**ANALISIS PENERAPAN KEAMANAN SISTEM INFORMASI**

**PADA PT. AXA MANDIRI FINANCIAL SERVICE**

**MENGGUNAKAN INDEKS KAMI**

Yuli Haryanto1) Reza Afrizal2)

*1), 2) Dosen Informatika Universitas Indraprasta PGRI*

*Jl Nangka No. 58 Tanjung Barat, Jakarta Selatan*

*Email : haryanto\_yuli@yahoo.co.id1),* [*reza.avrizal@unindra.ac.id*](mailto:reza.avrizal@unindra.ac.id) *2)*

**Abstrak**

PT. AXA Mandiri Financial Service merupakan salah satu perusahaan yang menerapkan keamanan sistem informasi yang didukung oleh teknologi komputerisasi. Perusahaan yang bergerak di bidang perbankan dan asuransi ini didukung oleh berbagai fasilitas komputerisasi dalam melakukan pelayanan kepada nasabahnya. Penanganan sistem informasi pada perusahaan ini memang sudah mengikuti perkembangan teknologi dan perangkat yang cukup pesat saat ini. Namun keamanan sistem informasi memiliki kerangka pedoman untuk menjamin bahwa keamanan sistem informasi layak diimplementasikan pada perusahaan baik pada skala kecil maupun skala besar. Penelitian ini berupaya menggunakan metode INDEKS KAMI untuk melakukan analisis terhadap penerapan keamanan sistem informasi pada perusahaan tersebut.

Kata kunci : Keamanan Informasi, Indeks KAMI*,* Informasi AXA.

1. **Pendahuluan**

Keamanan sistem informasi menjadi bagian yang sangat penting dalam upaya peningkatan kualitas pelayanan konsumen pada sebuah perusahaan. Keamanan sistem informasi saat ini dapat diterapkan dengan bantuan media komputer sehingga sistem informasi dapat lebih andal dalam mendukung kinerja perusahaan. PT. AXA Mandiri Financial Service merupakan salah satu perusahaan yang menerapkan keamanan sistem informasi yang didukung oleh teknologi komputerisasi. Perusahaan yang bergerak di bidang perbankan dan asuransi ini didukung oleh berbagai fasilitas komputerisasi dalam melakukan pelayanan kepada nasabahnya. Fasilitas komputerisasi tersebut antara lain dalam hal pelayanan pada bagian *customer service*, pengolahan data nasabah, kepegawaian, bahkan sistem monitoring nasabah.

Penanganan sistem informasi pada perusahaan ini memang sudah mengikuti perkembangan teknologi dan perangkat yang cukup pesat saat ini. Namun keamanan sistem informasi memiliki kerangka pedoman untuk menjamin bahwa keamanan sistem informasi layak diimplementasikan pada perusahaan baik pada skala kecil maupun skala besar. Untuk itu perlu adanya analisis keamanan sistem informasi yang diterapkan pada PT. AXA Mandiri Financial Service sehingga dapat diketahui kualitas keamanan sistem informasi yang sudah diterapkan. Penelitian ini berupaya menggunakan metode INDEKS KAMI untuk melakukan analisis terhadap penerapan keamanan sistem informasi pada perusahaan tersebut. Adapun rumusan masalah adalah :

1. Bagaimana penerapan keamanan sistem informasi yang ada pada PT. AXA Mandiri Financial Service?
2. Bagaimana kerangka kerja keamanan sistem informasi dan kebijakannya berdasarkan tingkat kebutuhan pengguna ?
3. Bagaimana tingkat keamanan sistem informasi berdasarkan hasil analisis menggunakan metode Indeks KAMI ?

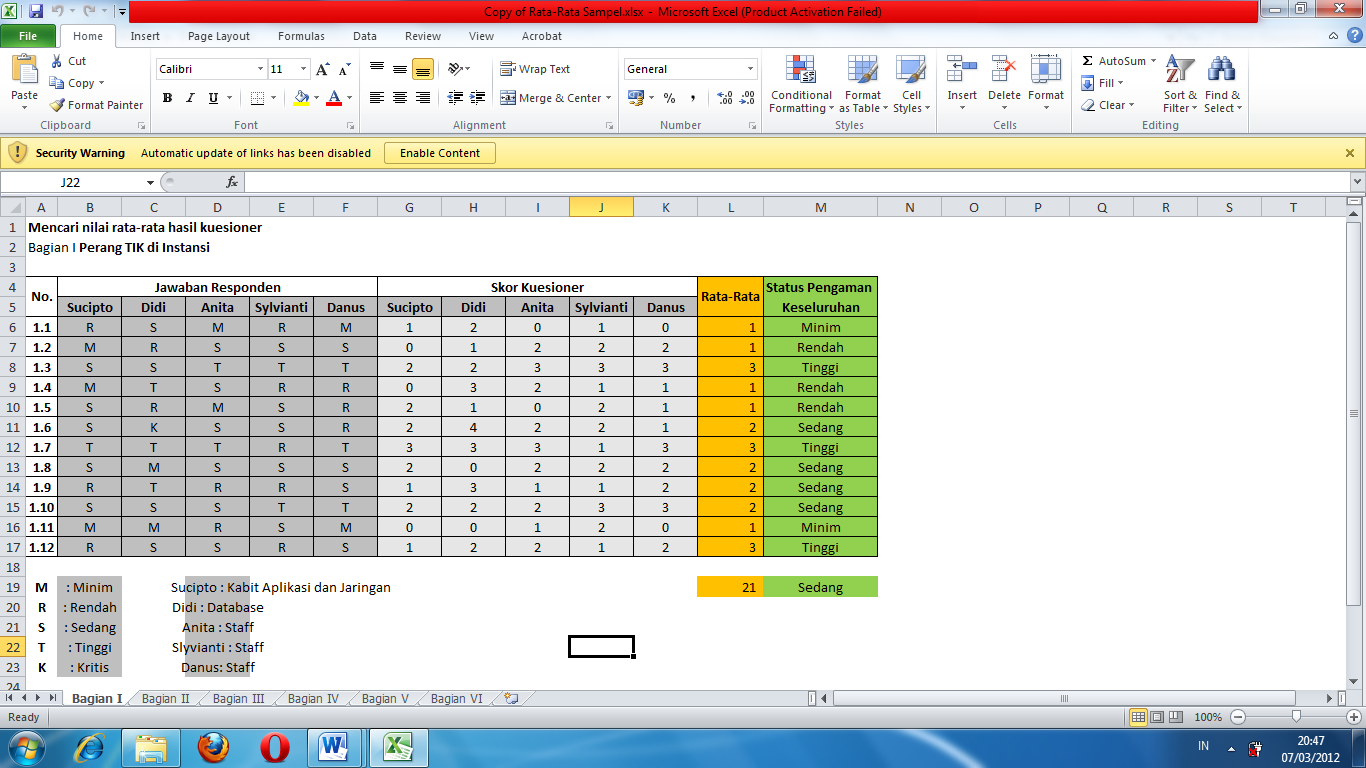
Adapun tujuan yang ingin dicapai dalam penelitian ini adalah melakukan analisis terhadap penerapan keamanan sistem informasi sehingga dari hasil analisis tersebut diupayakan adanya pencegahan terhadap pelanggaran keamanan maupun penyalahgunaan sumber daya informasi berdasarkan Indeks KAMI. Melakukan identifikasi, analisis, dan evaluasi tentang sejauh mana tingkat keamanan sistem informasi yang ada selama ini dan pengembangan keamanan sistem informasi tersebut. Memberikan rekomendasi pengembangan keamanan sistem informasi yang layak dan dapat menunjang profesionalisme perusahaan sesuai standarisasi yang ada pada model Indeks KAMI.

1. **Pembahasan**

Berdasarkan dari hasil penelitian, maka diketahui bahwa pengembangan keamanan sistem informasi yang ada pada PT. AXA Mandiri Financial Service ini memiliki tingkat kesiapan dalam mengelola suatu sistem informasi masih dikatakan sudah sangat baik.

