Sahl Ramadhan_5M51

by Sahlramadhan

General metrics

10,069	1,290	10	5 min 9 sec	9 min 55 sec
characters	words	sentences	reading time	speaking time

Writing Issues

No issues found

Unique Words

Measures vocabulary diversity by calculating the percentage of words used only once in your document

1%

unique words

Rare Words

Measures depth of vocabulary by identifying words that are not among the 5,000 most common English words.

23%

rare words

Word Length

Measures average word length

0.1

characters per word

Sentence Length

Measures average sentence length

129

words per sentence

Sahl Ramadhan_5M51

1

REVIEW JURNAL AUDIT SISTEM INFORMASI

Judul

Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019

Lembaga Pengindexs

Jurnal / Alamat

Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi Bandung

https://ojs.unikom.ac.id/index.php/jtk3ti/article/view/9672/3667

Vol. & Hal.

Volume 9 Nomor 1

Tahun

Tahun 2023

Penulis

Asro Nasiri

Tanggal

13 November 2024

Reviewer

Sahl Ramadhan (22.230.0130) 5M51

Abstrak

Ketergantungan organisasi terhadap dukungan tekonlogi imformasi semakin besar. Proses bisnis saat ini hamper tidak ada yang tidak menggunakan teknologi informasi untuk meningkatkan daya siang.
Penggunaan teknologi informasi harus disertasi dengan peningkatan keamanan informasinya. Gangguan terhadap keamanan informasi di organisasi akan menghambat pencapaian tujuan dan strategi organisasi. Informasi saat ini merupakan aset yang sangat penting bagi universitas XYZ, karena itu evaluasi terhadap seberapa baik pengendalian dan kegiatan dalam melindungi aset informasi perlu dilakukan di universitas XYZ. Evaluasi dilakukan menggunakan kerangka kerja COBIT 2019 pada domain APO12, APO13 dan DSS05 untuk mengidentifikasi berapa tingkat kapabilitas universitas XYZ dalam mengelola keamanan informasi. Hasil evaluasi menunjukkan pengelolaankeamanan informasi di Universitas XYZ masih di tingkat kepabilitas 2 untuk domain APO12, APO13 dan DSS05

Pendahuluan

Peran teknologi informasi dalam mendukung proses bisnis organisasi saat ini cukup tinggi. Penggunaan teknologi informasi harus juga disertasi dengan pengendalian terhadap faktor resikonya yaitu resiko kehilangan atau penyalahgunaan data karena aset informasi saat ini menarik bagi penyerang baik karena motif ekonomi atau motif lainnya [1] Informasi merupakan aset berharga bagi organisasi sehingga keamanan informasi menjadi penting untuk dikendalikan sesuai standar.
Keamanan informasi mempertimbang keamanan sistem komputer untuk melindunginya dari pengungkapan, modifikasi subyektif, akses tidak sah, pelecehan, atau perusakan yang bertujuan untuk memastikan integritas, kerahasiaan, dan ketersediaan informasi [2] Keamanan informasi adalah

bagian penting dari operasi organisasi mana pun, karena membantu melindungi aset teknologi dan informasi yang digunakan oleh organisasi. Keamanan informasi mencakup perlindungan informasi terhadap berbagai ancaman yang bertujuan untuk meminimalkan risiko aktivitas bisnis, memaksimalkan pengembalian investasi, memanfaatkan peluang bisnis, dan memastikan kelangsungan bisnis. Pertimbangan keamanan informasi menargetkan integritas, kerahasiaan, dan ketersediaan sumber daya informasi. Manajemen keamanan sistem informasi bertujuan untuk meminimalkan risiko yang dihadapi sistem informasi dalam operasinya

Kajian Pustaka

Evaluasi terhadap tingkat kepabilitas organisasi dalam pengendalian keamanan informasi dapat mengacu ke beberapa kerangka kerja seperti misalnya ISO 27001, ITIL,atau COBIT[6].

