Journal of Information Technology and Computer Science (INTECOMS)
Volume 4 Nomor 2, Desember 2021
e-ISSN : 2614-1574
p-ISSN : 2621-3249

ANALISIS MANAJEMEN RISIKO IT SISTEM ADMINISTRASI BISNIS *RETAIL* MENGGUNAKAN METODE NIST SP 800-30 *REVISI* 1

IT RISK MANAGEMENT ANALYSIS BUSINESS ADMINISTRATION SYSTEM RETAIL USING NIST SP 800-30 REVISION 1

Risma Damalia, Awalludiyah Ambarwati, Eman Setiawan
Sistem Informasi, Fakultas Ilmu Komputer,Universitas Narotama
Risma.damalia@mhs.fasilkom.narotama.ac.id

ABSTRACT

The application of Information Technology is very important in the business retail in providing convenience and improving the quality of performance according to the vision and mission of a company. Information security that is vulnerable to risk will have a negative impact on the system if it is not properly maintained. This study aims to identify information security risks using the NIST SP 800-30 revision 1 method with four stages, namely preparation for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment. This is done because of several events experienced, one of which is a virus attack and network problems that interfere with store administration activities. The final result of this research is a recommendation for a mitigation approach to protect the inventory administration system.

Keywords*: Information Security, Risk Management, NIST SP 800-30 revision 1.*

ABSTRAK

Penerapan Teknologi Informasi merupakan hal yang sangat penting pada bisnis *retail* dalam memberikan kemudahan serta meningkatkan kualitas kinerja sesuai visi dan misi suatu perusahaan. Keamanan informasi yang rentan terhadap risiko akan berdampak negatif pada sistem jika tidak dijaga dengan baik. Penelitian ini bertujuan untuk melakukan identifikasi risiko keamanan informasi menggunkan metode NIST SP 800-30 *revisi* 1 dengan empat proses tahapan yaitu persiapan penilaian, melakukan penilaian, komunikasikan hasil penilaian, serta mempertahankan penilaian. Hal ini dilakukan karena adanya beberapa kejadian yang dialami salah satunya serangan virus dan kendala jaringan yang mengganggu aktivitas administrasi toko. Hasil akhir penelitian ini berupa rekomendasi pendekatan mitigasi untuk perlindungan sistem administrasi inventori tersebut.

Kata Kunci: Keamanan Informasi, Manajemen risiko, NIST SP 800-30 revisi 1.

PENDAHULUAN

Manajemen risiko berperan penting dalam berbagai risiko yang terjadi. Antara lain membantu perkembangan teknologi informasi dan proses bisnis sebagai sumber daya yang menguntungkan serta efektif. Penelitian ini dilakukan pada sistem administrasi inventori yang digunakan pada bisnis *retail* di salah satu toko buku ternama di Surabaya yakni Toko Buku AG sebagai study kasus, dimana sering terjadi kendala *server* serta kendala pada sistem keamanan data yang berperan penting bagi kelangsungan sistem *BackOffice* milik Toko Buku AG yang berperan sebagai tempat penyimpanan data lengkap, inventori barang, data penjualan dan pembelian, serta *tools* tambahan yang menyangkut perpesanan *incoming* dan *outgoing* data barang yang terhubung dengan pusat Toko Buku AG..

Manajemen risiko merupakan langkah praktis dalam menangani skenario risiko dalam suatu organisasi, termasuk dalam bidang keamanan informasi (Al et al., 2019). Manajemen risiko juga memberikan keuntungan yakni mengatur risiko TI, membantu perkembangan proses bisnis (Putra, 2019). Maka dari itu manajemen risiko dapat diartikan sebagai segala proses pengelolaan risiko yang mencakup identifikasi, evaluasi, mitigasi serta pengendalian risiko yang berhubungan dengan keamanan informasi yang dapat

mengancam kelangsungan usaha, strategi visi misi dan aktivitas organisasi untuk saat ini dan masa yang akan datang (Mahardika, 2017). Manajemen Risiko akan membuat manajer TI dapat menyeimbangkan biaya operasional dan ekonomi agar dapat mengamankan sistem dan data TI yang ada serta mendukung misi dari organisasi tersebut yang memiliki tiga proses utama yaitu penilaian risiko, mitigasi risiko, serta evaluasi dan kontrol penilaian risiko (Nugraha et al., 2020).

Risiko adalah suatu entitas terancam oleh suatu keadaan atau peristiwa potensial, dan biasanya merugikan yang akan timbul jika keadaan atau peristiwa tersebut terjadi, dan mungkin terjadi adanya. Penilaian risiko adalah pembahasan mengenai potensi serta dampak yang merugikan terhadap operasi dan aset organisasi, individu, organisasi lain, dan kepentingan keamanan ekonomi yang timbul dari pengoperasian dan penggunaan sistem informasi yang diproses, disimpan, dan dikirimkan oleh sistem. Organisasi melakukan penilaian risiko untuk menentukan risiko pada misi inti/fungsi bisnis pada organisasi, proses bisnis, segmen bisnis, infrastruktur umum atau layanan pendukung pada sistem informasi. Penilaian risiko dapat mendukung berbagai keputusan dan aktivitas yang berisiko pada organisasi (NIST, 2012; Muslimin, dkk., 2020).

