Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 20, No. 2, Mei 2021, pp. 389~396
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v20i2.1093

Manajemen Risiko Sistem Informasi Menggunakan *ISO 31000* dan Standar Pengendalian *ISO/EIC 27001* di Tripio Purwokerto

Information System Risk Management Using ISO 31000 and ISO / EIC 27001 Control Standards in Tripio Purwokerto

Ito Setiawan, Aldistya Riesta Sekarini, Retno Waluyo, Fiby Nur Afiana

Universitas AMIKOM Purwokerto, Indonesia

Article Info

Article history:

Received, 3 Maret 2021
Revised, 20 April 2021
Accepted, 18 Mei 2021

Kata Kunci:

Manajemen Risiko
Sistem Informasi
ISO 31000:2018
ISO 27001:2013
Tripio Purwokerto

ABSTRAK

Bertambahnya ketergantungan organisasi terhadap penggunaan sistem informasi dalam rutinan sejalan dengan ancaman dan risiko yang timbul dari penggunaan sistem informasi tersebut. Permasalahan penggunaan sistem informasi juga dialami oleh Tripio Purwokerto. Tripio merupakan perusahaan yang bergerak di bidang teknologi di Purwokerto. Tripio memiliki dua sistem informasi untuk menunjang proses bisnisnya yaitu website dan *Point of Sales* (POS) *systems*. Dalam penggunaan sistem informasi mengalami permasalahan seperti *server* mengalami *error*, jaringan yang bermasalah, data yang rusak karena terkena virus dan *human error*. Tujuan penelitian adalah mengetahui risiko dan juga dampak dari penggunaan sistem informasi di Tripio Purwokerto. Metode yang digunakan adalah *International Organization for Standardization* (ISO) 3100:2018 dan standar pengendalian menggunakan *International Organization for Standardization* (ISO) 27001:2013. Dari hasil penelitian yang telah dilakukan dapat ditarik kesimpulan bahwa terdapat 15 risiko yang terdiri dari 6 risiko dengan tingkat risiko *high*, 7 risiko dengan tingkat risiko *medium*, dan 2 risiko dengan tingkat risiko *low*. Rekomendasi kontrol yang digunakan mengacu pada ISO 27001:2013 bagian *human recource security, access control, physical and environmental security, operations security, protection from malware, communications security, system acquisition, development and maintenance*.

Keywords:

Risk Management
Information System
ISO 31000:2018
ISO 27001:2013
Tripio Purwokerto

ABSTRACT

The increasing dependence of the organization on the use of information systems in routine in line with the threats and risks arising from the use of the information system. Tripio Purwokerto also experienced the problem of using the information system. Tripio is a technology company in Purwokerto. Tripio has two information systems to support its business processes, namely a website and Point of Sales (POS) systems. In the use of information systems there are problems such as servers experiencing errors, problematic networks, damaged data due to viruses and human errors. The research objective was to determine the risks and impacts of using the information system in Tripio Purwokerto. The method used is the International Organization for Standardization (ISO) 3100: 2018 and the control standards use the International Organization for Standardization (ISO) 27001: 2013. From the results of the research that has been done, it can be concluded that there are 15 risks consisting of 6 risks with a high risk level, 7 risks with a medium risk level, and 2 risks with a low risk level. The control recommendations used refer to ISO 27001: 2013, part of human resource security, access control, physical and environmental security, operations security, protection from malware, communications security, system acquisition, development and maintenance.

Penulis Korespondensi:

Ito Setiawan,
Program Studi Sistem Informasi,
Universitas AMIKOM Purwokerto,
Email: itosetiawan@amikompurwokerto.ac.id

