DOI: https://doi.org/10.26593/jrsi.v12i2.6315.155-164

Jurnal Rekayasa Sistem Industri
Volume 12 No 2 - Oktober 2023
http://journal.unpar.ac.id/index.php/jrsi/index
ISSN 2339-1499 (*online*) – ISSN 0216-1036 (*print*)

Disampaikan : 15 Desember 2022
Direview : 16 Februari 2023
Diterima : 27 Maret 2023

Hasil Penilaian Risiko Keamanan Informasi pada Laboratorium Klinik Berdasarkan Kriteria Kendali Dalam Penerapan ISO 27001

Eddy Susanto[1], Nilo Legowo[2]
[1,2)] Departemen Manajemen Sistem Informasi,
Program Pasca Sarjana Binus – Magister Manajemen Sistem Informasi
Universitas Bina Nusantara
Jl. Kebon Jeruk Raya No. 27, Kebon Jeruk, Jakarta, telp. 021 536-96969
Email: eddy.susanto001@binus.ac.id, nlegowo@binus.edu

Abstract

Information is part of an information system that is important to be protected in terms of confidentiality, integrity and availability, in order to increase its reliability. Moreover, information containing personal and health data is definitely available in the clinical laboratory. This becomes a consideration for clinical laboratory management to prepare for the development of its service system in digital transformation. This study aims to assess the information security risks that still arise in a clinical laboratory accredited to ISO 15189 and certified to ISO 9001, as a preparation for digital-based services. By using the ISO 27001 approach which is embedded in the qualitative method in this study, risk assessment is carried out by identification, analysis and evaluation through interviews with process owners at clinical laboratories in Jakarta. As a result, it was found that the Busdev&IT Department had the most information security risks (35 risks out of 384 total risks), which required further treatment based on the established risk appetite. Therefore, vigilance on the use of information systems in the laboratory needs to be improved in terms of information security.

Keywords: *ISO 27001, Information Security, Clinical Laboratory, Risk Management.*

Abstrak

Informasi merupakan bagian dari sistem informasi yang penting untuk dilindungi dari segi kerahasiaan, keutuhan dan ketersediaannya, dalam meningkatkan realibilitasnya. Apalagi informasi yang mengandung data diri dan kesehatan tentu tersedia di laboratorium klinik. Hal ini menjadi pertimbangan bagi manajemen laboratorium klinik untuk menyiapkan transformasi digital pada sistem layanannya. Penelitian ini bertujuan untuk menilai risiko keamanan informasi yang masih muncul pada sebuah laboratorium klinik yang terakreditasi ISO 15189 dan tersertifikasi ISO 9001, sebagai persiapan layanan berbasis digital. Dengan menggunakan pendekatan ISO 27001 yang disematkan pada metode kualitatif dalam penelitian ini, penilaian risiko dilakukan dengan identifikasi, analisis dan evaluasi melalui wawancara dengan pemilik proses pada laboratorium klinik di Jakarta. Sebagai hasilnya, ditemukan bahwa Departemen Busdev&TI memiliki risiko keamanan informasi terbesar (35 risiko dari total 384 risiko), yang memerlukan penanganan lebih lanjut berdasarkan selera risiko yang telah ditetapkan. Oleh karena itu, kewaspadaan pada penggunaan sistem informasi di laboratorium perlu ditingkatkan dari segi keamanan informasi.

Kata kunci: ISO 27001, Keamanan Informasi, Laboratorium Klinik, Pengelolaan Risiko

Pendahuluan

Menimbang bahwa akhir-akhir ini, telah terjadi banyak insiden pengungkapan kerahasiaan data serta dengan telah disetujuinya undang-undang perlindungan data pribadi, membuat banyak pelaku industri, khususnya yang menjadi pengelola dan pemroses data, menyadari akan pentingnya meningkatkan upaya peningkatan keamanan informasi. Terutama pada perusahaan dan

DOI: https://doi.org/10.26593/jrsi.v12i2.6315.155-164

institusi yang memberikan layanan digital melalui sistem informasi. Risiko keamanan informasi dapat menimbulkan gangguan pada proses bisnis, penurunan reputasi hingga kerugian finansial (Suroso & Fakhrozi, 2018).

Sering dijumpai baik pekerja maupun profesional keamanan informasi salah mengartikan risiko, mereka kadang menganggap enteng atau justru terlalu detail memetakan risiko, hingga melupakan risiko yang besarnya, karena memang penilaian risiko cenderung bersifat subyektif (Harkins, 2016). Digitalisasi membawa harapan baru, yaitu untuk meningkatkan dan mengembangkan masing-masing fungsi hingga seluruh rantai secara lebih cepat (Aagaard, 2019). Namun juga meningkat pula risiko keamananannya (Hill & Swinhoe, 2021).

Pada institusi Kesehatan, seperti laboratorium klinik, informasi pasien yang mencakup data diri dan data kesehatan dikelola sebagai aset informasi yang perlu dilindungi. Terlebih lagi dengan masuknya pandemi Covid-19, mendorong bisnis laboratorium klinik lebih cepat untuk bertransformasi digital untuk mempercepat transaksi data dari cabang dan outlet di luar laboratorium utamanya. Dengan demikian, pekerja laboratorium tidak hanya dihadapkan dengan tugas repetitif, namun juga sekaligus tugas administratif yang menjadi lebih berisiko jika tidak melibatkan sistem informasi di dalamnya (Weemaes et al., 2020). Di sisi lain, sistem informasi perlu diperhatikan pula risiko keamanan informasinya, yang meliputi kerahasiaan, keutuhan dan ketersediaanya, seiring dengan terbukanya akses padanya dari berbagai pihak yang terlibat (Wright, 2016).