Keamanan informasi berfungsi untuk melindungi informasi dari berbagai ancaman demi menjamin kelangsungan proses bisnis, meminimalisir risiko bisnis dan memaksimalkan laba investasi dan peluang bisnis. Peran keamanan informasi saat ini menjadi lebih penting karena telah banyak orang, bisnis dan lembaga pemerintah menyimpan data dalam bentuk digital dengan menggunakan berbagai jenis teknologi. Keamanan informasi didefinisikan sebagai perlidungan informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi atau pengrusakan (Syafitri, 2016).

Penelitian yang dilakukan pada sistem administrasi inventori bisnis *retail* ini menggunakan kasus pada sistem administrasi inventori yang di sebut *BackOffice* milik Toko Buku AG. Toko tersebut memiliki beberapa cabang di kota besar namun penelitian ini hanya dilakukan disalah satu cabangnya di Surabaya. Target sasaran Toko Buku AG ialah kelas menengah keatas sehingga barang yang dijual juga menyesuaikan khususnya pada buku dan alat tulis *import*. Toko Buku AG memiliki susunan struktur organisasi IT dipimpin oleh manager toko sebagai penanggungjawab atau bertindak mengambil keputusan atas infrastruktur yang berkaitan di area *store*, IT cabang atau penanggung jawab IT bertugas sebagai pemegang tanggung jawab atas segala sesuatu yang berkaitan dengan IT dalam hal *hardware* dan *software* di area *store* yang dibantu oleh bagian umum dalam hal pengerjaan dan perbaikan perangkat keras dan fasilitas IT. Peranan IT cabang yang dianggap penting dalam penanganan, penjagaan,serta perawatan aset IT di Toko Buku AG, sehingga perlunya ketelitian dalam menjalankan pekerjaan(Prabowo & Saputri, 2020).

Perbaikan infrastruktur IT pada toko buku AG sudah dijalankan degan standart Operasional Prosedur (SOP) IT yang berlaku namun belum adanya standart Operasional Prosedur (SOP) yang tertulis sehingga segala kendala dan risiko yang mungkin sedang terjadi atau bahkan telah terjadi di Toko Buku AG secara langsung oleh IT cabang serta manager toko sebagai pemegang segala keputusan.

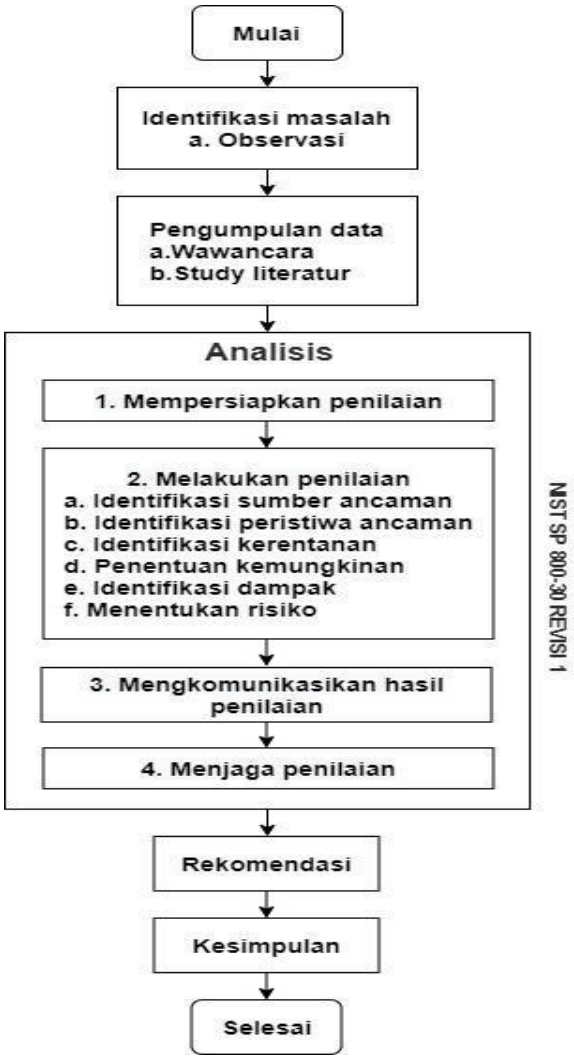
Tersedianya berbagai metode yang digunakan untuk menghadapi risiko serta ancaman yang mungkin terjadi salah satunya yaitu NIST *(National Institute Standard Technology)*, merupakan salah satu panduan yang sudah terstandarisasi oleh Pemerintah Amerika Serikat, yang mengatur tentang manajemen risiko untuk sistem teknologi informasi. Metode ini dirancang khusus untuk tipe data kualitatif serta dapat mengidentifikasi, mengevaluasi

