



VITKA Jurnal Manajemen Pariwisata

www.journal.btp.ac.id

Original Research

IDENTIFIKASI ENSURE SYSTEM SECURITY TEKNOLOGI INFORMASI DAN SISTEM INFORMASI DI WARUNK PAPAN

Heri Nuryanto^{1*}

¹Program Studi Manajemen Kuliner, Politeknik Pariwisata Batam, Batam, Indonesia

INFO ARTIKEL

Diterima : 15/08/20
Direvisi : 20/09/20
Disetujui : 20/09/20
Tersedia *online* : 20/09/20

Email korespondensi:
herihmi@gmail.com

ABSTRACT

Kurangnya pemahaman tentang seberapa baik Teknologi Informasi dan Sistem Informasi berfungsi, kegagalan melakukan operasional Teknologi Informasi dan Sistem Informasi, masalah penempatan karyawan serta kurangnya kemampuan dalam mengelola data menjadi permasalahan yang saat ini terjadi di Warunk Papan. Kondisi ini jika dibiarkan terus-menerus terjadi akan menjadi benalu dalam kesuksesan menjalankan Teknologi Informasi dan Sistem Informasi. Tujuan penelitian adalah melakukan identifikasi Ensure System. Untuk memperoleh hasil level pengelompokan kapabilitas Teknologi Informasi di Warunk Papan. Untuk memperoleh hasil level pengelompokan kapabilitas Sistem Informasi di Warunk Papan. Dan Ingin mengetahui apakah terdapat perbedaan hasil tingkat level pengelompokan kapabilitas antara Teknologi Informasi dan Sistem Informasi Warunk Papan. Populasi pada penelitian ini adalah semua pihak yang terlibat langsung dan bertanggung jawab terhadap infrastruktur TI dan SI Warunk Papan, metode sampel yang digunakan menggunakan non probability sampling dengan metode sampel jenuh dengan teknik pengambilan data Joint Application Design (JAD-Like Sessions). Model penelitian yang digunakan dengan cara melakukan perhitungan maturity level kuesioner penelitian pada masing-masing level model (non existent, initial atau ad hoc, repeatable but intuitive, defined process, managed and measurable dan optimised). Hasil penelitian standar operasional prosedur TI dan SI sudah diimplementasikan di Warunk Papan yang dapat dilihat dari Uji Coba Keamanan Penjagaan dan Pemantauan; Pertukaran Data Sensitif berada pada Level 3 (defined process). Sedangkan Manajemen Keamanan; Rencana Keamanan; Manajemen Identitas; Manajemen Akun Pengguna; Definisi Insiden Keamanan; Proteksi Teknologi Keamanan; Manajemen Kunci Kriptografi; Pencegahan Software Berbahaya, Deteksi dan Perbaikan; Keamanan Jaringan berada pada Level 4 (managed and measurable).

Keywords: Teknologi Informasi, Sistem Informasi, Ensure System Security, Warunk Papan, JAD Like Sessions, Maturity Level.

1. PENDAHULUAN

Salah satu aspek yang menjadi bagian penting dalam Teknologi Informasi (TI) dan Sistem Informasi (SI) serta pengembangannya adalah aspek keamanan dan manajemen risiko. Seiring dengan berkembangnya TI dan SI pada saat ini beberapa hal penting yang menjadi faktor penentu agar sistem yang berjalan dapat berfungsi dengan baik dan benar, karena selain efek positif yang muncul akibat berkembangnya sistem informasi maka permasalahan keamanan dan pengelolaan sumber daya TI juga

terjadi. Sebuah institusi atau tempat usaha yang menggantungkan sebagian besar proses bisnisnya pada sistem informasi akan mengalami kendala yang serius ketika SI dan TI yang diterapkan tidak berjalan dengan seperti yang diinginkan.