Perlindungan terhadap informasi dan pengendaliannya di laboratorium klinik menjadi penting karena: pembuatan keputusan perusahaan dan operasional fasilitas kesehatan dapat bergantung pada kapabilitas informasi dan elektronik yang disematkan padanya, melindungi informasi pribadi dan riwayat kesehatan, meningkatkan kepercayaan pasien pada fasilitas kesehatan, menghindari perselisihan, mengurangi risiko tuntutan medis, dan mematuhi ketentuan hukum serta mengurangi kerancuan yang menimbulkan saling tidak percaya dalam kasus hukum (Farn et al., 2007). Memang benar bahwa perkembangan teknologi dan teknik penguncian informasi serta enkripsi telah membantu pengamanan sistem informasi laboratorium, namun ancaman baru akan terus hadir dan membuat kendali saat ini terlihat usang.

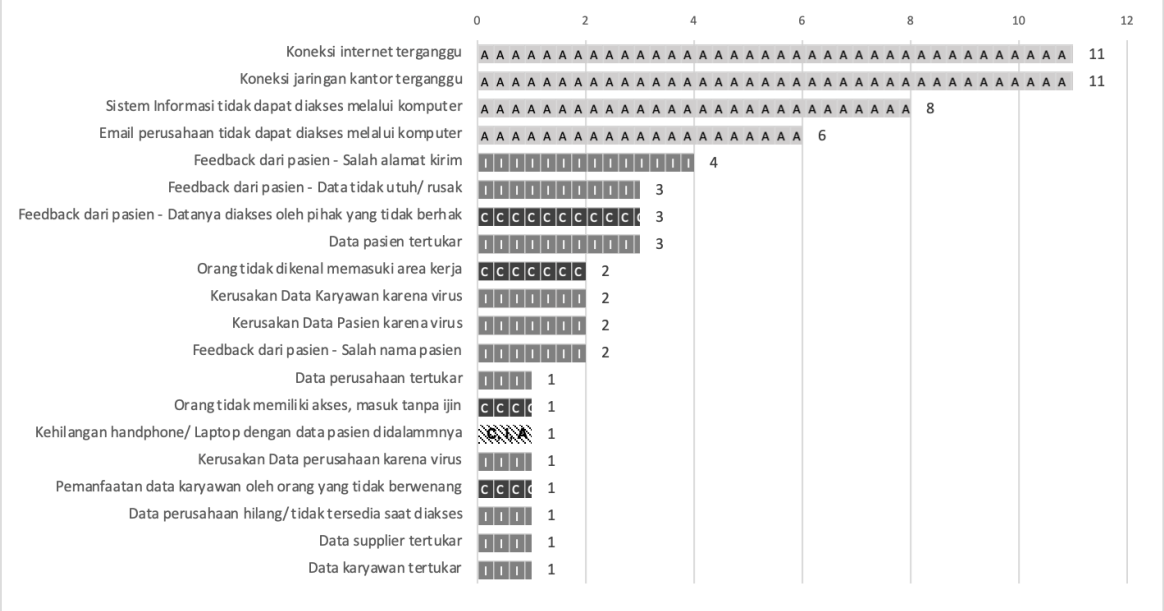
Berdasarkan wawancara dengan manajemen, subyek penelitian pada tahun lalu mengalami insiden keamanan informasi yang mengancam reputasi perusahaan dan menimbulkan keresahan di antara para karyawan. Bocornya data karyawan yang mencakup data pribadi, riwayat kerja hingga daftar gaji, dimana dimanfaatkan oleh oknum yang tidak berwenang untuk mengancam departemen HRD hingga tuntutannya dipenuhi.

Lebih jauh, penelitian awal dilakukan untuk mengetahui kategori risiko keamanan informasi apa saja yang dimiliki oleh laboratorium klinik. Dua belas manajer diwawancara untuk mencari tahu tentang risiko yang dihadapi. Seperti yang dapat dilihat pada Gambar 1, dimana risiko ketersediaaan (A = Availability 55%) menjadi perhatian utama dari para manajer, disusul risiko keutuhan (I = Integrity 33%), dan risiko kerahasiaan (C = Confidentiality 12%). Sebuah risiko, yaitu kehilangan handphone/ laptop memiliki ketiga kategori sekaligus.

Insiden keamanan informasi meningkatkan ancaman yang nyata bagi reputasi dan bisnis fasilitas kesehatan, termasuk berdampak pada temuan negatif dari regulator, tuntutan hukum dan terhentinya kelangsungan bisnis, dimana menjadi kekuatiran manajemen puncak. (Herzig, 2019) Dorongan tersebut makin kuat dengan adanya peraturan yang mendorong manajemen menerapkan Sistem Manajemen Pengamanan Informasi ISO/IEC 27001, yaitu Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 pasal 3 juncto Peraturan Badan BSSN Nomor 8 Tahun 2020 pasal 9 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

Jadi, sejalan dengan hasil penelitian awal, visi manajemen dan ketentuan pemerintah, penelitian ini dirancang untuk melakukan penilaian terhadap risiko keamanan informasi di laboratorium klinik menggunakan pendekatan ISO/IEC 27001:2013. Dengan pertimbangan hasil penilaian risiko tersebut, maka diharapkan laboratorium klinik yang juga telah menerapkan ISO 15189 dan ISO 9001 memiliki gambaran tentang risiko keamanan informasi yang perlu dikelola di seluruh jajaran organisasi. Terdapat beberapa penelitian sebelumnya yang juga dijadikan rujukan, menguraikan mengenai risiko keamanan informasi, namun penelitian ini lebih

DOI: https://doi.org/10.26593/jrsi.v12i2.6315.155-164



Gambar 1. Hasil penelitian awal terhadap risiko keamanan informasi

fokus pada penerapan pengendalian teknis pengamanan informasi di laboratorium klinik.

