PENILAIAN DAN KONTROL RISIKO TERHADAP INFRASTRUKTUR DAN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 (STUDI KASUS: INSTITUT TEKNOLOGI SEPULUH NOPEMBER)

Anindya Dwi Lestari Sugianto[1)], Febriliyan Samopa[2)], dan **Hanim Maria Astuti[3)]**

[1,2,3]Sistem Informasi Institut Teknologi Sepuluh Nopember
[1,2,3]Jl. Arif Rahman Hakim Surabaya, 60111
E-mail : personal.anin@gmail.com[1)], iyan@is.its.ac.id[2)], hanim@is.its.ac.id[3)]

ABSTRAK

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember (ITS) Surabaya merupakan direktorat yang memiliki fungsi menangani seluruh aktivitas yang berhubungan dengan sistem dan teknologi informasi di ruang lingkup ITS. Risiko yang muncul dalam organisasi di bidang sistem dan teknologi informasi terutama pada ruang lingkup infrastruktur dan keamanan informasi, seperti adanya kerusakan aset, pencurian data, layanan yang tidak bisa diakses. Tindakan penanganan risiko terkait ruang lingkup infrastruktur dan keamanan informasi di DPTSI ITS belum diterapkan dengan baik sehingga dapat mengakibatkan terganggunya proses bisnis. Sehingga untuk memenuhi kebutuhan terkait ruang lingkup infrastruktur dan keamanan informasi diperlukan adanya standar agar dapat meminimalisir risiko yang ada. Standar yang digunakan dalam penelitian ini adalah standar ISO/IEC 27001:2013 sebagai kerangka kerja dalam proses identifikasi dan penilaian risiko terkait ruang lingkup infrastruktur dan keamanan informasi yang dibuat berdasarkan hasil wawancara dan justifikasi dari pihak DPTSI ITS. Adapun standar lain yang digunakan yaitu ISO/IEC 27002:2013 sebagai standar penyusunan kontrol dari hasil penilaian risiko terkait ruang lingkup infrastruktur dan keamanan informasi. Hasil yang diharapkan dalam penelitian ini berupa dokumen penilaian beserta penyusunan kontrol risiko yang sesuai dengan kebutuhan terkait ruang lingkup infrastruktur dan keamanan informasi di DPTSI ITS dengan menggunakan standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013.

Kata Kunci: *Identifikasi Risiko, Penilaian Risiko, Kontrol Risiko, ISO/IEC 27001:2013, ISO/IEC 27002:2013*

1. PENDAHULUAN

Setiap organisasi akan menghadapi ketidakpastian yang dapat menyebabkan munculnya risiko. Risiko merupakan kemungkinan kejadian atau keadaan yang dapat mengancam pencapaian tujuan dan sasaran organisasi. Penerapan manajemen risiko sudah menjadi kebutuhan dan tuntutan di setiap organisasi dalam upaya perlindungan dan peningkatan kualitas keamanan informasi yang dimiliki. Dalam manajemen risiko terdapat beberapa proses yang perlu dilakukan yaitu dengan identifikasi, analisis, evaluasi serta penerapan kontrol atau kendali risiko sesuai dengan kebutuhan organisasi (International Organization for Standarization ISO 31000, 2009).

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember (ITS) Surabaya merupakan organisasi yang berperan dalam penyediaan dan pengelolaan layanan teknologi informasi ITS untuk mendukung aktivitas akademik, penelitian, pengabdian masyarakat, serta manajerial di lingkungan ITS dalam mencapai visi misinya. DPTSI ITS menggunakan teknologi informasi sebagai penunjang proses bisnisnya. Adapun beberapa fungsi DPTSI ITS yaitu pelaksanaan penjaminan keamanan sistem informasi, pelaksanaan pemberian layanan jasa di bidang teknologi dan sistem informasi, serta pelaksanaan monitoring dan evaluasi pengembangan teknologi dan sistem informasi (DPTSI, 2018).