Dari waktu ke waktu perkembangan TI selalu mempengaruhi struktur dan kinerja perusahaan dalam memberikan tingkat pelayanan yang berakhir pada kepuasan kebutuhan dan keinginan konsumen. Melalui ketersediaan tingkat layanan TI dalam menyediakan informasi yang tepat, relevan dan

memiliki akurasi yang tinggi merupakan kebutuhan yang sangat penting untuk mempertahankan daya saing perusahaan. Kondisi ini menunjukkan bahwa untuk mencapai tingkat layanan TI harus memiliki tata kelola teknologi informasi yang tepat sehingga dapat menjamin kinerja setiap proses bisnis perusahaan menjadi lebih efektif dan efisien dalam mencapai tujuan bisnis perusahaan.

Kurangnya pemahaman tentang seberapa baik TI dan SI berfungsi, kegagalan melakukan operasional TI dan SI, masalah penempatan karyawan serta kurangnya kemampuan dalam mengelola data menjadi permasalahan yang saat ini terjadi di Warunk Papan. Kondisi ini jika dibiarkan terus-menerus terjadi akan menjadi benalu dalam kesuksesan menjalankan TI dan SI.

Beberapa usaha yang dapat dilakukan agar TI dapat bekerja sebagaimana yang diinginkan adalah dengan menerapkan kebijakan memastikan keamanan sistem (*ensure system security*) seperti melakukan: *Management Security*; *Security Plan*; *Identity Management*; *User Account Management*; *Security Testing*, *Surveillance and monitoring*; *Security Incident Definition*; *Protection of Security Technology*; *Cryptographic Key Management*; *Malicious Software Prevention, Detection and Correction*; *Network Security*; *Exchange of Sensitive Data*. Sehingga Keberadaan IT Governance (tata kelola TI) menjadi bagian yang tak terpisahkan dalam mendukung kesuksesan tata kelola Warunk Papan dengan menjamin perbaikan yang terukur secara efektif dan efisien dari proses bisnis yang terkait dengan TI. Secara sederhana tata kelola TI didefinisikan sebagai struktur hubungan dan proses untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis dapat tercapai melalui penambahan nilai dan minimalisasi risiko terkait dengan pengelolaan TI. Sehingga pada akhirnya perkembangan kemajuan TI pada saat berdampak pada seluruh aspek, pemanfaatan TI dan SI sangat penting karena menuntut keakuratan informasi.

Kebijakan keamanan yang baik (*Cyber Security, Insight, 2017*) memiliki beberapa fitur seperti: pertama, ringkas dan jelas. Sebuah kebijakan keamanan harus ringkas dan jelas. Ketika mereka dibutuhkan mereka akan mudah untuk diterapkan di infrastruktur yang ada. Kebijakan yang rumit atau sulit dimengerti justru tidak akan diterapkan oleh para pegawai; Kedua, Dapat diterapkan dan bermanfaat. Kebijakan harus ditulis dan didesain sebagaimana mungkin agar dapat diterapkan di berbagai seksi dan organisasi. Kebijakan yang baik akan mudah diatur dan diterapkan; Ketiga, Layak secara ekonomi. Organisasi harus mengimplementasikan kebijakan yang ekonomis dan tetap dapat menjaga keamanan dari organisasi; Keempat, Dapat dimengerti. Kebijakan harus mudah dimengerti dan diikuti; Kelima, Realistis. Kebijakan harus berdasarkan praktis dan kenyataan, menggunakan hal-hal fiksi pada kebijakan malah mengacaukan organisasi itu sendiri; Keenam, Konsisten. Organisasi harus memiliki konsistensi ketika mengimplementasikan

kebijakan mereka; ketujuh, Dapat ditangguhkan secara prosedural. Ketika mengimplementasikan kebijakan mereka harus ramah kepada karyawan; Kedelapan, Memenuhi hukum dan regulasi. Setiap kebijakan yang diimplementasikan harus sesuai dengan semua hukum, aturan, dan regulasi yang ada.

2. BAHAN DAN METODE

2.1 Variabel Penelitian

Penelitian ini menggunakan satu variabel penelitian yaitu *Ensure System Security* dengan 11 (sebelas) indikator.

