Penentuan Strategi Mitigasi Risiko Kritis Aset IS/IT Perkara Berdasarkan ISO/IEC 27002:2013

Determining Critical Risk Mitigation Strategies for IS/IT Assets Case Based on ISO / IEC 27002: 2013

Fania Sofiyani[1], Asih Rohmani[2]
[1,2]Universitas Dian Nuswantoro Prodi Sistem Informasi, FIK UDINUS,
Jalan Imam Bonjol No. 207, 50131, Semarang (024) 3517261
e-mail: [1]112201405168@mhs.dinus.ac.id, [2]aseharsoyo@dsn.dinus.ac.id

Abstrak

Pengadilan Negeri Slawi memiliki beberapa aset TI/SI perkara yang masih memiliki beberapa kelemahan, seperti server yang sering down, kehilangan data dan peretasan website resmi Pengadilan Negeri Slawi. Permasalahan tersebut bisa menjadi celah keamanan yang berpotensi menimbulkan dampak buruk bagi Pengadilan Negeri Slawi, antara lain terganggunya proses bisnis, kehilangan data-data penting, bahkan pencurian data perkara dengan tujuan untuk dijual bebas sebagai konsumsi publik. Perlu dilakukan tindakan pencegahan agar tidak terjadi risiko-risiko tersebut, tidak hanya fokus kepada aset teknologi yang bermasalah saja, tetapi juga pada semua aset teknologi informasi yang digunakan dalam sistem informasi terkait perkara. Tujuan dilakukanya penelitian ini adalah untuk mengidentifikasi semua aset teknologi informasi terhadap penggunaan sistem informasi terkait proses bisnis perkara, menganalisa aset, mengevaluasi risiko, melakukan penilaian terhadap risiko dan mengetahui strategi mitigasi sebagai tindakan untuk merespon risiko kritis. Metode penelitian yang digunakan untuk mengolah hasil wawancara adalah metode OCTAVE, sedangkan metodeyang dipakai untuk penilaian terhadap risiko menggunakan metode Risk FMEA. Dari hasil penilaian dari 75 risikoyang ada, diperoleh 34 risiko kritis yang harus diperhatikan untuk memperoleh tindakan mitigasi berdasarkan standar ISO/IEC 27002:2013. Penentuan risiko kritis tersebut didasarkan pada nilai batas yang telah ditetapkan pada skor risiko dan nilai RPN.

Kata kunci— Mitigasi Risiko, OCTAVE, Risk FMEA, ISO 27002:2013, Aset IS/IT

Abstract

The Slawi District Court has several assets of IT / SI cases that still have some weaknesses, such as servers that are often down, data loss and hacking of the official website of the Slawi District Court. These problems could be a security hole that has the potential to cause adverse effects on the Slawi District Court, including disruption of business processes, loss of important data, and even theft of case data for the purpose of being sold freely as public consumption. Preventive measures need to be taken to avoid these risks, not only focus on problematic technology assets, but also on all information technology assets used in case-related information systems. The purpose of this research is to identify all information technology assets to the use of information systems related to business process cases, analyze assets, evaluate risks, conduct risk assessments and find out mitigation strategies as actions to respond to critical risks. The research method used to process interview results is the OCTAVE method, while the method used for risk assessment uses the Risk FMEA method. From the results of the assessment of 75 risks, 34 critical risks must be considered to obtain mitigation actions based on ISO / IEC 27002: 2013 standards. Determination of the critical risk is based on the limit value set at the risk score and the value of the RPN.

Keywords—*Risk Mitigation, OCTAVE, Risk FMEA, ISO 27002: 2013, IS / IT Assets*

1. PENDAHULUAN

Dengan adanya peningkatan daya kredibilitas proses bisnis dari suatu perusahaan, instansi maupun organisasi yang semakin berkembang pesat di era globalisasi ini, dibutuhkan sebuah faktor pendukung yaitu teknologi informasi [1, 2]. Teknologi informasi yang digunakan untuk menunjang keberhasilan proses bisnis telah diterapkan oleh beberapa sektor seperti sektor pendidikan, pemerintahan, telekomunikasi, keuangan maupun kesehatan. Dalam sektor pemerintahan, instansi memanfaatkan teknologi informasi untuk mendukung tercapainya keberhasilan proses bisnisnya agar dapat memberikan layanan, kemudahan, dan penyedia informasi dengan baik.

Penerapan teknologi informasi pada Kantor Pengadilan Negeri Slawi dapat membantu proses pengelolaan dan pengolahan informasi, baik itu dalam hal melakukan pengelolaan data dan informasi yang berkaitan dengan kinerja dan proses bisnis pada instansi tersebut, sehingga teknologi informasi dan sistem informasi apapun yang dilibatkan dalam proses bisnis Pengadilan Negeri Slawi termasuk dalam aset penting yang dimiliki organisasi, baik pengguna sistem ataupun pegawai, layanan sistem informasi baik pengelolaan perkara maupun sistem informasi lainnya, jaringan, *hardware, software,* data, dan SOP [3, 4].