Naskah akademis ini menjabarkan penelitian dengan urutan sebagai berikut: Bagian 2 membahas mengenai metodologi dan penelitian terkait sebelumnya; Bagian 3 menjabarkan tentang hasil dan pembahasan penilaian risiko laboratorium klinik; Lalu pada bagian 4, dipaparkan kesimpulan dan saran untuk penelitian selanjutnya.

Metodologi

Metode Penelitian

Berdasarkan hasil penelitian awal dan komitmen dari manajemen terhadap penerapan sistem manajemen keamanan informasi, tujuan penelitian ditetapkan. Kurun waktu penelitian disepakati berlangsung dalam 6 bulan, yang melibatkan 6 Departemen (Business Development & Information Technology - BusDev & IT, Operasional, Customer Relationship Management – CRM, Human Resources & General Affair – HR&GA, Logistik, Research and Development – R&D) dan Direktur di Kantor Pusat. Penelitian ini diawali dengan studi pustaka, metode yang digunakan adalah analisis isi, analisis konseptual, dan analisis relasional (Sekaran & Bougie, 2016). Selanjutnya adalah metode kualitatif untuk mengumpulkan data melalui survei singkat menggunakan kuesioner dan wawancara, yang memotivasi responden untuk dapat lebih jelas menggali gambaran kejadian tertentu berdasarkan wawasan mereka (Sekaran & Bougie, 2016). Kemudian interpretasi dan analisis terhadap hasil wawancara digunakan untuk membuat kesimpulan tentang pesan-pesan dalam teks, pengaruh variabel lingkungan terhadap isi pesan, dan pengaruh pesan terhadap penerima. Langkah penelitian berikutnya adalah menilai proses bisnis organisasi dan aset terkait, wawancara penilaian risiko dengan departemen yang menerapkan sistem informasi dan memaparkannya dalam tabel risiko sebagai hasil penelitian.

Saat menilai pengendalian risiko saat ini, setiap diskusi yang dilakukan dilandaskan pada daftar pertanyaan yang sesuai dengan faktor kendali teknis dalam ISO 27001:2013 dan juga tata cara organisasi dalam menerapkannya. Pada pemaparan hasil, resume hasil penilaian risiko akan disajikan berdasarkan departemen yang dikaji, domain aspek pengendalian risiko dari ISO 27001:2013, kategori risiko berdasarkan keberterimaannya dan klasifikasinya, untuk menjadi dasar pertimbangan bagi perusahaan dalam mengelola risiko keamanan informasi di laboratorium klinik.

Penelitian Terkait

Keamanan informasi menjadi salah satu persyaratan non fungsional yang perlu dipenuhi dalam suatu sistem (Satzinger et al., 2016). Hal yang perlu dilakukan oleh manajemen dalam

DOI: https://doi.org/10.26593/jrsi.v12i2.6315.155-164

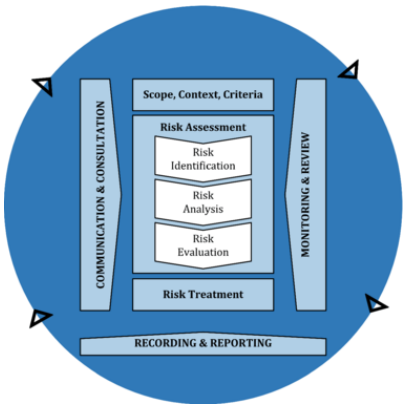
menjaga keamanan informasinya adalah memastikan bahwa kerentanan dalam suatu sistem, yaitu celah yang menyebabkan suatu sistem rusak oleh ancaman pada waktu mendatang, dapat ditangani oleh perusahaan (Rainer et al., 2020). Demikian halnya pada industri kesehatan, seperti industri perbankan yang mengelola risiko keamanan informasi, bertujuan untuk menjaga informasi yang terkandung di dalamnya (Wallin & Xu, 2008).

Risiko-risiko keamanan informasi dapat terjadi jika kerentanan sistem informasi berhasil dimanfaatkan oleh ancaman seperti yang disebutkan dalam dokumen NIST SP 800-30 (NIST, 2012; Zhiwei & Zhongyuan, 2012). Pengamanan informasi berarti melindungi informasi dari segala kemungkinan ancaman, untuk menjamin keberlangsungan proses bisnis, meminimalkan risiko dan memaksimalkan peluang (Eskaluspita, 2020).