1. Manajemen Keamanan TI (*Management of IT Security*)
 - a. Manajemen keamanan TI pada level organisasi yang tertinggi sehingga tindakan manajemen keamanan selaras dengan kebutuhan bisnis.
2. Rencana Keamanan TI (*IT Security Plan*)
 - a. Menerjemahkan bisnis, risiko dan kepatuhan (*compliance*) ke dalam rencana keamanan TI secara keseluruhan dengan mempertimbangkan infrastruktur TI dan budaya keamanan
 - b. Memastikan rencana diimplementasikan dalam prosedur dan kebijakan keamanan bersama-sama investasi yang tepat dalam layanan, personel, *software* dan *hardware*.
 - c. Mengkomunikasikan kebijakan dan prosedur keamanan kepada *stakeholder* dan *user*.
3. Manajemen Identitas (*Identity Management*)
 - a. Memastikan semua user (*internal, eksternal dan temporer*) dan aktivitas mereka dalam sistem TI (bisnis, aplikasi, lingkungan TI, operasi sistem, pengembangan dan pemeliharaan) secara unik teridentifikasi.
 - b. Memudahkan user mengidentifikasi melalui mekanisme otentikasi.
 - c. Mengkonfirmasi bahwa hak akses pengguna ke sistem dan data sesuai dengan yang ditetapkan, kebutuhan bisnis yang didokumentasikan, dan kebutuhan kerja yang melekat pada identitas pengguna.
 - d. Memastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung jawab keamanan.
 - e. Memelihara identitas pengguna dan hak akses dalam tempat penyimpanan utama.
 - f. Melakukan langkah-langkah teknis yang menghemat biaya, mengukur prosedural dan menjaganya agar terus update dalam membuat identifikasi user, implementasi otentikasi dan penggunaan hak akses.
4. Manajemen Akun Pengguna (*User Account Management*)
 - a. Menempatkan permintaan, penyusunan, penerbitan, penangguhan. Pemodifikasian dan penutupan akun pengguna serta hak-hak user yang berkaitan dengan rangkaian prosedur manajemen akun pengguna.

- Termasuk prosedur persetujuan yang menguraikan data atau pemilik sistem pemberian hak akses. Prosedur ini harus berlaku untuk semua pengguna termasuk administrator, pengguna internal dan eksternal, untuk normal dan kasus darurat.
- b. Hak dan kewajiban relatif terhadap akses ke sistem organisasi dan informasi seharusnya dicantumkan dalam kontrak kerja semua jenis pengguna.
 - c. Melakukan peninjauan manajemen secara teratur setiap akun dan hak yang terhubung.
5. Uji Coba Keamanan, Penjagaan dan Pemantauan (*Security Testing, Surveillance and monitoring*)
 - a. Menguji, menjaga dan memantau implementasi keamanan TI dalam langkah yang proaktif.
 - b. Keamanan TI seharusnya ditinjau secara periodik untuk memastikan landasan keamanan informasi organisasi yang disetujui dan dipelihara.
 - c. Logging dan fungsi pemantauan keamanan TI akan memudahkan untuk pencegahan, pendeteksi dini dan sewaktu-waktu untuk melaporkan aktivitas yang tidak seperti biasanya perlu diperhatikan.
 6. Definisi Insiden Keamanan (*Security Incident Definition*)
 - a. Mendefinisikan secara jelas dan mengkomunikasikan karakteristik dari insiden keamanan yang potensial sehingga dapat diklasifikasikan secara benar dan ditangani oleh proses pengelolaan insiden dan permasalahan.
 7. Proteksi Teknologi Keamanan (*Protection of Security Technology*)
 - a. Membuat teknologi keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentasi keamanan yang tidak perlu.
 8. Manajemen Kunci Kriptografi (*Cryptographic Key Management*)
 - a. Menentukan bahwa kebijakan dan prosedur sesuai untuk mengatur perubahan, pembatalan, penghancuran, distribusi, sertifikasi, penyimpanan, entry, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.
 9. Pencegahan Software Berbahaya, Deteksi dan Perbaikan (*Malicious Software Prevention, Detection and Correction*)
 - a. Memasang pencegahan, pendeteksi dan langkah-langkah perbaikan yang sesuai (terutama patch keamanan yang up-to-datedan pengendalian virus) diseluruh organisasi untuk melindungi sistem informasi dan teknologi darimalware (seperti *virus, worm, spyware dan spam*).
 10. Keamanan Jaringan (*Network Security*)
 - a. Menggunakan teknik dan prosedur manajemen keamanan (misalnya firewall, peralatan keamanan, segmentasi jaringan,