Pada penelitian ini kerangka kerja yang digunakan adalah COBIT 2019 yang merupakan versi terbaru dari COBIT. COBIT 20019 terdiri dari 40 kegiatan yang memberikan acuan praktek baik dalam mengelola TI baik dari sisi perencanaan, operasional maupun pengawasan kinerjanya[7]. 40 kegiatan dari COBIT 2019yang terkait dengan aspek keamanan hanya ada 3 domain yaitu domain APO12 (managed risk), APO13 (managed security) dan DSS05 (managed security services)

Beberapa penelitian sebelumnyayangtelah dilakukan untukevaluasi keamanan informasi menggunakan COBIT diantaranyayang dilakukan oleh Lilis [8] yang menggunakan COBIT 5 untuk mengevaluasi sebuah perusahaan yang menghasilkan skor tingkat kapabilitas, analisis gapdan juga rekomendasi peningkatan pengendalian keamanan

Penelitian lain ada yang menggunakanCOBIT 2019 tetapi untuk mendesain keamanan informasi di POLRI yang menghasilkan cetak biru implementasi keamanan informasi [9], bukan untuk melakukan evaluasi pengendalian keamanan. Penelitian berikut ini juga menggunakan COBIT 2019 untuk mendesain tata kelola keamanan e-governance [10]
Penelitian lain mengkombinasikan COBIT 2019 dan ITIL 4 untuk mengevaluasi tata kelola (govern) dan manajemen sebuah orgniasasi dengan terlebih dahulu memetakan proses teknologi informasi yang ada baik di COBIT 2019 dan ITIL 4.

Metode / Framework yang digunakan

Pemilihan Domain
Pengumpulan data: wawancara, kuisioner, dan observas
Menentukan tingkat kapabilitas (capability level): Capability and Maturity Model Integration (CMMI)
Proses pemeringkatan: NPFL yaitu Note, Partially, Fully, dan Largerly.
Rekomendasi
Framework: COBIT 2019

Hasil penelitian

Pemilihan Domain
Pemilihan proses dengan menggunakan perangkat faktor desain menghasilkan 3 domain dengan skor tertinggi yaitu domain terkait keamanan dan resiko informasi antara lain APO12, APO13 dan DSS05
Pemilihan responded

Pemetaan RACI COBIT 2019 terhadap struktur organisasi Universtas XYZ yang terkait dengan tugas dan wewenang keamanan informasi menghasilkan 4 responden untuk proses wawancara dan pengisian kuisioner. Kuisioner menggunakan pernyataan persyaratan yang terdapat di buku COBIT 2019 Design and Objective [1]

Perhitungan tingkat kapabilitas

Proses APO12:

Karena pada proses APO12 yang berada di capability level 2, hanya mendapatkan nilai 17% yang berarti ada di level partially, maka proses pengukuran capability leveldi level 3 tidak bisa dilakukan. Perlu dilakukan perbaikan di level 2 sebelum dapat diukur di level diatasnya.

Temuan: Universitas XYZ belum memiliki upaya yang memadai untuk mengidentifikasi dan mengelola risiko TI, seperti tidak adanya risk register dan catatan insiden yang memadai.

Rekomendasi:

Menetapkan metode pengumpulan dan analisis data terkait risiko TI.

Membangun dan memelihara catatan risiko TI serta insiden yang terjadi.

Proses APO13

Karena pada proses APO13 yang berada di capability level 2, hanya mendapatkan nilai 28% yang berarti ada di level partially, maka proses pengukuran capability leveldi level 3 tidak bisa dilakukan. Perlu dilakukan perbaikan di level 2 sebelum dapatdiukur di level diatasnya.

Rekomendasi untuk perbaikan di proses ini supaya bisa mencapai capability level 3adalah:

1.Tentukan ruang lingkup dan batasan sistem manajemen keamanan informasi (ISMS) dalam kaitannya dengan karakteristik organisasi yaitu sebagai universitas yang menyelenggarakan kegiaatan akademik, lokasinya, aset yang

dianggap penting, dan teknologi yang digunakan saat ini. Sertakan juga detail, dan justifikasinya kalau ada, pengecualian dari cakupan.