Sistem Manajemen Keamanan Informasi (SMKI) dirancang sesuai dengan standar internasional yang memberikan dasar implementasi strategi keamanan informasi untuk mengamankan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi dengan menerapkan proses manajemen risiko yang lebih efektif dan efisien (Basyarahil, 2017). Pendekatan dari keamanan informasi bergantung pada kondisi yang dihadapi setiap organisasi. DPTSI ITS sebagai organisasi yang terus berkembang dan memiliki aktivitas yang beragam, sehingga ada kemungkinan munculnya ancaman, kerentanan, dan risiko yang semakin kompleks terhadap infrastruktur dan keamanan informasi. Adapun penyebab permasalahan yang sering muncul di DPTSI ITS karena masih kurangnya pengelolaan serta langkah pengendalian terhadap infrastruktur dan keamanan informasi. Beberapa permasalahan tersebut yaitu tidak tepatnya

konfigurasi sistem dan teknologi informasi, adanya kerusakan pada beberapa aset infrastruktur teknologi informasi DPTSI ITS, masih adanya celah keamanan informasi sehingga diperlukan perbaikan kontrol, banyaknya keluhan dari pemangku kepentingan terhadap infrastruktur dan keamanan informasi yang tidak didokumentasikan dengan baik sehingga diperlukan kontrol untuk menanganinya, karena pada dasarnya seluruh permasalahan yang muncul juga berasal dari semua aset yang dimiliki DPTSI ITS.

Dengan adanya beberapa permasalahan tersebut, maka standar yang relevan terkait dengan penelitian ini, yaitu ISO/IEC 27001:2013 yang berfungsi sebagai acuan untuk penerapan, pengelolaan, dan peningkatan sistem manajemen keamanan informasi (International Organization for Standarization ISO 27001, 2013). Untuk melakukan penilaian risiko diperlukan justifikasi seputar nilai aset, probabilitas dan dampak risiko terhadap organisasi. Selanjutnya diperlukan langkah kontrol dalam penerapan manajemen risiko berdasarkan acuan ISO/IEC 27002:2013 yang berfungsi sebagai acuan dalam pemberian kontrol pada penerapan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001 sehingga kontrol yang diterapkan dapat disesuaikan dengan kebutuhan organisasi berdasarkan hasil analisis risiko terkait infrastruktur dan keamanan informasi yang telah dilakukan (International Organization for Standarization ISO 27002, 2013). Segala informasi yang berhubungan dengan perangkat keras, perangkat lunak, jaringan serta individu yang terlibat dalam kegiatan operasional merupakan aset penting sehingga membutuhkan perlindungan dari berbagai macam ancaman dalam organisasi. Adanya keamanan informasi ini dapat meminimalisir risiko dengan melakukan pengelolaan dan perlindungan dari ancaman, kerentanan dan dampaknya terhadap aset organisasi.

Demikian ini merupakan bentuk optimal berupa penilaian dan penyusunan kontrol risiko terhadap infrastruktur dan keamanan informasi, serta untuk mempersiapkan sertifikasi ISO/IEC 27001 di DPTSI ITS. Sehingga dapat menentukan risiko beserta langkah-langkah kontrol yang tepat terhadap infrastruktur dan keamanan informasi agar tidak mengganggu jalannya proses bisnis yang ada, serta untuk mencapai keberhasilan dalam sistem manajemen keamanan informasi yang ada di DPTSI ITS.

2. RUANG LINGKUP

Ruang lingkup permasalahan pada penelitian ini berfokus pada aset infrastruktur dan keamanan informasi untuk melakukan proses penilaian dan penyusunan kontrol risiko di DPTSI ITS.

Penilaian risiko dilakukan berdasarkan standar ISO/IEC 27001:2013 serta disesuaikan dengan wawancara ke pihak DPTSI ITS, tindakan manajemen risiko yang dilakukan dalam penelitian ini hanya sampai pada penilaian dan penyusunan kontrol risiko berdasarkan standar ISO/IEC 27002:2013, serta untuk penilaian dan penyusunan kontrol risiko hanya berfokus pada perangkat keras, perangkat lunak, dan jaringan di ITS.

