MANFAAT PEREALISASIAN TATA KELOLA KEAMANAN INFORMASI BERBASIS SNI ISO/IEC 27001:2009 PADA PRODUKSI FILM ANIMASI (Kasus di PT. XX)

Ayu Candra Dewi[1], Eko Nugroho[2], Rudy Hartanto[3]
Departemen Teknik Elektro dan Teknologi Informasi, Universitas Gadjah Mada
Jl. Grafika No.2 Yogyakarta – 55281, Bula Sumur, Sleman, Yogyakarta, Indonesia
ayu.cio15@mail.ugm.ac.id[1], nugroho@ugm.ac.id[2], rudy@ugm.ac.id[3]

Abstrak

Resiko keamanan informasi dapat dikurangi dan dihindari dengan salah satu bentuk dukungan adanya tata kelola yang terjamin kerahasiaannya, keutuhannya, dan ketersediannya. Berdasarkan hal tersebut, penelitian ini bertujuan menjawab kebutuhan akan penerapan tata kelola keamanan sistem informasi agar terjadi keselarasan teknologi informasi dan bisnis dalam membangun kompetitif unggulan. Keamanan Informasi sangatlah penting terhadap PT. XX sebelum film animasi yang diproduksi akan ditayangkan. Penelitian ini menggunakan metode kualitatif yang mengidentifikasi resiko dan permasalahan sistem yang sedang berlangsung saat ini dengan observasi dan wawancara kepada pihak-pihak Divisi IT dan Manajemen Produksi di perusahaan tersebut. Hasil pada penelitian ini adalah dampak perealisasian keamanan informasi yang diterapkan berbasis SNI ISO/IEC 27001:2009 pada produksi animasi yang dinilai sangat membutuhkan keamanan data sebelum film yang dibuat akan ditayangkan secara publik.

Kata Kunci : *Keamanan Informasi, SNI ISO/IEC 27001:2009, Produksi Animasi.*

1. PENDAHULUAN

Informasi merupakan aset yang penting bagi sebuah perusahaan, sehingga kemampuan untuk menyediakan informasi yang akurat dan cepat menjadi suatu hal yang penting. Sistem informasi digunakan untuk mendukung berbagai kegiatan dalam perusahaan, bahkan untuk memperoleh keuntungan dan memenangkan persaingan [1]. Sering kali, permasalahan keamanan sistem informasi mendapatkan perhatian dari para stakeholder dan pengelola sistem informasi ketika sudah terjadi sebuah ancaman yang menimbulkan kerugian pada perusahaan. Ketika sebuah ancaman sudah menimbulkan kerugian pada perusahaan, stakeholder dan pengelola sistem mulai melakukan berbagai tindakan pencegahan dan perbaikan atas keamanan sistem informasi [2]. Hal ini dapat menyebabkan perusahaan mengeluarkan pengeluaran ekstra untuk melakukan pengamanan sistem informasi dan perbaikan atas ancaman yang sudah terjadi. Apabila menggangu performansi dari sistem, sering kali keamanan dikurangi atau ditiadakan.

SNI ISO/IEC 27001:2009 merupakan standar yang mencakup semua jenis organisasi (misalnya usaha komersial, pemerintah, organisasi nir-laba). Standar ini menetapkan persyaratan untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, peningkatan dan pemeliharaan Sistem Manajemen Keamanan Informasi (SMKI) yang terdokumentasi dalam konteks risiko bisnis organisasi secara keseluruhan. Standar ini menetapkan persyaratan penerapan pengendalian keamanan yang disesuaikan dengan kebutuhan masing-masing organisasi atau bagian organisasi. SMKI didesain untuk memastikan pemilihan pengendalian keamanan yang memadai dan proposional untuk melindungi aset informasi dan memberikan kepercayaan kepada pihak terkait [3]. Dengan adanya standarisasi yang diacu untuk tata kelola keamanan informasi, maka dapat menghasilkan dampak-dampak yang baik bagi perusahaan. Dan PT. XX menggunakan standar SNI ISO/IEC 27001:2009 untuk acuan tata kelola informasi perusahaan.

Penelitian ini bertujuan untuk menilai apakah SNI ISO/IEC 27001:2009 yang telah diterapkan dapat berdampak baik bagi perusahaan dan apa saja manfaat yang didapat setelah menerapkan kebijakan tersebut.