* 1. **Hasil Identifikasi Peran Sistem Informasi di Instansi**

Berdasarkan Indeks KAMI, hasil yang didapat dari beberapa responden sebagaimana pada tabel berikut :



Gambar 2.1 Hasil Kuesioner Peran Sistem Informasi

Dari gambar di atas dapat diketahui bahwa peran sistem informasi di perusahaan ini sangat penting dalam mengelola suatu sistem inforamasi keuangan. Dengan tingkat ketergantungan yang tinggi maka perusahaan sangat membutuhkan suatu kesiapan dalam segi keamanan baik itu teknologinya maupun sistemnya, berikut ini acuan dari Indeks KAMI untuk mendapatkan hasil dari ketergantungan sistem informasi di perusahaan :



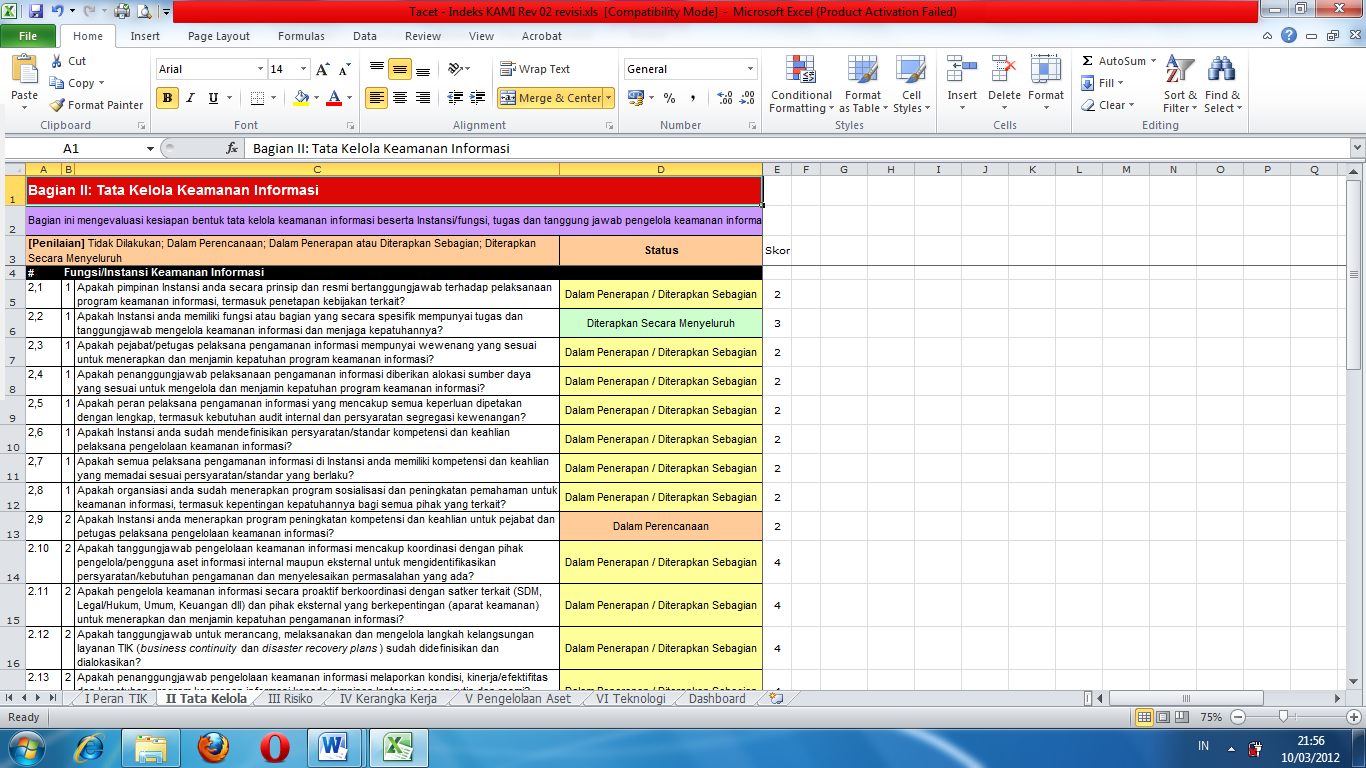
Gambar 2.2 Hasil Acuan Indeks KAMI

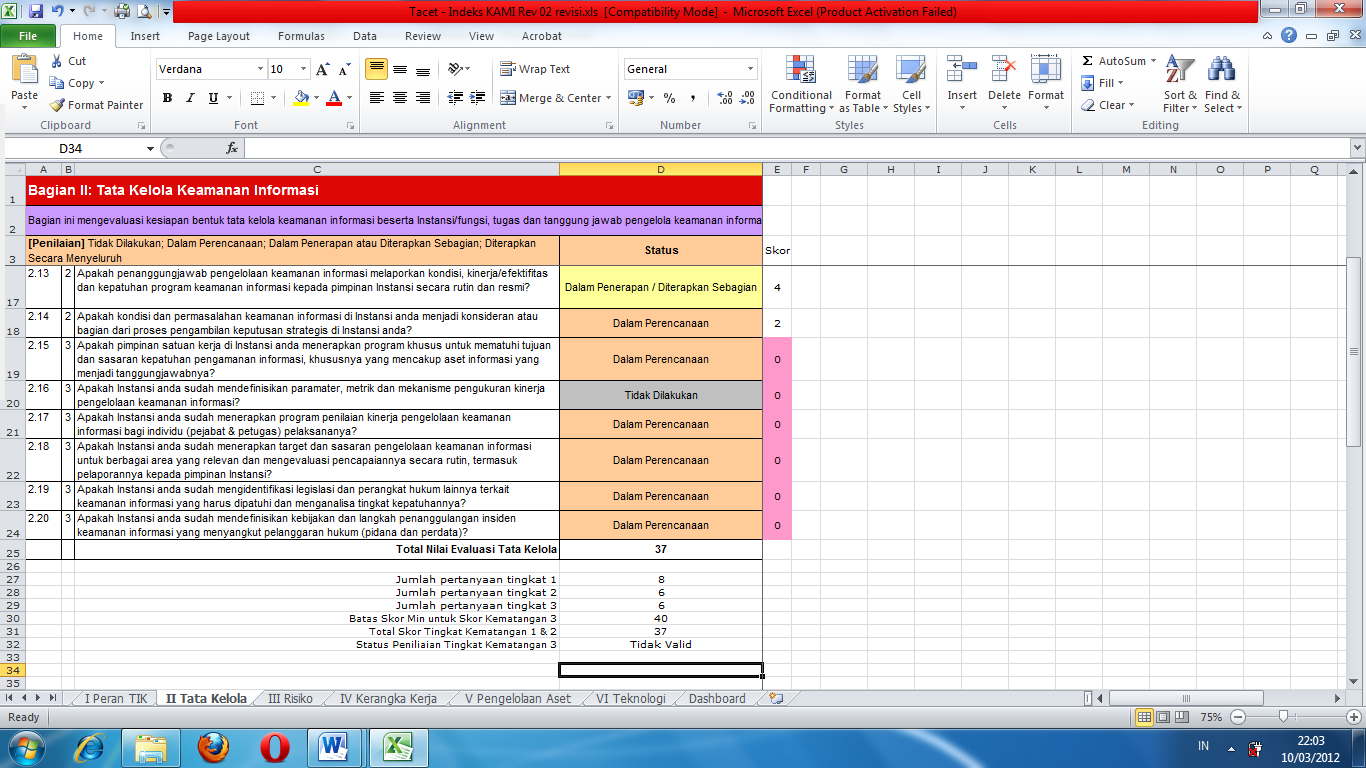
Dari gambar di atas dapat diketahui bahwa persamaan dari hasil rata-rata dengan hasil yang dipergunakan pada tools Indeks KAMI, bahwa beberapa dari pertanyaan yang ada menyinggung tentang tingkat ketergantungan suatu SI didalam mengelola informasi atau pun teknologi dalam menjaga suatu keamanan sistem informasi. Berikut adalah hal yang ketergantungan atau pun peran terhadap sistem informasi :

1. Pengolahan data keuangan
2. Pengaturan jadwal anggaran
3. Pengeluaran Anggaran
   1. **Hasil Identifikasi Tata Kelola Keamanan Informasi**

Tata kelola teknologi Informasi pada proses audit data adalah manajemen audit data yang merupakan aset penting bagi perusahaan. Secara umum Tata Kelola Teknologi Informasi adalah upaya menjamin pengolahan teknologi informasi agar mendukung bahkan selaras dengan strategi bisnis suatu perusahaan atau organisasi yang dilakukan oleh atasan, manajemen eksekutif dan manajemen teknologi informasi. Oleh karena itu suatu tata kelola yang baik tergantung bagaimana atasan ataupun pimpinan bertanggung jawab dalam menjamin suatu keamanan baik itu sistem ataupun teknologinya.