Standar internasional yang menyediakan persyaratan untuk menetapkan, menerapkan dan memelihara, serta meningkatkan sistem manajemen keamanan informasi secara berkesinambungan adalah ISO/IEC 27001 (International Organization for Standardization, 2013) Standar ini menggabungkan beberapa aturan informal yang memungkinkan organisasi untuk mengantisipasi meningkatnya jumlah ancaman, menyediakan solusi pada masalah keamanan dan meningkatkan pencapaian target keamanan secara umum. (Meriah & Arfa Rabai, 2019)

Sistem manajemen keamanan informasi adalah bagian dari proses bisnis organisasi dan struktur manajemen yang terintegrasi, dimana keamanan informasi dipertimbangkan dalam desain proses, sistem informasi, dan pengendaliannya (Barafort et al., 2017). Dalam mengelola risiko keamanan informasi, ISO/IEC 27001:2013 (pasal 6.1.3) menetapkan rujukan pada metodologi ISO 31000 tentang panduan manajemen risiko (International Organization for Standardization, 2013). Studi sebelumnya telah mengidentifikasi bahwa dalam menangani risiko, ISO 27001 akan memberikan persyaratan kontrol yang membantu organisasi untuk memahami domain keamanan informasi dan tindakan yang diperlukan (Eskaluspita, 2020).

Sebagai kerangka kerja pengelolaan risiko, ISO 31000 dapat memperjelas konsep manajemen risiko keamanan informasi yang diimplementasikan dalam organisasi (Suyasa & Legowo, 2019). Di dalamnya juga terdapat prinsip serta perspektif umum yang dapat menyatukan proses manajemen risiko dari berbagai standar, yang dikeluarkan oleh Organisasi Standardisasi Internasional (IOS) maupun lembaga lain (Barafort et al., 2019; Muzaimi et al., 2017). Penelitian dari Amraoui et al. (2019) menyimpulkan bahwa ISO 31000:2018 adalah pendekatan paling komprehensif untuk manajemen risiko, yang mencakup perihal: komunikasi dan konsultasi, penentuan ruang lingkup, konteks dan kriteria, identifikasi risiko, analisis risiko, evaluasi risiko, manajemen risiko, pemantauan dan tinjauan, serta pencatatan dan pelaporan, seperti yang diilustrasikan pada Gambar 2 (International Organization for Standardization, 2018).



Gambar 2. Proses manajemen risiko (International Organization for Standardization, 2018)

Lebih lanjut tentang topik ini, pembaca dapat menggali lebih jauh dari penelitian sebelumnya (Amraoui et al., 2019; Barafort et al., 2017; Eskaluspita, 2020; Grusho et al., 2020; Schnitzler, 2018; Suyasa & Legowo, 2019; Wallin & Xu, 2008; Zhiwei & Zhongyuan, 2012), beserta referensi didalamnya, untuk mendapatkan gambaran tentang penerapan sistem manajemen keamanan informasi, dimana diawali dengan penetapan konteks dan pemahaman proses kritis, serta menilai sensitivitas aset, yang dilanjutkan dengan penilaian risiko yang meliputi identifikasi, analisis dan evaluasi risiko untuk membantu organisasi dalam mewaspadai kerentanan dan mengantisipasi kemungkinan ancaman (Zhiwei & Zhongyuan, 2012).

Laboratorium yang mengimplementasikan sistem informasi sebagai pengelola proses utama, menangani informasi sensitif yang perlu diamankan melalui perencanaan mitigasi risiko

DOI: https://doi.org/10.26593/jrsi.v12i2.6315.155-164

keamanan informasi agar tidak terjadi risiko tersebut, sekaligus meningkatkan efektivitas sistem manajemen (Eskaluspita, 2020; Grusho et al., 2020). Dukungan lain dapat berasal dari penerapan berbagai standar ISO dengan perspektif manajemen risiko, guna meningkatkan kemampuan organisasi dalam beradaptasi dan memberikan dasar untuk meningkatkan, mengelola, serta menginteroperasikan aktivitas manajemen risiko dalam pengaturan TI, yang disesuaikan dengan tujuan penerapan sistem manajemen (Barafort et al., 2017).

Subyek Penelitian

Penelitian ini dilakukan pada sebuah laboratorium klinik di Indonesia, berdiri sejak tahun 1983 dan memiliki 14 cabang, yang menyediakan berbagai layanan pemeriksaan laboratorium, antara lain hematologi, kimia, mikrobiologi, dan serologi imun, termasuk layanan radiologi untuk mendukung operasional dan bisnisnya, sistem informasi menjadi tulang punggung pengelolaan proses dari registrasi, hingga pelaporan hasil, termasuk pengelolaan sistem pendukung manajerialnya. Sistem infomasi utama pada laboratorium ini adalah *Laboratory Information System* (LIS), *Management Information System* (MIS) dan *Human Resources Infromation System* (HRIS). Pemilihan ini juga mempertimbangkan bahwa subjek sangat berkomitmen untuk mempertahankan kinerjanya, melalui sertifikasi ISO 9001 dan akreditasi ISO 15189, yang berarti dapat relevan dengan laboratorium klinik lain pada lingkup implementasi yang sama yang juga menerapkan ISO 9001 dan ISO 15189. Disamping itu, subyek telah memiliki definisi nilai risiko yang dapat diadopsi dalam menilai risiko keamanan informasi dan menerapkan prinsip manajemen: pemikiran berbasis risiko (*risk-based thinking*).

Hasil dan Pembahasan

Pemetaan Konteks dan Identifikasi Aset

Pemahaman terhadap proses adalah cara yang lebih baik dalam melakukan identifikasi risiko, sekaligus menyingkap kerentanan yang dapat mengekspos aset (Zhiwei & Zhongyuan, 2012). Penggambaran proses bisnis berdasarkan analisis rantai nilai Porter (Fisher et al., 2020) terhadap laboratorium klinik dapat dilihat pada Gambar 3.

