokumentasi	**X**	
Organisasi **memiliki perencanaan dan prosedur informal dan tidak terdokumentasi** untuk mengendalikan akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI		

Pelatihan *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff terpilih **dibutuhkan untuk** ikut serta dalam pelatihan yang menyertakan evaluasi perencanaan dan prosedur kendali akses fisik organisasi	**X**	
Staff terpilih **dapat** ikut serta dalam pelatihan yang menyertakan evaluasi perencanaan dan prosedur kendali akses fisik organisasi, **jika yang bersangkutan menginginkannya**		
Organisasi **secara umum tidak menyediakan peluang** bagi staff terpilih untuk menghadiri pelatihan yang menyertakan evaluasi perencanaan dan prosedur kendali akses fisik organisasi. **Staff mempelajari kendali akses fisik atas inisiatif sendiri**		

**Staff terpilih yang dimaksud adalah staff yang telah ditugaskan dalam bidang yang bersangkutan.*

~~**PIHAK KETIGA :**~~

Step 25 **Step 29**

Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi untuk kendali akses fisik telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang		

mengendalikan akses fisik ke bangunan atau tempat tertentu, area kerja, dan hardware TI		
Persyaratan organisasi untuk kendali akses fisik telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang mengendalikan akses fisik ke bangunan atau tempat tertentu, area kerja, dan hardware TI		
Persyaratan organisasi untuk kendali akses fisik **tidak** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang mengendalikan akses fisik ke bangunan atau tempat tertentu, area kerja, dan hardware TI		

	Step 25	**Step 29**
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk kendali akses fisik		
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk kendali akses fisik		
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah		

memenuhi persyaratan untuk kendali akses fisik		

8. MONITORIG DAN AUDIT KEAMANAN FISIK

Status Stop Light : KUNING

	Step 25				**Step 29**		
Pertanggungjawaban *Tugas :*	**Kondisi saat ini**				**Perlu Perubahan**		
	Internal	**External**	**Kombinasi**	**Belum**	**Internal**	**External**	**Kombinasi**
Menyimpan record perawatan unutk mendokumentasikan perbaikan dan modifikasi terhadap hardware TI	**X**						
Memonitor akses fisik untuk mengedalikan hardware TI	**X**						
Memonitor akses fisik pada area kerja terlarang	**X**						
Meninjau record monitoring secara berkala				**X**	**X**		
Menyelidiki dan menangani segala aktifitas yang tidak teridentifikasi	**X**						

	Step 25	Step 29
Prosedur *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi memiliki **perencanaan dan prosedur** yang secara **formal terdokumentasi** untuk monitoring akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI		**X**
Organisasi memiliki **sebagian perencanaan dan prosedur** yang secara **formal terdokumentasi** untuk monitoring akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI. Sebagian kebijakan dalam area ini masih informal dan tidak terdokumentasi		
Organisasi **memiliki perencanaan dan prosedur informal dan tidak terdokumentasi** untuk monitoring akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI	**X**	

	Step 25	Step 29
Pelatihan *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff terpilih **dibutuhkan untuk** ikut serta dalam pelatihan monitoring akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI		

Staff terpilih **dapat** ikut serta dalam pelatihan monitoring akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI, **jika yang bersangkutan menginginkannya**		**X**
Organisasi **secara umum tidak menyediakan peluang** bagi staff terpilih untuk menghadiri pelatihan monitoring akses fisik ke bangunan dan tempat tertentu, area kerja dan hardware TI. **Staff mempelajari monitoring akses fisik atas inisiatif sendiri**	**X**	

**Staff terpilih yang dimaksud adalah staff yang telah ditugaskan dalam bidang yang bersangkutan.*

~~**PIHAK KETIGA :**~~

	Step 25	**Step 29**
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi untuk monitoring keamanan fisik telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memonitor akses fisik ke bangunan atau tempat tertentu, area kerja, dan hardware TI		
Persyaratan organisasi untuk monitoring keamanan fisik telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memonitor akses		

fisik ke bangunan atau tempat tertentu, area kerja, dan hardware TI		
Persyaratan organisasi untuk monitoring keamanan fisik **tidak** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memonitor akses fisik ke bangunan atau tempat tertentu, area kerja, dan hardware TI		

	Step 25	**Step 29**
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk monitoring keamanan fisik		
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk monitoring keamanan fisik		
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk monitoring keamanan fisik		

9. MENEJEMEN SISTEM DAN JARINGAN

Status Stop Light : KUNING

	Step 25				Step 29		
Pertanggungjawaban *Tugas :*	**Kondisi saat ini**				**Perlu Perubahan**		
	Internal	**External**	**Kombinasi**	**Belum**	**Internal**	**External**	**Kombinasi**
Konfigurasi hardware dan software TI			**X**				
Secara aman menyimpan informasi sensitive (misal : penyimpanan backup offline)	**X**						
Mengecek integritas dari software yang terinstal	**X**						
Menjaga sistem agar tetap *up to date* dengan memperhatikan revisi, dan rekomendasi dari konsultan keamanan	**X**						
Membuat dan melacak perubahan pada hardware dan software TI	**X**						
Menejemen password, akun dan hak-hak khusus	**X**						
Memilih tool menejemen sistem dan jaringan				**X**	**X**		

	Step 25	Step 29
Prosedur *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki prosedur** menejemen sistem dan jaringan yang secara **formal terdokumentasikan**		**X**
Organisasi **memiliki sebagian** prosedur menejemen sistem dan jaringan yang secara **formal terdokumentasikan.** Beberapa prosedur dalam area ini masih informal dan tidak terdokumentasikan		
Organisasi **memiliki prosedur** menejemen sistem dan jaringan yang **informal dan tidak terdokumentasikan**	**X**	

	Step 25	Step 29
Pelatihan *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff TI **diperlukan menghadiri** pelatihan untuk menejemen sistem dan jaringan dan menggunakan tool menejemen sistem dan jaringan		**X**
Staff TI **dapat menghadiri** pelatihan untuk menejemen sistem dan jaringan dan menggunakan tool menejemen sistem dan	**X**	

jaringan, **jika yang bersangkutan memintanya**		
Secara umum organisasi **tidak menyediakan peluang** bagi staff TI untuk menghadiri pelatihan menejemen sistem dan jaringan dan menggunakan tool menejemen sistem dan jaringan. **Staff TI mempelajari menejemen sistem dan jaringan atas inisiatif sendiri.**		

**Staff yang dimaksud adalah staff yang telah ditugaskan dalam bidang yang bersangkutan.*

PIHAK KETIGA : Perseorangan

	Step 25	**Step 29**
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi terkait keamanan pada menejemen sistem dan jaringan telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang merawat sistem dan jaringan.		**X**
Persyaratan organisasi terkait keamanan pada menejemen sistem dan jaringan telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang merawat sistem dan jaringan.	**X**	
Persyaratan organisasi terkait keamanan pada menejemen sistem dan jaringan **tidak dikomunikasikan** kepada seluruh kontraktor		

dan penyedia layanan yang merawat sistem dan jaringan.		