2.Tetapkan ISMS sesuai dengan kebijakan universitas terkait keamanan informasi dalam dunia Pendidikan

3.Selaraskan ISMS dengan pendekatan universitas secara keseluruhan dalam pengelolaan keamanan

4.Mempersiapkan dan memelihara pernyataan implementasi yang menjelaskan ruang lingkup SMKI

5.Menetapkan dan mengomunikasikan peran dan tanggung jawab manajemen keamanan informasi

Proses DSS05:

Proses DSS05 dari perhitungan diatas saat ini sebesar 69% yang berarti masih berada di level largerly(sebagian besar terpenuhi). Karena angka yang tercapai belum memenuhi kriteria Fully maka pengukuran pada capability level 3tidak bisa dilakukan sebelum ada perbaikan di level 2

Rekomendasi yang kami usulkan untuk peningkatan perbaikan pengelolaan layanan keamanan informasi supaya naik ke level 3 adalah sebagai berikut:Semua perangkat keras bekas yang masuk kategori endpointdeviceseperti server, komputer, laptop, harus dibuang dengan aman karena ada potensi data data penting yang tersimpan di perangkat tersebut bisa dipulihkan lagi oleh pihak yang tidak berhak.

Kesimpulan

Berdasarkan evaluasi pelaksanaan pengendalian keamanan informasi di Universitas XYZ untuk persyaratan domain APO12 yaitu mengelola resiko diperoleh hasil 20% pada evaluasi tingkat kapabilitasnya tingkat 2. Perolehan

angka 20% ini menunjukkan implementasi pengendalian resiko masih dilaksanakan sebagian saja (partly).
Sedangkan pada domain APO13 yaitupengendalian keamanan informasi diperoleh hasil sebesar 28% pada evaluasi tingkat kapabilitasnya di tingkat 2 yang artinya pelaksanaan SMKI masih jauh dari persyaratan yang distandarkan oleh COBIT 2019 karena secara pelaksanaan masih sebagian kecil (partly). Selain itu juga harus ada bagian yang khusus menangani kegiatan pengendalian keamanan informasi.
Pelaksanaan keamanan informasi untuk domain DSS05 yaitu Layanan keamanan informasi hasil perhitungan tercapai sebesar 69% pada tingkat kapabilitas 2 dan pelaksanaannya sudah sebagian besar (largely) persyaratan telah dilakukan.

Pendapat Reviewer
Pemilihan kerangka kerja COBIT 2019 merupakan kerangka kerja evaluasi yang tepat di gunakan di khasus ini dengan menggunakan COBIT 2019 ini meningkatkan standar internasional yang banyak di gunakan dalam mengelola keamanan informasi di berbagai organisasi
Untuk hasil evaluasi kapabilitas disini ada beberapa hasil yaitu dengan proses APO12 itu mendapatkan hasil mencapai 17% di level kapabilitas 2, yang berarti bahwa pengelolaan risiko TI masih sangat terbatas dan perlu banyak perbaikan.
Ada juga hasil proses APO13 yang mendaptkan hasil 28%, proses pengelolaan keamanan informasi juga masih berada pada tahap yang sangat awal.
Beberapa elemen penting dalam pengelolaan Sistem Manajemen Keamanan Informasi (SMKI), seperti ruang lingkup, kebijakan, dan komunikasi peran serta

tanggung jawab, belum diterapkan secara optimal. Dan ada juga hasil dari proses DSS05 dengan hasil 69%, namun pengelolaan layanan keamanan informasi belum mencapai tingkat optimal (fully) karena masih ada beberapa area yang belum sepenuhnya dilaksanakan. Meskipun demikian, pencapaian largely menunjukkan bahwa sebagian besar persyaratan telah dipenuhi, tetapi ada ruang untuk perbaikan.

Penting untuk segera mengambil langkah-langkah perbaikan yang disarankan, terutama dalam hal pengelolaan risiko, penetapan kebijakan keamanan informasi yang lebih kuat, dan penerapan kontrol keamanan yang lebih ketat di seluruh tingkat organisasi. Dengan ini, Universitas XYZ akan lebih siap untuk melindungi aset informasi mereka dari ancaman yang semakin kompleks.