dan mengelola risiko TI dalam sistem secara keseluruhan. Dengan proses yang sangat lengkap sehingga dapat meliputi semua kegiatan manajemen Risiko, mulai dari identifikasi ancaman, sampai rekomendasi kontrol (Nugraha et al., 2020). Kerangka kerja NIST *(National Institute Standard Technology)* dikembangkan oleh *US Department of Commerce*. Dan merupakan Organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standar, dan teknologi untuk meningkatkan fasilitas dan kualitas kehidupan. NIST mengeluarkan alat, teknik dan metode untuk penilaian dan perencanaan keamanan informasi berbasis risiko (Mahardika, 2017). Metode yang digunakan pada penelitian ini ialah NIST SP 800-30 *Revisi* 1 yang memiliki empat tahapan yang terdiri dari persiapan penialian, melakukan penilaian, mengkomunikasikan hasil penilaian, dan menjaga penilaian yang diharapkan menjadi acuan untuk menerapkan standart manajemen pada keamanan sistem administrasi inventori yang digunakan di Toko Buku AG tersebut serta memberikan rekomendasi penilaian pada pemilihan risiko berdasarkan analisis risiko yang dilakukan.

METODE

Alur Penelitian

Metodologi penelitian yang dikemas dalam bentuk diagram alur *(flowchart)* untuk mempermudah tahap pengerjaan penelitian terkait dengan risiko yang ada di Toko Buku AG agar berjalan dengan terarah seperti pada Gambar 1.



Gambar 1. *Flowchart* penelitian

Identifikasi Masalah

Pada tahap ini dilakukan observasi serta wawancara awal pada tempat penelitian terkait dengan kejadian yang pernah terjadi di toko buku tersebut. Hasil yang didapat berdasarkan observasi awal yang dilakukan, memperoleh informasi mengenai beberapa permasalahan yang ada dan sering terjadi di toko buku tersebut seperti misalnya gangguan virus dan serangan jaringan yang mengancam keamanan data Toko Buku AG.

Pengumpulan Data

Pengumpulan data dilakukan berdasarkan wawancara serta studi literatur. Pada tahap wawancara hasil yang diperoleh ialah data permasalahan serta data ancaman risiko yang ada dan pernah terjadi, sehingga mempengaruhi proses pengolahan data dan mengganggu kinerja sistem administrasi toko buku tersebut. Wawancara dilakukan secara tatap muka dan melakukan tanya jawab dengan IT cabang sebagai orang yang paham mengenai sistem administrasi pada toko buku tersebut. Sedangkan studi literatur dilakukan untuk memperoleh data seperti pada buku, jurnal, dan informasi dari internet terkait dengan manajemen risiko IT serta standar penerapan manajemen risiko dengan menggunakan metode NIST SP 800-30 *revisi* 1.

Analisis

Analisis yang dilakukan pada penelitian ini didasarkan pada metode yang digunakan yakni NIST SP 800-30 *revisi* 1. NIST SP 800-30 *revisi* 1 juga dapat digunakan sebagai pelengkap proses penilaian risiko dengan dokumen penialaian risiko keamanan informasi yang rinci dan lengkap (Al et al., 2019). Langkah-langkah yang digunakan dalam NIST adalah mengidentifikasi aset. Karakteristik sistem menggambarkan batas-batas sistem serta sumber daya dan informasi yang menyusun sistem. Sistem karakterisasi dalam mendefinisikan ruang lingkup dilakukan untuk upaya penilaian risiko serta menjelaskan tentang batasan otorisasi operasional, dan memberikan informasi yang diperlukan untuk menentukan risiko misalnya, perangkat keras, perangkat lunak, konektivitas sistem, dan departemen yang bertanggung jawab atau staf pendukung (Hashim et al., 2019). Kegunaan utamanya adalah meneliti berbagai ilmu untuk mempromosikan dan meningkatkan infrastruktur teknologi (Putra, 2019). Berikut langkah-langkah dalam melakukan analisis permasalahan pada penelitian ini menggunakan kerangka kerja NIST SP 800-30 *Revisi* 1.

Melakukan Penilaian

Merupakan gambaran sumber ancaman yang menjadi perhatian dan karakteristik penargetan untuk ancaman permusuhan dan non-permusuhan, yang di bagi dalam lima aspek penilaian (1) Identifikasi sumber ancaman, yang mencakup kapabilitas, niat, dan karakteristik penargetan untuk ancaman permusuhan serta efek ancaman non-permusuhan. (2) Identifikasi peristiwa ancaman, mencakup ancaman, relevansi peristiwa, dan sumber ancaman yang dapat memulai peristiwa tersebut. (3) Identifikasi kerentanan sebagai kondisi predesposisi yang mempengaruhi keungkinan ancaman yang terjadi sehingga menimbulkan dampak negatif. (4) Penentuan kemungkinan, yakni menentukan kemungkinan peristiwa ancaman yang menyebabkan dampak buruk yang merugikan dengan mempertimbangkan karakteristik sumber ancaman, kerentanan atau kondisi predesposisi yang di identifikasi, serta kerentanan organisasi yang mencerminkan upaya perlindungan yang direncanakan sebagai penghambat peristiwa tersebut. (5) Identifikasi dampak yakni menentukan dampak buruk dari peristiwa ancaman yang menjadi perhatian. (6) Menentukan risiko yakni menentukan pertimbangan antara dampak yang dihasilkan dari peristiwa/kejadian tersebut dengan kemungkinan terjadinya peristiwa.