1. PENDAHULUAN

Bertambahnya ketergantungan organisasi terhadap penggunaan sistem informasi dalam rutinan sejalan dengan ancaman dan risiko yang timbul dari penggunaan sistem informasi tersebut [1]. Risiko adalah suatu kondisi terjadinya keadaan dimana dampak yang ditimbulkan bisa merugikan bagi organisasi [2] [3]. Setiap kegiatan yang terjadi pada organisasi mempunyai dampak material atau konsekuensi yang signifikan bagi organisasi [4]. Sistem informasi memiliki risiko yang beragam seperti kegagalan kelistrikan karena faktor alam, *human error*, kebocoran data karena *hacker*, kerusakan sistem akibat terkena virus, kebakaran dan lainya [5] [6]. Agar risiko bisa berkurang maka dibutuhkan sebuah tata kelola risiko yang baik dan benar [7]. Kemampuan untuk mengatasi risiko-risiko yang telah terjadi, meminimalkan risiko yang mungkin akan terjadi dan mengatur tata kelola risiko dengan baik dapat dilakukan dengan manajemen risiko [8] [9]. Manajemen risiko merupakan sebuah proses yang didalamnya terdapat kegiatan seperti mengontrol risiko, mengidentifikasi risiko dan melakukan mitigasi risiko [10]. Selain itu manajemen risiko yang baik akan sangat berpengaruh pada manajemen kualitas, manajemen layanan teknologi informasi dan manajemen proyek [11]. Permasalahan penggunaan sistem informasi juga dialami oleh Tripio Purwokerto.

Tripio merupakan perusahaan yang bergerak di bidang teknologi di Purwokerto. Tripio memiliki dua sistem informasi untuk menunjang proses bisnisnya. Sistem informasi pertama berupa website penjualan. Sistem informasi kedua yaitu *Point of Sales* (POS) *systems*. POS adalah suatu kegiatan yang berorientasi pada penjualan untuk membantu dalam proses transaksi. POS terdiri dari *software* berupa *Inventory Management*, Pelaporan, *Purchasing*, *Customer Management*, Standar Keamanan Transaksi, dan *Return Processing* dan *hardware* berupa terminal/PC, *Receipt Printer*, *Cash Drawer*, terminal pembayaran, *Barcode Scanner* yang saling terintegrasi. Dalam penggunaan sistem informasi mengalami permasalahan seperti server mengalami *error*. Apabila *server* mengalami gangguan maka berakibat sistem informasi tidak bisa digunakan dan menganggu pelayanan terhadap pelanggan. Permasalahan lain seperti jaringan yang bermasalah, permasalahan jaringan sering terjadi yang mengakibatkan gangguan sistem informasi saat digunakan. Data-data penjualan hilang dan beberapa tidak bisa dibuka akibat terkena virus. Permasalahan-permasalahan yang terjadi perlu ditanggulangi. Cara menanggulangi risiko salah satunya adalah melakukan penilaian risiko sebagai langkah awal dalam melakukan manajemen risiko [12]. Selama ini Tripio Purwokerto belum pernah melakukan penilaian risiko terhadap penggunaan sistem informasi. Salah satu metode untuk penilaian risiko adalah ISO 31000 [13].

ISO 31000 merupakan panduan penerapan risiko yang terdiri atas tiga elemen, yaitu : kerangka kerja *(framework)*, prinsip *(principle)* dan proses *(process)* [14]. ISO 31000 menyediakan kerangka kerja, prinsip dan proses manajemen risiko yang bisa digunakan sebagai arsitektur manajemen risiko dan menjamin penerapan manajemen risiko yang efektif dalam organisasi [15]. Kerangka kerja manajemen risiko tertanam secara keseluruhan kebijakan dan praktik strategis dan operasional organisasi [10]. Dalam proses pengendalian risiko dapat mengacu menggunakan ISO/IEC 27001 [16] [17]. ISO/EIC 27001 merupakan standar Internasional yang dipersiapkan untuk mengimplementasikan, membangun, memonitor, mengoperasikan serta merawat sistem manajemen keamanan informasi (SMKI)[17] ISO/EIC 27001 menjadi standar manajemen keamanan informasi oleh organisasi secara luas, menyediakan panduan tertentu yang paling komprehensif untuk menajemen keamanan informasi di organisasi [19]. Standar ini tidak tergantung pada produk IT, membutuhkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk memastikan bahwa kontrol keamanan yang dipilih mampu untuk melindungi aset informasi dari berbagai risiko [3] [20].

Tujuan dari penelitian ini adalah mengetahui tingkat risiko penggunaan sistem informasi di Tripio Purwokerto. Penelitian serupa juga pernah dilakukan menggunakan metode ISO 31000:2018 pada bidang pendidikan [21] dan juga penelitian dilakukan menggunakan metode ISO 31000:2009 pada perusahaan teknologi [1] namun rekomendasi tindakan belum mengacu pada standar khusus sehingga hal tersebut mengacu penelitian yang akan dilakukan dengan memberikan rekomendasi penanangan pengacu pada standar ISO/EIC 27001.