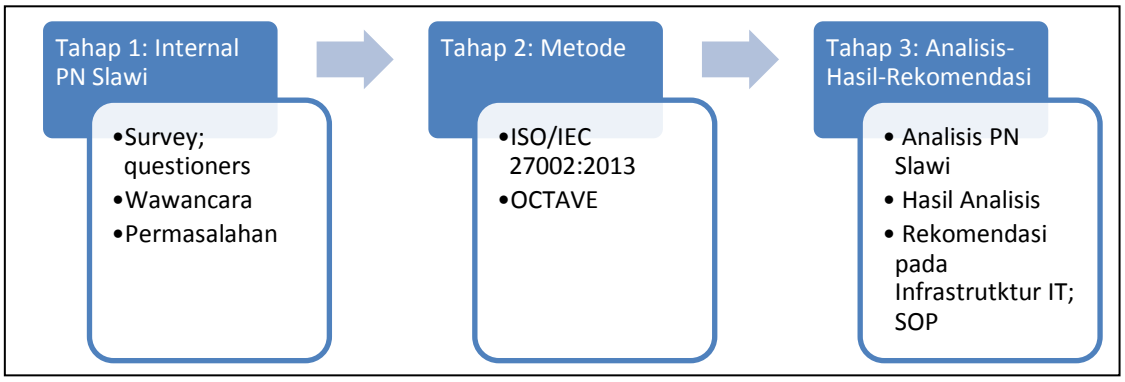
Aset-aset tersebut perlu diproteksi apalagi jika penting dan kritis dalam proses bisnis [5, 6], khususnya terkait pemrosesan perkara. Karena terkait pentingnya dan kritisnya aset tersebut sehingga Pengadilan Negeri Slawi harus memberikan perawatan dan penanganan yang tepat dan sesuai. Akan tetapi dengan segala bentuk kemudahan yang diperoleh atau dihasilkan, tidak dapat dibantah dan diperdebatkan apabila dalam pemanfaatan sekaligus penggunaan teknologi informasi dan sistem informasi memiliki pengaruh beberapa risiko yang kemungkinan besar dapat terjadi. Risiko yang pernah terjadi antara lain *server down*, data hilang, dan peretasan website milik Pengadilan Negeri Slawi. Dengan terjadinya permasalahan dan beberapa kemungkinan permasalahan krusial tersebut diharuskan untuk melakukan analisis dan identifikasi risiko yang mungkin terjadi pada aset teknologi informasi dan sistem informasi yang dimiliki oleh Pengadilan Negeri Slawi agar permasalahan tersebut dapat dicegah atau diantisipasi menggunakan standart yang sesuai seperti standart ISO/IEC 27002:2013, sehingga tidak akan terjadi kembali pada waktu yang akan datang [7, 8].

Dalam melakukan penentuan strategi mitigasi risiko terdapat beberapa metode penilaian atas risiko TI yang terjadi dengan memakai alat atau prosedur *Risk* FMEA dan untuk melakukan analisa dan identifikasi terhadap probabilitas risiko, peneliti juga melibatkan metode kerangka penelitian OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*). Dari permasalahan tersebut, maka terdapat beberapa pertanyaan penting: (1) Bagaimana melakukan analisa dan identifikasi risiko aset kritis teknologi informasi dan sistem informasi (IS/IT) yang kemungkinan akan terjadi di Kantor Pengadilan Negeri Slawi berdasarkan metode OCTAVE?; (2) Bagaimana melakukan penilaian risiko aset-aset kritis teknologi informasi dan sistem informasi (IS/IT) untuk menentukan risiko kritis di Kantor Pengadilan Negeri Slawi berdasarkan metode *Risk* FMEA? [9, 7]; (3) Bagaimana melakukan rencana mitigasi terhadap risiko kritis (penentuan strategi mitigasi pada risiko kritis) yang akan terjadi pada aset-aset kritis Kantor Pengadilan Negeri Slawi berdasarkan standart ISO/IEC 27002:2013?

Pertanyaan-pertanyaan ini akan dijawab pada hasil dan analisis, dimana tujuan penelitian ini menghasilkan tiga hal penting: (1) Mengetahui risiko aset-aset kritis IS/IT yang mungkin terjadi pada Kantor Pengadilan Negeri Slawi; (2) Mengetahui skor risiko dan nilai RPN dengan menggunakan kriteria penilaian *likelihood, impact,* dan *detection* sekaligus untuk mengetahui risiko kritis aset-aset kritis IS/IT pada Kantor Pengadilan Negeri Slawi; (3) Membantu Pengadilan Negeri Slawi dalam melakukan tindakan dan membuat bentuk rencana strategi mitigasi risiko kritis pada aset-aset kritis IS/IT di Kantor Pengadilan Negeri Slawi dan membantu Pengadilan Negeri Slawi dalam mencegah dan menghindari risiko kritis yang mungkin akan terjadi.

Hasil dari penelitian ini akan memberikan rekomendasi kepada PN Slawi, supaya dapat memberikan pelayanan yang lebih baik kepada masyarakat. Hal lainnya adalah PN Slawi akan dapat menekan tingkat resiko keamanan aset IS/IT yang ada, sehingga bisa melaksanakan SOP secara efektif, efesien dan tepat, dan PN Slawi akan dapat memiliki infrastruktur yang tepat dalam meningkatkan pelayanannya.

2. METODE PENELITIAN



Gambar 1. Proses Penelitian Dari Tahap 1-3

Dalam melakukan penelitian ini, metode penelitian yang digunakan menggunakan metode OCTAVE sebagai kerangka penelitian untuk mengolah hasil analisa dari wawancara aset teknologi informasi dan sistem informasi mengenai perkara. OCTAVE merupakan salah satu metode yang dikembangkan oleh *Software Engineering Institute* (SEI) pada tahun 2001. Metode OCTAVE merupakan suatu tools, teknik, dan metode dalam melakukan penilaian dan perencanaan strategi keamanan informasi berdasarkan pengidentifikasian risiko. Metode atau kerangka kerja tersebut digunakan untuk mengelola risiko kemanan informasi yang mana mendefinisikan suatu metode evaluasi secara menyeluruh yang memungkinkan organisasi untuk melakukan identifikasi aset informasi yang penting bagi perusahaan. Metode OCTAVE memiliki beberapa fase, diantaranya [10], [11]: Fase 0-Melakukan Persiapan Penelitian; Fase 1 : Menentukan aset berdasarkan profil ancaman; Fase 2 : Mengidentifikasi kerentanan atau kelemahan infrastruktur; Fase 3: Mengembangkan rencana untuk strategi keamanan.