Berikut adalah hasil penelitian yang didapat dari responden untuk Tata Kelola Keamanan Informasi :





Gambar 2.3. Hasil Tata Kelola Keamanan Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan/diterapkan sebagian. Untuk skor kematangan 3, didapat dengan rumus : ( 2\* jumlah pertanyaan tingkat 1) + (4\*jumlah pertanyaan tingkat 2)

(2\*8) + (4\*6) = 40

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana :

Skor tingkat 1 : 16

Skor tingakt 2 : 16

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (16+16)=32. Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar dibandingkan dengan batas skor min kematangan 3, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 yaitu vailid dan sebaliknya jika tidak memenuhi syarat maka hasilnya tidak valid.

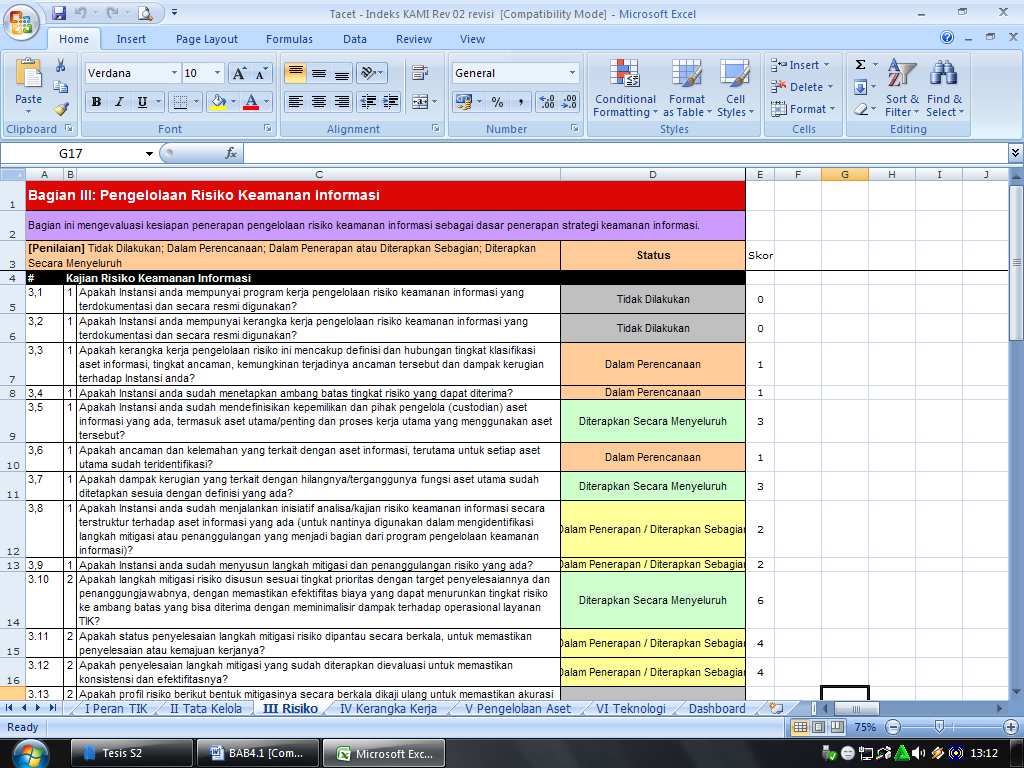
Dari hasil di atas kita bisa lihat bahwa sebagian yang sudah menerapkan tata kelola untuk keamanan sistem walaupun belum dikembangkan secara menyeluruh dalam segala hal. Oleh karena itu para pimpinan dari setiap bagian di perusahaan ini masih belum memahami betapa pentingnya suatu keamanan baik itu teknologi ataupun sistem untuk dijaga dan dimanfaatkan sedemikian rupa dan tidak semua kepala bagian memahami dunia teknologi dan sistem informasi.

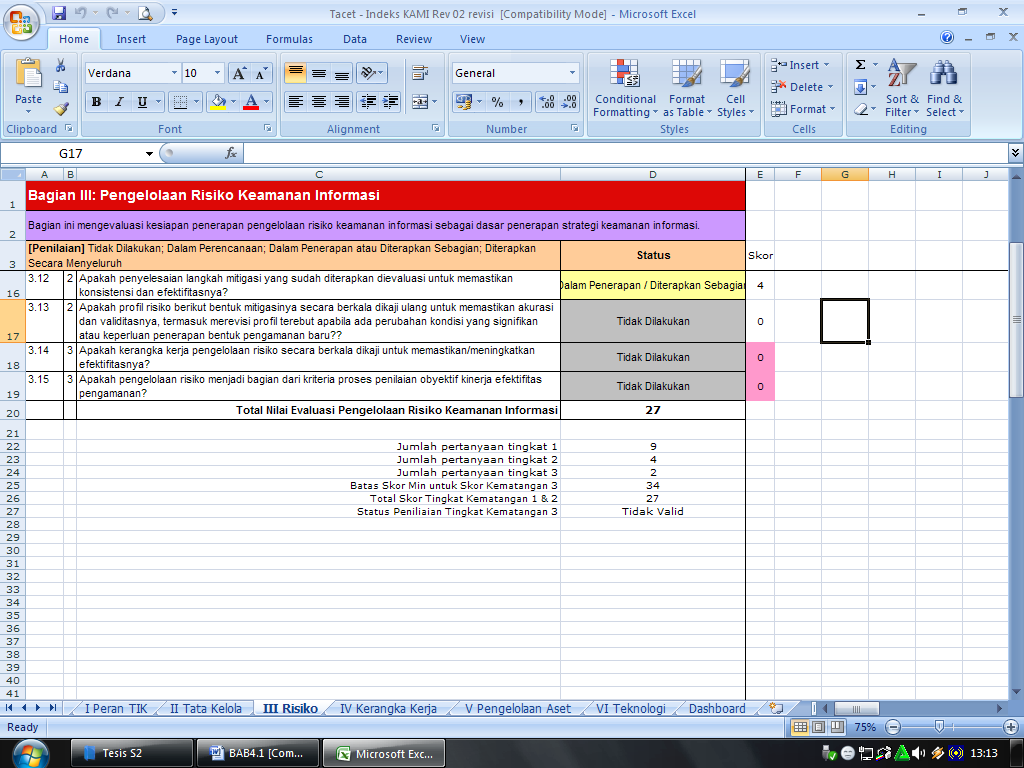
**Rekomendasi Tata Kelola Keamanan Informasi**

Agar terciptanya Tata Kelola Keamanan Informasi, maka diharapkan :

1. Adanya pelatihan khusus terhadap setiap pimpinan agar memahami betapa pentingnya suatu keamanan sistem informasi dan teknologi.
2. Pengkajian keamanan informasi secara berskala oleh pihak yang memahami dalam dunia keamanan infomasi dan teknologi.
3. Pimpinan setiap bagian wajib mengalokasikan tanggung jawab terhadap aset yang ada di perusahaan.
4. Setiap kepala bagian memastikan keutuhan data bebas dari perubahan dan modifikasi pihak-pihak tidak berwenang dan adanya kerja sama dengan pihak keamanan terkait.
   1. **Hasil Identifikasi Pengolahan Resiko Keamanan Informasi**

Resiko merupakan suatu ancaman terbesar dari setiap perusahaan ataupun instansi manapun, seperti halnya perusahaan yang tak pernah luput dari serangan. Serangan yang lebih sering terjadi setelah diteliti adalah seperti terjadinya kesalahan IP Addres yang telah dipakai oleh karyawan, jaringan kabel yang tidak beraturan, tidak ada yang setiap hari memonitoring setiap waktu dan masih bekerja sama dengan pihak vendor. Hal seperti ini terjadi karena adanya lubang keamanan yang dapat ditembus dikarenakan hal seperti ini hasil dari penelitian yang didapat menggunakan tools Indeks KAMI :





Gambar 2.4 Hasil Pengolahan Resiko Keamanan Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan diberbagi bidang hanya sebagian. Untuk skorkematangan 3, didapat dengan rumus : ( 2\* jumlah pertanyaan tingkat 1) + (4\*jumlah pertanyaan tingkat 2)

(2\*9) + (4\*4) = 34

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana :

Skor tingkat 1 : 20

Skor tingakt 2 : 14

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (20+14)=34. Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar atau sama dengan (≥), dibandingkan dengan batas skor min kematangan 3 yaitu 34, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 yaitu vailid. Hasil dari skor tingkat kematangan 1 dan 2= batas skor min kematangan 3, yaitu 34 = 34 dan status penilaian tingkat kematangan 3 bernilai valid.