2. METODE PENELITIAN

2.1 Tahap Pengumpulan Data

Pengumpulan data dilakukan dengan beberapa cara agar memenuhi data yang dibutuhkan. cara yang digunakan adalah

1. Wawancara.
   Wawancara dilakukan dengan karyawan Tripio Purwokerto sebagai admin online, dengan pimpinan Tripio Purwokerto sebagai pengambil kebijakan dan juga bagian IT sebagai pengelola sistem.
2. Observasi.
   Pada tahap ini, dilakukan pengamatan secara langsung dengan mengunjungi Tripio Purwokerto untuk melihat risiko apa yang pernah terjadi dan bagaimana proses bisnis yang berjalan.
3. Studi Pustaka.
   Studi pustaka dilakukan untuk mencari berbagai sumber terkait dengan tema penelitian yaitu manajemen risiko teknologi informasi agar dapat menjadi bahan referensi agar dapat memudahkan dalam proses penelitian, referensi diperoleh dari jurnal, prosiding, buku dan sumber dari internet.
4. Kuesioner.
   Kuesioner dilakukan untuk mengetahui tingkatan risiko yang ada di Tripio Purwokerto, kuesioner ini ditujukan kepada pengguna sistem, pembuat sistem dan penentu kebijakan.

5. Dokumentasi.
   Dokumentasi berupa foto pada saat wawancara, observasi, dan hasil kuesioner yang sudah diisi oleh karyawan Tripio Purwokerto.

2.2 Tahap indentifikasi masalah

Setelah memperoleh data melalui proses pengumpulan data selanjutnya melakukan identifikasi masalah dan mendeskripsikan hal-hal yang berkaitan dengan penerapan teknologi informasi di tempat penelitian.

2.3 Tahap Penerapan *International Organization for Standardization* (ISO) 31000:2018

Tahap ini merupakan tahap yang dilakukan untuk menganalisis proses manajemen risiko di tempat penelitian. Pada tahapannya [10].

1. Komunikasi dan konsultasi
   Pada tahap ini komunikasi dan konsultasi dilakukan di tempat penelitian, kamunikasi dan konsultasi dilakukan terhadap pimpinan, pengguna sIstem dan bagian IT. Pada tahap ini dilakukan observasi dan wawancara untuk mengetahui bagaimana penerapan manajemen risiko di Tripio Purwokerto.
2. Menetapkan konteks
   1. Konteks Eksternal
      Konteks eksternal pada tempat penelitian adalah lingkungan luar perusahaan agar membantu mencapai tujuan perusahaan.
   2. Konteks internal
      Konteks internal pada tempat penelitian adalah lingkungan dalam perusahaan agar membantu mencapai tujuan Konteks eksternal perusahaan.
3. Penilaian risiko
   Tahap penilaian risiko pada teknologi informasi di tempat penelitian terdiri dari tiga tahapan, yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko.
   1. Identifikasi Risiko
      Tahap identifikasi risiko dilakukan dengan mengetahui risiko apa saja yang berada pada tempat penelitian.
   2. Analisis Risiko
      Setelah mengetahui risiko yang ada, langkah berikutnya yaitu mengidentifikasi risiko tersebut sesuai dengan tingkatan dampak terhadap organisasi.
   3. Evaluasi risiko
      Pada tahap ini membandingkan risiko-risiko yang telah dihitung berdasarkan kriteria risiko dan kriteria dampak.
4. Kontrol Risiko
   Setelah tahap evaluasi risiko selesai dilakukan, tahap selanjutnya adalah perlakuan risiko yang mengacu pada standar ISO/EIC 27001:2013. Standar ini memberikan kontral-kontrol terhadap risiko yang ada agar dapat mengurangi terjadinya risiko.
5. Monitoring dan *Review*
   Tahap monitoring dan *review* dilakuakan secara menyeluruh dalam organisasi dan dilakukan secara berkala. Hasil pembahasan dari monitoring diarsipkan agar dapat menjadi dokumen bagi organisasi.