	Step 25	**Step 29**
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan terkait keamanan untuk menejemen sistem dan jaringan		**X**
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan terkait keamanan untuk menejemen sistem dan jaringan	**X**	
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan terkait keamanan untuk menejemen sistem dan jaringan		

10. MONITORING DAN AUDIT KEAMANAN TI

Status Stop Light : HIJAU

	Step 25	**Step 29**
Pertanggungjawaban *Tugas :*	**Kondisi saat ini**	**Perlu Perubahan**

	Internal	External	Kombinasi	Belum	Internal	External	Kombinasi
Menggunakan tool monitoring sistem dan jaringan untuk melacak aktifitas sistem dan jaringan	**X**						
Mengadit firewall dan komponen keamana lainnya secara peridok untuk memenuhi kebijakan	**X**						
Menginvestigasi dan menangani segala jenis aktifitas tidak wajar yang tidak teridentifikasi	**X**						

	Step 25	**Step 29**
Prosedur *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki prosedur** untuk memonitoring akses ke jaringan dan sistem berbasis jaringan yang secara **formal terdokumentasikan**		**X**
Organisasi **memiliki sebagian** prosedur untuk memonitoring akses ke jaringan dan sistem berbasis jaringan yang secara **formal terdokumentasikan.** Beberapa prosedur	**X**	

dalam area ini masih informal dan tidak terdokumetasikan		
Organisasi **memiliki prosedur** untuk memonitoring akses ke jaringan dan sistem berbasis jaringan yang **informal dan tidak terdokumentasikan**		

	Step 25	**Step 29**
Pelatihan *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff TI **diperlukan menghadiri** pelatihan untuk monitoring akses berbasis jarigan ke sistem dan jaringan dan menggunakan tool audit dan monitoring	**X**	
Staff TI **dapat menghadiri** pelatihan untuk monitoring akses berbasis jarigan ke sistem dan jaringan dan menggunakan tool audit dan monitoring, **jika yang bersangkutan memintanya**		
Secara umum organisasi **tidak menyediakan peluang** bagi staff TI untuk menghadiri pelatihan monitoring akses berbasis jarigan ke sistem dan jaringan dan menggunakan tool audit dan monitoring **Staff TI mempelajari monitoring sistem dan jaringan atas inisiatif sendiri**		

~~PIHAK KETIGA :~~

	Step 25	**Step 29**
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi untuk monitoring teknologi keamanan informasi telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memonitor sistem dan jaringan		
Persyaratan organisasi untuk monitoring teknologi keamanan informasi telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memonitor sistem dan jaringan		
Persyaratan organisasi untuk monitoring teknologi keamanan informasi **tidak dikomunikasikan** kepada seluruh kontraktor dan penyedia layanan yang memonitor sistem dan jaringan		

	Step 25	Step 29
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk monitoring teknologi keamanan informasi		
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk monitoring teknologi keamanan informasi		
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk monitoring teknologi keamanan informasi		

11. AUTENTIFIKASI dan OTORITASI

Status Stop Light : KUNING

	Step 25				Step 29		
Pertanggungjawaban *Tugas :*	**Kondisi saat ini**				**Perlu Perubahan**		
	Internal	**External**	**Kombinasi**	**Belum**	**Internal**	**External**	**Kombinasi**
Mengimplementasikan kendali akses (misal: perijinan file, konfigurasi jaringan) untuk melerang akses user ke informasi tertentu, sistem sensitive, aplikasi dan layanan tertentu, dan sambungan jaringan	**X**						
Mengimplemetasikan autentifikasi user (misal: password) untuk melarang akses user ke informasi tertentu, sistem sensitive, aplikasi dan layanan tertentu, dan sambungan jaringan	**X**						
Membuat dan memutus akses ke sistem dan informasi baik untuk individu maupun kelompok	**X**						

	Step 25	Step 29
Prosedur *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki** prosedur autentifikasi dan otoritasi untuk melarang akses user ke informasi tertentu, sistem sensitive, aplikasi dan layanan tertentu, dan sambungan jaringan yang secara **formal terdokumentasi**		**X**
Organisasi **memiliki sebagian** prosedur autentifikasi dan otoritasi untuk melarang akses user ke informasi tertentu, sistem sensitive, aplikasi dan layanan tertentu, dan sambungan jaringan yang secara **formal terdokumentasi**. Beberapa prosedur dalam area ini masih informal dan tidak terdokumetasikan	**X**	
Organisasi **memiliki prosedur** untuk melarang akses user ke informasi tertentu, sistem sensitive, aplikasi dan layanan tertentu, dan sambungan jaringan yang **informal dan tidak terdokumentasikan**		

	Step 25	Step 29
Pelatihan *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff TI **diperlukan menghadiri** pelatihan mengimplementasikan tindakan teknologi untuk melarang akses user ke informasi tertentu, sistem sensitive, aplikasi dan layanan tertentu, dan sambungan jaringan	**X**	
Staff TI **dapat menghadiri** pelatihan mengimplementasikan tindakan teknologi untuk melarang akses user ke informasi tertentu, sistem sensitive, aplikasi dan layanan tertentu, dan sambungan jaringan **jika yang bersangkutan memintanya**		
Secara umum organisasi **tidak menyediakan peluang** bagi staff TI untuk menghadiri pelatihan mengimplementasikan tindakan teknologi untuk melarang akses user ke informasi tertentu, sistem sensitive, aplikasi dan layanan tertentu, dan sambungan jaringan **Staff TI mempelajari autentifikasi dan otoritasi atas inisiatif sendiri**		

~~PIHAK KETIGA :~~

	Step 25	**Step 29**
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi untuk mengendalikan akses ke sistem dan informasi telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang menyediakan layanan autentifikasi dan otoritasi.		
Persyaratan organisasi untuk mengendalikan akses ke sistem dan informasi telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang menyediakan layanan autentifikasi dan otoritasi.		
Persyaratan organisasi untuk mengendalikan akses ke sistem dan informasi **tidak dikomunikasikan** kepada seluruh kontraktor dan penyedia layanan yang menyediakan layanan autentifikasi dan otoritasi.		

	Step 25	Step 29
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk autentifikasi dan otoritasi		
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk autentifikasi dan otoritasi		
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk autentifikasi dan otoritasi		

12. MENEJEMEN KERENTANAN

Status Stop Light : ORANYE

	Step 25				**Step 29**		
Pertanggungjawaban *Tugas :*	**Kondisi saat ini**				**Perlu Perubahan**		
	Internal	**External**	**Kombinasi**	**Belum**	**Internal**	**External**	**Kombinasi**
Memilih checklist, script dan tool evaluasi	**X**						
Menjadwalkan dan melakukan evaluasi kerentanan teknologi secara periodik	**X**						
Tetap *up-to-date* dengan tipe-tipe kerentanan dan metode serangan yang telah diketahui			**X**				
Menerapkan hasil dari evaluasi kerentanan teknologi	**X**						
Menangani kerentanan teknologi yang telah teridentifikasi	**X**						
Menjaga penyimpanan yang aman dan disposisi data kerentanan teknologi	**X**						

	Step 25	Step 29
Prosedur *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki** prosedur menejemen kerentanan yang secara **formal terdokumentasi**		**X**
Organisasi **memiliki sebagian** prosedur menejemen kerentanan yang secara **formal terdokumentasi**. Beberapa prosedur dalam area ini masih informal dan tidak terdokumetasikan	**X**	
Organisasi **memiliki prosedur** menejemen kerentanan yang **informal dan tidak terdokumentasikan**		

	Step 25	Step 29
Pelatihan *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff TI **diperlukan menghadiri** pelatihan menejemen kerentanan teknologi dan menggunakan tool evaluasi kerentanan	**X**	
Staff TI **dapat menghadiri** pelatihan menejemen kerentanan teknologi dan menggunakan tool evaluasi kerentanan **jika yang bersangkutan memintanya**		

Secara umum organisasi **tidak menyediakan peluang** bagi staff TI untuk menghadiri pelatihan menejemen kerentanan teknologi dan menggunakan tool evaluasi kerentanan**. Staff TI mempelajari autentifikasi dan otoritasi atas inisiatif sendiri**		

PIHAK KETIGA : Perseorangan

	Step 25	**Step 29**
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi untuk menejemen kerentanan telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memenejemen kerentanan teknologi		**X**
Persyaratan organisasi untuk menejemen kerentanan telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memenejemen kerentanan teknologi	**X**	
Persyaratan organisasi untuk menejemen kerentanan **tidak dikomunikasikan** kepada seluruh kontraktor dan penyedia layanan yang memenejemen kerentanan teknologi		