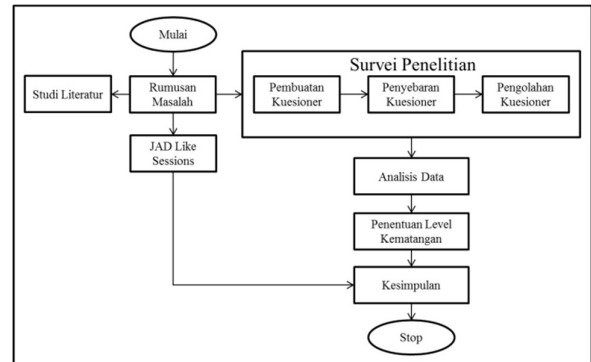
intruksideteksi) untuk mengotorisasi akses dan kontrol informasi mengalir dari dan ke jaringan.

11. Pertukaran Data Sensitif (*Exchange of Sensitive Data*)

- a. Pertukaran data transaksi sensitif hanya melalui jalur terpercaya atau media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman, bukti penerimaan dan non-repudiation

2.1 Desain Penelitian

Desain penelitian identifikasi Ensure System Security TI dan SI Warunk Papan dilakukan sesuai gambar dibawah ini:



Gambar 2.1 Desain Penelitian

2.3 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini diantaranya adalah

1. Survei menggunakan kuisisioner penelitian
2. Joint Application Design (JAD-Like Sessions). Dengan melibatkan pihak-pihak yang terlibat dalam pengelolaan TI dan SI di Warunk Papan.

2.4 Metode Analisis Data

Metode analisis data yang digunakan dalam penelitian ini adalah dengan menggunakan maturity level model. Dengan menggunakan maturity level model maka dapat diketahui posisi kematangannya saat ini, dan secara terus menerus serta berkesinambungan dapat untuk meningkatkan levelnya sampai tingkat tertinggi agar aspek governance terhadap TI dapat berjalan secara efektif.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Setelah tahap penyusunan indikator Identifikasi Ensure System Security, pada tahap berikutnya adalah membagi dalam 2 kelompok JAD antara pengelola TI dan SI pada Warunk Papan. Maka didapatkan data sebagai berikut:

3.1.1 Level Managed And Measurable JAD TI Warunk Papan

1. Logging dan fungsi pemantauan keamanan TI akan memudahkan untuk pencegahan, pendeteksi dini dan sewaktu-waktu untuk

melaporkan aktivitas yang tidak seperti biasanya perlu diperhatikan.

2. Memastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung jawab keamanan.
3. Pertukaran data transaksi sensitif hanya melalui jalur terpercaya atau media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman, bukti penerimaan dan non-repudiation
4. Manajemen keamanan TI pada level organisasi yang tertinggi sehingga tindakan manajemen keamanan selaras dengan kebutuhan bisnis.
5. Memastikan rencana diimplementasikan dalam prosedur dan kebijakan keamanan bersama-sama investasi yang tepat dalam layanan, personel, software dan hardware.
6. Melakukan langkah-langkah teknis yang menghemat biaya, mengukur prosedural dan menjaganya agar terus update dalam membuat identifikasi user, implementasi otentikasi dan penggunaan hak akses.
7. Mendefinisikan secara jelas dan mengkomunikasikan karakteristik dari insiden keamanan yang potensial sehingga dapat diklasifikasikan secara benar dan ditangani oleh proses pengelolaan insiden dan permasalahan.
8. Memasang pencegahan, pendeteksi dan langkah-langkah perbaikan yang sesuai (terutama patch keamanan yang up-to-date dan pengendalian virus) diseluruh organisasi untuk melindungi sistem informasi dan teknologi darimalware (seperti virus, worm, spyware dan spam).
9. Menerjemahkan bisnis, risiko dan kepatuhan (compliance) ke dalam rencana keamanan TI secara keseluruhan dengan mempertimbangkan infrastruktur TI dan budaya keamanan
10. Mengkomunikasikan kebijakan dan prosedur keamanan kepada stakeholder dan user.
11. Memudahkan user mengidentifikasi melalui mekanisme otentikasi.
12. Hak dan kewajiban relatif terhadap akses ke sistem organisasi dan informasi seharusnya dicantumkan dalam kontrak kerja semua jenis pengguna.
13. Melakukan peninjauan manajemen secara teratur setiap akun dan hak yang terhubung.
14. Menentukan bahwa kebijakan dan prosedur sesuai untuk mengatur perubahan, pembatalan, penghancuran, distribusi, sertifikasi, penyimpanan, entry, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.