3. HASIL DAN ANALISIS

Tripio Purwokerto selama ini belum menerapkan manajemen risiko penggunaan teknologi informasi dengan baik, penggunaan teknologi informasi tidak didukung dengan standar operasional prosedur yang ada. Terjadinya risiko penggunaan teknologi informasi masih ditangani tanpa prosedur yang jelas, hanya berdasarkan pengalaman tanpa adanya panduan tertentu dalam penanganan risiko, oleh sebab itu peneliti ingin melihat sajauh mana pengelolaan risiko di Tripio Purwokerto menggunakan metode ISO 31000. Berikut tahapan dari ISO 31000:

3.1 Menetapkan Konteks.

Konteks eksternal yang mempengaruhi pengelolaan risiko teknologi informasi yaitu:

1. Distributor.
   Bekerja sama dengan beberapa distributor untuk memenuhi kebutuhan produk penjualan.
2. *Leasing*
   Bekerja sama dengan leasing seperti BAF (Bussan Auto Finance), FIF *(Federal International Finance)*, Adira dan Kredit++.
3. *Marketplace*
   Dalam memudahkan dalam proses pemasaran dan penjualan menggunakan *marketplace* seperti tokopedia, blibli.com, dan siplah.

Konteks internal adalah lingkungan dimana perusahaan berusaha mencapai tujuan dari apa yang diterapkan. Konteks internal berisi tentang struktur organisasi dan sumber daya manusia

3.2 Penilaian Risiko

Pada tahap penilaian risiko di Tripio Purwokerto terdiri dari tiga tahapan, yaitu identifikasi risiko, analisis risiko dan evaluasi risiko. Berikut penjelasan dari tahapan tersebut, Tahap ini dilakukan untuk mengidentifikasi risiko yang akan terjadi pada aset-aset yang ada Identifikasi risiko pada tabel 1.

Tabel 1. Identifikasi Risiko

No.	Risiko	Dampak
1	*Human error*	Salah penginputan data
2	Server down.	Menghambat kegiatan bisnis, Sistem yang sedang berjalan tidak sinkron antara sistem gudang dengan sistem POS.
3	Kerusakan pada hardware	Mengurangi jumlah aset, memperlambat proses bisnis.
4	Overheat	Aplikasi yang digunakan mengalami gangguan.
5	Overload	Kinerja server mengalami penurunan performa.
6	Pencurian perangkat/data.	Kehilangan data penting perusahaan.
7	Kebocoran data informasi perusahaan.	Data penting yang dicuri.
8	Listrik padam.	Mengganggu proses kerja, Performa server menurun.
9	Kebakaran	Kerusakan sarana dan prasana
10	Petir	Kerusakan sarana dan prasarana
11	Penyalahgunaan hak akses.	Rentan terjadinya kebocoran data
12	Virus dan sejenisnya	Data hilang, rusak dan bisa dicuri
13	Koneksi jaringan terputus tidak stabil.	Kegiatan bisnis terhambat.
14	Genset tidak berfungsi	Menganggu proses bisnis perusahaan.
15	Program crash.	Data hilang dan rusak.

Pada tahap ini dilakukan penilaian terhadap risiko yang ada. Frekuensi penilaian risiko diisi dengan angka 1 sampai 5 sesuai dengan kondisi yang ada. Dengan keterangan nilai 1(Insignificant), 2(Minor), 3(Moderate), 4(Major) dan 5(Catastrophic). Tabel analisis risiko dapat dilihat pada tabel 2 berikut.

Tabel 2. Analisis Risiko

No	Risiko	Analisis Risiko
1	*human error*	3
2	Server down.	5
3	Kerusakan pada hardware	5
4	Overheat	3
5	Overload	3
6	Pencurian perangkat/data.	5
7	Kebocoran data informasi perusahaan.	5
8	Listrik padam.	5
9	Kebakaran	5
10	Petir	3
11	Penyalahgunaan hak akses.	4
12	Virus dan sejenisnya	2
13	Koneksi jaringan terputus tidak stabil.	5
14	Genset tidak berfungsi	4
15	Program crash.	5

Setelah tahap analisis risiko dilakukan selanjutnya adalah tahap evaluasi risiko. Tahap ini membandingkan hasil dari analisis risiko terhadap parameter risiko yang telah diidentifikasi. Level risiko yang telah diidentifikasi dapat dilihat pada tabel di bawah ini:

Tabel 3. Evaluasi Risiko

No	Nama Risiko	Analisis Risiko	Tingkatan Risiko
13	Koneksi jaringan terputus tidak stabil.	5	*High*
2	Server *down*	5	*High*
3	Kerusakan pada *hardware*	5	*High*
8	Listrik padam.	5	*High*
14.	Genset tidak berfungsi atau rusak.	4	*High*
15.	Program *crash*.	5	*High*
9	Kebakaran	5	*Medium*
1	*human error*	3	*Medium*
6	Pencurian perangkat/data.	5	*Medium*
7	Kebocoran data informasi perusahaan.	5	*Medium*
4	*Overheat*	3	*Medium*
5	*Overload*	3	*Medium*
11	Penyalahgunaan hak akses	4	*Medium*
10	Petir	3	*Low*
12	Virus dan Sejenisnya	2	*Low*

3.3 Kontrol Risiko

Pada tahap ini, risiko yang telah diidentifikasi dan dievaluasi akan diberi usulan-usulan dalam memperlakukan risiko agar semua risiko dapat dicegah maupun dikurangi sehingga proses bisnis dapat berjalan secara maksimal. Usulan perlakuan risiko disusun berdasarkan dari tingkatan risiko (level of risk) dengan tingkatan paling tinggi (high) ke tingkatan paling rendah (low). Perlakuan risiko mengacu pada standar ISO/EIC 27001:2013, penjelasan tersebut dapat dilihat pada tabel 4 berikut:

Tabel 4. Evaluasi Risiko

Risiko	Kontrol Risiko (ISO/IEC 27001:2013)
Koneksi jaringan terputus tidak stabil.	Pekerjaan jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi. A.13.1.1 Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan kerja jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan, baik layanan ini disediakan di rumah atau di-outsourcing.A.13.1.2
Server *down*	Prosedur harus diterapkan untuk mengontrol instalasi perangkat lunak pada sistem operasional.A12.5.1 Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan.A.11.2.4 Salinan cadangan informasi, perangkat lunak, dan citra sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati. A.12.3.1.
Kerusakan pada *hardware*	Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan.A.11.2.4
Listrik padam.	Prinsip-prinsip untuk sistem keamanan teknik harus ditetapkan, didokumentasikan, dipelihara dan diterapkan pada sistem informasi apapun upaya implementasi.A.14.2.5
Genset tidak berfungsi atau rusak.	Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan.A.11.2.4
Program *crash*.	prosedur harus diterapkan untuk mengontrol instalasi perangkat lunak pada sistem operasional.A.12.5.1. Deteksi, pencegahan dan kontrol pemulihan untuk melindungi malware harus diterapkan, digabungkan dengan pengguna yang sesuaikesadaran. A.12.2.1 Salinan cadangan informasi, perangkat lunak, dan citra sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati. A.12.3.1. prosedur harus diterapkan untuk mengontrol instalasi perangkat lunak pada sistem operasional.A.12.5.1
Kebakaran	Perlindungan fisik terhadap bencana alam, serangan jahat atau kecelakaan harus dirancang dan diterapkan. A.11.1.4 Salinan cadangan informasi, perangkat lunak, dan citra sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati. A.12.3.1.
Human error	Semua karyawan organisasi dan, jika relevan, kontraktor harus menerima pendidikan dan pelatihan kesadaran yang sesuai dan pembaruan rutin dalam kebijakan dan prosedur organisasi, yang relevan dengan fungsi pekerjaan mereka.A.7.2.2 Harus ada proses disipliner formal dan yang dikomunikasikan untuk mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran keamanan informasi. .A.7.2.3
Pencurian perangkat/data.	Area aman harus dilindungi oleh kontrol masuk yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses.A.11.1.2
Kebocoran data informasi perusahaan.	Kebijakan pengendalian akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi.A.9.1.1 Sistem manajemen kata sandi harus interaktif dan harus memastikan kata sandi yang Berkualitas. A.9.4.3.
Overheat	Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.A.11.1.3
Overload	Log peristiwa yang merekam aktivitas pengguna, pengecualian, kesalahan, dan peristiwa keamanan informasi harus diproduksi, disimpan, dan ditinjau secara berkala.A.12.4.1
Penyalahgunaan hak akses.	Kebijakan pengendalian akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi.A.9.1.1 akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses.A.9.4.1 Sistem manajemen kata sandi harus interaktif dan harus memastikan kata sandi yang Berkualitas. A.9.4.3 Semua karyawan organisasi dan, jika relevan, kontraktor harus menerima pendidikan dan pelatihan kesadaran yang sesuai dan pembaruan rutin dalam kebijakan dan prosedur organisasi, yang relevan dengan fungsi pekerjaan mereka.A.7.2.2
Petir	Perlindungan fisik terhadap bencana alam, serangan jahat atau kecelakaan harus dirancang dan diterapkan. A.11.1.4 Salinan cadangan informasi, perangkat lunak, dan citra sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati. A.12.3.1.