	Step 25	Step 29
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk menejemen kerentanan		**X**
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk menejemen kerentanan	**X**	
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk menejemen kerentanan		

PIHAK KETIGA : Perusahaan

	Step 25	Step 29
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi untuk menejemen kerentanan telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memenejemen kerentanan teknologi	**X**	

Persyaratan organisasi untuk menejemen kerentanan telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang memenejemen kerentanan teknologi		
Persyaratan organisasi untuk menejemen kerentanan **tidak dikomunikasikan** kepada seluruh kontraktor dan penyedia layanan yang memenejemen kerentanan teknologi		

	Step 25	**Step 29**
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk menejemen kerentanan	**X**	
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk menejemen kerentanan		
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk menejemen kerentanan		

13. ENKRIPSI

Status Stop Light : KUNING

	Step 25				Step 29		
Pertanggungjawaban *Tugas :*	**Kondisi saat ini**				**Perlu Perubahan**		
	Internal	**External**	**Kombinasi**	**Belum**	**Internal**	**External**	**Kombinasi**
Mengimplementasikan teknologi enkripsi untuk melindungi informasi yang secara elektronik tersimpan dan dikelola (misal: enkripsi data, infrastruktur kunci publik)	**X**						
Mengimplementasikan protocol enkripsi untuk pengelolaan sistem, router dan firewall jarak jauh	**X**						

	Step 25	Step 29
Prosedur (jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki** prosedur untuk mengimplematasikan dan menggunakan teknologi enkripsi yang secara **formal terdokumentasi**	**X**	

Organisasi **memiliki sebagian** prosedur untuk mengimplematasikan dan menggunakan teknologi enkripsi yang secara **formal terdokumentasi**. Beberapa prosedur dalam area ini masih informal dan tidak terdokumetasikan		
Organisasi **memiliki prosedur** untuk mengimplematasikan dan menggunakan teknologi enkripsi yang **informal dan tidak terdokumentasikan**		

Step 25 **Step 29**

Pelatihan Staff TI *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff TI **diperlukan menghadiri** pelatihan mengimplementasikan teknologi enkripsi	**X**	
Staff TI **dapat menghadiri** pelatihan mengimplementasikan teknologi enkripsi **jika yang bersangkutan memintanya**		
Secara umum organisasi **tidak menyediakan peluang** bagi staff TI untuk menghadiri pelatihan mengimplementasikan teknologi enkripsi. **Staff TI mempelajari tentang mengimplementasikan teknologi enkripsi atas inisiatif sendiri.**		

	Step 25	Step 29
Pelatihan Staff *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Semua staff **diperlukan menghadiri** pelatihan menggunakan teknologi enkripsi		
Semua staff **dapat menghadiri** pelatihan menggunakan teknologi enkripsi **jika yang bersangkutan memintanya**		**X**
Secara umum organisasi **tidak menyediakan peluang** bagi semua staff untuk menghadiri pelatihan menggunakan teknologi enkripsi. **Staff mempelajari tentang menggunakan teknologi enkripsi atas inisiatif sendiri.**	**X**	

~~**PIHAK KETIGA :**~~

	Step 25	Step 29
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi untuk melindungi informasi sensitif telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang menyediakan teknologi enkripsi		
Persyaratan organisasi untuk melindungi informasi sensitif telah **secara tidak formal**		

dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang menyediakan teknologi enkripsi		
Persyaratan organisasi untuk melindungi informasi sensitif **tidak dikomunikasikan** kepada seluruh kontraktor dan penyedia layanan yang menyediakan teknologi enkripsi		

	Step 25	**Step 29**
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk mengimplementasikan teknologi enkripsi		
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk mengimplementasikan teknologi enkripsi		
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk mengimplementasikan teknologi enkripsi		

14. ARSITEKTUR dan RANCANGAN KEAMANAN

Status Stop Light : KUNING

	Step 25				Step 29		
Pertanggungjawaban *Tugas :*	**Kondisi saat ini**				**Perlu Perubahan**		
	Internal	**External**	**Kombinasi**	**Belum**	**Internal**	**External**	**Kombinasi**
Merancang kendali kamanan pada sistem dan jaringan yang baru dan yang direvisi	**X**						
Mendokumentasikan dan merevisi diagram yang menujukkan arsitektur keamanan organisasi secara luas dan topologi jaringan				**X**			**X**

	Step 25	Step 29
Prosedur *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki** arsitektur dan rancangan praktik keamanan yang secara **formal terdokumentasi**		**X**
Organisasi **memiliki sebagian** arsitektur dan rancangan praktik keamanan yang secara **formal terdokumentasi**. Beberapa prosedur	**X**	

dalam area ini masih informal dan tidak terdokumetasikan		
Organisasi **memiliki** arsitektur dan rancangan praktik keamanan yang **informal dan tidak terdokumentasikan**		

	Step 25	**Step 29**
Pelatihan *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff **diperlukan menghadiri** pelatihan merancang sistem dan jaringan yang aman	**X**	
Staff **dapat menghadiri** pelatihan merancang sistem dan jaringan yang aman **jika yang bersangkutan memintanya**		
Secara umum organisasi **tidak menyediakan peluang** bagi staff untuk menghadiri pelatihan merancang sistem dan jaringan yang aman. **Staff mempelajari tentang mengimplementasikan teknologi enkripsi atas inisiatif sendiri.**		

PIHAK KETIGA : Perusahaan

	Step 25	Step 29
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan terkait keamanan milik organisasi telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang merancang sistem dan jaringan		**X**
Persyaratan terkait keamanan milik organisasi telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang merancang sistem dan jaringan	**X**	
Persyaratan terkait keamanan milik organisasi telah **tidak dikomunikasikan** kepada seluruh kontraktor dan penyedia layanan yang merancang sistem dan jaringan		

	Step 25	Step 29
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk arsitektur dan rancangan keamanan	**X**	
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah		

memenuhi persyaratan untuk arsitektur dan rancangan keamanan		
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk arsitektur dan rancangan keamanan		

15. PENGELOLAAN INSIDEN

Status Stop Light : MERAH

	Step 25				**Step 29**		
Pertanggungjawaban *Tugas :*	Kondisi saat ini				**Perlu Perubahan**		
	Internal	**External**	**Kombinasi**	**Belum**	**Internal**	**External**	**Kombinasi**
Mendokumentasikan dan merevisi prosedur untuk mengidentifikasi, melaporkan dan merespon dugaan insiden dan pelanggaran				**X**	**X**		
Mendokumetasikan dan merevisi kebijakan dan prosedur untuk bekerjasama dengan pihak penegak hukum				**X**	**X**		
Menguji prosedur pengelolaan insiden secara periodik	**X**						

	Step 25	Step 29
Prosedur *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi **memiliki** prosedur pengelolaan insiden yang secara **formal terdokumentasi**		**X**
Organisasi **memiliki sebagian** prosedur pengelolaan insiden yang secara **formal terdokumentasi**. Beberapa prosedur dalam area ini masih informal dan tidak terdokumetasikan	**X**	
Organisasi **memiliki** prosedur pengelolaan insiden yang **informal dan tidak terdokumentasikan**		

Pelatihan *(jika staf dari organisasi separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Staff terpilih **diperlukan menghadiri** pelatihan pengeloalaan insiden	**X**	
Staff terpilih **dapat menghadiri** pelatihan pengeloalaan insiden, **jika yang bersangkutan memintanya**		

Secara umum organisasi **tidak menyediakan peluang** bagi staff terpilih untuk menghadiri pelatihan pengeloalaan insiden. **Staff mempelajari tentang mengimplementasikan teknologi enkripsi atas inisiatif sendiri.**		