Metode RISK FMEA sebagai metode penilaian risiko aset kritis teknologi informasi dan sistem informasi terkait perkara. Risk FMEA adalah alat bantu secara sistematis dalam mengidentifikasi dan menilai kegagalan (*mode*), penyebab (*cause*) dan dampak (*effect*) dari kegagalan suatu sistem sebelum terjadi sekaligus sebagai metode/alat bantu/kerangka kerja yang digunakan dalam menganalisis risiko secara kuantitatif. Risk FMEA memiliki beberapa langkah, diantaranya [3]: (1) Identifikasi peristiwa berisiko; (2) Menetapkan nilai kemungkinan (*likelihood*), dampak (*impact*), deteksi (*detection*); (3) Meninjau Pareto RPN dan menetapkan nilai kritis RPN; (4) Meninjau Pareto skor risiko dan menetapkan nilai kritis skor risiko; (5) Meninjau diagram tebar untuk RPN vs skor risiko; (6) Meninjau perpotongan (*intersection*) dari nilai kritis skor risiko dan nilai kritis RPN; (7) Mengembangkan rencana tanggap risiko terhadap risiko-risiko yang kritis (penting); (8) Mengevaluasi kembali skor risiko dan nilai RPN berdasarkan rencana tanggap risiko

3. HASIL DAN PEMBAHASAN

Kebutuhan teknologi informasi (TI) mengalami peningkatan yang semakin tinggi, seperti pemanfaatan teknologi informasi yang digunakan untuk menjalankan aktifitas-aktifitas penting dan banyak memberikan kemudahan pada berbagai aspek kegiatan bisnis. Teknologi informasi merupakan aset penting dalam mengelola dan menghasilkan informasi yang bisa membuat perusahaan memiliki daya saing dan nilai tambah [12]. Demi tercapainya hal tersebut, maka perlu

ditunjang dengan pengelolaan teknologi informasi yang memadai supaya teknologi informasi mampu menyukseskan perusahaan dalam mencapai tujuan bisnisnya [13], [14]. Oleh sebab itu, perlunya inovasi, perbaikan dan perkembangan yang dapat membuat sebuah proses menjadi lebih efektif dan efisien serta dapat menekan tingkat risiko [15]. Pembahasan ini akan dibagi menjadi beberapa bagian penting, antara lain: identifikasi aset kritis; kebutuhan keamanan dan ancaman aset kritis.

3.1. Identifikasi Aset Kritis

Aset Kritis Pengadilan Negeri Slawi merupakan aset kritis yang terdapat dan dimiliki oleh kantor PN Slawi, dimana pemanfaatan dalam pemakaianya memiliki arti penting dalam proses bisnis yang sedang berjalan. Berikut ini adalah daftar aset kritis yang dimiliki PN Slawi :

1. *Hardware : PC, Server, Router, Switch, UPS, Printer, Scanner, CCTV, Fingerprint, Access Point*, Kabel jaringan
2. *Software : Operating System (Windows, Linux*), Sistem Aplikasi (Website PN.Slawi, SIPP, JDIH, Aplikasi surat, SIKEP, SIWAS, KOMDANAS), *Antivirus*(SMADAV, AVAST, KASPERSKY)
3. Jaringan : Jaringan Internet dan Jaringan Komputer
4. Data : *Database* pada semua sistem informasi khususnya data perkara
5. SOP : SOP Bagian PTIP
6. *User/People : Admin* Bagian PTIP, *User*/Pengguna Sistem

3.2. Identifikasi Kebutuhan Keamanan

Identifikasi kebutuhan keamanan tiap aset kritis yang terdapat pada PN Slawi akan digolongkan berdasarkan 3 aspek keamanan informasi, diantaranya:

1. Aspek Kerahasiaan (*Confidentiality*)

   Aset kritis PN. Slawi yang membutuhkan keamanan kerahasian adalah *PC, Server, Router, Switch, UPS, CCTV, Fingerprint, Access point,* Kabel Jaringan, *Operating System (Windows, Linux*), Sistem Aplikasi (Website PN.Slawi, SIPP, JDIH, Aplikasi surat, SIKEP, SIWAS, KOMDANAS), *Antivirus* (SMADAV, AVAST, KASPERSKY), Jaringan internet, Jaringan Komputer, *Database* pada semua sistem informasi khususnya data perkara, *Admin* Bagian PTIP, *User*/Pengguna Sistem.
2. Aspek Integritas (*Integrity*)

   Aset kritis PN. Slawi yang membutuhkan keamanan integritas adalah *PC, Server, Router, Switch, CCTV, Fingerprint, Access point,* Kabel Jaringan, *Operating System (Windows, Linux*), Sistem Aplikasi (Website PN.Slawi, SIPP, JDIH, Aplikasi surat, SIKEP, SIWAS, KOMDANAS), *Antivirus* (SMADAV, AVAST, KASPERSKY), Jaringan internet, Jaringan Komputer, *Database* pada semua sistem informasi khususnya data perkara, SOP Bagian PTIP *Admin* Bagian PTIP, *User*/Pengguna Sistem.
3. Aspek Ketersediaan (*Availability*)

   Aset kritis PN. Slawi yang membutuhkan keamanan ketersediaan adalah*PC, Server, Router, Switch, UPS, Printer, Scanner, CCTV, Fingerprint, Access Point, Operating System (Windows, Linux*), Sistem Aplikasi (Website PN.Slawi, SIPP, JDIH, Aplikasi surat, SIKEP, SIWAS, KOMDANAS), *Antivirus* (SMADAV, AVAST, KASPERSKY), Jaringan internet, Jaringan Komputer, *Database* pada semua sistem informasi khususnya data perkara, SOP Bagian PTIP.

3.3. Identifikasi Ancaman Aset Kritis

Identifikasi selanjutnya adalah identifikasi ancaman pada semua aset kritis yang akan digolongkan sebagai berikut:

1. Pencurian
2. Mati listrik
3. Kerusakan hardware
10. Manipulasi konfigurasi
11. Gagal *booting*
12. *Crash*

4. Penyalahgunaan
5. *Virus atau malware*
6. *Server down*
7. *Server overheat*
8. Kapasitas server penuh
9. Gagal fungsi
13. *Hacking*
14. Kerusakan data
15. Kegagalan *Backup*
16. *Human eror*
17. *Technican eror*

Berdasarkan hasil analisa dan identifikasi di atas, diperoleh 75 risiko yang kemungkinan akan terjadi pada aset kritis IS/IT terkait perkara yang meliputi kelompok aset *hardware*, *software*, jaringan, data, *SOP dan user/people.* Hasil penilaian terhadap masing-masing risiko yang telah diperoleh dari penyebaran kuisioner, akan dilakukan pencarian nilai RPN dan skor risiko [3], dimana :

Nilai RPN = *Likelihood* x *Impact* x *Detection*
Skor Risiko = *Likelihood* x *Impact*

Keterangan :
L (*Likelihood*) : Kemungkinan atau peluang terjadinya suatu risiko
I (*Impact*) : Besar kecilnya pengaruh dalam proses bisnis baik waktu, biaya maupun teknikal
D (*Detection*) : tingkat efektivitas metode atau teknik deteksi dalam kemampuanya mendeteksi terjadinya suatu risiko