2. METODE PENELITIAN

Metode yang digunakan dalam melakukan pengumpulan data adalah:

1) Studi Literatur
   Merupakan tahapan pembelajaran tentang topik-topik yang relevan dengan penelitian yang akan dilakukan tentang tata kelola informasi, SNI ISO/IEC 27001:2009, serta literatur-literatur terkait.
2) Wawancara
   Pengambilan data dengan cara melakukan wawancara langsung dengan Divisi IT dan Manajemen Produksi pada PT. XX.

3. HASIL DAN PEMBAHASAN

3.1 Tata Kelola

Sebuah kebijakan informasi organisasi biasanya memberikan arahan baik bagi para pengelola maupun para pengguna informasi. Bagi para pengelola kebijakan informasi merupakan sebuah kerangka kerja yang berisi prinsip-prinsip organisasi yang berhubungan dengan informasi, penggunaannya dan pengelolaannya. Diantaranya menjamin pengalokasian sumber-sumber informasi penting dalam manajemen informasi [4].

Sebuah kebijakan informasi organisasi biasanya memberikan arahan baik bagi para pengelola maupun para pengguna informasi. Bagi para pengelola kebijakan informasi merupakan sebuah kerangka kerja yang berisi prinsip-prinsip organisasi yang berhubungan dengan informasi, penggunaannya dan pengelolaannya. Diantaranya menjamin pengalokasian sumber-sumber informasi penting dalam manajemen informasi [5]. Sebagai sebuah perusahaan produksi film animasi yang berkaitan erat dengan bidang teknologi informasi sangat diperlukan tata kelola keamanan teknologi informasi untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis tercapai.

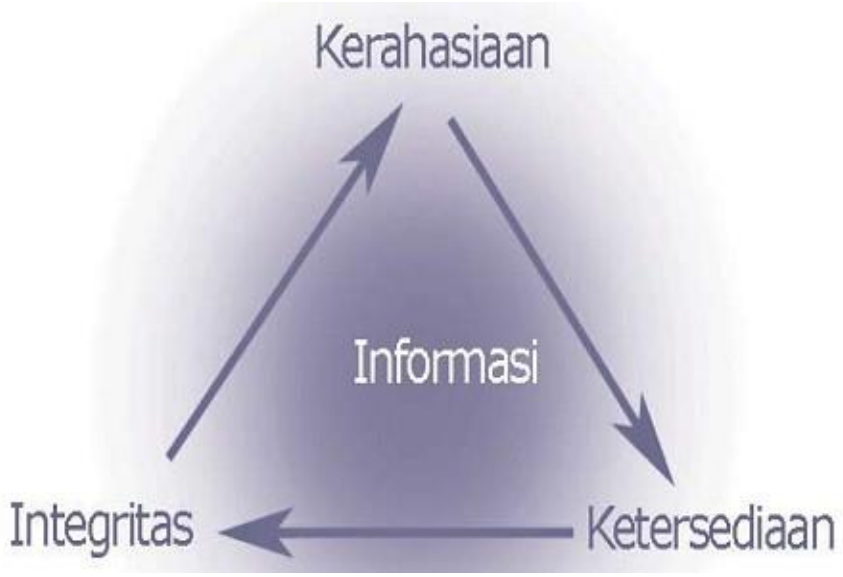
3.2 Keamanan Informasi

Keamanan informasi, menurut Howard dalam Raharjo [2] merupakan suatu usaha pencegahan atas serangan untuk mendapatkan sesuatu dari sistem informasi, baik melalui akses yang tidak semestinya maupun penggunaan yang tidak semestinya. Sedangkan Sarno [6] pada bukunya Sistem Manajemen Keamanan Informasi mendefinisikan keamanan informasi sebagai penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis.

Beragam bentuk informasi yang mungkin dimiliki oleh sebuah perusahaan meliputi : informasi yang tersimpan dalam computer (baik *desktop* komputer maupun *mobile* komputer, *server* dan *workstation*), segala data yang melintas dijaringan, informasi yang dicetak pada kertas, dikirim melalui fax, data atau informasi yang tersimpan dalam disket, *CD, DVD, Flashdisk*, atau penyimpanan data lain termasuk juga informasi yang disampaikan dalam pembicaraan (termasuk hal percakapan melalui telepon), tersimpan di *mobile phone*, melalui sms, *e-mail*, tersimpan dalam *database*, tersimpan dalam film, dipresentasikan dengan OHP atau media presentasi lain dan metode-metode lain yang dapat digunakan untuk menyampaikan informasi berupa ide-ide baru perusahaan [7].