**Staff terpilih yang dimaksud adalah staff yang telah ditugaskan dalam bidang yang bersangkutan.*

~~PIHAK KETIGA :~~

	Step 25	**Step 29**
Permasalahan Kolaborasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Persyaratan organisasi untuk mengelola insiden telah **secara formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang menyediakan layanan pengelolaan insiden		
Persyaratan organisasi untuk mengelola insiden telah **secara tidak formal** dikomunikasikan kepada seluruh kontraktor dan penyedia layanan yang menyediakan layanan pengelolaan insiden		
Persyaratan organisasi untuk mengelola insiden telah **tidak dikomunikasikan** kepada seluruh kontraktor dan penyedia layanan yang menyediakan layanan pengelolaan insiden		

	Step 25	Step 29
Verifikasi *(jika pihak ketiga separuhnya atau sepenuhnya bertanggungjawab pada area ini)*	**Kondisi saat ini**	**Perlu Perubahan**
Organisasi secara **formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk mengelola insiden		
Organisasi secara **tidak formal** memverfikasi bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk mengelola insiden		
Organisasi **tidak memverfikasi** bahwa kontraktor dan penyedia layanan telah memenuhi persyaratan untuk mengelola insiden		

LAMPIRAN 10

MITIGATION PLAN WORKSHEET

Catatan	**Step**
	28
Mitigation Plan Worksheet disesuaikan dengan kebutuhan DINKOMINFO untuk mengevaluasi risiko tidak hanya dari cabang pohon risiko yang terbentuk (step 12, 13, 14, 15, 16, 22, 24, 26, 27) tetapi evaluasi risiko juga dilakukan untuk setiap kelemahan atau risiko yang teridentifikasi pada beberapa worksheet yang telah dibentuk. Nomor evaluasi yang terdapat dalam *worksheet* ini tidak menentukan prioritas evaluasi. Evaluasi yang dilakukan untuk setiap area praktik keamanan (step 3, 4, 25, 29) adalah evaluasi diluar evaluasi yang telah terekam dalam *Security Practise Worksheet* (step 3a,3b dan step 4) dan *Protection Strategy Worksheet* (step 25 dan 29)	

No. Evaluasi	001
Objek Evaluasi	Area dampak : Denda dan hukum yang berlaku
Worksheet	Impact Evaluation Criteria Worksheet
Penanggungjawab	Kepala Dinas

Aktivitas Evaluasi	**Rasionalisasi**
1. Pemberlakuan sanksi dan atau denda terhadap setiap pelanggaran terhadap SOP, undang-undang atau undang-undang teknologi informasi.	Hukum atau undang-undang yang berlaku dapat menjadi perisai bagi organisasi dalam menjalankan tugasnya dari serangan-serangan terhadap organisasi, baik serangan

2. Menyiapkan organisasi untuk bekerjasama dengan pihak penegak hukum 3. Menyiapkan organisasi untuk menerima sanksi sesuai peraturan apabila organisasi melakukan pelanggaran dalam melaksanakan tugasnya.	dari luar organisasi maupun serangan dari dalam organisasi yang bertujuan untuk merusak proses bisinis atau layanan yang disediakan organisasi
Pendukung tambahan	
Pemberlakuan sanksi dan atau denda perlu adanya dukungan dan komitmen dari pihak menejemen (atasan). Hal ini juga menuntut adanya pelaporan dan kerjasama yang baik dengan pihak penegak hukum.	

No. Evaluasi	002
Objek Evaluasi	Area dampak : Kesehatan
Worksheet	Impact Evaluation Criteria Worksheet
Penanggungjawab	Subag. Umum dan Kepegawaian
Aktivitas Evaluasi	**Rasionalisasi**
1. Peninjauan terhadap standart keselamatan kerja (K3) staff. 2. Pembaharuan terhadap K3 jika diperlukan 3. Pendokumentasian formal dan pengesahan K3 setelah terjadi revisi atau pembaharuan.	Staff (SDM) adalah salah satu aset yang dimiliki oleh organisasi dan sudah selayaknya kesehatan dan keselamatan kerja menjadi hak masing-masing staff.
Pendukung tambahan	

Standart yang telah ditetapkan oleh Subag. Umum dan Kepegawaian selayaknya mendapatkan dukungan dari masing-masing Kepala Bagian. Pelanggaran terhadap standart K3 dapat langsung dievaluasi oleh Kepala Bagian. Jika memang dibutuhkan untuk menambah *safety tools* , maka hal ini perlu adanya dukungan pendanaan dari pihak menejemen.

No. Evaluasi	003
Objek Evaluasi	Pendokumentasian aset organisasi
Worksheet	Asset Identification Worksheet
Penanggungjawab	Subag. Umum dan Kepegawaian Bid. Persandian & Aplikasi Informatika

Aktivitas Evaluasi	**Rasionalisasi**
1. Pendataan secara formal terkait aset SDM organisasi lengkap dengan data *skill* dan sertifikasi setiap staff. 2. Pendataan secara formal terkait aset sistem dan informasi yang dimiliki oleh organisasi, lengkap dengan sejarah dibangunnya, data yang terdapat dalam sistem, dan dimana sistem ini berada.	Adanya pendataan aset SDM dalam organsasi dapat memudahkan organisasi untuk menentukan *skill* apa yang sedang dibutuhkan organisasi jika terjadi mutasi staff atau pengembangan organisasi. Adanya pendataan aset sistem dapat membatu organisasi setiap kali ada evaluasi dari pusat, dengan menyajikan data yang menunjukkan seberapa baik kualitas layanan organisasi.
Pendukung tambahan	

Pendataan aset SDM harus diikuti oleh semua staff, dalam hal ini staff diminta memberikan data yang bersih, termasuk melampirkan sertifikasi yang dimiliki staff untuk menunjukkan *skill* yang dimiliki. Setiap dokumen hasil pendataan harus mendapatkan legalitas / persetujuan dari pihak menejemen.

No. Evaluasi	004
Objek Evaluasi	Kesadaran keamanan dan pelatihan
Worksheet	Security Practise Worsheet Protection Strategy Worksheet
Penanggungjawab	Bid. Persandian & Aplikasi Informatika

Aktivitas Evaluasi	**Rasionalisasi**
1. Penambahan pelatihan bagi staff terkait dengan materi-materi keamanan informasi. 2. Pemilihan pelatihan diusahakan adalah pelaithan yang bersertifikat.	Penambahan pelatihan bagi staff akan memperdalam pemahaman dan *skill* yang dimiliki masing-masing staff. Adanya sertifikat menunjukkan bahwa staff terkait telah memenuhi standart tertentu dan memudahkan organisasi dalam melacak jenis-jenis pelaithan yang pernah diberikan kepada staff.

Pendukung tambahan
Penambahan frekuensi pelatihan dan pemilihan pelatihan yang tepat perlu adanya dukungan menejer dan pendanaan yang disesuaikan dengan kebutuhan organisasi

No. Evaluasi	005
Objek Evaluasi	Regulasi dan Kebijakan Keamanan
Worksheet	Security Practise Worsheet Protection Strategy Worksheet
Penanggungjawab	Kepala Dinas

Aktivitas Evaluasi	**Rasionalisasi**
1. Pembentukan kerjasama yang baik dengan pihak-pihak penegak hukum untuk menegakkan kebijakan 2. Pemberlakuan sanksi internal jika terjadi pelanggaran	Penegakan kebijakan akan lebih efektif jika didukung oleh badan hukum atau penegak hukum.
Pendukung tambahan	
Semua staff harus tunduk dan patuh terhadap regulasi dan kebijakan yang berlaku dan siap menerima sanksi apabila melanggar	

No. Evaluasi	006
Objek Evaluasi	Rencana Kemungkinan / Pemulihan Bencana
Worksheet	Security Practise Worksheet Protection Strategy Worksheet
Penanggungjawab	Kepala Dinas Subag Umum dan Kepegawaian