Berikut ini adalah diagram pareto perolehan hasil nilai RPN dan skor risiko pada semua risiko :

Gambar 2. Diagram Pareto Skor Risiko

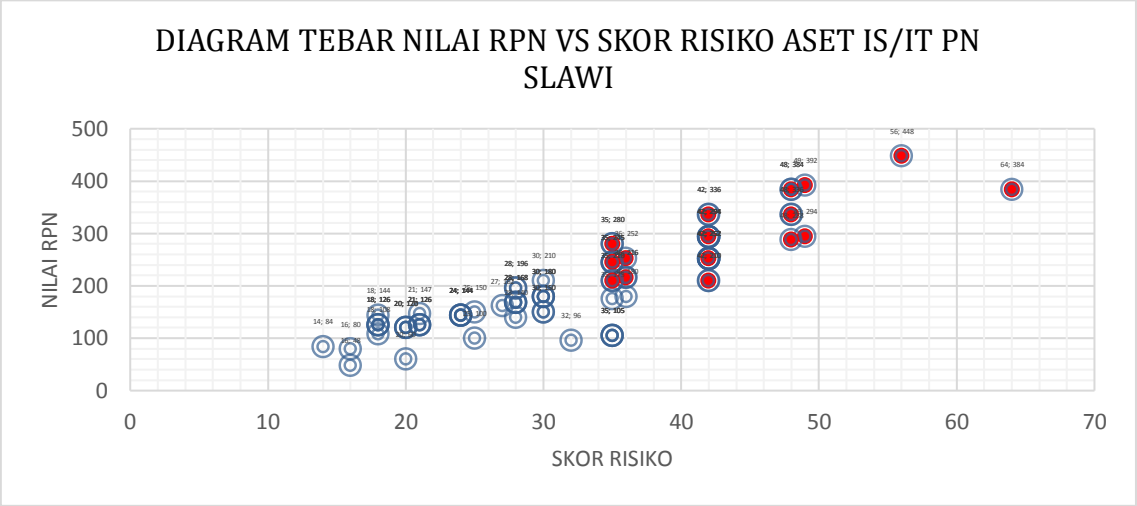
Cara menentukan penetapan nilai kritis RPN adalah total nilai RPN dari semua risiko dibagi dengan total risiko yang diidentifikasikan. Begitu juga cara menentukan penetapan nilai kritis skor risiko adalah total nilai skor risiko dari semua risiko dibagi dengan total risiko yang diidentifikasikan. Hal ini dapat dijabarkan sebagai berikut:

Nilai Kritis RPN = Total Nilai RPN dari semua risiko : total risiko yang diidentifikasi
= 15346 : 75
= 204.666 dibulatkan menjadi **205**

Nilai Kritis Skor risiko = Total Nilai skor risiko dari semua risiko : total risiko yang diidentifikasi
= 2470 : 75
= 32.933 dibulatkan menjadi **33**

Sehingga menghasilkan Penetapan nilai kritis RPN sebesar 205 menunjukan bahwa risiko dikatakan tergolong kritis apabila nilai RPN lebih besar atau sama dengan 205 (nilai kritis RPN). Dan juga sebaliknya, penetapan nilai kritis skor risiko sebesar 33 bahwa risiko dikatakan tergolong kritis apabila nilai skor risiko lebih besar atau sama dengan 33. Sehingga akan diperoleh

diagram *scatter* berdasarkan penetapan nilai kritis RPN dan nilai kritis skor risiko, sebagai berikut :



Gambar 3. Diagram Tebar Perpotongan Nilai RPN VS Skor Risiko

Berdasarkan diagram tebar diatas diperoleh 34 risiko kritis pada aset kritis IS/IT terkait perkara yang memiliki ID RISK US1, US3, US6, HW33, US2, HW34, HW35, HW12, HW32, SW1, HW11, HW36, HW37, HW39, US4, US10, HW10, HW30, SW2, SW3, SW15, JR4, JR5, DB1, DB5, HW31, HW38, SW14, SW4, DB4, JR1, JR3, SW16, DB2. Berikut ini adalah penentuan strategi mitigasi risiko berdasarkan ISO 27002:2013 terhadap risiko kritis:

Tabel 1. Control pada Aset sesuai ISO/IEC 27002:2013

Kelompok Aset	Risiko kritis pada asset	Rekomendasi *control* yang harus diterapkan pada aset berdasarkan ISO/IEC 27002 2013
Hardware	*PC*	A.5.1.1, A.7.2.2, A.7.2.3, A.8.3.1, A.9.4.3, A.11.1.4, A.11.2.1, A.16.1.2, A.17.1.1, dan A.18.2.2
	Perangkat (*Router, UPS, Printer, Scanner, CCTV, Fingerprint, Access Point*)	A.6.1.2, A.7.2.1, A.7.2.3, A.8.1.3, A.8.2.3, A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.17.1.1 dan A.18.2.2
	Kabel Jaringan	A.11.1.3, A.11.1.4, A.11.2.1, A.11.2.3, A.11.2.4, A.13.1.1 dan A.17.1.1
Software	*Operating System*	A.7.2.1, A.8.1.3, A.8.2.3, A.9.4.4, A.12.2.1, A.12.5.1, A.12.6.2, dan A.16.1.2
	Sistem Aplikasi	A.7.2.3, A.9.4.1, A.9.4.2, A.16.1.2, A.16.1.3
	Antivirus	A.12.5.1, A.12.6.2, dan A.14.1.1
Jaringan	Jaringan Internet	A.5.1.1, A.7.2.2 , A.9.3.1, A.9.4.3, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.13.1.1, A.13.1.2, A.13.1.3, dan A.17.1.1
Data	Database Sistem Informasi	A.7.2.2 , A.7.2.3, A.9.2.2, A.9.2.3, A.9.4.1, A.9.4.2, A.9.4.3, A.12.1.2, A.12.3.1, A.16.1.3 dan A.17.1.2
User/People	*Admin* Bagian PTIP	A.6.1.1, A.7.1.1, A.7.2.2, A.7.2.3, A.16.1.2, A.16.1.6, A.18.2.2 dan A.18.2.3
	User/Pengguna Sistem	A.5.1.1, A.7.2.2, A.7.2.3, A.9.3.1, A.9.4.3,A.13.1.1, A.13.1.2, A.13.1.3, A.14.2.9