Berdasarkan informasi yang didapat dari analisis rantai nilai pada Gambar 3 dan keterangan hasil wawancara dengan wakil manajemen, aset-aset organisasi dikelompokkan berdasarkan sensitivitasnya. Semakin tinggi sensitivitasnya, maka perlindungan terhadapnya makin perlu diperhatikan. Pengelompokan aset dilakukan berdasarkan kriteria: Sumber Daya Manusia (SDM), informasi, teknologi (perangkat keras dan lunak), layanan dan aset tak berwujud Sedangkan untuk sensitivitas aset, ditentukan berdasarkan wawancara dengan pengelola aset masing-masing. Hasil identifikasi aset dapat dilihat pada Tabel 1.

SUPPORT ACTIVITIES	**ADMINISTRATION AND MANAGEMENT**	Pengelolaan Kepatuhan, Keuangan dan akunting, Manajemen, Audit Internal, Kerjasama B2B dan Dokter.	MIS, Outlook (mail messaging), Microsoft Office, Zoom (coordination meeting), PC+Printer, LAN + Internet.		
	HUMAN RESOURCE MANAGEMENT	Pengelolaan SDM, Rekrutmen, Pelatihan, Pengembangan Karir, *Compensation and Benefit.*	HRIS, Outlook (mail messaging), Microsoft Office, Zoom, PC+Printer, LAN + Internet		
	PRODUCT AND TECHNOLOGY DEVELOPMENT	Perancangan dan pengembangan layanan, Pengembangan solusi untuk operasional.	- xampp, Sublime Text (Frontend web & mobile apps); - Visual Studio, nodeJS (Backend web & mobile apps); - Web hosting; - HeidiSQL, MySQL (Database); - Microsoft Office, LIS (R&D).		
	PROCUREMENT	*Supplier Management,* Penyimpanan Stok dan Pembelian.	Microsoft Office, Aplikasi Logistik, PC+Printer, LAN + Internet.		
PRIMARY ACTIVITIES	**INBOUND**	**OPERATIONS**	**OUTCOME**	**MARKETING AND SALES**	**CUSTOMER SERVICE**
	• Registrasi Pasien • Pembayaran • Pengambilan Spesimen	• Penginputan data spesimen; • Pre Analisis; • Analisis; • Pengendalian Kualitas; • Otorisasi.	• Penerbitan Laporan; • Penyerahan Laporan.	• Promosi dan Iklan di berbagai platform dan sosial media; • Webinar; • Kerja Sama Dokter; • Pemasaran B2B.	• Pelayanan komplain dan tindak lanjutnya; • Pengukuran kepuasan pelanggan; • Penjadwalan Home Service.
	• LIS; • Mesin EDC • PC • Internal LAN	• LIS • Mesin Pre Analisis • Mesin Analisis • PC • Internal LAN	• LIS • Printer • PC • Internal LAN	• Website Perusahaan; • Email; • Zoom; • Aplikasi Perpesananan • Sosial Media (Facebook, Instagram); • PC + Printer; • Microsoft Office; • LAN + Internet; • Telepon	• LIS; • MIS; • Website Perusahaan; • Email; • Telepon; • Aplikasi Perpesanan (SMS, whatsapp). • PC + Printer; • Microsoft Office; • LAN + Internet

KEUNGGULAN KOMPETITIF

Gambar 3. Hasil analisis rantai nilai laboratorium klinik (Fisher et al., 2020)

DOI: https://doi.org/10.26593/jrsi.v12i2.6315.155-164

Penilaian Risiko

Subyek memiliki definisi nilai risiko (tertera pada pada Tabel 2) yang telah ditetapkan sebelumnya dalam sistem manajemen yang diimplementasikan sehingga dapat digunakan untuk melakukan penilaian risiko keamanan informasi. Dari hasil identifikasi risiko kualitatif melalui wawancara dengan narasumber dari masing-masing departemen pengguna sistem informasi (Wheeler, 2011), dikaitkan dengan aset-aset yang digunakan pada tiap proses, didapatkan hasil penilaian sesuai yang tercantum pada Tabel 3.

Dari tiap risiko yang teridentifikasi dapat dikaitkan dengan kategori risiko keamanan informasi, yaitu: kerahasiaan (*Confidentiality*), keutuhan (*Integrity*), ketersediaan (*Availability*), atau kombinasinya. Dalam hal ini, tiap risiko yang dipetakan, dapat terkorelasi lebih dari satu kategori risiko keamanan informasi, seperti yang dapat dilihat pada Tabel 4.

Dengan memperhatikan selera risiko perusahaan yang hanya menerima risiko pada tingkat rendah dan sedang, empat puluh enam (46) risiko akan membutuhkan tindak lanjut. Dari hasil evaluasi risiko tersebut, teridentifikasi dibutuhkannya kontrol tambahan untuk mendukung sistem manajemen dalam melindungi proses dan informasi dari ancaman keamanan informasi.

Dari Tabel 5, yang selaras dengan persyaratan ISO 27001:2013, ditemukan bahwa faktor kendali yang paling membutuhkan ditingkatkan adalah A.8.2 terkait Klasifikasi Informasi dan A.15.2 terkait Manajemen Penyediaan Layanan Pemasok. Pemilik risiko yang perlu melaksanakan peningkatan kendali meliputi manajer cabang, perawat dan/ atau analis, petugas layanan pelanggan, GM Busdev&IT, staf IT dan fungsi administrasi lainnya. Gambaran tersebut menunjukkan pula bahwa keamanan informasi bukan hanya menjadi tanggung jawab fungsi TI, namun juga tanggung jawab setiap fungsi dalam organisasi, hal ini tertuang dalam Tabel 6.