Aktivitas Evaluasi	**Rasionalisasi**
1. Pembentukan tim pemulihan bencana harus dilakukan sesingkat mungkin setelah bencana terjadi	Pembentukan tim dalam waktu yang singkat dapat mempercepat penanganan bencana dan dengan komposisi tim yang berasal tidak dari

2. Tim yang terbentuk harus terdiri dari beberapa bidang keahlian dengan mempertimbangkan *skill* dari masing-masing anggota tim	satu bidang memungkinkan pemulihan bencana dari berbagai aspek.
Pendukung tambahan	
Pembentukan tim perlu rekomendasi dan dukungan dari maasing-masing Kepala Bagian yang ikut ambil peran dalam penanganan bencana	

No. Evaluasi	007
Objek Evaluasi	Kendali Akses Fisik
Worksheet	Security Practise Worksheet Protection Strategy Worksheet
Penanggungjawab	Kepala Dinas
Aktivitas Evaluasi	**Rasionalisasi**
1. Pembentukan satuan keamanan pada beberapa area sensitif, jika diperlukan 2. Pembentukan dan peninjauan log akses pada area sensitif.	Satuan keamanan mungkin dibutuhkan untuk menjaga beberapa area sensitif, guna memberikan rasa aman.
Pendukung tambahan	
Penambahan SDM satuan keamanan perlu dikomunikasikan dengan Subag. Umum dan Kepegawaian dan pendanaan yang mencukupi.	

No. Evaluasi	008
Objek Evaluasi	Menejemen Sistem dan Jaringan
Worksheet	Security Practise Worksheet Protection Strategy Worksheet
Penanggungjawab	Seksi Investigasi dan Pelaporan (rekomendasi no : 011)

Aktivitas Evaluasi	**Rasionalisasi**
1. Pembentukan kerjasama dengan pihak ketiga yang bergerak dibidang *assessment* sistem dan atau jaringan	Kerjasama dapat meringankan aktifitas penilaian sistem dan atau jaringan, sehingga Bid. Investigasi dan Pelaporan dapat lebih focus menangani permasalahan internal organisasi yang lain. Pihak ketiga yang kredibel juga menjamin hasil yang optimum dari penilaian sistem dan atau jaringan.

Pendukung tambahan
Pemahaman dan dukungan dari kepala dinas untuk *assessment* dibutuhkan agar aktifitas ini dapat berjalan

No. Evaluasi	009
Objek Evaluasi	Monitoring dan Audit Keamanan TI
Worksheet	Security Practise Worksheet Protection Strategy Worksheet
Penanggungjawab	Seksi Investigasi dan Pelaporan (rekomendasi no : 011)

Aktivitas Evaluasi	Rasionalisasi
1. Pembentukan kerjasama dengan pihak ketiga yang bergerak dibidang *assessment* keamanan dan risiko teknologi informasi	Kerjasama dapat meringankan aktifitas penilaian keamanan dan risiko teknologi informasi, sehingga Bid. Investigasi dan Pelaporan dapat lebih focus menangani permasalahan internal organisasi yang lain. Pihak ketiga yang kredibel juga menjamin hasil yang optimum dari penilaian keamanan dan risiko informasi
Pendukung tambahan	
Pemahaman dan dukungan dari kepala dinas untuk *assessment* dibutuhkan agar aktifitas ini dapat berjalan	

No. Evaluasi	010
Objek Evaluasi	Enkripsi
Worksheet	Security Practise Worksheet Protection Strategy Worksheet
Penanggungjawab	Bid. Persandian & Aplikasi Informatika

Aktivitas Evaluasi	Rasionalisasi
1. Melakukan uji coba penetrasi sistem yang telah menerapkan enkripsi. 2. Membuat dan memfervikasi laporan hasil uji penetrasi sistem	Uji penetrasi akan membuktikan apakah protokol enkripsi yang diterapkan sudah memenuhi level keamanana yang dibutuhkan oleh organisasi
Pendukung tambahan	

Bid. Persandian & Aplikasi Informatika dapat membangun kerjasama secara profesional dengan perseorangan maupun organisasi (pihak ketiga) yang menyediakan jasa uji penetrasi sistem lengkap dengan hasil dan rekomendasi hasil uji penetrasi.

No. Evaluasi	011
Objek Evaluasi	Pengeloaan Insiden
Worksheet	Security Practise Worksheet Protection Strategy Worksheet
Penanggungjawab	Kepala Dinas

Aktivitas Evaluasi	**Rasionalisasi**
1. Pemecahan Subag. Perencanaan, Evaluasi, dan Pelaporan 2. Pembentukan Seksi Investigasi dan Pelaporan. 3. Penetapan tugas pokok dan fungsi Seksi Investigasi dan Pelaporan 4. Penetapan wewenang dan kewajiban Seksi Investigasi dan Pelaporan.	Pemecahan Subag. Perencanaan, Evaluasi dan Pelaopran dapat memfokuskan kinerja subag ini kedalam perencanaan, untuk evaluasi, investigasi dan pelaporan terkait perencanaan yang telah dibuat dapat dikerjakan oleh Seksi Investigasi dan Pelaporan. Seksi Investigasi dan Pelaporan ditempatkan pada masing-masing bidang, karena masing-masing bidang tersebut memiliki karakter permasalahan yang berbeda untuk diinvestigasi. Seksi ini juga harus diberikan garis koordinasi dengan Kepala Dinas dan Subag.

<table>
<tr><td></td><td>Perencanaan agar dapat melaporkan insiden secara langsung</td></tr>
<tr><td colspan="2">Pendukung tambahan</td></tr>
<tr><td colspan="2">Penambahan SDM dan pembentukan seksi baru dikomunikasikan dengan Subag, Umum dan Kepegawaian dan masing-masing kabid dan kasek dalam satu rapat, sehingga keputusan dapat didokumentasikan secara formal.</td></tr>
<tr><td>No. Evaluasi</td><td>012</td></tr>
<tr><td>Objek Evaluasi</td><td>Integrity</td></tr>
<tr><td>Worksheet</td><td>Critical Asset Information Worksheet for System</td></tr>
<tr><td>Penanggungjawab</td><td>Bid. Persandian & Aplikasi Informatika</td></tr>
<tr><td>Aktivitas Evaluasi</td><td>Rasionalisasi</td></tr>
<tr><td>1. Pengembangan sistem penjadwalan rapat atau koordinasi dan sistem notulensi yang nantinya terintegrasi dengan sistem Tele-Presence
2. Penegakan rule sistem mengenai siapa yang dapat mengakses informasi pada level konferensi yang berbeda.</td><td>Integrasi antara sistem penjadwalan, sistem tele-presence, dan sistem notulensi memberikan data yang lengkap mengenai agenda rapat, mulai dari pra acara, pelaksanaan, dan pasca acara.
Kebutuhan evaluasi hasil koordinasi dapat dimudahkan dengan adanya data koordinasi yang terintegrasi.
Sistem notulensi juga dapat digunakan untuk mencatat hasil koordinasi diluar penggunaan sistem tele-presence</td></tr>
<tr><td colspan="2">Pendukung tambahan</td></tr>
</table>

Seksi Pengembangan Aplikasi Informatika perlu mengadakan koordinasi dengan Bid. Persandian & Aplikasi Informatika untuk menetukan kebutuhan awal sistem yang akan dikembangkan, terutama kebutuhan keaman sistem. Hal ini juga perlu dukungan pendanaan yang sesuai dengan porsi pekerjaan yang dilakukan.