**Rekomendasi Pengelolaan Resiko Keamanan Informasi**

Setelah diteliti oleh penulis, maka merekomendasikan beberapa hal yang dapat membantu agar kekurangan suatu resiko yang terjadi, diantaranya :

1. Memperhatikan kebutuhan audit yang melibatkan pengecekan sistem

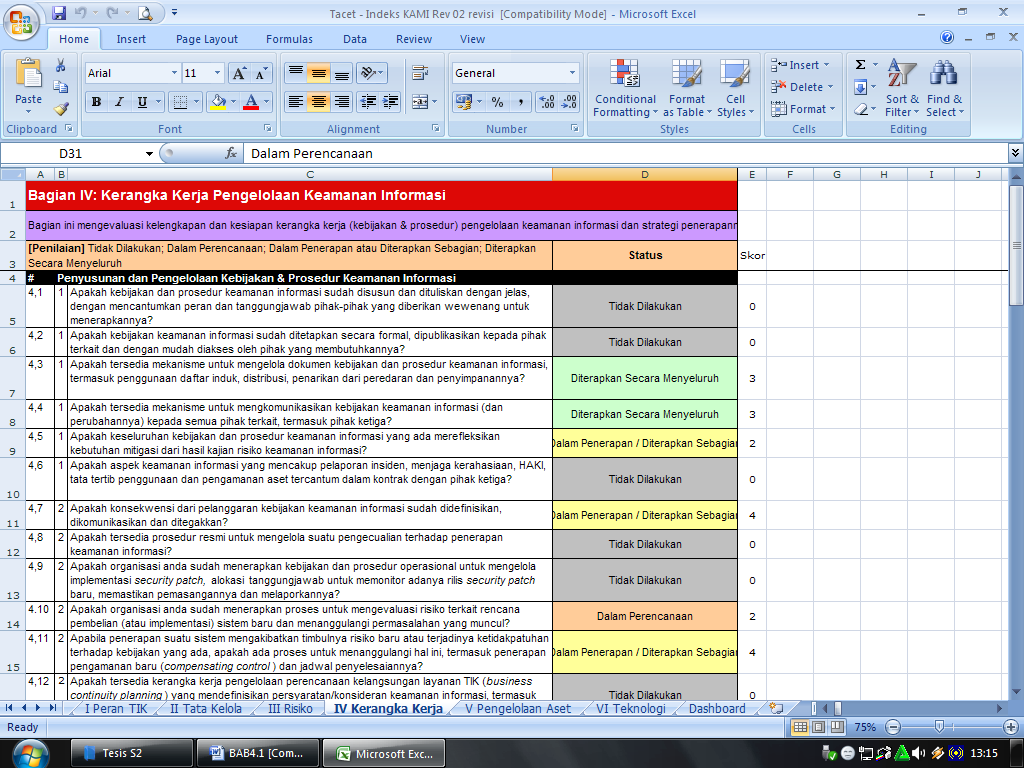
operasional untuk meminimalkan resiko dari gangguan proses bisnis.

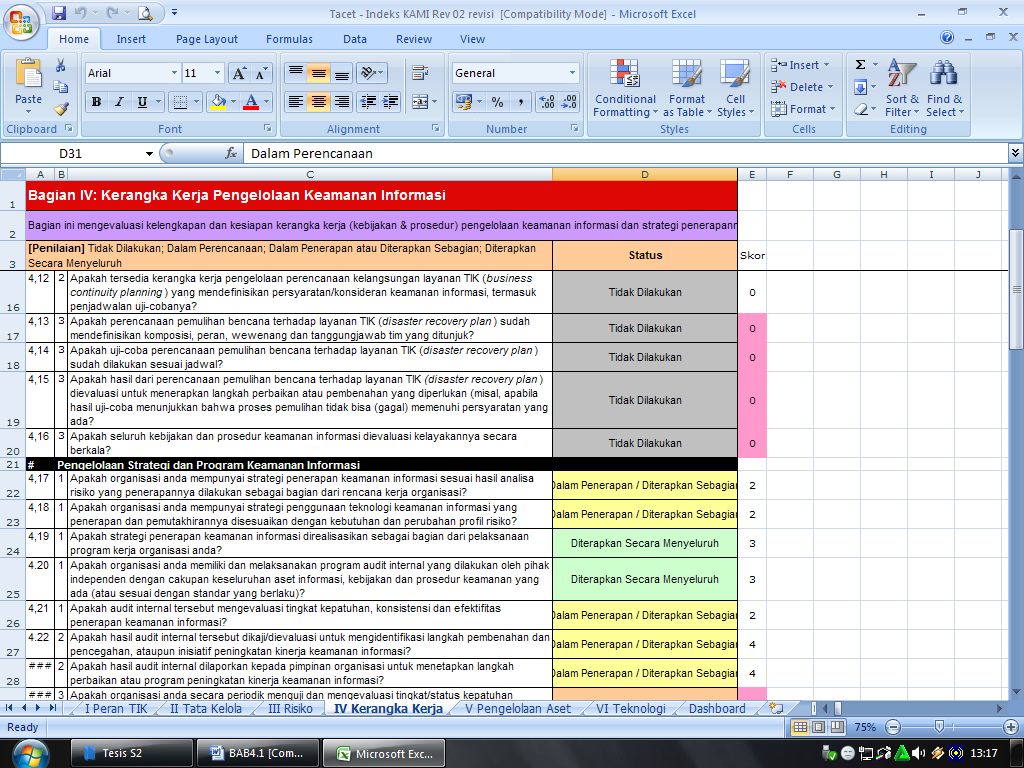
1. Membatasi pengguna sistem aplikasi untuk bagian yang tidak berkompeten di bagiannya.
2. Mengupdate berskala untuk anti virus, kesalahan IP Addres komputer dan diinstrumenkan oleh setiap kepala bagian yang lebih memahami di bidang teknologi dan sistem informasi.
3. Prosedur untuk mengontrol instalasi software pada sistem operasi dan

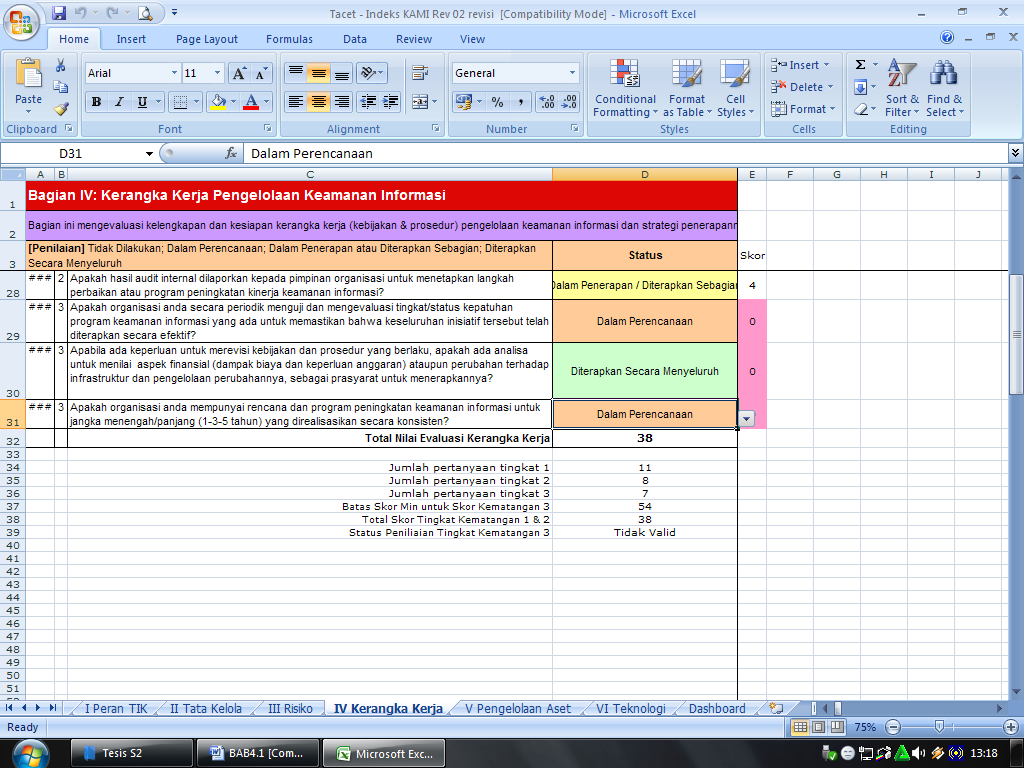
instalasi jaringan pada komputer.