Mengkomunikasikan Hasil Penilaian

Mengkomunikasikan hasil penilaian risiko kepada pembuat keputusan pada perusahaan/organisais untuk mendukung respon risiko serta membagikan informasi terkait dengan risiko yang dihasilkan selama penilaian risiko dengan personil organisasi yang tepat.

Menjaga Penilaian

Melakuakan pantauan lanjutan terhadap beberapa faktor risiko yang berkontribusi terhadap risiko dan aset perusahaan, individu dan organisasi lain. Dalam menjaga penilaian terdapat dua aspek penting yakni, (1) Faktor risiko monitor, (2) Penilaian risiko yang baru yakni memperbaruhi penilaian risiko yang ada dengan hasil dari pemantauan berkelanjutan dari faktor risiko.

HASIL DAN PEMBAHASAN

Melakukan Penilaian

Dalam pemeliharaan aset harus ada orang yang bertanggung jawab atas aset tersebut. Orang tersebut tidak memiliki hak atas aset namun memiliki tanggungjawab atas pengembangan, penggunaan, pemeliharaan dan perbaikan, serta keamanan yang sesuai. Di toko buku AG IT cabang bertanggung jawab atas aset IT yang dimiliki toko sekaligus orang yang paham dalam menentukan nilai aset yang digunakan. Aset utama merupakan aset inti kegiatan dalam lingkup Toko Buku AG. Berikut beberapa aset yang digunakan Toko Buku AG pada sistem *BacOffice* miliknya seperti pada Tabel 1.

Tabel 1. Daftar Aset

Aset	Jenis Aset	Penanggung Jawab	Spesifikasi
1 komputer yang digunakan sebagai *sever* data	Aset pendukung	IT Cabang	Intel® core™ i3-3220 CPU @ 3.30 GHz 3.30 GHz (2 socket) RAM 8.00 GB HD 500 GB
Router D-link DSL-2730E	Aset pendukung	IT Cabang	10/100 Mbps Wirelless Speed, 2.4 GHz WPA, WPA2

Sumber : Hasil Observasi

Identifikasi Sumber Ancaman

Pada tahap ini menjelaskan ancaman apa saja yang teridentifikasi pada setiap aset sistem *BackOffice*. Penilaian yang dilakukan menggunakan pendekatan kuantitatif dengan pengembangan model *rating* dan *scoring*. Tingkat kerentanan, dampak, dan penentuan risiko dalam penilaian ini dikategorikan *Very High*, *High*, *Moderate*, *Low*, *Very Low* yang diperoleh dari hasil wawancara dengan pihak Toko Buku AG terhadap sistem *BackOffice.* Tabel dibagi berdasarkan identifikasi ancaman yang terjadi pada aset Toko Buku AG yang dijelaskan pada Tabel 2 sampai 6.

Tabel 2. Identifikasi Ancaman Pada Sistem *BackOffice*

Sumber Ancaman	Rentan Efek
Akses *password* oleh karyawan yang tidak berwenang.	*Hight*
Salah pengoprasian sistem yang menyebabkan sistem terhenti.	*Hight*
Kesalahan pengolahan data oleh karyawan yang berwenang.	*Very Hight*
Serangan *malware* atau virus yang disebabkan akses oleh pihak karyawan berwenang/ tidak berwenang.	*Very Hight*
Kesalahan oprasional yang disebabkan oleh pihak IT cabang.	*Moderate*
Update aplikasi sistem yang belum dilakukan menyebabkan sistem terhenti/*error*.	*Moderate*
Kehilangan data yang bersifat sensitif.	*Very Hight*
Pemanfaatan celah keamanan aplikasi oleh pihak karyawan berwenang/ tidak berwenang.	*Very Hight*

Sumber : Hasil Penelitian dan diolah kembali

Tabel 3. Identifikasi Ancaman Pada *Windows Server* (SQL Server 2000)

Sumber Ancaman	Rentan Efek
Windows tidak berjalan sebagaimana mestinya.	*Hight*

Sumber : Hasil Penelitian dan diolah kembali

Tabel 4. Identifikasi Ancaman Pada Komputer *Server*

Identifikasi	Sumber Ancaman	Rentan Efek
Database server	Tidak ada konfigurasi standar keamanan pada *server* aplikasi dan konfigurasi standart.	*Hight*
Storage server	Menggunakan Password lemah/*default*.	*Moderate*
OS *server*	Os *server* tidak berjalan semestinya.	*Hight*

Sumber : Hasil Penelitian dan diolah kembali

Tabel 5. Identifikasi Ancaman Komputer *Server* (Lanjutan)

Sumber Ancaman	Rentan Efek
Terjadi bencana alam (kebakaran, bom, gempa bumi).	*Very Hight*
Suhu ruangan yang tidak stabil.	*Moderate*
Gangguan tegangan listrik/tegangan listrik tidak stabil.	*Moderate*
Kerusakan pada aset yang usianya menua/sudah rusak.	*Hight*