Keamanan Informasi terdiri dari perlindungan terhadap aspek-aspek berikut [5] :

1. *Confidentiality* (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity* (integritas) aspek yang menjamin bahwa data tidak akan dirubah tanpa ada izin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *integrity* ini.
3. *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).



Gambar 2. Aspek Keamanan Informasi [5]

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang berupa kebijakan (*policy*), pedoman kerja (*guidance work* atau *SOP*), struktur organisasi hingga perngkat lunak.

3.3 SNI ISO/IEC 27001:2009

ISO/ IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di perusahaan.

SNI ISO/ IEC 27001 yang diterbitkan pada tahun 2009 dan merupakan versi Indonesia dari ISO/ IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Standar Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol kemanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan [8]. ISO/IEC 27001 mendefinisikan keperluan-keperluan untuk sistem manajemen keamanan informasi. SMKI yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari risiko kerugian/bencana dan kegagalan serius pada pengamanan sistem informasi. Dalam penerapan SMKI akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang tidak lama.

ISO/ IEC 27001 memberikan gambaran umum mengenai kebutuhan yang dibutuhkan perusahaan/ organisasi dalam usahanya untuk mengimplementasikan konsep-konsep keamanan informasi. Penerapan ISO/ IEC 27001 disesuaikan dengan tujuan, sasaran dan kebutuhan organisasi. Pendekatan proses ini menekankan pada beberapa hal sebagai berikut [9]:

1) Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi,
2) Penerapan dan pengoperasioan kontrol untuk mengelola risiko keamanan informasi dalam bentuk konteks risiko bisnis organisasi secara keseluruhan,
3) Pemantauan dan tinjau ulang kinerja dan efektivitas *ISMS* , dan
4) Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.
   Standar ini mengadopsi model *"Plan-Do-Check-Art" (PDCA),* untuk membentuk seluruh proses SMKI.

3.4 Hasil Identifikasi

Pada tahapan identifikasi awal ini membahas tentang kondisi terkini yang ada pada PT. XX sebagai fokus penelitian dalam rangka penerapan kebijakan keamanan informasi. Hasil identifikasi awal yang telah dilakukan di PT. XX meliputi aspek kebijakan, aspek kelembagaan, aspek infrastruktur, dan aspek perencanaan.

Saat ini PT. XX belum memiliki dokumen untuk mengelola keamanan informasi yang dimiliki, *security policy* yang coba ditetapkan selama ini hanya berupa aturan-aturan yang coba ditetapkan berdasarkan pengetahuan para pengelola TI saja.

Kondisi jaringan yang ada di PT. XX awalnya dibangun tanpa perncaanaan yang matang, dikarenakan organisasi belum mempersiapkan diri untuk mengantisipasi ekspansi bisnis yang berkembang dengan pesat, perencanaan pengembangan menyedot energi sumber daya perusahaan yang terbatas, dan pada akhirnya perusahaan akan memilih program atau *resource* mana yang akan dikembangan terlebih dahulu. Salah satu sumber daya yang mungkin memperoleh urutan belakang untuk dikembangkan atau mendapat perhatian khusus adalah Keamanan Teknologi Informasi.

3.5 Penerapan dan Pengoperasian SNI ISO/IEC 27001:2009

Pada tahap ini menghasilkan dokumen kebijakan penggunaan *e-mail, internet,* komputer/laptop, *temporary*, akses penyimpanan data serta aturan sumber daya informasi yang merupakan bagian dari dokumen kebijakan keamanan informasi yang akan diajukan untuk Rancangan Tata Kelola Informasi.

Dalam proses menerapkan dan mengoperasikan dokumen kebijakan keamanan informasi mengacu kepada beberapa sasaran pengendalian yang terdapat pada standar SNI ISO/IEC 27001:2009. Dan fokus sasaran pengendalian pada tahap ini adalah pembuatan dokumen kebijakan penggunaan aset TIK, kebijakan penyimpanan informasi, kebijakan pengendalian akses, manajemen akses pengguna, manajeman pengendalian akses aplikasi dan informasi.