Berikut adalah klausul yang akan digunakan beserta kesimpulan *control* yang harus diterapkan pada aset berdasarkan klausul ISO 27002:2013, diantaranya:

Tabel 2. Penggunaan Klausul pada ISO 27002:2013

Klausul	Control
Klausul 5	A.5.1.1
Klausul 6	A.6.1.1; A.6.1.2
Klausul 7	A.7.1.1; A.7.2.1; A.7.2.2; A.7.2.3
Klausul 8	A.8.1.3; A.8.2.3; A.8.3.1
Klausul 9	A.9.2.2; A.9.3.1; A.9.4.1; A.9.4.2; A.9.4.3; A.9.4.4
Klausul 11	A.11.1.1; A.11.1.2; A.11.1.3; A.11.1.4; A.11.2.1; A.11.2.2; A.11.2.3; A.11.2.4
Klausul 12	A.12.1.2; A.12.2.1; A.12.3.1; A.12.4.1; A.12.5.1; A.12.6.2
Klausul 13	A.13.1.1; A.13.1.2; A.13.1.3
Klausul 14	A.14.1.1; A.14.2.9
Klausul 16	A.16.1.2; A.16.1.3; A.16.1.6
Klausul 17	A.17.1.1; A.17.1.2
Klausul 18	A.18.2.2; A.18.2.3

Dari tabel 1 dan 2, dapat menghasilkan strategi mitigasi yang dapat dijelaskan sebagai berikut:

Tabel 3. Strategi Mitigasi Risiko Aset IS/IT PN Slawi Berdasarkan Klausul ISO 27002:2013

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
1	US1	*User* : Admin Bagian PTIP	Bagian PTIP tidak dapat merespon masalah mengenai aset kritis IS/IT	• Masalah atau risiko tersebut terlalu rumit • Kurangnya pengetahuan mengenai masalah atau risiko tersebut	**A.7.2.2 Kesadaran terhadap pengetahuan, dan pelatihan dalam melakukan keamanan informasi** **Kontrol** Semua karyawan pada PN Slawi harus mengikuti atau menerima pendidikan dan pelatihan untuk meningkatkan kesadaran dalam kepedulian melakukan keamanan informasi sekaligus sebagai kegiatan berlanjut yang mana relevan dengan fungsi dan pekerjaan mereka. **A.16.1.2 Melaporkan kejadian keamanan informasi** **Kontrol** Peristiwa keamanan informasi harus dilaporkan melalui jalur manajemen yang tepat secepat mungkin. **A.16.1.6 Belajar dari insiden keamanan informasi** **Kontrol** Pengetahuan yang diperoleh dari menganalisis dan menyelesaikan kejadian atau risiko keamanan informasi yang telah terjadi harus digunakan untuk mengurangi kemungkinan atau dampak insiden di masa yang akan datang.
2	US3	*User* : Admin Bagian PTIP	Bagian PTIP merespon risiko atau masalah yang terjadi dengan lambat	• Kurangnya SDM pada bagian PTIP	**A.7.1.1 *Screening*** **Kontrol** Seluruh kandidat sebelum melakukan pekerjaan harus dicek verifikasinya berupa CV, apakah relevan dan sesuai dengan hukum yang ada, peraturan, serta etika, dan apakah ini memenuhi dari syarat kalasifikasi yang sudah ditetapkan. Hal ini dilakukan untuk mengurangi tingkat risiko.
3	US6	*User* : *User*/Pengguna Sistem	*PC* yang digunakan *User* tidak memiliki *password*/ tidak menerapkan proteksi *password*	• Tidak mengetahui pentingnya menerapkan *password* pada PC	**A.5.1.1 Kebijakan keamanan informasi** **Kontrol** Kumpulan kebijakan untuk keamanan informasi didefinisikan /diidentifikasi, disetujui oleh manajemen organisasi, dipublikasi dan dikomunikasikan kepada karyawan dan pihak eksternal terkait. **A.7.2.2 Kesadaran terhadap pengetahuan, dan pelatihan dalam melakukan keamanan informasi** **Kontrol** Semua karyawan pada PN. Slawi harus mengikuti atau menerima pendidikan dan pelatihan untuk meningkatkan kesadaran dalam kepedulian melakukan keamanan informasi sekaligus sebagai kegiatan berlanjut yang mana relevan dengan fungsi dan pekerjaan mereka. **A.9.3.1 Penggunaan informasi otentikasi rahasia (*password*)** **Kontrol**

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
					Pengguna diharuskan mengikuti praktik organisasi dalam penggunaan informasi otentikasi rahasia (penggunaan *password).* **A.9.4.3 Manajemen *password*** **Kontrol** Pengelolaan *password* terhadap sistem harus interaktif dan harus memastikan kualitas *password*
4	HW33	*Hardware* : *Router, UPS, Printer, Scanner, CCTV, Fingerprint , Access Point*	Perangkat gagal fungsi	• Kesalahan konfigurasi dan kabel rusak	**A.8.1.3 Prosedur penggunaan aset** **Kontrol** Prosedur dalam penggunaan aset informasi yang berhubungan dengan informasi serta fasilitas pengolah informasi harus diidentitifikasi, didokumentasikan dan diimplementasikan **A.8.2.3 Penanganan aset** **Kontrol** Prosedur penanganan aset harus dikembangkan dan dilaksanakan sesuai dengan skema klasifikasi informasi yang ditetapkan oleh organisasi. **A.11.2.3 Keamanan kabel** **Kontrol** Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, gangguan atau kerusakan. **A.11.2.4 Pemeliharaan peralatan** **Kontrol** Peralatan harus dipelihara dengan benar untuk memastikan selalu siap guna dan tidak mengalami kegagalan fungsi
5	US2	*User* : Admin Bagian PTIP	Bagian PTIP tidak menerapkan SOP yang ada dibagian PTIP	• Melakukan *maintenance* seminggu sekali sudah cukup dan melakukan *maintenance* pada saat risiko/ masalah terjadi sudah cukup	**A.6.1.1 Peran dan tanggung jawab keamanan informasi** **Kontrol** Semua tanggung jawab dalam melakukan keamanan informasi harus didefinisikan dan dialokasikan **A.7.2.1 Pengelolaan tanggung jawab atau kewajiban** **Kontrol** Pengelolaan tanggung jawab semua karyawan dalam menerapkan keamanan informasi agar sesuai dengan syarat ketentuan dan prosedur yang ditetapkan organisasi **A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.18.2.2 Kepatuhan terhadap kebijakan dan standar keamanan** **Kontrol** Manajer harus secara teratur meninjau kepatuhan pemrosesan dan prosedur informasi di dalam area tanggung jawab mereka dengan kebijakan keamanan, standar dan persyaratan keamanan lainnya yang sesuai. **A.18.2.3 Tinjauan kepatuhan teknis** **Kontrol** Sistem informasi harus ditinjau secara berkala untuk mematuhi kebijakan dan standar keamanan informasi organisasi
6	HW34	*Hardware* : *Router, UPS, Printer, Scanner,CCTV, Fingerprint , Access Point*	Perangkat rusak	• Bencana alam (petir/kilat, hujan lebat, banjir, gempa bumi, dan kebakaran)	**A.11.1.4 Melindungi terhadap ancaman dari luar dan lingkungan sekitar** **Kontrol** Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan berbahaya harus dirancang dan diterapkan. **A.11.2.1 Penempatan dan perlindungan peralatan** **Kontrol** Peralatan harus ditempatkan pada tempat yang aman dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan kesempatan untuk akses yang tidak sah. **A.17.1.1 Merencanakan keamanan informasi yang berkelanjutan** **Kontrol** Organisasi harus menentukan persyaratannya untuk keamanan informasi dan keberlanjutan pengelolaan