Sumber : Hasil Penelitian dan diolah kembali

Tabel 6. Identifikasi Ancaman Router D-link DSL-2730E

Sumber Ancaman	Rentan Efek
Menggunakan *Password* lemah/*default*.	*Hight*
Gangguan tegangan listrik/tegangan listrik tidak stabil.	*Moderate*
Terjadi bencana alam (kebakaran, bom, gempa bumi, cuaca curam).	*Very Hight*
Gangguan jaringan yang disebabkan penyedia layanan.	*Very Hight*
Kerusakan kabel LAN akibat hewan pengerat.	*Very Hight*

Sumber : Hasil Penelitian dan diolah kembali

Identifikasi Peristiwa Ancaman

Pada tahap ini dilakukannya penentuan peristiwa ancaman selama penilaian risiko serta gambaran tingkat perincian yang peristiwa tersebut. Pertimbangan organisasi dalam seragkaian peristiwa ancaman yang representatif berfungsi sebagai awal identifikasi ancaman yang spesifik dalam penilaian risiko serta keperluan konfirmasi sehingga peristiwa ancaman dianggap relevan untuk penilaian risiko.

Identifikasi Kerentanan

Pada tahap ini dilakukan untuk memahami sifat umum kerentanan dan juga kondisi predisposisi yang dapat mempengaruhi kerentanan terhadap kerentanan tertentu yang masuk atau meliputi ruang lingkup pada sistem adminstrasi *BackOffice*, dengan menentukan kerentanan mana yang relevan dengan kejadian ancaman yang terjadi untuk risiko potensial yang akan dinilai. Kerentanan tersebut berkaitan dengan sistem informasi administrasi *BackOffice* misalnya perangkat keras dan perangkat lunak, kontrol internal, serta prosedur keamanan atau lingkungan dimana sistem tersebut dioprasikan yang dapat dilihat pada Tabel 7 sampai 10 sebagai berikut.

Tabel 7. Identifikasi Kerentanan Pada Sistem *BackOffice*

Kerentanan	Tingkatan
Akses password sistem oleh semua karyawan akibat berkurangnya SDM.	*Hight*
Salah pengoprasian sistem yang menyebabkan sistem *error*/terhenti.	*Low*
Kesalahan input data oleh karyawan yang berwenang.	*Hight*
Penggunaan komuputer oleh semua karyawan yang memungkinkan adanya pencurian data atau memasukkan *malware* pada sistem.	*Hight*
Kurangnya ketelitian IT cabang dan kurang berhati – hati dalam bekerja.	*Moderate*
Update antivirus yang terlambat memungkinkan *malware*/virus masuk dan mengancam sistem.	*Hight*
Kehilangan sebagian data penting pada sistem.	*Very Hight*
Belum adanya *upgrade* bahasa pemrograman yang digunakan/versi *database* yang digunakan sehingga keamanan pada sistem kurang.	*Moderate*
Update atau tambahan fitur yang dirubah oleh pusat namun belum dirubah di cabang.	*Moderate*

Sumber : Hasil Penelitian dan diolah kembali

Tabel 8. Identifikasi Kerentanan Pada *Windows Server* (SQL Server 2000)

Kerentanan	Tingkatan
Antivirus yang tidak *update* pada komputer/OS bajakan.	*Moderate*

Sumber : Hasil Penelitian dan diolah kembali

Tabel 9. Identifikasi Kerentanan Pada Komputer *Server*

Kerentanan	Tingkatan
Belum adanya konfigurasi standar keamanan pada *database*.	*Moderate*
Kerusakan pada aset yang usianya menua/sudah rusak.	*Hight*
Terjadinya bencana alam (kebakaran, bom, gempa bumi)	*Moderate*
Tegangan listrik yang tidak stabil/ naik dan turun/lampu mati.	*Hight*
Kebersihan ruangan yang menyebabkan rusaknya kabel oleh hewan pengerat.	*Hight*

Sumber : Hasil Penelitian dan diolah kembali

Tabel 10. Identifikasi Kerentanan Router D-link DSL-2730E

Kerentanan	Tingkatan
Mengalami gangguan jaringan yang terhubung pada perangkat.	*Hight*
Kerusakan kabel LAN akibat hewan pengerat.	*Hight*

Sumber : Hasil Penelitian dan diolah kembali

Penentuan Kemungkinan

Pada tahap ini menjelaskan bagaimana eksplist proses yang digunakan untuk menentukan kemungkinan serta asumsi yang terkait dengan proses penentuan kemungkinan terhadap peristiwa ancaman pada sistem administrasi *BackOffice* Toko Buku AG. Dengan menentukan kerentanan yang relevan dengan kejadian ancaman yang terjadi untuk risiko potensial yang akan dinilai. misalnya perangkat keras dan perangkat lunak, kontrol internal, serta prosedur keamanan atau lingkungan dimana sistem tersebut dioprasikan Yang dapat dilihat pada Tabel 11.