No. Evaluasi	013
Objek Evaluasi	Availability
Worksheet	Critical Asset Information Worksheet for System
Penanggungjawab	Bid. Infrastruktur Teknologi Informasi dan Komunikasi

Aktivitas Evaluasi	**Rasionalisasi**
1. Pemilihan penyedia jasa layanan internet (ISP) yang baru jika gangguan jaringan internet semakin rutin terjadi	Gangguan jaringan (dari pihak ketiga) tidak dapat ditangani secara langsung oleh organisasi, sejauh ini hanya complain.
2. Jika dimungkinkan, organisasi dapat memiliki jaringan miliki pribadi (yang mendukung berjalannya sistem tele-presence) yang dikelola secara mandiri.	Adanya jaringan mandiri miliki organisasi lebih menjamin keberlangsungan sistem, karena setiap permasalahan yang terjadi dapat secara langsung ditangani, baik ditangani oleh internal, maupun kolaborasi dengan pihak ketiga yang menyediakan jasa evaluasi dan perbaikan jaringan.
Pendukung tambahan	

Seksi Pengembangan Infrastruktur Teknologi Informasi dan Komunikasi harus mendapatkan dukungan pendanaan yang mencukupi jika organisasi memutuskan untuk membangun jaringan mandiri

No. Evaluasi	014
Objek Evaluasi	Basic Risk Profile – Human Actors Using Network Access Aktor : internal Motif : tidak disengaja Hasil : terpapar ; terganggu
Worksheet	Risk Profile Worksheet
Penanggungjawab	Seksi Pemberdayaan Aplikasi Informatika

Aktivitas Evaluasi	**Rasionalisasi**
1. Penyusunan dan verifikasi SOP pelaksanaan koordinasi menggunakan sistem Tele-Presence. 2. Pelatihan ulang staff (user sistem) disesuaikan dengan SOP baru mengenai pelaksanaan koordinasi menggunakan sistem Tele-Presence	SOP pelaksanaan koordinasi akan menjelaskan tata cara penggunaan sistem beserta penggunaan fitur yang dibutuhkan secara formal. SOP juga dapat mengidentifikasi kebutuhan dan langkah-langkah yang perlu dilakukan pra kegiatan koordinasi yang dapat menjadi acuan staff dalam menjalankan sistem Tele-Presence untuk koordinasi.

Pendukung tambahan
Pengadaan pelatihan terkait SOP baru harus tepat sasaran. Hal ini membutuhkan dukungan dari pihak menejemen yang secara formal terdokumentasikan. Pelatihan juga membutuhkan pendanaan kegiatan sesuai dengan bobot pelatihan.

No. Evaluasi	015
Objek Evaluasi	Basic Risk Profile – Human Actors Using Network Access Aktor : internal Motif : tidak disengaja Hasil : rusak
Worksheet	Risk Profile Worksheets
Penanggungjawab	Bid. Persandian & Aplikasi Informatika

Aktivitas Evaluasi	**Rasionalisasi**
1. Penyimpanan dan pencadangan data koordinasi virtual secara periodik 2. Pengadaan pelatihan tambahan jika risiko ini terus terulang	Penyimpanan dan pencadangan data koordinasi ke penyimpanan yang aman dapat menyelamatkan data terkait koordinasi meskipun data secara tidak sengaja terhapus dari sistem.

Pendukung tambahan
Pemahaman dari pihak menejemen mengenai pencadangan data penting menentukan berjalnnya aktivitas evaluasi ini.

No. Evaluasi	016
Objek Evaluasi	Basic Risk Profile – Human Actors Using Network Access Aktor : internal Motif : disengaja Hasil : modifikasi ; rusak

Worksheet	Risk Profile Worksheets
Penanggungjawab	Seksi Investigasi dan Pelaporan
Aktivitas Evaluasi	**Rasionalisasi**
1. Penegakan hukum atau pemberlakuan sanksi terhadap staff yang dengan sengaja melakukan modifikasi atau merusak sistem dengan tujuan tertentu. 2. Investigasi dan pembuatan laporan yang secara formal diverifikasi.	Hukuman atau sanksi yang berlaku dapat mengurangi kemungkinan terjadinya risiko ini. Investigasi dan pembuatan laporan dapat membantu dalam mengevaluasi bagaimana risiko ini terjadi, sehingga langkah peningkatan keamanan dapat dilakukan di masa mendatang.
Pendukung tambahan	
Kerjasama dengan pihak penegak hukum dapat melancarkan jalannya sanksi yang memberikan efek jera pada aktor.	

No. Evaluasi	017
Objek Evaluasi	Basic Risk Profile – Human Actors Using Network Access Aktor : eksternal Motif : disengaja Hasil : terpapar ; terganggu
Worksheet	Risk Profile Worksheets
Penanggungjawab	Seksi Pengembangan Aplikasi Informatika
Aktivitas Evaluasi	**Rasionalisasi**

1. Penerapan sejumlah teknik enkripsi pada data yang tersimpan.	Enkripsi membuat penyerang (hacker) kesusahan dalam menterjemahkan data, meskipun serangan telah berhasil dilakukan
Pendukung tambahan	
Pendanaan dibutuhkan terkait dengan teknologi enkripsi yang akan diterapkan	

No. Evaluasi	018
Objek Evaluasi	Basic Risk Profile – Human Actors Using Network Access Aktor : eksternal Motif : disengaja Hasil : modifikasi ; rusak
Worksheet	Risk Profile Worksheets
Penanggungjawab	Bid. Persandian & Aplikasi Informatika
Aktivitas Evaluasi	**Rasionalisasi**
1. Koordinasi dengan pemilik dan pengembang aplikasi 2. Membuat laporan resmi mengenai serangan yang terjadi dan dampak yang diterima 3. Menyerahkan perbaikan sistem dan meminta revisi sistem sesuai dengan kesepakatan oraganisasi dengan pengembang sistem	Sistem dan aplikasi ini sebenarnya dikembangkan oleh pihak ketiga. Penanganan permaslahan terkait risiko yang muncul pada evaluasi ini dapat dikerjasamakan dengan pengembang sistem, sesuai kesepakatan organisasi.

Pendukung tambahan
Seksi Investigasi dan Pelaporan dari berbagai bidang dibutuhkan untuk bekerjasama dalam penginvestigasian dan pembuatan laporan resmi.

No. Evaluasi	019	
Objek Evaluasi	Basic Risk Profile – Human Actors Using Physical Access Aktor : internal Motif : tidak disengaja Hasil : terpapar ; modifikasi ; rusak ; terganggu	
Worksheet	Risk Profile Worksheets	
Penanggungjawab	Seksi Pemberdayaan Aplikasi Informatika	
Aktivitas Evaluasi		**Rasionalisasi**
1. Pembentukan peraturan dan SOP untuk penggunaan PC dan area kerja. 2. Pembentukan SOP untuk fungsi dasar keamanan PC 3. Pembentukan SOP perubahan konfigurasi PC pada area kerja 4. Penyesuaian PC dan area kerja dengan SOP terkait pengelolaan aset dan area kerja		SOP dapat memberikan informasi secara terperinci mengenai bagaimana penggunaan aset pada are kerja dan menjelaskan kebutuhan dasar konfigurasi PC pada area kerja terkait keamanan yang dibutuhkan. Penyesuaian PC dengan standart (SOP) yang baru dapat menghindari dampak risiko pada cabang pohon risiko ini.
Pendukung tambahan		

Pembentukan SOP perubahan konfigurasi PC perlu adanya pengawasan dari Bid. Persandian dan Aplikasi Informatika. Penyesuaian atau konfigurasi PC terkait kebutuhan keamanan pada area kerja perlu dilakukan diluar hari kerja dengan pengawasan dari Bid. Persandian & Aplikasi Informatikan untuk memastikan tidak ada data organisasi maupun data pribadi yang hilang selama proses konfigurasi.