Tabel 4. Penerapan & Pengoperasian Dokumen

No.	Klausul SNI 27001	Nama Dokumen	Cakupan Dokumen
1.	A.7.1.3	Kebijakan Penggunaan Aset TIK	Berisi tentang aturan untuk penggunaan Komputer, Laptop, dan *Server.*
2.	A.10.7.3	Kebijakan Penyimpanan Informasi	Berisi tentang penanganan dan penyimpanan serta pemindahan informasi yang diizinkan.
3.	A.11.1.1	Kebijakan Pengendalian Akses	Berisi tentang aturan akses kontrol terhadap informasi dan sistem informasi (*temporary*, data akses, *internet, e-mail* dan *server*).
4.	A.11.2.1	Manajemen Akses Pengguna	Berisi pengelolaan mengenai siapa saja yang dapat mengakses data informasi tertentu.
5.	A.11.6	Manajemen Pengendalian Akses Aplikasi dan Informasi	Berisi tentang batasan aplikasi yang dapat digunakan untuk mencegah akses yang tidak sah terhadap informasi pada sistem aplikasi.

3.6 Manfaat Penerapan SNI ISO/IEC 27001:2009

Penerapan tata kelola informasi yang berbasis SNI ISO/IEC 27001:2009 pada perusahaan tidak semudah menerapkan produk atau solusi teknologi, karena dibutuhkan kesadaran dan pendekatan agar mampu menjalankan kebijakan yang telah dibuat dengan penyesuaian kondisi yang ada pada perusahaan.

Adapun manfaat dengan adanya penerapan tata kelola informasi dengan berbasis SNI ISO/IEC 27001:2009 adalah :

1. Membantu perusahaan untuk berkompetisi di bidang yang sama dengan perusahaan-perusahaan yang besar.
2. Standar-standar yang ada dapat membuka pasar ekspor bagi produk-produk dan jasa-jasa yang ditawarkan.
3. Membantu menemukan praktek bisnis yang baik.
4. Menuju kepada efisiensi proses bisnis.
5. Memberikan kredibilitas dan kepercayaan bagi pelanggan.
6. Membuka peluang bisnis dan penjualan baru.
7. Memberikan keunggulan kompetitif.
8. Menjadikan perusahaan terstandarisasi secara International.
9. Membantu perusahaan untuk berkembang.
10. Menjadikan kebijakan yang ada untuk penerapan kedisiplinan yang selaras.

4. KESIMPULAN

Penyelenggaraan tata kelola TIK di PT. XX memberikan manfaat pada perusahaan.

a. Keamanan informasi mutlak diperlukan dalam tata kelola TIK pada PT. XX untuk melindungi informasi rahasia/tidak dari pihak yang tidak berkepentingan.
b. Menjamin seluruh sumber daya manusia perusahaan untuk peduli terhadap ancaman dan risiko yang dapat terjadi pada data informasi.
c. Keamanan informasi, nilai informasi akan dikelola dengan baik sehingga informasi yang tepat akan dikirimkan pada orang yang tepat, waktu yang tepat dan bentuk yang tepat.

Seri SNI ISO/IEC 27001:2009 dapat digunakan sebagai standar untuk pengelolaan yang memberikan gambaran umum mengenai kebutuhan yang dibutuhkan perusahaan dalam usahanya untuk mengimplementasikan konsep-konsep keamanan informasi.

DAFTAR PUSTAKA

[1] J. Informasi, “Jurnal Informasi Volume VII No.2 / November / 2015,” vol. VII, no. 2, pp. 48–57, 2015.
[2] B. Rahardjo, “Keamanan Sistem Informasi Berbasis Internet,” Bandung: PT. Insan Indonesia, 2005.
[3] BSNI (Badan Standardisasi Nasional), “SNI ISO/IEC 27001:2009,” 2009.
[4] Susan Henczel, *The Information Audit: a practical guide*. Munchen: Saur, 2001.
[5] and I. I. R. Sarno, “Sistem Manajemen Keamanan Informasi (Berbasis ISO 27001),” Surabaya: ITS Press, 2009.
[6] R. Sarno, “Information Technology Security Techniques Informa Security Management System Requirements,” in *Audit Sistem & Teknologi Informasi*, Surabaya: ITS Press 2, 2009.
[7] Calder A, Watkisn S, *A Manager’s Guide to Data Security and ISO 27001/ISO 27002*, 4th Editio. IT Governance Publishing, 2008.
[8] Kementrian Komunikasi dan Informatika Republik Indonesia, “Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelanggara Pelayanan Publik,” 2011.
[9] S. and G. S. Garfinkel, “Practical UNIX & Internet Security2nd edition,” *O’Reilly Assoc.*, 1996.