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
					keamanan informasi dalam situasi yang merugikan, mis. Setelah bencana.
7	HW35	*Hardware* : *Router, UPS, Printer, Scanner, CCTV,Fingerprint, Access Point*	Manipulasi konfigurasi perangkat	• Di *hack* oleh pihak yang tidak bertanggung jawab, dimana *hacker* bersifat merusak	**A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.11.1.1 Perimeter (pembatasan area) keamanan fisik** **Kontrol** Perimeter keamanan harus didefinisikan dan digunakan untuk melindungi area yang mengandung fasilitas informasi dan pengolahan informasi sensitif atau penting. **A.11.1.2 Kontrol masuk fisik** **Kontrol** Area yang aman harus dilindungi oleh kontrol masuk fisik yang sesuai pastikan hanya personil yang berwenang yang diizinkan mengaksesnya. **A.11.1.3 Keamanan kantor, ruangan dan fasilitas** **Kontrol** Keamanan fisik untuk perkantoran, ruangan dan fasilitas harus dirancang dan diterapkan.
8	HW12	*Hardware:* PC	*PC* rusak	• Bencana alam (petir/kilat, hujan lebat, banjir, gempa bumi, dan kebakaran)	**A.11.1.4 Melindungi terhadap ancaman dari luar dan lingkungan sekitar** **Kontrol** Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan berbahaya harus dirancang dan diterapkan. **A.11.2.1 Penempatan dan perlindungan peralatan** **Kontrol** Peralatan harus ditempatkan pada tempat yang aman dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan kesempatan untuk akses yang tidak sah. **A.17.1.1 Merencanakan keamanan informasi yang berkelanjutan** **Kontrol** Organisasi harus menentukan persyaratannya untuk keamanan informasi dan keberlanjutan pengelolaan keamanan informasi dalam situasi yang merugikan, mis. setelah bencana.
9	HW32	*Hardware* : *Router, Printer, Scanner, CCTV,Fingerprint, Access Point*	Perangkat gagal fungsi	• Listrik padam secara tiba-tiba	**A.11.2.2 *Supporting utilities* (peralatan pendukung)** **Kontrol** Peralatan harus dilindungi dari gangguan listrik dan gangguan lainnya yang menyebabkan kegagalan dalam utilitas pendukung.
10	SW1	*Software* : *Operating System*	OS terkena *virus/malware*	• Penyimpanan eksternal	**A.12.2.1 Mengontrol malware** **Kontrol** Kontrol deteksi, pencegahan dan pemulihan untuk melindungi terhadap malware harus dilaksanakan, dikombinasikan dengan kesadaran pengguna. **A.12.5.1 Pemasangan perangkat lunak pada sistem operasional** **Kontrol** Prosedur harus diimplementasikan dengan jelas untuk mengendalikan pemasangan perangkat lunak pada sistem operasional.
11	HW11	*Hardware* : *PC*	Pencurian hak akses *PC*	• *Social engineering* (meminta akses langsung kepada pemilik *PC*)	**A.5.1.1 Kebijakan keamanan informasi** **Kontrol** Kumpulan kebijakan untuk keamanan informasi didefinisikan/ diidentifikasi, disetujui oleh manajemen organisasi, dipublikasi dan dikomunikasikan kepada karyawan dan pihak eksternal terkait. **A.7.2.2 Kesadaran terhadap pengetahuan, dan pelatihan dalam melakukan keamanan informasi**