3.1.2 Level Optimised JAD TI Warunk Papan

1. Menguji, menjaga dan memantau implementasi keamanan TI dalam langkah yang proaktif.
2. Memelihara identitas pengguna dan hak akses dalam tempat penyimpanan utama.

3. keamanan TI seharusnya ditinjau secara periodik untuk memastikan landasan keamanan informasi organisasi yang disetujui dan dipelihara.
4. Menggunakan teknik dan prosedur manajemen keamanan (misalnya firewall, peralatan keamanan, segmentasi jaringan, intruksideteksi) untuk mengotorisasi akses dan kontrol informasi mengalir dari dan ke jaringan.
5. Memastikan semua user (internal, eksternal dan temporer) dan aktivitas mereka dalam TI (bisnis, aplikasi, lingkungan TI, operasi sistem, pengembangan dan pemeliharaan) secara unik teridentifikasi.
6. Mengkonfirmasi bahwa hak akses pengguna ke sistem dan data sesuai dengan yang ditetapkan, kebutuhan bisnis yang didokumentasikan, dan kebutuhan kerja yang melekat pada identitas pengguna.
7. Menempatkan permintaan, penyusunan, penerbitan, penangguhan. Pemodifikasian dan penutupan akun pengguna serta hak-hak user yang berkaitan dengan rangkaian prosedur manajemen akun pengguna. Termasuk prosedur persetujuan yang menguraikan data atau pemilik sistem pemberian hak akses. Prosedur ini harus berlaku untuk semua pengguna termasuk administrator, pengguna internal dan eksternal, untuk normal dan kasus darurat.
8. Membuat teknologi keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentasi keamanan yang tidak perlu.

3.1.3 Level Repeatable But Intuitive JAD SI Warunk Papan

1. Menguji, menjaga dan memantau implementasi keamanan SI dalam langkah yang proaktif.
2. Logging dan fungsi pemantauan keamanan SI akan memudahkan untuk pencegahan, pendeteksi dini dan sewaktu-waktu untuk melaporkan aktivitas yang tidak seperti biasanya perlu diperhatikan.

3.1.4 Level Defined Process JAD SI Warunk Papan

1. Memastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung jawab keamanan.
2. Memelihara identitas pengguna dan hak akses dalam tempat penyimpanan utama.
3. keamanan SI seharusnya ditinjau secara periodik untuk memastikan landasan keamanan informasi organisasi yang disetujui dan dipelihara.
4. Menggunakan teknik dan prosedur manajemen keamanan (misalnya firewall, peralatan keamanan, segmentasi jaringan, intruksideteksi) untuk mengotorisasi akses dan kontrol informasi mengalir dari dan ke jaringan.
5. Pertukaran data transaksi sensitif hanya melalui jalur terpercaya atau media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman, bukti penerimaan dan non-repudiation