1. Adanya sangsi untuk pihak yang melanggar proses audit data.
   1. **Hasil Identifikasi Kerangka Kerja Pengelolaan Keamanan Informasi**

Dalam upaya meningkatkan kinerja Sistem di perusahaan, maka perlu melakukan evaluasi terhadap aktifitas kerja terutama sistem kerja yang baik pada peningkatan pelayanan untuk masyarakat. Suatu kerangka kerja yang baik pasti akan menghasilkan nilai yang baik pula. Hasil dari penelitian dengan Indeks KAMI maka dapat disimpulkan sebagai berikut :







Gambar 2.5 Hasil Kerangka Kerja Pengolahan Keamanan Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan/diterapkan sebagian. Untuk skor kematangan 3, didapat dengan rumus : ( 2\* jumlah pertanyaan tingkat 1) + (4\*jumlah pertanyaantingkat 2)

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana :

Skor tingkat 1 : 21

Skor tingakt 2 : 20

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (21+20)=41.

Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar atau sama dengan (≥), dibandingkan dengan batas skor min kematangan 3 yaitu 54, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah valid, dan sebaliknya jika memenuhi syarat hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 < batas skor min kematangan 3, yaitu 41 < 54 dan status penilain tingkat kematangan 3 bernilai tidak valid.

Dari hasil evaluasi yang telah diteliti di atas dengan menggunakan Indeks KAMI maka dapat disimpulkan bahwa kerangka kerja yang ada masih belum layak. Hal ini dikarenakan masih banyak proses yang belum diterapkan sama sekali sehingga proses pelayanan terhadap karyawan masih sering terjadi keterlambatan.

**Rekomendasi Kerangka Kerja Keamanan Informasi**

Beberapa hal yang dapat diajukan untuk Kerangka Kerja Keamanan Informasi diantaranya :

1. Kerangka kerja keamanan informasi sebaiknya harus dibuat dan mendapat perhatian khusus dari para pemimpin bagian.
2. Kerangka kerja keamanan informasi sebaiknya dikomunikasikan ke setiap karyawan oleh para pimpinan bagian masing-masing di perusahaan.
3. Diterapkan kerangka kerja yang terpadu baik segi efektivitas maupun dari segi kualitas secara keseluruhan.
4. Adanya landasan hukum pelaksanaan keamanan informasi di dalam perusahaan.
   1. **Identifikasi Pengelolaan Asset Informasi**

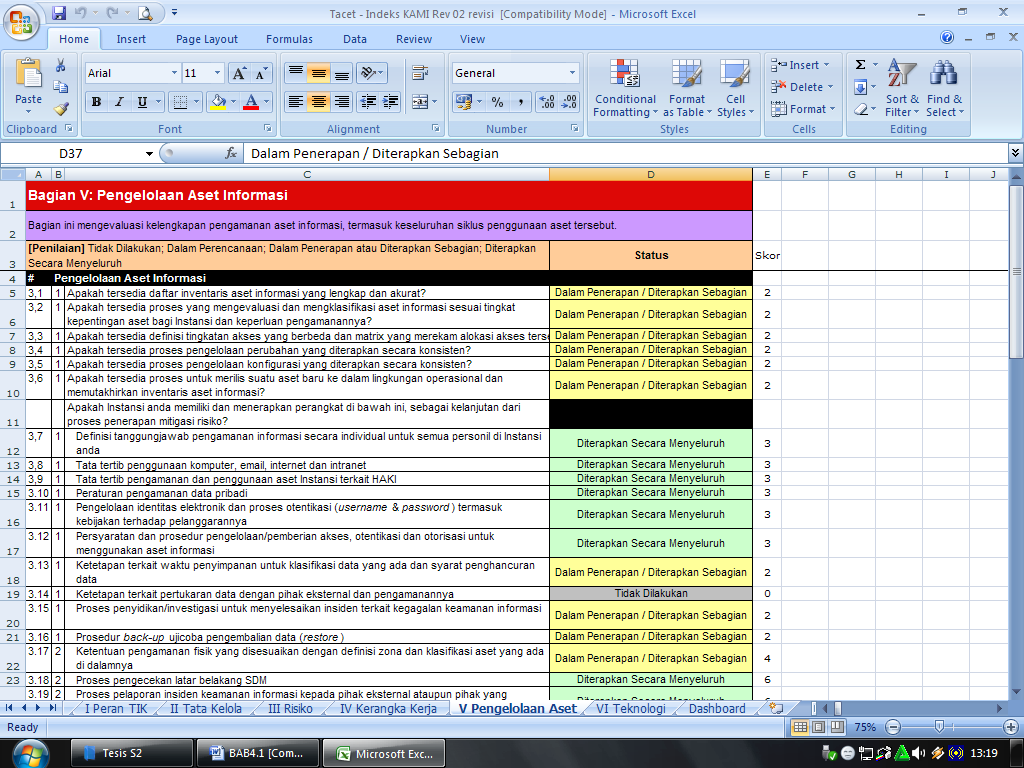
Asset merupakan suatu nilai yang sangat berharga bagi kelangsungan hidup suatu instansi terkait, sehingga harus dijaga dan dikelola dengan baik dan benar.Dengan adanya asset ini, pastinya pengguna TIK sangat dibutuhkan dan menjadi hal utama dalam pengelolaannya. Bebarapa asset yang diidentifikasi, di antaranya :

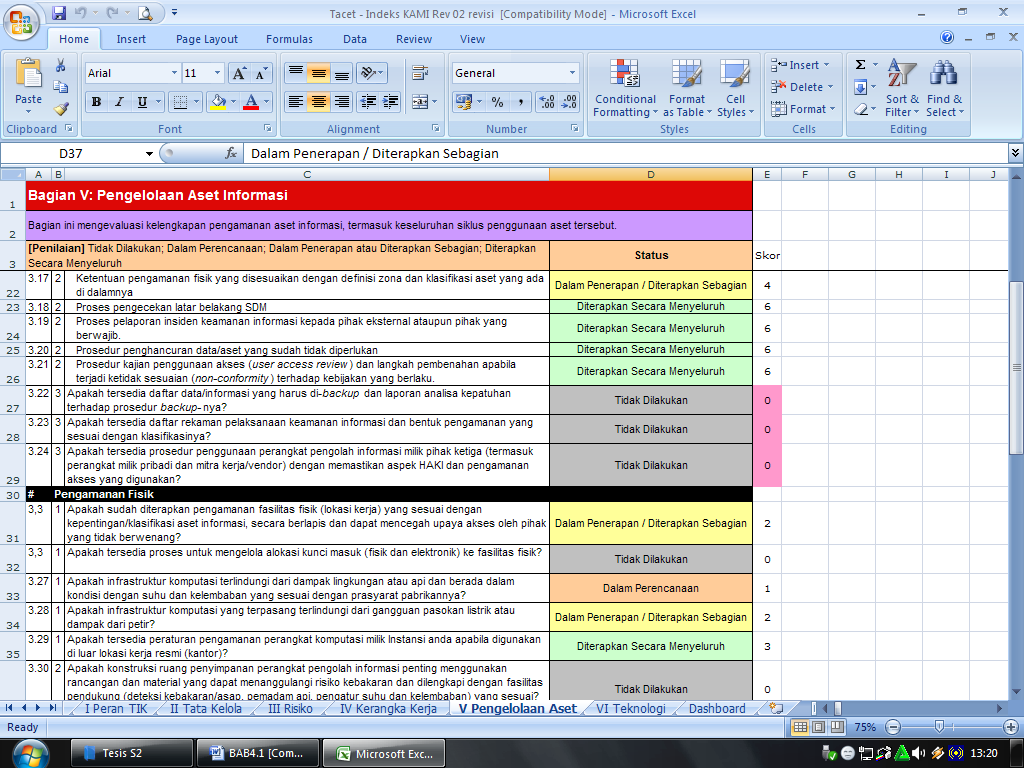
1. Konfigurasi jaringan
2. Perangkat jaringan komputer
3. Fasilitas internet yang digunakan