No. Evaluasi	020
Objek Evaluasi	Basic Risk Profile – Human Actors Using Physical Access Aktor : internal Motif : disengaja Hasil : modifikasi
Worksheet	Risk Profile Worksheet
Penanggungjawab	Bid. Presandian & Aplikasi Informatika Bid. Infrastruktur Teknologi Informasi dan Komunikasi

Aktivitas Evaluasi	**Rasionalisasi**
1. Pendokumentasian secara formal mengenai spesifikasi server 2. Pembuatan log aktifitas terkait server (misal: *upgrade*, konfigurasi, perbaikan perangkat,dll) 3. Penetapan sanksi internal apabila terjadi pelanggaran.	Dokumentasi spesifikasi server dapat memberikan informasi kemampuan server dari sisi hardware, informasi aplikasi yang telah terinstal, dan data yang dikelola. Dokumentasi ini memudahkan identifikasi kebutuhan *upgrade* server. Log aktifitas memudahkan pelacakan pertanggung jawaban ketika terjadi modifikasi

	Sanksi yang diberikan dapat memberikan efek jera.
Pendukung tambahan	
Peraturan harus ditaati oleh semua pihak atau staff yang mengakses server secara fisik.	

No. Evaluasi	021
Objek Evaluasi	Basic Risk Profile – Human Actors Using Physical Access Aktor : internal Motif : disengaja Hasil : rusak
Worksheet	Risk Profile Worksheet
Penanggungjawab	Seksi Investigasi dan Pelaporan (rekomendasi no : 011)
Aktivitas Evaluasi	**Rasionalisasi**
1. Investigasi formal dan pendokumentasian hasil investigasi. 2. Pelaporan secara formal terkait pelanggaran yang terjadi untuk ditindak lanjuti 3. Penegakan sanksi dengan dukungan pihak penegak hukum jika diperlukan	Kerusakan yang terjadi diinvestigasi, dan dilaporkan untuk mengurangi munculnya risiko ini di masa mendatang, meskipun dampak kerusakan telah terlanjur dirasakan oleh organisasi.
Pendukung tambahan	

Kerjasama dengan pihak penegak hukum jika pelanggaran yang terjadi terkait suatu kebijakan atau peraturan perundang-undangan.

No. Evaluasi	022
Objek Evaluasi	Basic Risk Profile – Human Actors Using Physical Access Aktor : internal Motif : disengaja Hasil : terganggu
Worksheet	Risk Profile Worksheet
Penanggungjawab	Seksi Investigasi dan Pelaporan (rekomendasi no : 011)

Aktivitas Evaluasi	**Rasionalisasi**
1. Pemantauan dan pengawasan terhadap setiap aktifitas terkait server (misal: konfigurasi, *upgrade*) 2. Pemantauan dan pengawasan terhadap log aktifitas terkait server	Pengawasan dilakukan selama aktifitas terkait server berlangsung, sehingga setiap modifikasi dapat dipastikan sesuai dengan yang direncanakan, dan memastikan bahwa sistem dapat terus memberikan askses ketika dibutuhkan.

Pendukung tambahan
Bid. Presandian & Aplikasi Informatika dan Bid. Infrastruktur Teknologi Informasi dan Komunikasi bekerjasama untuk memberikan wewenang kepada Seksi Investigasi dan Pelaporan untuk mengambil tindakan yang diperlukan ketika menemui aktifitas yang mencurigakan.

No. Evaluasi	023
Objek Evaluasi	Basic Risk Profile – System Problem Aktor : kegagalan sistem Hasil : terganggu
Worksheet	Risk Profile Worksheet
Penanggungjawab	Seksi Investigasi dan Pelaporan (rekomendasi no : 011)

Aktivitas Evaluasi	**Rasionalisasi**
1. Pengecekan *Backup* sebelum melakukan perubahan pada sistem atau server 2. *Rolling Back Action* ketika perubahan pada sistem gagal berjalan. 3. Pendokumentasian laporan terkait kegagalan perubahan yang terjadi	Adanya *Backup* sistem dapat mengembalikan kondisi jika aktifitas perubahan terhadap sistem atau server mengalami kegagalan. Laporan yang didokumentasikan memberikan review permasalahan yang terjadi, sehingga permasalahan dapat dikaji.

Pendukung tambahan
Bid. Presandian & Aplikasi Informatika dan Bid. Infrastruktur Teknologi Informasi dan Komunikasi diperlukan untuk melakukan eksekusi *backup* dan *rolling back action*, sementara Seksi Investgasi dan Pelaporan bertanggungjawab untuk memastikan bahwa sistem dapat berjalan seperti sebelum terjadinya aktifitas perubahan.

No. Evaluasi	024
Objek Evaluasi	Basic Risk Profile – System Problem Aktor : kecacatan hardware Hasil : rusak ; terganggu
Worksheet	Risk Profile Worksheet

Penanggungjawab	Bid. Persandian & Aplikasi Informatika Bid. Infrastruktur Teknologi Informasi dan Komunikasi

Aktivitas Evaluasi	**Rasionalisasi**
1. Evaluasi spesifikasi hardware yang dibutuhkan dengan meninjau *record* hardware. 2. Perencanaan pembelian atau perbaikan hardware yang disesuaikan dengan kebutuhan 3. Pengawasan pada proses pengadaan hardware atau perbaikan hardware 4. Pendokumentasian aktifitas pembelian atau perbaikan	Kecacatan hardware biasanya terjadi karena kurangnya evaluasi kebutuhan dan peninjauan spesifikasi hardware yang dimiliki, sebelum pengadaan hardware atau perbaikan hardware dan kurangnya pengwasan saat pengadaan hardware.

Pendukung tambahan
Kebutuhan secara mendetail mengenai sepsifikasi hardware terkait sistem atau aplikasi dapat dibantu oleh Seksi Pengembangan Aplikasi Informatika. Kebutuhan secara mendetail mengenai spesifikasi hardware terkait jaringan dapat dibantu oleh Seksi Pengembangan & Pengawasan Infrastruktur Jaringan. Pengadaan hardware juga membutuhkan dukungan dar Subag. Keuangan, terkait alokasi dana oleh organisasi.

No. Evaluasi	025
Objek Evaluasi	Basic Risk Profile – System Problem Aktor : kode berbahaya Hasil : terpapar ; terganggu
Worksheet	Risk Profile Worksheet
Penanggungjawab	Seksi Pengembangan Aplikasi Informatika

Aktivitas Evaluasi	Rasionalisasi
1. Penerapan aktivitas evaluasi mereferensi evaluasi no 017	Kode berbahaya merupakan objek atau tipe serangan yang berasala dari pihak eksternal, sehingga penanganan dapat dilakukan dengan mereferensi aktifitas evaluasi pada evaluasi no 017
Pendukung tambahan	

No. Evaluasi	026
Objek Evaluasi	Basic Risk Profile – System Problem Aktor : kode berbahaya Hasil : modifikasi ; rusak
Worksheet	Risk Profile Worksheet
Penanggungjawab	Seksi Pengembangan Aplikasi Informatika

Aktivitas Evaluasi	Rasionalisasi
1. Penerapan aktivitas evaluasi mereferensi evaluasi no 018	Kode berbahaya merupakan objek atau tipe serangan yang berasala dari pihak eksternal, sehingga penanganan dapat dilakukan dengan mereferensi aktifitas evaluasi pada evaluasi no 018
Pendukung tambahan	

No. Evaluasi	027
Objek Evaluasi	Basic Risk Profile – Other Problem Aktor : permasalahan power supply Hasil : terganggu
Worksheet	Risk Profile Worksheet
Penanggungjawab	Seksi Pengembangan Aplikasi Informatika

Aktivitas Evaluasi	**Rasionalisasi**
1. Penyediaan unit *emergency power supply*. 2. Penetapan standart (SOP) jika permaslahan terjadi dalam durasi yang berbeda.	Unit *emergency power supply* pada beberapa server atau aset tertentu dapat menjaga sistem agar berjalan untuk beberapa waktu. SOP dibuat untuk menangani permasalahan dengan durasi waktu yang berbeda, dengan mempertimbangkan kemampuan unit *emergency power supply*.