Tabel 1. Hasil identifikasi aset laboratorium klinik

Kelompok	Deskripsi	Sensitivitas
SDM	Seluruh karyawan di semua cabang, termasuk jajaran direksi	Tinggi
Informasi	Kebijakan dan prosedur, website perusahaan, data pasien, rekam medis pasien, data karyawan, data keuangan, data aset usaha dan informasi legal perusahaan	Tinggi
Teknologi	Perangkat Keras: Server, PC/ Laptop, *Printer, Router, Firewall*, CCTV, Telepon, Pemindai *Barcode*	Sedang - Tinggi
	Perangkat Lunak: Ms. Office, Zoom, MIS, LIS, HRIS, Aplikasi Pengembangan	Tinggi
Layanan	Pengembangan LIS, ISP, *Web Hosting, Mail Server*, Layanan pemeliharaan (utilitas, jaringan telepon, gedung serta kendali api)	Tinggi
Aset Tak Berwujud	*Brand Image*, logo, merk dagang, perijinan usaha	Sedang

Pemaparan sepuluh risiko keamanan informasi tertinggi pada Tabel 6, diperoleh dengan mengurutkan hasil perkalian antara nilai dampak dengan nilai kemungkinan terjadinya, yang menjadi kebijakan subyek dalam mengelola risiko seperti yang disampaikan pada Tabel 2.

Setiap risiko yang teridentifikasi, harus ditindaklanjuti dengan menambahkan faktor kendali tunggal atau gabungan dari persyaratan kendali teknis yang direkomendasikan oleh ISO/IEC 27001:2013.

Tabel 2. Tabel penilaian risiko

Frekuensi \ Dampak		Kecil	Minor	Menengah	Mengganggu	Mayor	Kritikal
		1	2	3	4	5	6
Sangat Sering	6	Sedang	Moderat	Moderat	Tinggi	Tinggi	Tinggi
Sering	5	Sedang	Sedang	Moderat	Moderat	Tinggi	Tinggi
Agak Sering	4	Sedang	Sedang	Sedang	Moderat	Moderat	Tinggi
Sesekali	3	Rendah	Sedang	Sedang	Moderat	Moderat	Tinggi
Jarang	2	Rendah	Rendah	Sedang	Sedang	Moderat	Tinggi
Sangat Jarang	1	Rendah	Rendah	Rendah	Sedang	Sedang	Tinggi

DOI: https://doi.org/10.26593/jrsi.v12i2.6315.155-164

Tabel 3. Hasil identifikasi risiko keamanan informasi dengan klasifikasinya

#	Departemen	SI	TR	T	M	S	R
1	BusDev & IT	LIS, MIS	87	0	35	43	9
2	Operasional	LIS, MIS	87	1	6	65	15
3	CRM	LIS, MIS	68	0	1	15	52
4	HR&GA	HRIS, MIS	61	0	2	44	15
5	Logistik	LIS	50	0	1	35	14
6	R&D	LIS, MIS	31	0	0	8	23
		Total	384	1	45	210	128

**SI=Sistem Informasi; TR=Total Risiko; T=Tinggi; M=Moderat; S=Sedang; R=Rendah*

Tabel 4. Hasil pemetaan risiko keamanan informasi berdasarkan kategorinya

#	Departemen	SI	TR	C	I	A
1	BusDev & IT	LIS, MIS	87	18	49	53
2	Operasional	LIS, MIS	87	10	37	49
3	CRM	LIS, MIS	68	5	32	35
4	HR&GA	HRIS, MIS	61	5	32	37
5	Logistik	LIS	50	2	34	27
6	R&D	LIS, MIS	31	2	14	15
		Total	384	42	198	216

**SI=Sistem Informasi; TR=Total Risiko; C=Confidentiality; I=Integrity; A=Availability*

Tabel 5. Resume hasil evaluasi risiko keamanan informasi terhadap persyaratan ISO/IEC 27001

			Kebutuhan Faktor Kendali Tambahan berdasarkan Annex A ISO/IEC 27001:2013																													
#	**Pemilik risiko**	**Risiko yang melebihi selera risiko**	**A.5**	**A.6.1**	**A.6.2**	**A.7.2**	**A.7.3**	**A.8.1**	**A.8.2**	**A.8.3**	**A.9.1**	**A.9.2**	**A.9.3**	**A.9.4**	**A.10**	**A.11.1**	**A.11.2**	**A.12.1**	**A.12.2**	**A.12.3**	**A.12.4**	**A.12.5**	**A.12.6**	**A.12.7**	**A.13.1**	**A.13.2**	**A.14.1**	**A.14.2**	**A.14.3**	**A.15.1**	**A.15.2**	**A.16**	**A.17**	**A.18.1**	**A.18.2**
1	BusDev & IT	35 risiko	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	Operasional	7 risiko				✓		✓	✓											✓					✓				✓	✓			✓	
3	CRM	1 risiko						✓																										
4	HR&GA	2 risiko				✓										✓	✓	✓																✓
5	Logistik	1 risiko							✓																					✓				
6	R&D	0 risiko																																

Tabel 6. Sepuluh hasil evaluasi risiko keamanan informasi dengan nilai risiko tertinggi