3.1.5 Level Managed And Measurable JAD SI Warunk Papan

1. Manajemen keamanan SI pada level organisasi yang tertinggi sehingga tindakan manajemen keamanan selaras dengan kebutuhan bisnis.
2. Memastikan rencana diimplementasikan dalam prosedur dan kebijakan keamanan bersama-sama investasi yang tepat dalam layanan, personel, software dan hardware.
3. Memastikan semua user (internal, eksternal dan temporer) dan aktivitas mereka dalam SI (bisnis, aplikasi, lingkungan SI, operasi sistem, pengembangan dan pemeliharaan) secara unik teridentifikasi.
4. Mengkonfirmasi bahwa hak akses pengguna ke sistem dan data sesuai dengan yang ditetapkan, kebutuhan bisnis yang didokumentasikan, dan kebutuhan kerja yang melekat pada identitas pengguna.
5. Melakukan langkah-langkah teknis yang menghemat biaya, mengukur prosedural dan menjaganya agar terus update dalam membuat identifikasi user, implementasi otentikasi dan penggunaan hak akses.
6. Menempatkan permintaan, penyusunan, penerbitan, penangguhan. Pemodelan dan penutupan akun pengguna serta hak-hak user yang berkaitan dengan rangkaian prosedur manajemen akun pengguna. Termasuk prosedur persetujuan yang menguraikan data atau pemilik sistem pemberian hak akses. Prosedur ini harus berlaku untuk semua pengguna termasuk administrator, pengguna internal dan eksternal, untuk normal dan kasus darurat.
7. Mendefinisikan secara jelas dan mengkomunikasikan karakteristik dari insiden keamanan yang potensial sehingga dapat diklasifikasikan secara benar dan ditangani oleh proses pengelolaan insiden dan permasalahan.
8. Membuat teknologi keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentasi keamanan yang tidak perlu.
9. Memasang pencegahan, pendeteksi dan langkah-langkah perbaikan yang sesuai (terutama patch keamanan yang up-to-date dan pengendalian virus) diseluruh organisasi untuk melindungi sistem informasi dan teknologi darimalware (seperti virus, worm, spyware dan spam).

3.1.6 Level Optimised JAD SI Warunk Papan

1. Menerjemahkan bisnis, risiko dan kepatuhan (compliance) ke dalam rencana keamanan SI secara keseluruhan dengan mempertimbangkan infrastruktur SI dan budaya keamanan
2. Mengkomunikasikan kebijakan dan prosedur keamanan kepada stakeholder dan user.
3. Memudahkan user mengidentifikasi melalui mekanisme otentikasi.
4. Hak dan kewajiban relatif terhadap akses ke sistem organisasi dan informasi seharusnya

dicantumkan dalam kontrak kerja semua jenis pengguna.

5. Melakukan peninjauan manajemen secara teratur setiap akun dan hak yang terhubung.
6. Menentukan bahwa kebijakan dan prosedur sesuai untuk mengatur perubahan, pembatalan, penghancuran, distribusi, sertifikasi, penyimpanan, entry, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.

Tabel 3.1. Hasil Indikator TI dan SI

No	Indikator	Rata-rata TI	Rata-rata SI	Rata-Rata
1	Manajemen Keamanan	4.0	4.0	4.0
2	Rencana Keamanan	4.0	4.7	4.4
3	Manajemen Identitas	4.5	3.8	4.2
4	Manajemen Akun Pengguna	4.3	4.7	4.5
5	Uji Coba Keamanan, Penjagaan dan Pemantauan	4.7	2.3	3.5
6	Definisi Insiden Keamanan	4.0	4.0	4.0
7	Proteksi Teknologi Keamanan	5.0	4.0	4.5
8	Manajemen Kunci Kriptografi	4.0	5.0	4.5
9	Pencegahan Software Berbahaya, Deteksi dan Perbaikan	4.0	4.0	4.0
10	Keamanan Jaringan	5.0	3.0	4.0
11	Pertukaran Data Sensitif	4.0	3.0	3.5
Rata-rata		4.3	3.9	4.1

3.2 Pembahasan

Berdasarkan hasil Identifikasi Ensure System Security yang telah dilakukan di warunk papan dengan menggunakan model kematangan (maturity models) untuk mengontrol dengan menggunakan metode penilaian (scoring) skala nonexistent sampai dengan optimised (dari 0 sampai 5) didapatkan hasil sebagai berikut:

3.2.1 Pada level Non Existent dan Initial Atau Ad Hoc

Tidak ditemukan sehingga dapat dijelaskan bahwa penggunaan TI dan SI di Warunk Papan:

1. Sudah sadar dan memiliki pengetahuan akan kebutuhan dan keamanan SI dalam usaha menjalankan proses bisnis.

2. Pegawai Warung Papan sudah sadar dan memiliki tanggung jawab keamanan dalam menjalankan TI dan SI.
3. Tidak saling melempar tanggung jawab terhadap pelanggaran keamanan SI yang terdeteksi.
4. Sudah memiliki aturan mekanisme terhadap karyawan apabila melakukan pelanggaran keamanan data dan transaksi penjualan makanan dan minuman secara online.