Dengan adanya penelitian ini, maka rencana hasil yang didapatkan berupa daftar risiko, penilaian, serta kontrol risiko yang dapat digunakan sebagai rekomendasi dan pedoman manajemen risiko bagi pihak DPTSI ITS.

3. BAHAN DAN METODE

Berikut ini merupakan penjelasan bahan dan metode yang digunakan dalam penelitian.

3.1 Aset

Beberapa definisi aset antara lain sebagai berikut:

1. Sumber daya organisasi yang dilindungi, sehingga aset dapat berupa bentuk logis seperti situs web atau informasi yang dapat dikontrol atau dimiliki oleh organisasi; serta aset yang berbentuk fisik seperti sistem komputer atau objek nyata lainnya (Mattord, 2016).
2. Segala sesuatu yang memiliki nilai pada organisasi, termasuk di dalamnya terdapat informasi yang dapat mendukung misi organisasi (International Organization for Standarization ISO 13335, 2004)

Berdasarkan beberapa definisi aset di atas, maka dapat disimpulkan bahwa aset merupakan segala sumber daya yang memiliki nilai bagi organisasi sehingga membutuhkan upaya pengelolaan dan perlindungan tertentu.

3.2 Risiko

Risiko adalah ketidakpastian (*uncertainty*) yang mungkin melahirkan peristiwa kerugian (*loss*) (Salim, 2007). Dalam referensi lain juga menyebutkan bahwa risiko adalah kemungkinan (*likelihood*) sumber ancaman (*threat-source*) yang mengeksploitasi kerentanan (*vulnerability*) potensial, serta menghasilkan dampak (*impact*) berupa kejadian yang merugikan organisasi (Spremic, 2008). Risiko terdiri atas tiga faktor, antara lain (Corporation, 2012).

1. Aset (*asset)*
   Aset terbagi atas dua jenis yaitu *tangible* berupa aset berbentuk yang memiliki nilai finansial seperti uang, gedung, *hardware*, *software*, serta pegawai. Sedangkan aset *intangible* dapat berupa *data*, catatan, dokumen yang berbentuk *hardcopy* ataupun *softcopy*
2. Ancaman (*Threat)*
   Ancaman merupakan keadaan dan kejadian yang memiliki kemungkinan atau juga bisa diartikan potensi hilang dan kerusakan pada aset.
3. Kerentanan(*vulnerability)*
   Kerentanan merupakan kelemahan dari sebuah aset atau desain infrastruktur, implementasi, aktivitas operasional yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

3.3 Risiko Sistem Informasi

Risiko sistem informasi dapat berupa ancaman terhadap aset sistem informasi seperti kegagalan pada perangkat lunak, perangkat keras, kesalahan manusia (Putri, 2017). Kegagalan sistem informasi di asumsikan jika sistem informasi tidak memenuhi harapan pengguna atau ketidakmampuan kinerja yang baik pada sistem yang berfungsi. Risiko teknologi informasi sangat erat kaitannya dengan keamanan informasi, dimana informasi merupakan aset yang sangat penting bagi sebuah organisasi dan jika terganggu dapat menimbulkan dampak yang signifikan terhadap proses bisnis organisasi. Risiko tersebut dapat berupa ancaman teknologi informasi dan kerentanan teknologi informasi dari sebuah organisasi (Perdana, 2018).

3.4 Manajemen Risiko

Manajemen risiko merupakan proses identifikasi, penilaian, dan pengambilan langkah untuk mengurangi risiko ke tingkat yang dapat diterima oleh organisasi. Ancaman atau risiko di sini dapat berasal dari internal dan eksternal sehingga dalam penanganannya diperlukan strategi untuk mengatasi atau meminimalisir risiko yang mungkin terjadi. Manajemen risiko memiliki tiga komponen (Mattord, 2016).