Tabel 11. Identifikasi Kemungkinan

Risiko	Kemungkinan Peristiwa Ancaman Yang Terjadi	Kemungkinan Ancaman yang Menghasilkan Dampak Buruk	Kemungkinan Keseluruhan
Akses *password* oleh karyawan yang tidak berwenang.	*Hight*	*Hight*	*Hight*
Salah pengoprasian sistem yang menyebabkan sistem terhenti.	*Hight*	*Low*	*Moderate*
Kesalahan pengolahan data oleh karyawan yang berwenang.	*Very Hight*	*Hight*	*Very Hight*
Serangan *malware* atau virus yang disebabkan akses oleh pihak karyawan berwenang/ tidak berwenang.	*Very Hight*	*Hight*	*Very Hight*
Kesalahan oprasional yang disebabkan oleh pihak IT cabang.	*Moderate*	*Moderate*	*Moderate*
Update aplikasi sistem yang belum dilakukan menyebabkan sistem terhenti/*error*.	*Moderate*	*Hight*	*Moderate*
Kehilangan data yang bersifat sensitif.	*Very Hight*	*Moderate*	*Hight*
Windows tidak berjalan semestinya.	*Hight*	*Moderate*	*Moderate*
Gangguan tegangan listrik/tegangan listrik tidak stabil.	*Modarete*	*Hight*	*Moderate*
Terjadi bencana alam (kebakaran, bom, gempa bumi).	*Very Hight*	*Moderate*	*Hight*
Kerusakan pada aset yang usianya menua/sudah rusak.	*Hight*	*Hight*	*Hight*
Gangguan jaringan yang disebabkan penyedia layanan.	*Very Hight*	*Hight*	*Very Hight*
Kerusakan kabel LAN akibat hewan pengerat.	*Very Hight*	*Hight*	*Very Hight*

Sumber : Hasil Penelitian dan diolah kembali

Identifikasi Dampak

Pada tahap identifikasi dampak dilakukan untuk menentukan potensi dampak buruk dalam operasi Toko AG yang mencakup misi spesifik/proses bisnis atau sumber daya informasi, misalnya informasi, personel, peralatan, dana, serta teknologi informasi. Informasi dari analisis dampak untuk penilaian risiko dapat dilihat pada Tabel 12.

Menentukan Risiko

Dalam menentukan risiko ini dilakukan penilaian risiko peristiwa ancaman kombinas dari identifikasi kemungkinan dan dampak yang yang telah dilakukan. Tingkat risiko tersebut yang teridentifikasi menjadi salah satu penentu sejauh mana sistem *BackOffice* terancam oleh berbagai peristiwa tersebut. Efektivitas dari hasil penilaian risiko sebagian ditentukan oleh pengambil keputusan untuk menentukan kelangsungan asumsi yang dibuat yang termasuk dari bagian penilaian. Informasi mengenai ketidakpastian tersebut disusun dan disajikan dengan cara mendukung kepputusan manajemen risiko dapat dilihat pada Tabel 13.

Tabel 12. Identifikasi Dampak

Jenis Dampak	Dampak Maksimal	Keterangan
Kehilangan data yang bersifat sensitif.	*Very Hight*	Dampaknya *very hight* karena data didalamnya berisi tentang data sensitif yang mempengaruhi penjualan dan stok barang.
Kesalahan pengolahan data oleh karyawan yang berwenang.	*Hight*	Kesalahan biasa terjadi pada proses *input* data stok barang masuk yang berdampak *hight* karena mempengaruhi data stok barang untuk kedepannya.
Update aplikasi sistem yang belum dilakukan menyebabkan sistem	*Moderate*	Sistem *BackOffice* yang belum *update* akan berhenti, menampilkan *error message* sehingga perlunya *update* sistem agar sistem dapat diakses kembali.
Akses *password* oleh karyawan yang tidak berwenang.	*Hight*	Dampaknya *hight* karena penyalahgunaan akses membuat sistem di dalamnya kacau yang seharusnya akses *password* hanya untuk karyawan yang berwenang seperti pemegang jabatan *supervisor* serta jabatan yang setara atau lebih tinggi.
Kerusakan pada aset Toko Buku AG yang usianya menua/sudah rusak.	*Hight*	Dampaknya *hight* karena bisa terjadi pada komputer *server*.
Serangan *malware* atau virus yang disebabkan akses oleh pihak karyawan berwenang/ tidak berwenang dalam	*Hight*	Dampaknya *hight* karena sistem akan terhenti jika *server* terkena virus.
Windows tidak berjalan sebagaimana mestinya.	*Moderate*	Dampaknya *moderate* karena jika windows mengalami kendala maka sistem *BackOffice* juga tidak dapat diakses. Namun hal tersebut bisa diatasi dengan mudah.
Gangguan tegangan listrik/tegangan listrik *mall* yang tidak stabil.	*Moderate*	Dampaknya *moderate* karena seringkali tegangan listrik pada *Mall* menglami gangguan secara mendadak sehingga hal tersebut juga berdampak pada komputer *server* serta kinerja sistem *BackOffice.*
Kesalahan operasional yang disebabkan oleh IT Cabang	*Moderate*	Dampaknya *moderate* biasanya terjadi kesalahan *setting* sistem oleh IT Cabang.
Kerusakan kabel LAN akibat hewan pengerat.	*Moderate*	Dampaknya *moderate* karena berpengaruh dengan jaringan yang digunakan.
Terjadi bencana alam (kebakaran, bom, gempa bumi).	*Hight*	Dampaknya *hight* karena jika terjadi bencana yang tidak terduga dengan tingkat kerusakan yang juga tidak terduga maka kemungkinan terjadinya kerusakan aset serta fasilitas yang ada juga bisa terjadi.