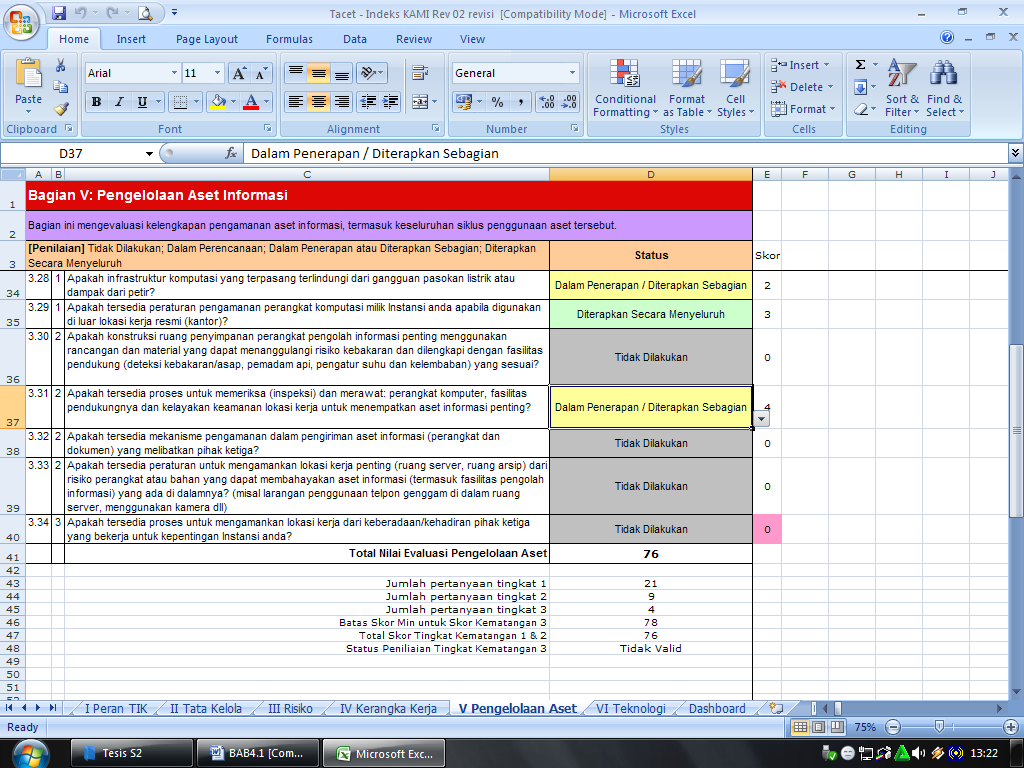
Infrastruktur Teknologi dan Informasi:

1. Spesifikasi Server
2. Spesifikasi Hardware (PC)
3. Sistem Operasi
4. Software kantor yang digunakan
5. Sistem Aplikasi

Dari hasil evaluasi yang didapat dengan menggunakan Indeks KAMI adalah sebagai berikut :







Gambar 2.6 Hasil Evaluasi Pengelolaan Asset Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan/diterapkan sebagian. Untuk skor kematangan 3, didapat dengan rumus :

( 2\* jumlah pertanyaan tingkat 1) + (4\*jumlah pertanyaan tingkat 2)

(2\*21) + (4\*9) = 76

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana :

Skor tingkat 1 : 46

Skor tingakt 2 : 32

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (46+32)=78.

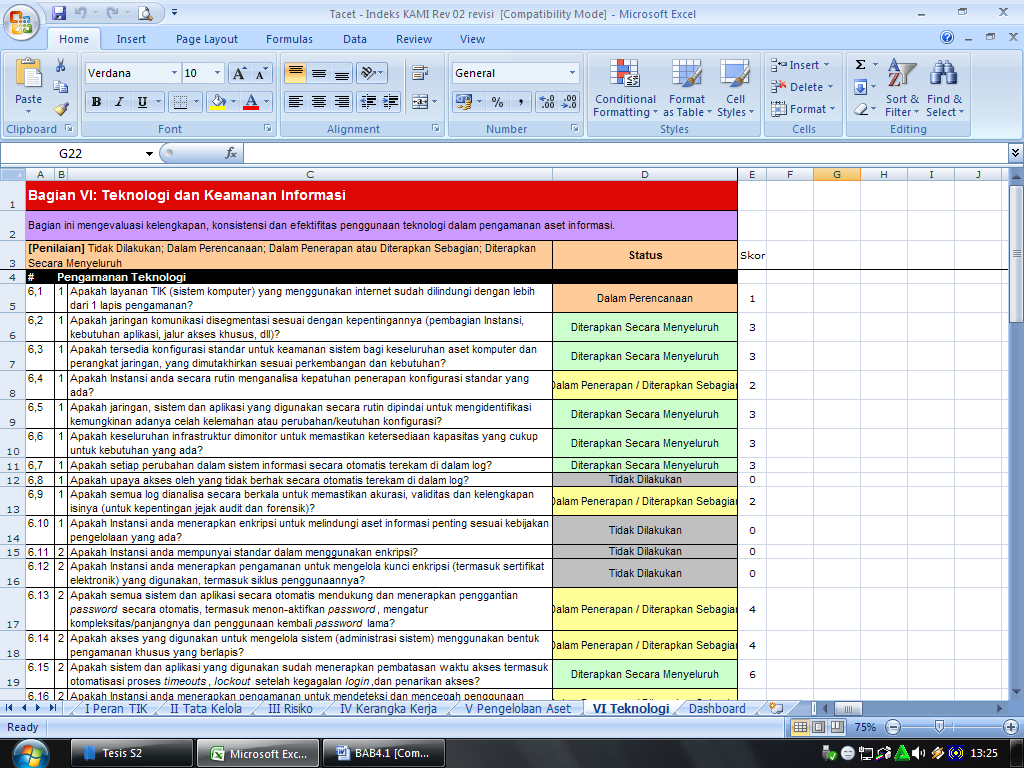
Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar atau sama dengan (≥), dibandingkan dengan batas skor min kematangan 3 yaitu 54, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah valid, dan sebaliknya jika memenuhi syarat hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 < batas skor min kematangan 3, yaitu 78 < 76 dan status penilain tingkat kematangan 3 bernilai valid.