1. *Risk Identification* (Identifikasi Risiko)
   Dokumentasi risiko terhadap aset informasi yang dimiliki oleh organisasi.
2. *Risk Assessment* (Penilaian Risiko)
3. Menentukan dampak risiko aset informasi terhadap organisasi.
4. *Risk Control* (Pengendalian Risiko)
   Penerapan pengendalian untuk mengurangi risiko aset informasi ke tingkat yang dapat diterima oleh organisasi. Sehingga manajemen risiko adalah proses organisasi dalam melakukan tindakan untuk meminimalisir risiko keamanan informasi yang dianggap dapat mengurangi kemungkinan terjadinya risiko atau mengurangi dampak dari risiko yang terjadi.

3.5 Kriteria Penilaian

Kriteria penilaian digunakan untuk mengidentifikasi keadaan yang memiliki dampak bagi organisasi. Dimana kriterianya harus mencerminkan nilai, tujuan, dan sumber daya organisasi. Untuk penentuan kerangka penilaian berdasarkan aset, probabilitas dan dampak.

3.6 ISO/IEC 27001:2013

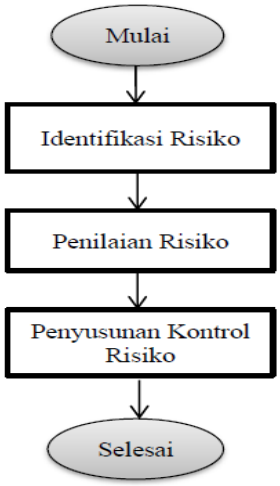
International Organization for Standardization (ISO), dan *International Electrotechnical Commission* (IEC) adalah badan yang menetapkan standar internasional yang terdiri dari perwakilan dari badan standardisasi setiap negara. Salah satu standar yang dikeluarkan adalah ISO/IEC 27001 yang merupakan standar yang menetapkan kebutuhan dalam membangun, menerapkan, mempertahankan, dan peningkatan berkelanjutan sebuah sistem manajemen keamanan informasi (SMKI) dalam organisasi yang mencakup penilaian dan perlakuan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi. ISO/IEC 27001 terdiri atas 7 klausul kontrol dalam 35 kategori keamanan informasi.

3.7 ISO/IEC 27002:2013

Standar ISO/IEC 27002:2013 merupakan penanaman ulang dari ISO/IEC 17799:2005. ISO/IEC 27002:2013 merupakan panduan standar keamanan informasi organisasi dan praktik manajemen keamanan informasi yang termasuk di dalamnya pemilihan, implementasi, dan manajemen kontrol dengan pertimbangan risiko keamanan informasi di lingkungan organisasi yang dirancang untuk digunakan oleh organisasi. ISO/IEC 27002 terdiri atas 14 klausul kontrol keamanan dalam 35 kategori keamanan utama dan 114 kendali.

3.8 Tahapan Penelitian

Tahapan atau kerangka penelitian menjadi acuan dalam melakukan proses penelitian, sehingga pelaksanaan penelitian dapat berjalan dengan terstruktur pada Gambar 1.



Gambar 1. Tahapan Penelitian

1. Identifikasi Risiko

Pada tahapan ini dilakukan proses identifikasi risiko terkait infrastruktur dan keamanan informasi yang berdampak terhadap *confidentiality*, *integrity* dan *availability* serta pemilik risiko pada DPTSI ITS. Identifikasi dilakukan untuk menentukan potensi kerusakan, agar mendapatkan wawasan terhadap bagaimana, dimana, dan kenapa kerusakan bisa terjadi. Selain itu dilakukan juga identifikasi terhadap aset, proses bisnis, ancaman, kontrol yang telah ada, kerentanan, dan konsekuensi terhadap komponen infrastruktur dan keamanan informasi.

2. Penilaian Risiko

Tahap ini terdiri dari 2 bagian yaitu proses analisis dan evaluasi risiko. Untuk proses analisis risiko dilakukan dengan membandingkan kriteria risiko dengan

daftar risiko yang telah diperoleh sebelumnya dan selanjutnya menghasilkan prioritas risiko sebagai langkah untuk menentukan kontrol risiko terhadap infrastruktur dan keamanan informasi terhadap aset dan proses bisnis organisasi.

