Nama Kelompok :

1. Eristya Rieke Firnanda [3130023001]
2. Rama Wahyu Satrio [3130023006]
3. Fara Fadillah Namira Adjani [3130023019]
4. Moch. Azizi Alfarizki [3130023043]
5. Moh. Qois Fathur Rohman [3130023045]

Judul Artikel :

RISK ASSESSMENT MATURITY LEVEL OF ACADEMIC INFORMATION SYSTEM USING ISO 27001 SYSTEM SECURITY ENGINEERING-CAPABILITY MATURITY MODEL

Topik yang dibahas:

Penilaian Tingkat Kematangan Risiko Sistem Informasi Akademik (AIS) menggunakan standar ISO 27001 System Security Engineering-Capability Maturity Model (SSE-CMM). Tujuan utamanya adalah untuk menentukan tingkat layanan AIS saat ini dengan mengukur kematangan dan risiko keamanannya.

Ringkasan:

Penelitian ini bertujuan untuk menentukan tingkat kematangan dan risiko keamanan layanan Sistem Informasi Akademik (SIA) pada Fakultas Sains dan Teknologi di UIN Syarif Hidayatullah Jakarta. Metode yang digunakan adalah kuantitatif dengan mengukur tiga klausul ISO 27001 menggunakan model SSE-CMM: Manajemen Aset, Keamanan Sumber Daya Manusia, dan Kontrol Akses.

Hasil penelitian menunjukkan bahwa nilai rata-rata kontrol keamanan informasi pada SIA adalah 3.51, yang diklasifikasikan sebagai Level 3 (Defined) dalam SSE-CMM, namun disimpulkan sebagai "baik atau rata-rata pemrosesan standar telah dilakukan mengikuti prosedur" dan termasuk dalam Level 4 (Managed) berdasarkan interpretasi penulis pada bagian gap analysis. Secara spesifik per klausul, Manajemen Aset berada di Level 3.29 (Defined), Keamanan Sumber Daya Manusia di Level 4.00 (Managed), dan Kontrol Akses di Level 3.24 (Defined).

Terdapat gap rata-rata sebesar 1.49 antara kondisi saat ini (rata-rata 3.51) dan kondisi yang diharapkan (Level 5 - Optimized). Rekomendasi diberikan untuk masing-masing klausul guna meningkatkan layanan keamanan informasi

Latar Belakang:

Penelitian ini dilatarbelakangi oleh kenyataan bahwa layanan akademik yang cepat dan tepat, sangat bergantung pada Sistem Informasi Akademik (AIS) yang didukung oleh teknologi informasi dan sumber daya manusia (SDM) yang memadai. Stabilitas layanan aplikasi ini sangat ditentukan oleh keamanan sistem informasi. Pemerintah mewajibkan implementasi Tri Dharma Perguruan Tinggi (pendidikan, penelitian, dan pengabdian masyarakat) dalam sistem informasi akademik di setiap universitas di Indonesia. Oleh karena itu, penelitian ini bertujuan untuk mengukur tingkat layanan AIS dengan menentukan tingkat kematangan dan risiko keamanannya, menggunakan standar internasional ISO/IEC 27001:2005 dan SSE-CMM sebagai tolok ukur. Responden penelitian ini adalah unit kerja pendidikan di Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta.

Landasan Teori:

A. ISO/IEC 27001:2005

ISO/IEC 27001 adalah standar internasional yang mengatur sistem manajemen keamanan informasi (SMKI). Standar ini menyediakan kerangka kerja dan seperangkat prinsip untuk menangani risiko keamanan informasi dalam organisasi. ISO 27001 dibagi menjadi 14 fase dan berisi 11 klausul yang terbagi menjadi 133 kontrol. ISO 27001 direkomendasikan sebagai dasar untuk merancang dan menilai tingkat kapabilitas manajemen keamanan informasi SIA.

B. Sistem Security Engineering-Capability Maturity Model (SSE-CMM)

SSE-CMM adalah model referensi proses yang berfokus pada persyaratan untuk mengimplementasikan keamanan dalam serangkaian sistem terkait dalam domain keamanan TI. Penilaian dengan SSE-CMM dapat menentukan tingkat kapabilitas setiap area proses, yang berguna sebagai fokus perbaikan. Tingkat kapabilitas SSE-CMM terdiri dari 5 Level:

1. Level 1, Performed Informally: Kinerja dasar mungkin tidak direncanakan dan dilacak dengan cermat.
2. Level 2, Performed Informally: Kinerja sesuai dengan prosedur yang ditentukan terverifikasi.
3. Level 3, Performed Informally**:** Praktik dasar dilakukan sesuai dengan proses yang terdefinisi dengan baik.