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
					Kontrol Semua karyawan pada PN.Slawi harus mengikuti atau menerima pendidikan dan pelatihan untuk meningkatkan kesadaran dalam kepedulian melakukan keamanan informasi sekaligus sebagai kegiatan berlanjut yang mana relevan dengan fungsi dan pekerjaan mereka. **A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.18.2.2 Kepatuhan terhadap kebijakan dan standar keamanan** **Kontrol** Manajer harus secara teratur meninjau kepatuhan pemrosesan dan prosedur informasi di dalam area tanggung jawab mereka dengan kebijakan keamanan, standar dan persyaratan keamanan lainnya yang sesuai.
12	HW36	*Hardware* : Kabel Jaringan	Kabel jaringan rusak	• Tergigit oleh binatang	**A.11.2.1 Penempatan dan perlindungan peralatan** **Kontrol** Peralatan harus ditempatkan pada tempat yang aman dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan kesempatan untuk akses yang tidak sah. **A.11.2.3 Keamanan kabel** **Kontrol** Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, gangguan atau kerusakan. **A.11.2.4 Pemeliharaan peralatan** **Kontrol** Peralatan harus dipelihara dengan benar untuk memastikan selalu siap guna dan tidak mengalami kegagalan fungsi
13	HW37	*Hardware* : Kabel Jaringan	Kabel jaringan rusak	• Penempatan tidak sesuai dan tidak dilapisis oleh pelindung	**A.11.2.1 Penempatan dan perlindungan peralatan** **Kontrol** Peralatan harus ditempatkan pada tempat yang aman dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan kesempatan untuk akses yang tidak sah. **A.11.2.3 Keamanan kabel** **Kontrol** Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, gangguan atau kerusakan. **A.11.2.4 Pemeliharaan peralatan** **Kontrol** Peralatan harus dipelihara dengan benar untuk memastikan selalu siap guna dan tidak mengalami kegagalan fungsi.
14	HW39	*Hardware* : Kabel Jaringan	Kabel jaringan rusak	• Sengaja diputus oleh pihak yang tidak bertanggung jawab	**A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.11.1.3 Keamanan kantor, ruangan dan fasilitas** **Kontrol** Keamanan fisik untuk perkantoran, ruangan dan fasilitas harus dirancang dan diterapkan. **A.11.2.1 Penempatan dan perlindungan peralatan** **Kontrol** Peralatan harus ditempatkan pada tempat yang aman dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan kesempatan untuk akses yang tidak sah. **A.11.2.3 Keamanan kabel** **Kontrol** Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, gangguan atau kerusakan. **A.11.2.4 Pemeliharaan peralatan** **Kontrol**

NO	ID Risk	Aset Kritis	Risk Event	Cause	Strategi Mitigasi (ISO/IEC 27002:2013)
					Peralatan harus dipelihara dengan benar untuk memastikan selalu siap guna dan tidak mengalami kegagalan fungsi.
15	US4	*User* : *User*/Pengguna Sistem	Pengguna Sistem (*User*) tidak mampu mengatasi masalah yang terjadi pada sistem	• Sistem tidak *User friendly*/ sistem tidak memberi kemudahan kepada pengguna untuk mencapai tujuan tertentu	**A.7.2.2 Kesadaran terhadap pengetahuan, dan pelatihan dalam melakukan keamanan informasi** **Kontrol** Semua karyawan pada PN.Slawi harus mengikuti atau menerima pendidikan dan pelatihan untuk meningkatkan kesadaran dalam kepedulian melakukan keamanan informasi sekaligus sebagai kegiatan berlanjut yang mana relevan dengan fungsi dan pekerjaan mereka. **A.14.2.9 Pengujian penerimaan sistem** **Kontrol** Program pengujian penerimaan dan kriteria terkait harus ditetapkan untuk sistem informasi baru (*upgrade* dan versi baru)
16	US10	*User* : *User*/Pengguna Sistem	*User* melakukan kesalahan dalam penginputan dan penghapusan data	• Ketidaksengajaan *User* terhadap koneksi jaringan yang lambat	**A.7.2.1 Pengelolaan Tanggung jawab atau kewajiban** **Kontrol** Pengelolaan tanggungjawab semua karyawan dalam menerapkan keamanan informasi agar sesuai dengan syarat ketentuan dan prosedur yang ditetapkan organisasi **A.7.2.2 Kesadaran terhadap pengetahuan, dan pelatihan dalam melakukan keamanan informasi** **Kontrol** Semua karyawan pada PN.Slawi harus mengikuti atau menerima pendidikan dan pelatihan untuk meningkatkan kesadaran dalam kepedulian melakukan keamanan informasi sekaligus sebagai kegiatan berlanjut yang mana relevan dengan fungsi dan pekerjaan mereka. **A.13.1.1 Kontrol jaringan** **Kontrol** Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi. **A.13.1.2 Keamanan Layanan jaringan** **Kontrol** Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan termasuk di dalamnya perjanjian layanan jaringan, apakah layanan ini disediakan *in-house* atau *outsource*. **A.13.1.3 Pemisahan jaringan (segregasi jaringan)** **Kontrol** Kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan pada jaringan.
17	HW10	*Hardware* : *PC*	Pencurian hak akses *PC*	• *Password* tidak bervariasi, *password* tidak pernah diganti, dan password terlalu pendek	**A.9.4.3 Manajemen *password*** **Kontrol** Pengelolaan *password* terhadap sistem harus interaktif dan harus memastikan kualitas *password* **A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi.
18	HW30	*Hardware* : *Router, UPS, Printer, Scanner,CCTV, Fingerprint , Access Point*	Perangkat rusak	• Konfigurasi tidak sesuai, penggunaan tidak sesuai dengan prosedur dan kesengajaan dirusak oleh pihak yang tidak bertanggungjawab	**A.7.2.1 Pengelolaan tanggung jawab atau kewajiban** **Kontrol** Pengelolaan tanggungjawab semua karyawan dalam menerapkan keamanan informasi agar sesuai dengan syarat ketentuan dan prosedur yang ditetapkan organisasi **A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.8.1.3 Prosedur penggunaan aset** **Kontrol**