3. Penyusunan Kontrol Risiko

Pada tahapan ini dilakukan penyusunan kontrol sebagai aksi pengendalian risiko terkait infrastruktur dan keamanan informasi. Proses penyusunan kontrol ini dilakukan dengan mengacu pada kontrol yang telah dibuat sebelumnya dengan mempertimbangkan adanya penambahan serta perbaikan kontrol yang diperlukan agar dapat memaksimalkan proses pengendalian risiko terkait infrastruktur dan keamanan informasi dengan tepat. Kontrol risiko terhadap infrastruktur dan keamanan informasi yang digunakan berdasarkan ISO/IEC 27002:2013. Dalam proses pembuatan kontrol, setiap risiko akan dipetakan berdasarkan kontrol yang relevan dan sesuai dengan kebutuhan risiko.

4. PEMBAHASAN

Berikut ini merupakan pembahasan dari hasil pada setiap tahapan penelitian yang telah dilakukan.

4.1 Identifikasi Risiko

Pembahasan hasil identifikasi risiko dibuat berdasarkan ancaman, kerentanan dan kontrol yang telah diidentifikasi sebelumnya berdasarkan aset yang ada di DPTSI ITS.

Pada Tabel 1 dibuat tabel risiko berdasarkan penyebab, kerentanan dan dampak risiko berdasarkan hasil wawancara dengan narasumber dari pihak Subdit Infrastruktur dan Keamanan Teknologi Informasi DPTSI ITS serta analisis yang dilakukan dalam penelitian ini.

Tabel 1. Identifikasi Risiko

Nama Aset	Penyebab	Kerentanan	Risk ID	Risiko	Dampak
Application Server (Perangkat Keras)	AC di ruangan server mati	*Monitoring* AC yang kurang baik	HR-01	Kerusakan *application server*	Proses bisnis terkait dengan penggunaan *application server* terganggu
	Suhu panas menyebabkan *down* (suhu normal < 20-25 derajat Celsius)	Server *down*	HR-02	Kerusakan *application server*	
Lisensi Perangkat Keras (Perangkat Lunak)	Adanya lisensi *subscription/terpisah dengan perangkat*	Terikat batas waktu kontrak	SR-01	Sistem keamanan perangkat kurang terjamin karena tidak bisa *update*	Proses bisnis terkait dengan penggunaan Lisensi Perangkat Keras (*server*) terganggu
Kabel UTP/LAN (Jaringan)	Kualitas fisik kabel (faktor usia dan merek perangkat)	Kabel UTP/LAN tidak bisa digunakan secara optimal	NR-01	*End of life* (faktor usia perangkat idealnya 5 tahun/sesuai garansi)	Proses bisnis terkait dengan penggunaan kabel UTP/LAN terganggu
	Kabel dimakan tikus	Kesalahan penempatan kabel UTP/LAN yang kurang rapi dan kurang rapat	NR-02	Kerusakan kabel UTP/LAN	

4.2 Penilaian Risiko

Penilaian risiko dikategorikan berdasarkan nilai aset, probabilitas dan dampak terhadap organisasi. Untuk nilai aset dibedakan menjadi 3 kategori yaitu 1 untuk nilai aset tinggi, 2 untuk nilai aset sedang, dan 3 untuk nilai aset rendah. Adapun untuk probabilitas dan dampak dibedakan menjadi 4 kategori yaitu 1 dengan skala berat, 2 dengan skala menengah, 3 dengan skala ringan, dan 4 dengan skala sangat kecil. Sehingga nantinya risiko dapat dibedakan menjadi 3 kategori risiko yaitu rendah, sedang dan tinggi. Untuk menentukan kategori risiko tinggi berdasarkan analisis pada nilai aset (skala 1-2), probabilitas (skala 1-3) dan dampak (skala 1-3). Adapun untuk menentukan kategori risiko sedang berdasarkan analisis pada nilai aset (skala 1-3), probabilitas (1-4) dan dampak (skala 1-4). Sedangkan untuk menentukan kategori risiko rendah berdasarkan analisis pada nilai aset, probabilitas dan dampak (skala 1-4). Berikut ini merupakan hasil pemetaan kategori risiko yang digunakan sebagai acuan dalam melakukan penilaian risiko berdasarkan justifikasi dari pihak Direktur DPTSI ITS seperti pada Tabel 2.