Risiko	Kontrol Risiko (ISO/IEC 27001:2013)
Virus dan Sejenisnya	Perubahan organisasi, proses bisnis, fasilitas pemrosesan informasi dan sistem yang mempengaruhi informasi keamanan harus dikendalikan.A.12.1.2 Deteksi, pencegahan dan kontrol pemulihan untuk melindungi malware harus diterapkan, digabungkan dengan pengguna yang sesuaikesadaran. A.12.2.1 Salinan cadangan informasi, perangkat lunak, dan citra sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati. A.12.3.1

3.4 Monitoring dan *Review*

Kegiatan monitoring dan *review* dilakukan setelah penilaian risiko dilakukan dan rekomendasi kontrol telah diimplementasikan di organisasi. Berdasarkan monitoring yang dilakukan secara rutin terdapat penurunan risiko dan dampak yang ditimbulkan. Kegiatan monitoring dan *review* dilakukan dengan mengadakan pertemuan dengan topik bahasan penerapan teknologi informasi untuk membahas kendala-kendala atau kemungkinan risiko yang akan mengganggu proses bisnis organisasi dan membahas pencegahan agar dapat meminimalisir risiko yang akan terjadi dikemudian hari.

4. KESIMPULAN

Setelah dilakukan penilaian risiko mengacu pada metode ISO 3100:2018 pada Tripio Purwokerto dapat dinilai bahwa perusahaan tersebut belum menerapkan manajemen risiko dengan baik, hal tersebut dapat dilihat bahwa terdapat 15 risiko yang terdiri dari 6 risiko dengan tingkat risiko *high*, 7 risiko dengan tingkat risiko *medium*, dan 2 risiko dengan tingkat risiko *low*. Dari kontrol risiko yang ada diharapkan pihak organisasi segera mengimplementasikan rekomendasi yang ada sesuai dengan kondisi organisasi sehingga bisa mencegah maupun mengurangi risiko yang akan terjadi dikemudian hari. Rekomendasi kontrol yang digunakan mengacu pada ISO 27001:2013 bagian *human recource security, access control, physical and environmental security, operations security, protection from malware, communications security, system acquisition, development and maintenance*. Rekomendasi kontrol tersebut dituangkan dalam bentuk standar operasional prosedur dalam penanganan risiko yang terjadi di Tripio Purwokerto.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada Lembaga Penelitian Pengabdian Masyarakat Universitas AMIKOM Purwokerto dan Fakultas Ilmu Komputer Universitas AMIKOM Purwokerto yang telah mendukung penelitian ini.

REFERENSI

[1] A. Rahmawati and A. F. Wijaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP," *J. SITECH : Sistem Informasi dan Teknologi.*, vol. 2, no. 1, pp. 13–20, 2019.

[2] E. G. Monica and P. Pangeran, "The Integration of Balanced Scorecard and ISO 31 . 000 Based Enterprise Risk Management Process to Mitigate Supply Chain Risk : Case Study at PT Anugerah Bintang Meditama," *International Journal of Multicultural and and Multireligious Understanding (IJMMU).*, vol. 7, no. 10, pp. 616–628, 2020.

[3] I. Sulistyowati and R. V. H. Ginardi, "Information Security Risk Management with Octave Method and ISO/EIC 27001: 2013 (Case Study: Airlangga University)," in *IPTEK Journal of Proceedings Series*, 2019, vol. 1, pp. 32–38.

[4] Z. Putra, S. Chan, and M. IHA, "Design of Risk Management Based on ISO 31000 in PDAM Tirta Meulaboh," *J. AFEBI Management and Business Review.*, vol. 2, no. 1, p. 21, 2017.

