BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang dilakukan terhadap tingkat keamanan informasi di perusahaan Gk Jeans Group menggunakan pendekatan INDEKS KAMI (Keamanan Informasi), dapat disimpulkan bahwa secara umum tingkat kesiapan dan kematangan pengelolaan keamanan informasi pada perusahaan ini masih berada pada tahap awal dan belum memenuhi kriteria kelayakan.

Pada evaluasi Indeks KAMI menunjukkan variasi tingkat kematangan keamanan informasi dengan skor Tata Kelola (13/Tingkat I) yang masih sangat dasar, Pengelolaan Risiko (23/Tingkat I+) yang mulai menunjukkan kesadaran risiko namun belum optimal, Kerangka Kerja Keamanan Informasi (50/Tingkat II) sebagai dimensi terkuat yang sudah memiliki struktur memadai, Pengelolaan Aset (33/Tingkat I+) yang sudah mulai terkelola namun masih memerlukan penyempurnaan, serta Teknologi dan Keamanan Informasi (61/Tingkat I+) yang secara teknis cukup mumpuni namun belum terintegrasi sempurna dengan kebijakan, sehingga secara keseluruhan organisasi perlu fokus pada peningkatan tata kelola dan manajemen risiko sambil mempertahankan kualitas kerangka kerja yang telah baik.

Sementara itu, Skor Kategori SE sebesar 11 mengindikasikan bahwa perusahaan masih berada pada tahap dasar dalam perencanaan keamanan informasi. Hasil akhir menunjukkan bahwa status kelayakan perusahaan adalah "Tidak Layak" berdasarkan kriteria INDEKS KAMI.

Dengan demikian, dapat disimpulkan bahwa tingkat keamanan informasi di perusahaan Gk Jeans Group belum dikelola secara optimal. Perusahaan belum memiliki kebijakan dan implementasi yang menyeluruh dalam aspek tata kelola, manajemen risiko, hingga infrastruktur teknis keamanan informasi. Hal ini menjawab rumusan masalah bahwa penerapan sistem keamanan informasi di Gk Jeans Group masih perlu ditingkatkan, baik dari sisi perencanaan strategis maupun pelaksanaan operasionalnya.

5.2 Rekomendasi

Berikut adalah rekomendasi spesifik perbaikan tata kelola keamanan informasi :

1. Tata Kelola Keaman Informasi : Bentuk komite tata kelola TI dan tunjuk CISO, kembangkan kebijakan keamanan yang komprehensif, tetapkan tanggung jawab yang jelas, dan lakukan pelatihan kesadaran keamanan untuk semua karyawan.
2. Pengelolaan risiko keamanan : lakukan assessment risiko secara menyeluruh, terapkan framework manajemen risiko standart (ISO 27005 atau NIST SP 800-30)

3. Penyempurnaan kerangka kerja: sesuaikan framework dengan standart internasional lalu kembangkan dokumentasi prosedur operasional.

5.3 Saran

Berdasarkan hasil yang diperoleh dan berbagai kendala yang ditemukan dalam proses evaluasi, penulis menyampaikan beberapa saran sebagai berikut:

1. Perusahaan perlu segera menyusun dan mendokumentasikan kebijakan keamanan informasi yang bersifat formal dan mengikat, serta mengembangkan kerangka kerja yang komprehensif agar implementasi keamanan informasi dapat berjalan secara sistematis dan terukur.
2. Perlu ditunjuk penanggung jawab keamanan informasi secara struktural, dengan eskalasi pelaporan ke tingkat manajemen puncak, agar pengelolaan risiko dan pengambilan keputusan terkait keamanan informasi lebih efektif dan cepat.
3. Perusahaan disarankan untuk melakukan identifikasi dan klasifikasi terhadap seluruh aset informasi yang dimiliki, beserta tingkat kritikalitasnya. Hal ini penting sebagai dasar untuk penerapan kontrol keamanan yang sesuai.
4. Penguatan pada sisi teknologi, seperti penerapan firewall, enkripsi, sistem deteksi intrusi, segmentasi jaringan, serta pengelolaan hak akses, harus dilakukan agar perlindungan terhadap data dan sistem menjadi lebih kuat.
5. Perusahaan perlu membangun siklus evaluasi dan audit keamanan informasi secara berkala, untuk memastikan bahwa langkah-langkah mitigasi yang

diterapkan tetap relevan, efektif, dan adaptif terhadap ancaman yang terus berkembang.

6. Seluruh karyawan, khususnya yang terlibat dalam pengelolaan sistem informasi, harus diberikan pelatihan dan sosialisasi tentang pentingnya keamanan informasi, agar tercipta budaya keamanan di lingkungan kerja.