3.2.2 Level Repeatable But Intuitive

Dapat dijelaskan bahwa Uji Coba Keamanan, Penjagaan dan Pemantauan (Security Testing, Surveillance and monitoring). Tanggung jawab akan keamanan SI ditugaskan kepada seorang koordinator keamanan SI, walaupun kewenangan pengelolaan koordinator tersebut dibatasi dalam kondisi (1) Menguji, menjaga dan memantau implementasi keamanan SI dalam langkah yang proaktif; (2) Logging dan fungsi pemantauan keamanan SI akan memudahkan untuk pencegahan, pendeteksi dini dan sewaktu-waktu untuk melaporkan aktivitas yang tidak seperti biasanya perlu diperhatikan.

3.2.3 Level Defined Process Warunk Papan

1. Kesadaran akan keamanan telah ada dan dipromosikan oleh manajemen Warunk Papan dijalankan pada kondisi:
 - a. Menggunakan teknik dan prosedur manajemen keamanan (misalnya firewall, peralatan keamanan, segmentasi jaringan, intruksideteksi) untuk mengotorisasi akses dan kontrol informasi mengalir dari dan ke jaringan.
 - b. Pertukaran data transaksi sensitif hanya melalui jalur terpercaya atau media dengan kontrol untuk menyediakan keaslian konten, bukti pengiriman, bukti penerimaan dan non-repudiation.
2. Prosedur keamanan SI telah didefinisikan dan sejalan dengan kebijakan keamanan SI dalam hal ditinjau secara periodik untuk memastikan landasan keamanan informasi warunk papan.
3. Rencana dan solusi keamanan SI dilakukan karena adanya analisis risiko. Kondisi ini untuk memastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung jawab keamanan.
4. Pelaporan keamanan mencakup fokus bisnis yang jelas, hal ini bertujuan untuk memelihara identitas pengguna dan hak akses di simpan dalam database.

3.2.4 Level Managed And Measurable JAD SI Warunk Papan

1. Tanggung jawab untuk keamanan SI telah ditugaskan secara jelas, teratur dan dijalankan.
2. Analisis risiko dan dampak keamanan SI dilakukan secara konsisten.
3. Proses keamanan SI dikoordinasikan dengan seluruh fungsi keamanan organisasi.

4. Kebijakan dan praktik dari keamanan dilengkapi dengan baseline keamanan tertentu.
5. Sertifikasi keamanan disarankan untuk staf yang bertanggung jawab untuk audit dan manajemen keamanan.
6. Pelatihan keamanan SI dilakukan baik dalam lingkup SI maupun bisnis.
7. Pelatihan keamanan SI direncanakan dan diatur agar mampu menanggapi kebutuhan bisnis dan profil risiko keamanan yang telah terdefinisi.
8. Identifikasi pengguna, otentifikasi dan otorisasi terstandar
9. Tujuan dan metrik untuk manajemen keamanan telah didefinisikan tetapi belum diukur

3.2.5 Level Optimised JAD SI Warunk Papan

1. Keamanan SI adalah tanggung jawab bersama pihak manajemen bisnis dan manajemen SI dan terintegrasi dengan tujuan bisnis keamanan perusahaan.
2. Kebutuhan keamanan SI didefinisikan dengan jelas, dioptimasi dan dimasukkan dalam rencana keamanan yang telah disetujui.
3. Pengguna dan pelanggan makin akuntabel dalam mendefinisikan kebutuhan keamanan dan fungsi keamanan terintegrasi dengan aplikasi pada saat tahap desain.
4. Penilaian keamanan periodik dilaksanakan untuk mengetahui efektivitas implementasi dari rencana keamanan.
5. Kontrol yang cukup untuk mengurangi resiko telah dikomunikasikan dan diimplementasikan.
6. Proses keamanan dan teknologi terintegrasi diseluruh lini perusahaan