Tabel 2. Pemetaan Kategori Risiko (Kominfo, 2017)

Nilai Aset	Dampak	Probabilitas	Kategori Risiko
3	4	4	Rendah
3	3	4	Rendah
3	2	4	Rendah
3	1	4	Sedang
3	4	3	Rendah
3	3	3	Rendah
3	2	3	Sedang
3	1	3	Sedang
1	1	2	Tinggi
1	4	1	Sedang
1	3	1	Tinggi
1	2	1	Tinggi
1	1	1	Tinggi
…	…	…	…

Dalam tahap ini dilakukan penilaian risiko berdasarkan hasil wawancara dengan narasumber dari pihak Subdit Infrastruktur dan Keamanan Teknologi Informasi DPTSI ITS, serta didukung dengan analisis yang dilakukan dalam penelitian ini. Hasil dan pembahasan dari penilaian risiko dapat dilihat pada Tabel 3.

Tabel 3. Penilaian Risiko (M. S. Toosarvandani, N. Modiri, M. Afzali, 2012)

Nama Aset	Risk ID	Nilai Aset	Nilai Dampak	Nilai Probabilitas	Kategori Risiko
Application Server (Perangkat Keras)	HR-01	1	3	3	Sedang
…	…	…	…	…	…
Lisensi Perangkat Keras (Perangkat Lunak)	SR-01	1	1	4	Sedang
...	…	…	…	…	…
Kabel UTP/LAN (Jaringan)	NR-01	1	1	4	Sedang
…	…	…	…	…	…

4.2 Penyusunan Kontrol Risiko

Setelah melakukan penilaian terhadap risiko, selanjutnya akan dilakukan identifikasi dan pemilihan kontrol untuk meminimalisir risiko dengan menggunakan acuan standar ISO/IEC 27002:2013. Serta juga diperlukan justifikasi narasumber dari pihak Subdit Infrastruktur dan Keamanan Teknologi Informasi DPTSI ITS untuk memetakan opsi tindakan kontrol sebagai bentuk implementasi dan mengukur sejauh mana risiko tersebut agar dapat ditangani. Untuk tindakan *accept* dilakukan analisis jika risiko berdasarkan nilai aset, dampak serta probabilitasnya sangat kecil. Lalu untuk tindakan *mitigate* dilakukan analisis jika risiko berdasarkan nilai, dampak dan probabilitasnya menengah. Adapun untuk tindakan *migrate* dilakukan analisis jika risiko berdasarkan nilai aset dan probabilitasnya tinggi. Serta untuk tindakan *avoid* dilakukan analisis jika risiko berdasarkan nilai aset, dampak dan probabilitasnya tinggi. Berikut ini merupakan hasil pemetaan opsi tindakan kontrol dari penilaian risiko yang telah dilakukan seperti pada Tabel 4.

Tabel 4. Pemetaan Opsi Kontrol Risiko

Nilai Aset	Dampak	Probabilitas	Kategori Risiko	Opsi Tindakan Kontrol
3	4	4	Rendah	*Accept*
3	3	4	Rendah	*Accept*
3	2	4	Rendah	*Mitigate*
3	1	4	Sedang	*Mitigate*
3	4	3	Rendah	*Accept*
…	…	…	…	**…**

Selanjutnya pada Tabel 5 dibuat tabel kontrol risiko yang berisi bentuk kontrol risiko dengan mengacu pada ISO/IEC 27002:2013. Pada tabel ini kontrol yang disarankan dilakukan secara lebih teknis berbeda dengan *implementation guideline*. Hasil dan pembahasan dari beberapa kontrol risiko dapat dilihat pada Tabel 5.