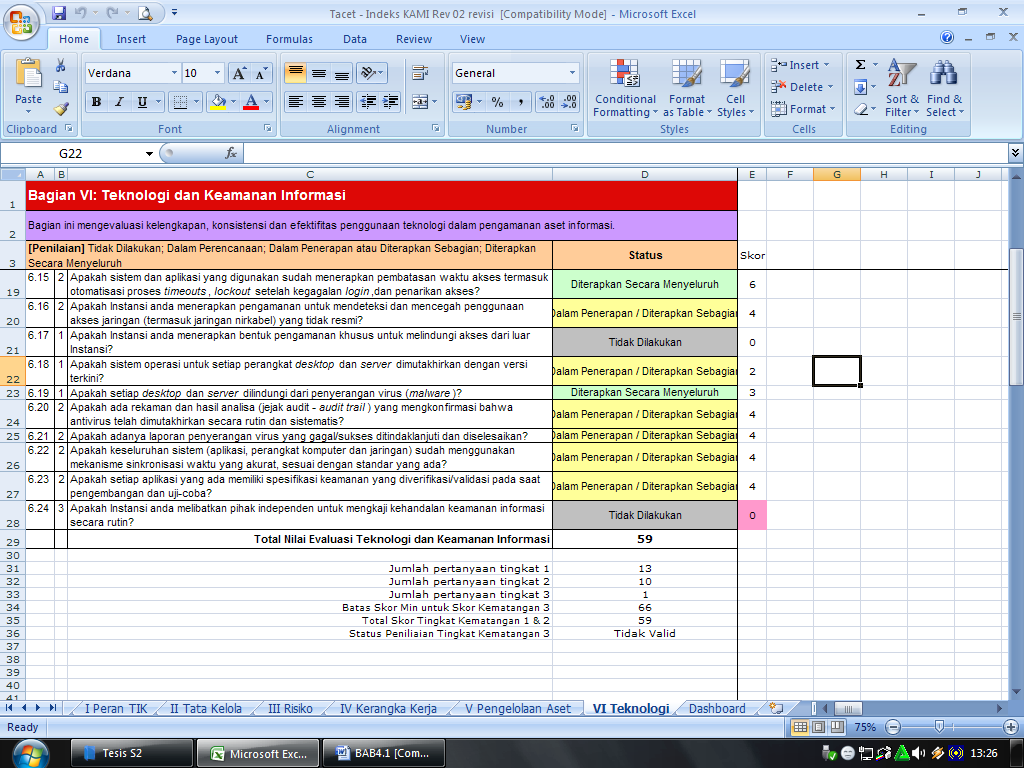
Dari gambar di atas maka dapat dievaluasi bahwa Pengolahaan Asset Informasi dan Teknologi ini sudah valid karena setiap bagian di perusahaan sebagian besar memiliki data asset yang lengkap dan akurat dan dipertanggung jawabkan dalam pengamanan data.

**Rekomendasi Asset Pengelolaan Informasi**

Walaupun Asset Informasi di perusahaan ini sudah dikatakan valid akan tetapi harus ada peningkatan untuk menjadi lebih baik lagi, beberapa rekomendasi yang diusulkan diantaranya :

1. Memastikan asset yang ada terhubung dengan sarana pengolahan informasi mempunyai pemilik atau tanggung jawab.
2. Pembatasan akses yang dikaji ulang secara berkala.
3. Kesadaran dari setiap penanggung jawab asset untuk meng-update informasi keamanan dan teknologi informasi.
   1. **Hasil Identifikasi Teknologi dan Keamanan Informasi**





Gambar 2.7 Hasil Teknologi dan Keamanan Sistem Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan/diterapkan sebagian. Untuk skor kematangan 3, didapat dengan rumus :

( 2\* jumlah pertanyaan tingkat 1) + (4\*jumlah pertanyaan tingkat 2)

(2\*13) + (4\*10) = 66

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana :

Skor tingkat 1 : 28

Skor tingakt 2 : 34

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (28+34)=62.

Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar atau sama dengan (≥), dibandingkan dengan batas skor min kematangan 3 yaitu 54, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah valid, dan sebaliknya jika memenuhi syarat hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 < batas skor min kematangan 3, yaitu 62 = 66 dan status penilain tingkat kematangan 3 bernilai tidak valid.

Dari hasil di atas maka dapat disimpulkan bahwa keamanan teknologi dan informasi rata-rata diterapkan secara menyeluruh, walaupun hasil yang diperoleh masih tidak valid dikarenakan skor akhir dari evaluasi tersebut masih di bawah batas skor minimal sehingga dapat disimpulkan kembali bahwa teknologi dan keamanan informasi masih butuh penerapan untuk yang lebih baik.

Beberapa hal yang sering terjadi pengaruh dari teknologi dan keamanan informasi diantaranya :

1. Terjadinya kemungkinan informasi di jaringan tidak terlindungi dan bisa terjadi hacker yang bisa membobol sistem di perusahaan.
2. Adanya virus jaringan yang terjadi dan ada juga pembobolan lewat jaringan.
3. Sering terjadi kegagalan dalam pengolahan data pada beberapa bagian dikarenakan sambungan jaringan wifi yang putus dan sangat berantakan.
4. Keterlambatan backup data sehingga koneksi pada server sering terjadi kesalahan pada IP Adders dan tidak ada yang memegangnya.

**Rekomendasi teknologi dan Keamanan Informasi**

Beberapa hal yang dapat direkomendasikan adalah sebagai berikut :

1. Memastikan jaringan komputer diatur dan dikontrol secara baik dan dapat memadai untuk memelihara keamanan pada sistem dan aplikasi yang menggunakan jaringan komputer.
2. Penggunaan Teknologi yang lebih baru untuk mendapatkan hasil yang baik dan maksimal.
3. Adanya proteksi jaringan untuk menjaga keamanan dari pihak yang tidak diinginkan.
4. **Hasil Evaluasi**

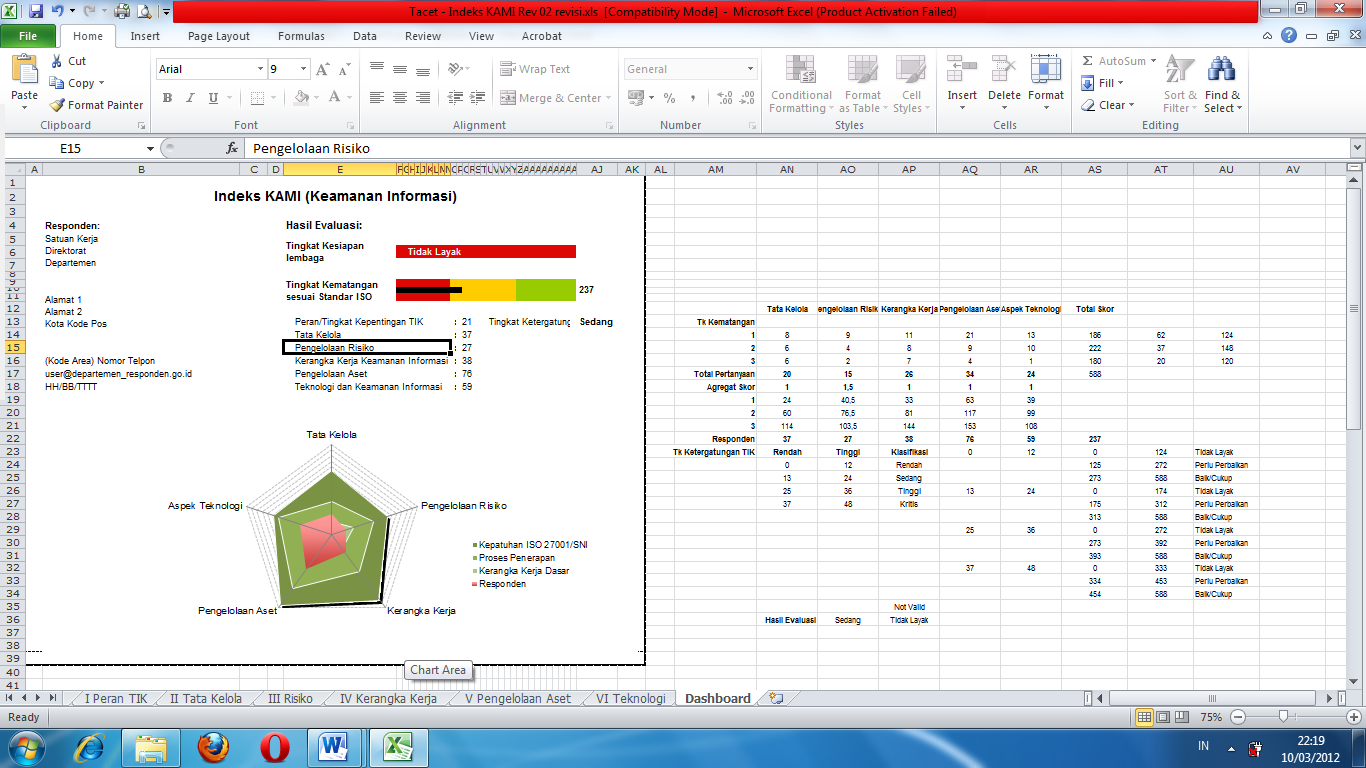
Untuk mengukur suatu tingkat kematangan kerangka kerja keamanan informasi yang memenuhi aspek keamanan berdasarkan ISO 27001:2005 ini menggunakan tools Indeks KAMI. Dimana terdapat Aspek penting yang perlu diketahui oleh setiap pimpinan bagian di perusahaan, diantaranya :