Pendukung tambahan
Pendanaan yang mencukupi dibutuhkan untuk pengadaan unit *emergency power supply* sesuai dengan kebutuhan organisasi.

No. Evaluasi	028
Objek Evaluasi	Basic Risk Profile – Other Problem Aktor : permasalahan telekomunikasi dan ketidaktersediaan Hasil : terganggu
Worksheet	Risk Profile Worksheet
Penanggungjawab	Bid. Infrastruktur Teknologi Informasi dan Komunikasis

Aktivitas Evaluasi	**Rasionalisasi**
1. Penyampaian *complain* kepada pihak ketiga penyedia layanan jaringan atau internet	Layanan internet yang digunakan untuk mengakses sistem atau menjalankan konferensi adalah layanan kerjasama dengan pihak *Internet Service Provider*. Maka permasalahan ketidaktersediaan jaringan internet sepenuhnya dapat disampaikan kepada pihak ketiga yang bersangkutan.

Pendukung tambahan

No. Evaluasi	029
Objek Evaluasi	Basic Risk Profile – Other Problem Aktor : konfigurasi fisik Hasil : modifikasi ; rusak

Worksheet	Risk Profile Worksheet
Penanggungjawab	Kepala Dinas

Aktivitas Evaluasi	**Rasionalisasi**
1. Pembentukan satuan keamanan dan log akses serta peninjauan log akses (evaluasi no 007) 2. Pengawasan pada area-area sensitive yang dimiliki organisasi	Satuan keamanan dapat mengendalaikan pihak yang memasuki area sensitf dan jika evaluasi ini digabungkan dengan evaluasi akses fisik aset (evaluasi no 020 dan 021) maka dampak dapat sepenuhnya dihindari.

Pendukung tambahan
Penambahan SDM satuan keamanan perlu dikomunikasikan dengan Subag. Umum dan Kepegawaian dan pendanaan yang mencukupi.

No. Evaluasi	030
Objek Evaluasi	Basic Risk Profile – Other Problem Aktor : bencana alami Hasil : rusak
Worksheet	Risk Profile Worksheet
Penanggungjawab	Seksi Investigasi dan Pelaporan

Aktivitas Evaluasi	**Rasionalisasi**
1. Pendokumentasian bencana yang terjadi secara medetail	Dampak bencana tidak dapat dikurangi, namun dengan adanya laporan atau *record* diharapkan pada masa yang akan datang bencana dapat dihindari.

Pendukung tambahan
Seluruh staff dibutuhkan bekerjasama untuk memberikan gambaran dan laporan yang akurat mengenai bencana yang terjadi dan kerugian yang diderita.

No. Evaluasi	031
Objek Evaluasi	Storage Device
Worksheet	Network Access Path Worksheet
Penanggungjawab	Bid. Infrastruktur Teknologi Informasi dan Komunikasi Seksi Pengeloalaan Data Center

Aktivitas Evaluasi	**Rasionalisasi**
1. Pengadaan perangkat penyimpanan untuk tujuan *backup* sistem 2. Mencadangkan data sistem Tele-Presence secara periodik dan standart yang telah ditetapkan.	*Backup* sistem dapat digunakan untuk pemulihan ketika sistem mengalami kerusakan atau sedang dalam masa perawatan. Pencadangan data sudah seharusnya menjadi salah satu standart berjalnnya sebuah sistem. Pencadangan data secara periodik menjaga data yang tersimpan tetap *up-to-date*.

Pendukung tambahan
Pengadaan perangkat penyimpanan membutuhkan dukungan pendanaan yang dapat disesuaikan dengan kebutuhan organisasi.

No. Evaluasi	032
Objek Evaluasi	VMeet Server
Worksheet	Infrastructure Review Worksheet
Penanggungjawab	Bid. Infrastruktur Teknologi Informasi dan Komunikasi Seksi Pengeloalaan Data Center

Aktivitas Evaluasi	**Rasionalisasi**
1. Penetapan protokol keamanan tertentu untuk melindungi data 2. Pencadangan data secara periodik kedalam penyimpanan yang aman	VMeet server menyimpan data terkait sistem Tele-Presence. Kerusakan pada server (fisik maupun digital) dapat menghambat jalannya sistem, bahkan dapat menyebabkan sistem berhenti total.
Pendukung tambahan	

No. Evaluasi	033
Objek Evaluasi	Kurangnya ketersediaan data *record* sebagai pendukung evaluasi
Worksheet	
Penanggungjawab	Seksi Investigasi dan Pelaporan

Aktivitas Evaluasi	**Rasionalisasi**

1. Penyusunan, penetapan dan pengesahan SOP untuk merekam insiden yang terjadi 2. Simulasi pendokumentasian insiden sesuai dengan SOP yang telah disahkan. 3. Pendokumentasian setiap insiden sesuai dengan SOP organisasi	Sejarah kejadian atau insiden dapat menjadi data kritis dan mendukung dalam evaluasi di masa mendatang
Pendukung tambahan	
Kesadaran dan kerjasama seluruh staff dibutuhkan dalam hal ini, tidak hanya dalam mendokumentasikan insiden yang terjadi, tetapi peran dan keikutsertaan staff dalam mengisi dokumen-dokumen yang dapat menjadi sumber data (misal: log aktifitas, *record* reparasi, *record* pengadaan, dll) benar-benar dibutuhkan untuk memberikan data pendukung evaluasi di masa mendatang.	

LAMPIRAN 11

NEXT STEP WORKSHEET

Catatan	**Step**
	30
Next Step Worksheet mendefinisikan secara garis besar langkah-langkah yang dilakukan untuk memfasilitasi implementasi evaluasi OCTAVE –S. Langkah-langkah tersebut antara lain : 1. Dukungan pihak menejemen Mendefinisikan langkah yang dilakukan menejemen untuk mendukung implementasi evaluasi OCTAVE –S 2. Pengawasan implemetsasi Mengidentifikasi langkah yang dilakukan untuk melacak dan memastikan hasil dari evaluasi telah diimplementasikan 3. Expansi evaluasi Mengidentifikasi apakah evaluasi OCTAVE –S saat ini dapat dikembangkan untuk memasukkan aset kritis yang lain 4. Informasi lanjutan Mendefinisikan kapan organisasi dapat menjalankan evaluasi OCTAVE –S atau menajalankan evaluasi selanjutnya.	

Dukungan Pihak Menejemen
Kepala Dinas harus melakukan : 1. Pembagian tugas implementasi hasil OCTAVE –S kepada bidang yang bersangkutan. 2. Mengalokasikan dana untuk implementasi 3. Mempertimbangkan penambahan SDM, terkait hasil evaluasi. Semua level menejer harus mengalokaiskan SDM dan waktu yang mencukupi untuk berpartisipasi dalam proses implementasi hasil evaluasi, dimana bidang yang mereka menejemen ditugaskan dan bertanggungjawab untuk melaksakan implemetasi tersebut.

Pengawasan Implemetasi
Setiap tim yang telah ditugaskan untuk mengimplementasi hasil evaluasi harus : 1. Menetapkan dan bertanggungjawab terhadap jadwal implementasi evaluasi. 2. Membentuk *check-list* untuk memantau perkembangan proses implementasi Membentuk penjadwalan pertemuan antar tim implementor dengan Kepala Dinas untuk mengkoordinasikan dan melaporkan aktivitas atau proses implementasi hasil evaluasi.

Ekspansi Evaluasi
Evaluasi OCTAVE –S masih bisa dikembangkan mengingat masih banyak aset kritis baik berupa sistem, aplikasi, informasi, maupun sumber daya manusia yang belum masuk pada evaluasi saat ini.

Informasi Lanjutan
Evaluasi OCTAVE –S dapat kembali dilakukan pada 12 bulan ke depan.