Tabel 5. Penyusunan Kontrol Risiko

Risiko	Penyebab	Level	Kontrol ISO/IEC 27002:2013	Justifikasi ISO/IEC 27002:2013	Opsi Kontrol Risiko	Bentuk Kontrol Risiko
Kerusakan *application server* (Perangkat Keras)	AC di ruangan server mati	Sedang	11.2.2 *Supporting utilities*	Kontrol yang memastikan perangkat/aset terbebas dari gangguan listrik	*Mitigate*	Memastikan kesesuaian penanganan AC Presisi/PAC sesuai dengan standar yang ada
			12.1.1 *Document and operational procedure*	Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	*Mitigate*	Membuat prosedur monitoring terhadap AC Presisi/PAC
…	…	…	…	…	...	…

5. KESIMPULAN

Berdasarkan proses dan tahapan penilaian risiko yang telah dilakukan, maka diperoleh risiko tertinggi yang meliputi pelayanan yang kurang siaga terkait keluhan sistem informasi, jaringan *down*, kerusakan *server*, kerusakan *router*, pencurian atau pengubahan informasi yang ada di dalam sistem, serta kerusakan kabel *Fiber Optic* yang terhubung ke *Data Centre*, serta hasil rekomendasi kontrol berdasarkan ISO/IEC 27002:2013 terdiri atas 12 kontrol risiko.

6. SARAN

Proses penilaian risiko hanya mencakup aset yang terkait infrastruktur dan keamanan informasi, diharapkan untuk penelitian selanjutnya lebih difokuskan pada komponen sistem informasi yang lainnya.

7. DAFTAR PUSTAKA

Corporation, S. 2012 Assets, Threats and Vulnerabilities: Discovery and Analysis, pp. 1–9.

DPTSI. 2018 *Tentang DPTSI*. Available at: https://www.its.ac.id/dptsi/id/tentang-dptsi/ (Accessed: 23 November 2018).

Basyarahil, F. A., Astuti, H. M., & Hidayanto, B. C. 2017 Evaluasi Manajemen Keamanan Informasi Menggunakan Indekss Keamanan Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya, 6.

International Organization for Standarization ISO 13335. 2004 Information technology. Security techniques. Management of information and communications technology security. Concepts and models for information and communications technology security management, (ISO/IEC 13335-1:2004).

International Organization for Standarization ISO 27001 2013 *ISO/IEC 27001:2013*. Available at: https://www.iso.org/standard/54534.html. (Accessed: 23 November 2018).

International Organization for Standarization ISO 27002. 2013 Information technology - Security techniques - Code of practice for information security controls, *ISO 27002 2013*.

International Organization for Standarization ISO 31000. 2009 Risk management – Principles and guidelines, *ISO 31000*, 31000, p. 24.

Kominfo. 2017 Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks KAMI, 1.0.

Toosarvandani, M. S., Modiri, N., Afzali. M. 2012 The Risk Assessment and Treatment Approach in Order to Provide LAN Security Based on ISMS Standard", International Journal in Foundations of Computer Science & Technology (IJFCST), 2.

Mattord, M. E. W. and H. J. 2016 Principles of Information Security Fifth Edition.

Perdana, A. S. 2018 Penilaian dan Mitigasi Risiko Keamanan Sistem Informasi Berdasarkan Standar ISO/IEC 27001:2013 Menggunakan Metode PMBOK (Studi Kasus : Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS).

Putri, C. U. 2017 Penilaian Risiko Proses Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5 pada Helpdesk Subdirektorat Layanan Teknologi dan Sistem Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember.

Salim, A. 2007 Asuransi dan Manajemen Risiko. Jakarta: Raja Grafindo Persada.

Spremic, M. 2008 *Emerging issues in IT Governance: Implementing the Corporate IT Risk Management Model*, *WSEAS Transaction on Systems*.

UCAPAN TERIMA KASIH

Penelitian ini merupakan penelitian yang di danai oleh Institut Teknologi Sepuluh Nopember dengan skema Penelitian Kebijakan 2019. Terima kasih kepada Lembaga Penelitian dan Pengabdian Masyarakat, Institut Teknologi Sepuluh Nopember atas kesempatan yang diberikan. Semoga penelitian ini membawa kemanfaatan untuk Institut Teknologi Sepuluh Nopember.