Sumber : Hasil Penelitian dan diolah kembali

Tabel 13. Penentuan Risiko

Ancaman	Keseluruhan Kemungkinan	Tingkatan Dari Dampak	Risiko Keseluruhan
Kehilangan data yang bersifat sensitif.	*Hight*	*Very Hight*	*Very Hight*
Kesalahan pengolahan data oleh karyawan yang berwenang.	*Very Hight*	*Hight*	*Hight*
Kesalahan operasional yang disebabkan oleh IT Cabang	*Moderate*	*Moderate*	*Moderate*
Update aplikasi sistem yang belum dilakukan menyebabkan sistem terhenti, *error*.	*Moderate*	*Moderate*	*Moderate*
Akses *password* oleh karyawan yang tidak berwenang.	*Hight*	*Hight*	*Hight*
Serangan *malware* atau virus yang disebabkan akses oleh pihak karyawan berwenang/ tidak berwenang.	*Very Hight*	*Hight*	*Hight*
Windows tidak berjalan sebagaimana mestinya.	*Hight*	*Moderate*	*Moderate*
Kerusakan pada aset Toko Buku AG yang usianya menua/sudah rusak.	*Hight*	*Hight*	*Hight*
Terjadi bencana alam (kebakaran, bom, gempa bumi).	*Hight*	*Moderate*	*Moderate*
Kerusakan kabel LAN akibat hewan pengerat.	*Very Hight*	*Moderate*	*Moderate*

Sumber : Hasil Penelitian dan diolah kembali

Mengkomunikasikan Hasil Penilaian

Membagikan informasi hasil penilaian terhadap sistem *BackOffice* Toko Buku AG kepada IT Cabang serta Manager toko mengenai penilaian risiko sistem informasi yang berpengaruh pada fungsi misi, proses bisnis, ketergantungan pada sistem lain, serta infrastruktur yang ada di Toko Buku AG.

Setelah identifikasi masalah, menentukan penilaian pada aset maupun sistem *BackOffice* yang bertujuan untuk mengetahui tingkat permasalahan yang terjadi serta menggambarkan tingkat risiko keseluruhan yang harus segera dilakukan tindakan mitigasi terhadap permasalahan yang ada di Toko Buku AG. Tahap informasi terkait tingkat risiko Toko Buku AG dikomunikasikan dengan pihak terkait yang disusun dalam bentuk laporan penilaian guna mendukung respon risiko.

Menjaga Penilaian

Pada tahap ini dilakukan pantauan terhadap risiko secara berkesinambungan untuk memastikan agar informasi yang diperlukan Toko Buku AG dapat membuat keputusan yang kredibel dan berbasis risiko yang tersedia seiring berjalannya waktu. Pemantauan faktor risiko ini dilakukan dengan urutan penilaian yang sudah dilakukan sehingga dapat memberikan informasi penting tentang perubahan kondisi yang berpotensi mempengaruhi kemampuan Toko Buku AG untuk melakukan misi inti dan fungsi bisnis.

Pada tahap ini dilakukan penentuan frekuensi serta kaeadaan dimana penilaian risiko diperbaruhi. Penilaian ini dilakukan dengan mengidentifikasi tingkat risiko saat ini. Mengkomunikasikan hasil penilaian risiko kepada semua entitas tingkatan manajemen risiko yakni IT Cabang untuk memastikan agar IT Cabang dapat bertanggung jawab terhadap akses informasi penting yang diperluakan untuk membuat keputusan berbasis risiko.

Rekomendasi

Seteleah identifikasi risiko serta penilaian risiko dan beberapa tahapan

penilaian yang dilakukan pada sisem *BackOffice* maka tahap selanjutnya yang dilakukan ialah tahap rekomendasi dari tingkatan yang berguna untuk meminimalisir atau bahkan mencegah masalah pada sistem agar proses operasional kedepannya terhindar dari berbagai risiko atau ancaman yang dapat dilihat pada Tabel 14 sampai 16 yang dibedakan berdasarkan tingkat risiko *Very Hight*, *Hight*, dan *Moderate*.