4. Level 4, Performed Informally: Ukuran kinerja terperinci dikumpulkan dan dianalisis.
5. Level 5, Performed Informally: Target kinerja kuantitatif untuk efektivitas dan efisiensi proses.

C. Risiko

Risiko didefinisikan sebagai kemungkinan sesuatu yang mempengaruhi tujuan. Terdapat empat aspek utama dari penilaian risiko keamanan: identifikasi Ancaman, memprioritaskan Ancaman berdasarkan risiko, memutuskan tindakan pengendalian dan perlindungan, dan mengembangkan strategi untuk implementasi tindakan tersebut. Model penilaian risiko mencakup: Ancaman (Hazards), Aset Berisiko (Assets at Risk), dan Dampak (Impacts)

Hasil:

Hasil pengukuran menunjukkan bahwa nilai rata-rata kontrol keamanan informasi pada AIS adalah 3.51. Nilai ini menyiratkan bahwa pemrosesan standar telah dilaksanakan dengan baik atau rata-rata dan mengikuti prosedur. Secara spesifik per klausul, tingkat kematangan yang dicapai adalah:

1. Klausul 7 (Manajemen Aset): 3.29, yang didefinisikan sebagai level 3.
2. Klausul 8 (Keamanan Sumber Daya Manusia): 4.00, yang berarti proses telah dikelola (*handled*) dan termasuk level 4.
3. Klausul 11 (Kontrol Akses): 3.24, yang menunjukkan bahwa proses didokumentasikan, terjamin kualitasnya, dan memiliki metode manajemen perubahan, dan termasuk level 3.

Berdasarkan audit keamanan, sistem manajemen kata sandi (kontrol 11.5.3) memiliki nilai terendah, yaitu 2.73, karena peraturan yang kurang ketat dan spesifik mengenai kerahasiaan kata sandi, yang berpotensi menyebabkan kebocoran informasi.

Gap Analysis dan Rekomendasi

Analisis kesenjangan (Gap Analysis) menunjukkan bahwa tingkat kematangan saat ini (rata-rata 3.51) berada di bawah tingkat kematangan yang diharapkan, yaitu Level 5 (Optimized). Terdapat gap rata-rata sebesar 1.49 antara kondisi saat ini dan kondisi yang diharapkan. Klausul yang memiliki gap terbesar adalah Kontrol Akses (Klausul 11), dengan gap 1.76, sedangkan gap terendah ada pada Klausul 8 (Keamanan SDM) dengan nilai 1.00.

Rekomendasi utama yang diberikan untuk perbaikan adalah:

1. Manajemen Aset (Klausul 7): Pemeliharaan aset yang rutin (misalnya bulanan) untuk melindungi dari virus, serta penambahan aset yang diperlukan untuk mendukung kinerja.
2. Keamanan SDM (Klausul 8): Pembaruan standar operasional dan persyaratan kerja, serta perlunya wawancara dan tes untuk menentukan kapabilitas calon anggota organisasi sebelum bekerja.
3. Kontrol Akses (Klausul 11): Memaksa pengguna untuk mengubah kata sandi mereka setelah jangka waktu tertentu dan menolak penggunaan kata sandi yang sama dengan yang pernah digunakan sebelumnya, serta menyimpan kata sandi dengan aman (terenkripsi).

Kesimpulan:

Secara keseluruhan, tingkat kematangan keamanan informasi pada Sistem Informasi Akademik (SIA) berdasarkan tiga klausul ISO 27001 (Manajemen Aset, Keamanan Sumber Daya Manusia, dan Kontrol Akses) adalah 3.51. Skor ini menunjukkan bahwa kontrol keamanan berada pada Level 3 atau Level 4 (Managed) dengan interpretasi bahwa pemrosesan standar telah dilakukan dengan baik atau rata-rata dan mengikuti prosedur. Meskipun sudah mencapai level "Defined/Managed," diperlukan penyesuaian untuk menutup gap sebesar 1.49, terutama pada Klausul 11 (Kontrol Akses), yang memiliki gap tertinggi (1.76) dan masalah utama terkait kebijakan dan pelaksanaan sistem manajemen kata sandi.