Klasifikasi *	Kategori *	Proses	Annex	Deskripsi	Pemilik Risiko
T	I	Penanganan Hasil Kritis	A.13.2.2	*Agreement on information transfer*	Manajer Cabang
			A.13.2.3	*Electronic messaging*	
			A.15.1.3	*Information and communication technology supply chain*	
			A.18.1.1	*Identification of applicable legislation and contractual agreement*	
M	I	*Home Services*	A.13.2.1	*Information transfer policies and procedures*	Perawat atau Analis
M	I & A	Transportasi Spesimen	A.8.3.1	*Management of removable media*	Staf Operasional
			A.8.3.3	*Physical media transfer*	
			A.12.3.1	*Information backup*	
M	A	Penerimaan Spesimen Rujukan	A.8.2.3	*Handling of asset*	Transporter
M	I	Penyerahan Hasil ke Pasien	A.8.2.3	*Handling of Asset*	Petugas Layanan Pelanggan
			A.8.3.3	*Physical media transfer*	
M	A	Pengiriman Hasil ke Pasien	A.8.2.3	*Handling of asset*	Manajer Cabang
			A.8.3.3	*Physical media transfer*	
			A.13.2.1	*Information transfer policies and procedures*	
			A.13.2.3	*Electronic messaging*	
M	A	Pemeliharaan Peralatan	A.11.2.4	*Equipment maintenance*	Staf GA
			A.12.1.1	*Documented operating procedures*	
M	C & I	Otorisasi Akses	A.9.1.1	*Access control policy*	Staf IT
			A.9.2.1	*User registration and de-registration*	
M	C & I	Otentikasi Pengguna	A.9.2.1	*User registration and de-registration*	Staf IT
			A.9.2.2	*User access provisioning*	

DOI: https://doi.org/10.26593/jrsi.v12i2.6315.155-164

Tabel *6.* Sepuluh hasil evaluasi risiko keamanan informasi dengan nilai risiko tertinggi (Lanjutan)

Klasifikasi*	Kategori*	Proses	Annex	Deskripsi	Pemilik Risiko
M	I & A	Pengembangan LIS	A.14.2.7	*Outsourced development*	GM Busdev&IT
			A.15.1.3	*Information and communication technology supply chain*	
M	C	Penanganan Dokumen	A.8.2.1	*Classification of information*	Pengendali Dokumen
			A.8.2.2	*Labelling of information*	
			A.8.2.3	*Handling of asset*	

** T = Tinggi, M = Moderat, C = Confidentiality, I = Integrity, A = Availability*

Sebagai contoh, pada risiko terhadap penanganan hasil kritis (Tabel 6), tindak lanjut yang direncanakan mencakup antara lain: memberikan catatan di amplop hasil untuk segera konsultasi ke dokter dan kirim sms/wa, untuk pemeriksaan yang dapat masuk ke parameter hasil kritis, pasien diminta mengkonfirmasi nomor kontak sejak registrasi. Perihal penting lain adalah selain diterapkan, faktor kendali tersebut juga perlu dikomunikasikan kepada setiap karyawan, manajemen juga pihak eksternal yang menunjang layanan laboratorium klinik, untuk mencapai pemahaman yang seragam terhadap penanganan keamanan informasi.

Tentu saja, penilaian terhadap risiko tidak dapat hanya dilakukan sekali saja, namun harus dilakukan secara periodik agar dapat mengantisipasi risiko-risiko yang mencul karena adanya pengaruh eksternal maupun internal organisasi, seperti teknologi, persyaratan pelanggan dan pemerintah, pengembangan organisasi dan kompetensi karyawan.

Kesimpulan dan Saran

Mengingat insiden yang dialami oleh subyek dan meningkatnya desakan akan perlindungan informasi, dan telah teridentifikasinya akar penyebab dari beberapa insiden pada penelitian awal, langkah pengamanan terhadap informasi sensitif laboratorium klinik perlu diawali dengan melakukan penilaian terhadap risiko keamanan informasi menggunakan pendekatan ISO/IEC 27001:2013, sesuai dengan tujuan penelitian ini.

Pada subyek telah teridentifikasi sejumlah tiga puluh lima risiko di departemen Busdev&IT yang berkategori moderat dengan cakupan kebutuhan kendali yang banyak berdasarkan ISO/IEC 27001:2013, dimana manajemen perlu mempertimbangkan untuk menindaklanjutinya agar potensi risiko tersebut tidak terjadi di masa yang akan datang.

Ketersediaan adalah perhatian utama yang menjadi bagian dalam keamanan informasi laboratorium klinik, hal ini mengkonfirmasi penelitian pendahuluan yang dilakukan tehadap kedua belas manajer. Penilaian risiko keamanan informasi telah membantu manajemen dan jajarannya untuk memahami perilaku proses secara lebih komprehensif, termasuk mengungkap kelemahan yang melekat pada aset dan ancaman yang mungkin datang sewaktu-waktu. Faktor kendali teknis yang disediakan oleh ISO/IEC 27001:2013 adalah rujukan penting yang membantu pemilik proses mengambil peran dalam pengendalian risiko di lapangan, yang mana sejalan dengan visi manajemen dalam melaksanakan transformasi digital tingkat lanjut dari organisasi. Bagian ini memberikan simpulan yang singkat tentang penelitian yang dibahas di artikel ini disertai dengan saran untuk pengembangan atau lanjutan penelitian berikutnya.

Penelitian ini perlu dilanjutkan dengan penetapan faktor kendali tambahan yang tepat untuk laboratorium klinik dan penilaian ulang saat rekomendasi hasil evaluasi telah terlaksana, ataupun terdapat perubahan proses dan atau layanan baru yang dihasilkan oleh laboratorium klinik. Tentunya hal ini sejalan dengan prinsip peningkatan berkesinambungan yang digariskan dalam penerapan sistem manajemen keamanan informasi.