4. KESIMPULAN

Berdasarkan hasil penelitian Identifikasi Ensure System Security di Warunk Papan maka sudah menjalankan standar operasional prosedur yang jelas dalam menjalankan TI dan SI. Kondisi ini dapat dilihat dari Uji Coba Keamanan Penjagaan dan Pemantauan; Pertukaran Data Sensitif berada pada Level 3 (defined process). Sedangkan Manajemen Keamanan; Rencana Keamanan; Manajemen Identitas; Manajemen Akun Pengguna; Definisi Insiden Keamanan; Proteksi Teknologi Keamanan; Manajemen Kunci Kriptografi; Pencegahan Software Berbahaya, Deteksi dan Perbaikan; Keamanan Jaringan berada pada Level 4 (managed and measurable).

DAFTAR PUSTAKA

- Ciptaningrum, Dewi. dkk. 2015. "Cobit 5 Sebagai Metode Alternatif Bagi Audit Keamanan Sistem Informasi (Sebuah Usulan Untuk Diterapkan di Pemerintah Kota Yogyakarta)". Seminar Nasional Teknologi Informasi dan Multimedia 2015. STMIK AMIKOM Yogyakarta, 6-8 Februari 2015. pp 1.2-
<http://ojs.amikom.ac.id/index.php/semnasteknome>

dia/article/viewFile/829/795. (Diakses 08 Juni 2016, 09.02 wib)

- Ciptaningrum, Dewi. dkk. 2015. "Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan Cobit 5". Seminar Nasional Teknologi Informasi dan Komunikasi 2015 (SENTIKA 2015). Yogyakarta, 28 Maret 2015, pp65-75.
<https://fti.uajy.ac.id/sentika/publikasi/makalah/2015/9.pdf>. (Diakses 01 Juni 2016, 18.27 wib)
- Fernandes Andry, Johanes. 2016. "Audit Tata Kelola TI Menggunakan Kerangka Kerja Cobit Pada Domain DS dan ME di Perusahaan Kreavi Informatika Solusindo". Seminar Nasional Teknologi Informasi dan Komunikasi 2016 (SENTIKA 2016). Yogyakarta, 18-19 Maret 2016, pp 287-294.
<https://fti.uajy.ac.id/sentika/publikasi/makalah/2016/15.pdf>. (Diakses 02 Juni 2016, 11.48 wib)
- Iba Ricoida, Desy. 2015. "Tingkat Kematangan Teknologi Informasi Menggunakan Framework COBIT pada Layanan Teknologi Informasi (Studi Kasus : STIE MDP)". Jatisi, Vol. 2 No. 1 September 2015, pp 56- 64.
http://www.mdp.ac.id/jatisi/vol-2-no-1/JATISI_Vol_2_No_1_September_2015_5%20%5B56-64%5D.pdf. (Diakses 02 Juni 2016, 11.51 wib)
- Sarno, Riyanarto. 2009. "Audit Sistem dan Teknologi Informasi". UPT Penerbitan ITS (ITS Press). Surabaya.
- Setiawan, Herri. 2010. "IT Governance & Penggunaan COBIT Framework". Jurnal Sistem Informasi (JSI), VOL. 2, NO. 2, Oktober 2010, pp 219-237.
<http://ejournal.unsri.ac.id/index.php/jsi/article/view/725>. (Diakses 01 Juni 2016, 18.27 wib)
- Sheikhpour, Razieh. 2012. "An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls". International Journal of Security and Its Applications. Vol. 6, No. 2, April, 2012, pp 13-28.
http://www.sersc.org/journals/IJISA/vol6_no2_2012/2.pdf. (Diakses 02 Juni 2016, 11.00 wib)
- The IT Governance Institute. 2008. "Understanding How Business Goals Drive IT Goals". USA.