Tabel 14. Rekomendasi Tingkat Risiko *Very Hight*

Ancaman	Tingkat Risiko	Rekomendasi
Kehilangan data yang bersifat sensitif.	*Very Hight*	Menambahkan *storage* khusus untuk sistem *backup.*

Sumber : Hasil Penelitian dan diolah kembali

Tabel 15. Rekomendasi Tingkat Risiko *Hight*

Ancaman	Tingkat Risiko	Rekomendasi
Kesalahan pengolahan data oleh karyawan yang berwenang.	*Hight*	Meneliti kembali data yang dimasukkan dengan dokumen yanag telah diterima.
Akses *password* oleh karyawan yang tidak berwenang.	*Hight*	Pembatasan penggunaan akses sistem *BackOffice* untuk keperluan tertentu
Serangan *malware* atau virus yang disebabkan akses oleh pihak karyawan berwenang/ tidak berwenang.	*Hight*	1. Menambahkan komputer lain untuk penggunaan karyawan selain akses masuk pada sistem *BackOffice*. *2.* Pembatasan penggunaan akses sistem *BackOffice.*
Kerusakan pada aset Toko Buku AG yang usianya menua/sudah rusak.	*Hight*	Melakukan pengecekan rutin serta mengganti aset yang usianya sudah menua.

Sumber : Hasil Penelitian dan diolah kembali

Tabel 16. Rekomendasi Tingkat Risiko *Moderate*

Ancaman	Tingkat Risiko	Rekomendasi
Kesalahan operasional yang disebabkan oleh IT Cabang	*Moderate*	1. *Training* IT cabang agar lebih paham saat melakukan *setting* sistem. 2. Menjaga ketelitian serta konsentrasi saat bekerja.
Update aplikasi sistem yang belum dilakukan menyebabkan sistem terhenti, *error*.	*Moderate*	Dilakukan pengujian dan cek perbaruan fitur secara berkala.
Windows tidak berjalan sebagaimana mestinya.	*Moderate*	*Update* antivirus secara berkala serta memakai OS asli yang bukan bajakan.
Terjadi bencana alam (kebakaran, bom, gempa bumi).	*Moderate*	1. Menambahkan *storage* khusu untuk sistem *backup.* 2. Tidak panik dan menyelamatkan beberapa barang penting jika sempat.
Kerusakan kabel LAN akibat hewan pengerat.	*Moderate*	1. Melakukan pengecekan rutin. 2. Tetap menjaga kebersihan ruangan.

Sumber : Hasil Penelitian dan diolah kembali

SIMPULAN

Berdasarkan penelitian yang dilakukan melalui wawancara serta observasi yang pada sistem *BackOffice* Toko Buku AG tentang risiko yang ada pada sistem tersebut: (1) Penelitian ini dilakukan dengan menggunakan metode NIST SP 800-30 *Revisi* 1 untuk mempermudah tahap penilaian risiko yang dilakukan pada sistem administrasi *BackOffice* yang berguna untuk mengetahui ancaman serta permasalahan yang terjadi pada sistem administrasi *BackOffice* sehingga dapat dilakukan tindakan mitigasi, deteksi atau koreksi. (2) Hasil dari penilaian risiko yang dilakukan pada sistem *BackOffice* Toko Buku AG mendapati tingkat risiko *Very Hight* pada saat kehilangan data yang bersifat sensitif, karena sebagian data yang ada merupakan data penting yang meliputi data stok serta penjualan maka dari itu perlunya menambahkan *storage* khusus untuk sistem *backup*, agar ada *backup* data yang berisiko hilang .

DAFTAR PUSTAKA

Al, M., Aditya, F., Suryanto, Y., & Ramli, K. (2019). ScienceDirect ScienceDirect Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study Combination Technique in Profit-Based O. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Hashim, N. A., Abidin, Z. Z., Zakaria, N. A., & Ahmad, R. (2019). *Risk Assessment Method for Insider Threats in Cyber Security : A Review*. *January 2018*.

Idah, Y. M., & Prima, R. A. (2021). Analisis Manajemen Risiko Sistem Pembelajaran Online Pada Perguruan Tinggi Menghadapi Pandemi Covid-19. *JURNAL REKAYASA INFORMASI*, *10*(1), 50-56. https://doi.org/10.14569/IJACSA.2018.090119Mahardika, F. (2017). *Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)*. *02*(02), 1–8.

NIST. (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Special Publication*, *September*, 95. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-30r1.pdf

Nugraha, B. A., Perdanakusuma, A. R., & Rachmadi, A. (2020). Analisa Manajemen

Muslimin, A., Raharjo, A. S., & Lestari, S. (2020, October). Manajemen Resiko Teknologi Informasi Terkait Pandemi COVID-19 Pada SDN 1 Negara Batin Menggunakan Framework COBIT 5 dan ISO/IEC 31000. In *Prosiding Seminar Nasional Darmajaya* (Vol. 1, pp. 88-94).

Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *4*(1), 223–231.

Putra, R. R. (2019). Analisis Manajemen Risiko Ti Pada Keamanan Data E - Learning Dan Aset It Menggunakan NIST SP 800 – 30 Revisi 1. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *6*(1), 96–105. https://doi.org/10.35957/jatisi.v6i1.154

Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800- 30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, *2*(2), 8. https://doi.org/10.24014/coreit.v2i2.2356.