Daftar Pustaka

Aagaard, A. (2019). *Digital Business Models*. Springer International Publishing. https://doi.org/10.1007/978-3-319-96902-2

Amraoui, S., Elmaallam, M., Bensaid, H., & Kriouile, A. (2019). Information Systems Risk Management: Litterature Review. *Computer and Information Science*, *12*(3), 1. https://doi.org/10.5539/cis.v12n3p1

Barafort, B., Mesquida, A.-L., & Mas, A. (2017). Integrating risk management in IT settings

from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, *54*, 176–185. https://doi.org/10.1016/j.csi.2016.11.010

Barafort, B., Mesquida, A.-L., & Mas, A. (2019). ISO 31000-based integrated risk management process assessment model for IT organizations. *Journal of Software: Evolution and Process*, *31*(1), e1984. https://doi.org/10.1002/smr.1984

Eskaluspita, A. Y. (2020). ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University. *IOP Conference Series: Materials Science and Engineering*, *879*(1), 012074. https://doi.org/10.1088/1757-899X/879/1/012074

Farn, K.-J., Hwang, J.-M., & Lin, S.-K. (2007). Study on Applying ISO/DIS 27799 to Healthcare Industry's ISMS. *WSEAS TRANSACTIONS on BIOLOGY and BIOMEDICINE*, *4*(8).

Fisher, G., Wisneski, J. E., & Bakker, R. M. (2020). Value Chain Analysis. In *Strategy in 3D* (pp. 118–129). Oxford University Press. https://doi.org/10.1093/oso/9780190081478.003.0014

Grusho, A. A., Zabezhailo, M. I., Piskovski, V. O., & Timonina, E. E. (2020). Industry 4.0: Opportunities and Risks in the Context of Information Security Problems. *Automatic Documentation and Mathematical Linguistics*, *54*(2), 55–63. https://doi.org/10.3103/S000510552002003X

Harkins, M. W. (2016). *Managing Risk and Information Security*. Apress. https://doi.org/10.1007/978-1-4842-1455-8

Herzig, T. W. (2019). *Information Security in Healthcare: Managing Risk*. Taylor & Francis.

Hill, M., & Swinhoe, D. (2021, July 16). *The 15 biggest data breaches of the 21st century*. Https://Www.Csoonline.Com/Article/2130877/the-Biggest-Data-Breaches-of-the-21st-Century.Html.

International Organization for Standardization. (2013). *Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC Standard No. 27001:2013)*.

International Organization for Standardization. (2018). *Risk Management - Guideline (ISO Standard no. 31000:2018)*.

Meriah, I., & Arfa Rabai, L. ben. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. *Procedia Computer Science*, *160*, 85–92. https://doi.org/10.1016/j.procs.2019.09.447

Muzaimi, H., Chew, B. C., & Hamid, S. R. (2017). *Integrated management system: The integration of ISO 9001, ISO 14001, OHSAS 18001 and ISO 31000*. 020034. https://doi.org/10.1063/1.4976898

NIST. (2012). *Guide for Conducting Risk Assessments (NIST Special Publication 800-30)*.

Rainer, R. K., Prince, B., Splettstoesser-Hogeterp, I., Sanchez-Rodriguez, C., & Ebrahimi, S. (2020). *Introduction to Information Systems*. John Wiley & Sons Canada, Ltd.

Satzinger, J. W., Jackson, R. B., & Burd, S. D. (2016). *Systems Analysis and Design in a Changing World* (7th ed.). Cengage Learning.

Schnitzler, S. (2018). *A universal guideline for the implementation of a specific ISMS for all Bavarian universities and universities of applied sciences using the example of the University of Applied Sciences Augsburg* [Case Study]. University of Applied Science Hochschule Ausburg.

Sekaran, U., & Bougie, R. (2016). *Research Methods For Business: A Skill Building Approach* (7th ed.). John Wiley & Sons Ltd.

Suroso, J., & Fakhrozi, M. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution. *Procedia Computer Science*, *135*, 202–213. https://doi.org/10.1016/j.procs.2018.08.167

Suyasa, G. W. A., & Legowo, N. (2019). The Implementation of System Enterprise Risk Management Using Framework ISO 31000. *Journal of Theoretical and Applied Information Technology*, *97*(10).

Wallin, E., & Xu, Y. (2008). *Managing Information Security in Healthcare: A Case Study in Region Skåne*. Lund University.

Weemaes, M., Martens, S., Cuypers, L., van Elslande, J., Hoet, K., Welkenhuysen, J., Goossens, R., Wouters, S., Houben, E., Jeuris, K., Laenen, L., Bruyninckx, K., Beuselinck, K., André, E., Depypere, M., Desmet, S., Lagrou, K., van Ranst, M., Verdonck, A. K. L. C., & Goveia, J. (2020). Laboratory information system requirements to manage the COVID-19 pandemic: A

report from the Belgian national reference testing center. *Journal of the American Medical Informatics Association*, *27*(8), 1293–1299. https://doi.org/10.1093/jamia/ocaa081

Wheeler, E. (2011). *Security Risk Management*. Syngress - Elsevier Inc.

Wright, C. (2016). *Fundamentals of Information Risk Management Auditing* (1st ed.). IT Governance Publishing.

Zhiwei, Y., & Zhongyuan, J. (2012). A Survey on the Evolution of Risk Evaluation for Information Systems Security. *Energy Procedia*, *17*, 1288–1294. https://doi.org/10.1016/j.egypro.2012.02.240.