1. Tata Kelola Keamanan Informasi
2. Pengelolaan Risiko Keamanan Informasi
3. Kerangka Kerja Pengelolaan Keamanan Informasi
4. Pengelolaan Asset Informasi, dan
5. Teknologi Keamanan dan Informasi

Beberapa hal di atas akan dinilai kematangannya berdasarkan 3 kerangka penilaian, diantaranya :

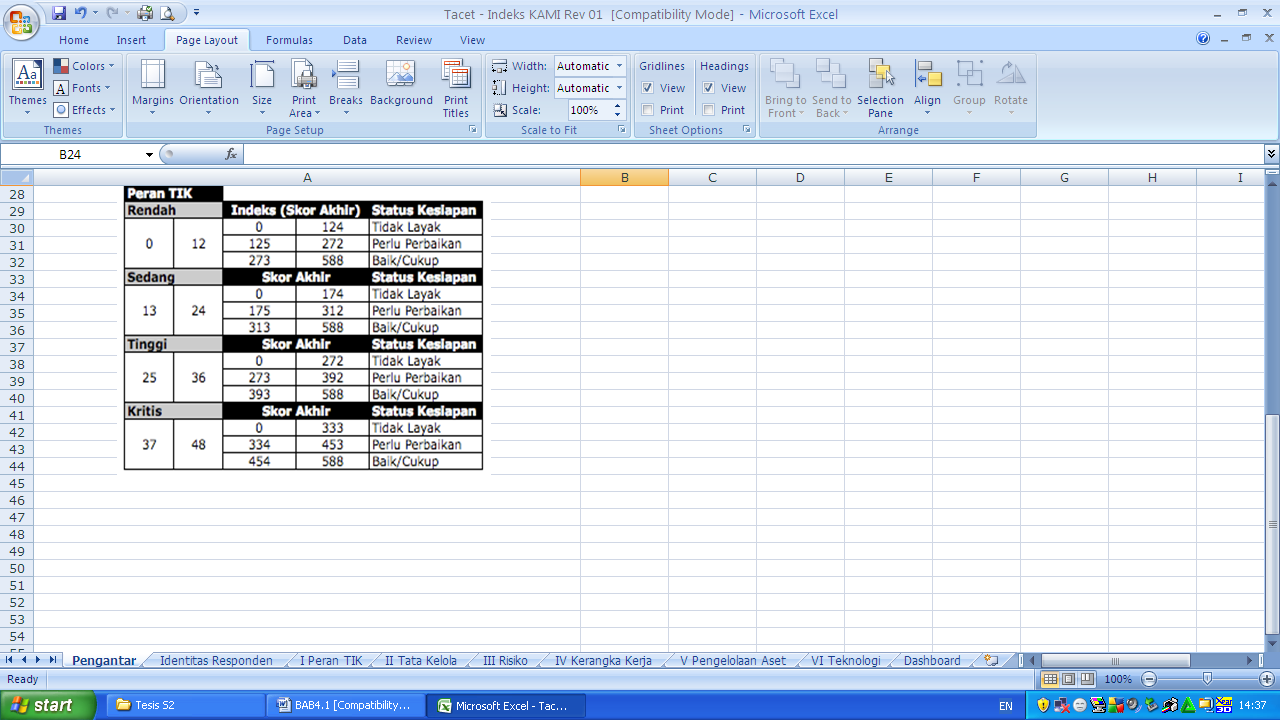
1. Keputusan ISO 2700/SNI
2. Proses Penerapan
3. Kerangka Kerja Dasar

Data yang didapat oleh penulis melalui kuesioner dan dihitung rata-rata untuk mendapatkan hasil akhir yang dimasukan ke dalam bagian-bagian Indeks KAMI seperti gambar 2.6 sampai dengan gambar 3.7, maka dapat dihasil Dashbordnya sebagai berikut :

****

Gambar 3.8 Dashboard Hasil Evaluasi Berdasarkan Indek KAMI

Berdasarkan hasil evaluasi gambar di atas bahwa perusahaan memiliki tingkat ketergantungan yang sangat tinggi terhadap pengguna TIK, dengan skor nilai akhir tingkat ketergantungan tersebut yaitu 28 dari batas nilai 26-34. Untuk tingkat kematangan sesuai standar ISO 27001 bahwa perusahaan sudah memasuki 1/3nya ke dalam proses penerapan yaitu tingkat yang ke 2 dengan nilai hasil akhirnya adalah 249, dikarenakan bebarapa aspek yang diketahui seperti aspek teknologi, tata kelola, kerangka kerja serta pengolahan asset sudah dalam proses penerapan walaupun belum begitu maksimal. Sedangkan untuk satu aspek yang masih belum menuju proses penerapan yaitu pengolahan risiko, dimana aspek ini masih berada dalam kerangka kerja dasar.



Sumber : Depkominfo 2008

Gambar 3.9 TIK dan Indeks Skor Akhir

Dengan skor akhir 249 yang masuk kedalam tingkat ketergantungan yang tinggi maka status kesiapan perusahaan bisa dijadikan acuan setiap pemimpin kepala bagian atau pun atasan langsung. Untuk melakukan pembenahan atau perubahan manejerial demi menjaga keamana sistem informasi dan teknologi yang sedang berjalan dari pihak atau ancaman yang tidak diinginkan.

1. **KESIMPULAN**

Penerapan keamanan sistem informasi yang ada pada PT. AXA Mandiri Financial Service dalam Pengolahaan Asset Informasi dan Teknologi ini sudah valid karena setiap bagian di perusahaan sebagian besar memiliki data asset yang lengkap dan akurat dan dipertanggung jawabkan dalam pengamanan data.Kerangka kerja keamanan sistem informasi dan kebijakannya berdasarkan tingkat kebutuhan pengguna rata-rata diterapkan secara menyeluruh, walaupun hasil yang diperoleh masih tidak valid dikarenakan skor akhir dari evaluasi tersebut masih di bawah batas skor minimal sehingga dapat disimpulkan kembali bahwa teknologi dan keamanan informasi masih butuh penerapan untuk yang lebih baik.Tingkat keamanan sistem informasi berdasarkan hasil analisis menggunakan metode Indeks KAMI bahwa perusahaan memiliki tingkat ketergantungan yang sangat tinggi terhadap pengguna sistem informasi, dengan skor nilai akhir tingkat ketergantungan tersebut yaitu 28 dari batas nilai 26-34. Untuk tingkat kematangan sesuai standar ISO 27001 bahwa perusahaan sudah memasuki 1/3nya ke dalam proses penerapan yaitu tingkat yang ke 2 dengan nilai hasil akhirnya adalah 249, dikarenakan bebarapa aspek yang diketahui seperti aspek teknologi, tata kelola, kerangka kerja serta pengolahan asset sudah dalam proses penerapan walaupun belum begitu maksimal. Sedangkan untuk satu aspek yang masih belum menuju proses penerapan yaitu pengolahan risiko, dimana aspek ini masih berada dalam kerangka kerja dasar.

**Daftar Pustaka**

Ariefianto, Eko. 2006. **Perencanaan Tata Kelola Keamanan Informasi Berdasarkan ISMS ISO 27001.** Fasilkom UI.

Afrianto, Irawan. 2015. **Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009**. Fakultas Teknik dan Ilmu Komputer. Universitas Multimedia Nusantara.

Arikunto, Suharsimi. 2010. **Prosedur Penelitian : Suatu Pendekatan Praktik.** Jakarta. Penerbit : PT Rineka Cipta.

Ferbrian, Jack. 2004. **Pengetahuan Komputer dan Teknologi Informasi**. Bandung. Penerbit : Informatika.

Lastyono Putra, Endi. 2014. **Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. dengan Menggunakan Indeks Keamanan Informasi (KAMI).** Jurusan Sistem Informasi. Fakultas Teknologi Informasi. Institut Teknologi Sepuluh Nopember (ITS).

McLeod, Jr, Raymond. 2004. **Sistem Informasi Manajemen, Jilid 8**. PT. Buana Ilmu Populer.

Nazir, Moh. 2005. **Metode Penelitian**. Bogor. Penerbit : Ghalia Indonesia.

Syafrizal, Melwin. 2005. **Information Security Management System (ISMS) Menggunakan Standar Iso/Iec 27001.**