[5] Y. E. Patabang, S. Suprayitno, E. Sahiri, and I. M. J. A, "Operational Risk Management of Surabaya Main Naval Base V Repair and Maintenance Facility Based on ISO 31000 Framework," *International Journal of ASRO*, vol. 10, no. 03, pp. 111–123, 2019.

[6] C. Kuntoro, "Implementasi Manajemen Risiko Kebakaran Berdasarkan (IS) ISO 31000 PT Apac Inti Corpora," *Higeia Journal of Public Health Research and Development (HIGEIA).*, vol. 1, no. 4, pp. 109–119, 2017.

[7] I. Setiawan, R. Waluyo, and W. A. Pambudi, "Perancangan Business Continuity Plan dan Disaster Recovery Plan Teknologi dan Sistem Informasi Menggunakan ISO 22301," *J. RESTI (Rekayasa Sistem. dan Teknologi. Informasi)*, vol. 3, no. 2, pp. 148–155, 2019.

[8] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," in *3rd International Conference on Computer Science and Computational Intelligence 2018*, 2018, vol. 135, no. March, pp. 202–213.

[9] D. S. Valena, R. Prabowo, anie rose Irawati, and A. Aristoteles, "Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode Nist Sp 800-30," *J. Komputasi*, vol. 7, no. 1, 2019.

[10] A. Syihabuddin, Y. Suryanto, and M. Salman, "Risk Management in Data Centers Using ISO 31000 Case Study : XYZ Agency," In *The 1st STEEEM 2019*, 2019, vol. 1, no. 1, pp. 341–352.

[11] W. S. Prabowo, . W., N. A Setiawan, M. H. Muslim, and Y. S. Utama, "Manajemen Risiko Infrastruktur Cloud Pemerintah Menggunakan Nist Framework Studi Kasus Lembaga Ilmu Pengetahuan Indonesia (LIPI)," *J. Penelitian Pos dan Informatika.*, vol. 7, no. 1, p. 17, 2017.

[12] F. I. S. Yudha and R. E. Gunadhi, "Risk Assessment Pada Manajemen Resiko Keamanan Informasi Mengacu Pada British Standard ISO/IEC 27005 Risk Management," *J. Algoritma.*, vol. 13, no. 1, pp. 1689–1699, 2016.

[13] A. Y. Wicaksono, "Applying ISO:31000:2018 as Risk Management Strategy on Heavy Machinery Vehicle Division," *International Journal of Science, Engineering and Information Technology.*, vol. 4, no. 2, pp. 198–202, 2020.

[14] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 : 2018 (Studi Kasus: Cv. XY)," *J. Sebatik*, vol. 23, no. 1, pp. 277–284, 2019.

[15] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengembangan Teknologi Informasi dan Ilmu Komputer.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[16] I. Setiawan, M. Sutopo, and A. Azis, "Manajamen Risiko SIMRS Menggunakan Metode OCTAVE-S dan Standar Pengendalian ISO / EIC 27001," *J. Teknik Informatika dan Sistem Informasi.*, vol. 7, no. 3, pp. 1–8, 2020.

[17] A. Fathurohman and R. W. Witjaksono, "Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)," *Bulletin of Computer Science and Electrical Engineering.*, vol. 1, no. 1, pp. 1–11, 2020.

[18] R. R. Wijayanti, "Implementasi Octave-S dan Standar Pengendalian ISO 27001:2013 Pada Manajemen Risiko Sistem Informasi Perguruan Tinggi," *J. Pengkajian dan Penerapan Teknik Informatika (PETIR).*, vol. 11, no. 2, pp. 221–233, 2018.

[19] P. Februari and F. Fitria, "Audit Sistem Keamanan Informasi Menggunakan ISO 27001 Pada SMKN 1 Pugung, Lampung," *POSITIF J. POSITIF : Jurnal Sistem dan Teknologi Informasi.*, vol. 5, no. 2, p. 97, 2019.

[20] R. Tatiara, A. N. Fajar, B. Siregar, and W. Gunawan, "Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001," in *Journal of Physics: Conference Series*, 2018, vol. 978, no. 1, pp. 12–39.

[21] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 Pada Smart Canteen SMA XYZ," *J. JURIKOM : Jurnal Riset Komputer*, vol. 7, no. 1, p. 91, 2020.