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
					Prosedur dalam penggunaan aset informasi yang berhubungan dengan informasi serta fasilitas pengolah informasi harus diidentitifikasi, didokumentasikan dan diimplementasikan **A.8.2.3 Penanganan aset** **Kontrol** Prosedur penanganan aset harus dikembangkan dan dilaksanakan sesuai dengan skema klasifikasi informasi yang ditetapkan oleh organisasi. **A.11.1.3 Keamanan kantor, ruangan dan fasilitas** **Kontrol** Keamanan fisik untuk perkantoran, ruangan dan fasilitas harus dirancang dan diterapkan. **A.11.2.4 Pemeliharaan peralatan** **Kontrol** Peralatan harus dipelihara dengan benar untuk memastikan selalu siap guna dan tidak mengalami kegagalan fungsi.
19	SW2	*Software* : *Operating System*	OS terkena *virus/malware*	• Antivirus gagal fungsi (tidak pernah di *update*)	**A.12.2.1 Mengontrol malware** **Kontrol** Kontrol deteksi, pencegahan dan pemulihan untuk melindungi terhadap malware harus dilaksanakan, dikombinasikan dengan kesadaran pengguna. **A.12.5.1 Pemasangan perangkat lunak pada sistem operasional** **Kontrol** Prosedur harus diimplementasikan dengan jelas untuk mengendalikan pemasangan perangkat lunak pada sistem operasional. **A.16.1.2 Melaporkan kejadian keamanan informasi** **Kontrol** Peristiwa keamanan informasi harus dilaporkan melalui jalur manajemen yang tepat secepat mungkin.
20	SW3	*Software* : *Operating System*	OS terkena *virus/malware*	• Kurangnya *control* dan *maintenance*	**A.7.2.1 Pengelolaan tanggung jawab atau kewajiban** **Kontrol** Pengelolaan tanggungjawab semua karyawan dalam menerapkan keamanan informasi agar sesuai dengan syarat ketentuan dan prosedur yang ditetapkan organisasi **A.12.2.1 Mengontrol malware** **Kontrol** Kontrol deteksi, pencegahan dan pemulihan untuk melindungi terhadap malware harus dilaksanakan, dikombinasikan dengan kesadaran pengguna. **A.12.5.1 Pemasangan perangkat lunak pada sistem operasional** **Kontrol** Prosedur harus diimplementasikan dengan jelas untuk mengendalikan pemasangan perangkat lunak pada sistem operasional. **A.16.1.2 Melaporkan kejadian keamanan informasi** **Kontrol** Peristiwa keamanan informasi harus dilaporkan melalui jalur manajemen yang tepat secepat mungkin.
21	SW15	*Software* : Antivirus	Antivirus gagal fungsi	• Versi gratis dan tidak sesuai dengan kebutuhan	**A.12.5.1 Pemasangan perangkat lunak pada sistem operasional** **Kontrol** Prosedur harus diimplementasikan dengan jelas untuk mengendalikan pemasangan perangkat lunak pada sistem operasional. **A.12.6.2 Pembatasan instalasi perangkat lunak** **Kontrol** Aturan yang mengatur pemasangan perangkat lunak oleh pengguna harus dibuat dan diimplementasikan **A.14.1.1 Analisis dan persyaratan spesifikasi keamanan informasi** **Kontrol** Persyaratan terkait keamanan informasi harus disertakan dalam persyaratan untuk pembangunan sistem informasi atau penyempurnaan sistem informasi dan sistem operasi yang ada.

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
22	JR4	Jaringan : Jaringan Internet	Jaringan internet bermasalah	• Kesalahan dalam konfigurasi *access point*	**A.13.1.1 Kontrol jaringan** **Kontrol** Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi. **A.13.1.2 Keamanan layanan jaringan** **Kontrol** Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan termasuk di dalamnya perjanjian layanan jaringan, apakah layanan ini disediakan *in-house* atau *outsource*.
23	JR5	Jaringan : Jaringan Internet Jaringan Komputer	Jaringan terputus	• Kabel jaringan rusak dan listrik padam	**A.11.2.1 Penempatan dan perlindungan peralatan** **Kontrol** Peralatan harus ditempatkan pada tempat yang aman dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan kesempatan untuk akses yang tidak sah. **A.11.2.2 *Supporting utilities*** **Kontrol** Peralatan harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan dalam utilitas pendukung. **A.11.2.3 Keamanan kabel** **Kontrol** Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, gangguan atau kerusakan. **A.11.2.4 Pemeliharaan peralatan** **Kontrol** Peralatan harus dipelihara dengan benar untuk memastikan selalu siap guna dan tidak mengalami kegagalan fungsi **A.13.1.1 Kontrol jaringan** **Kontrol** Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi.
24	DB1	Data : Database Sistem Informasi	Pencurian data (*interception*)	• Kurangnya proteksi keamanan sistem	**A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.9.2.2 Penyediaan akses pengguna** **Kontrol** Proses penyediaan akses pengguna resmi harus diterapkan untuk menetapkan atau mencabut hak akses untuk semua jenis pengguna ke semua sistem dan layanan. **A.9.2.3 Pengelolaan hak akses istimewa** **Kontrol** Alokasi dan penggunaan hak akses istimewa harus dibatasi dan dikontrol. **A.9.4.1 Pembatasan akses informasi** **Kontrol** Akses terhadap informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan pengendalian akses. **A.9.4.2 Prosedur keamanan *log-on*** **Kontrol** Bila diperlukan oleh kebijakan kontrol akses, akses terhadap sistem dan aplikasi harus dikendalikan oleh prosedur *log-on* yang aman prosedur *login* demi memperoleh keamanan **A.16.1.3 Melaporkan kelemahan keamanan informasi** **Kontrol** Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus mencatat dan melaporkan setiap kelemahan keamanan informasi yang teramati atau dicurigai dalam sistem atau layanan. **A.17.1.2 Melaksanakan keamanan informasi yang berkelanjutan** **Kontrol** Organisasi harus menetapkan, mendokumentasikan, melaksanakan dan memelihara proses, prosedur dan

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
					pengendalian untuk memastikan tingkat kelanjutan keamanan informasi yang diperlukan selama situasi yang merugikan
25	DB5	Data : Database Sistem Informasi	Kegagalan *back up* data	• *Server down*	**A.12.3.1 Melakukan *backup* informasi** **Kontrol** *backup* salinan informasi, perangkat lunak dan sistem aplikasi harus diambil dan dilakukan secara teratur sesuai dengan kebijakan cadangan yang disepakati.
26	HW31	*Hardware* : *Router, UPS, Printer, Scanner, CCTV, Fingerprint, Access Point*	Penyalahgunaan Perangkat	• Digunakan selain urusan proses bisnis PN. Slawi	**A.6.1.2 Pemisahan tugas** **Kontrol** Tugas yang bertentangan dengan bidang kerja dan tanggung jawab harus dipisahkan untuk mengurangi peluang untuk modifikasi yang tidak sah atau ketidaksengajaan dalam menyalahgunaan aset organisasi **A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.18.2.2Kepatuhan terhadap kebijakan dan standar keamanan** **Kontrol** Manajer harus secara teratur meninjau kepatuhan pemrosesan dan prosedur informasi di dalam area tanggung jawab mereka dengan kebijakan keamanan, standar dan persyaratan keamanan lainnya yang sesuai.
27	HW38	*Hardware* : Kabel Jaringan	Kabel jaringan rusak	• Bencana alam (petir/kilat, hujan lebat, banjir, gempa bumi, dan kebakaran)	**A.11.1.4 Melindungi terhadap ancaman dari luar dan lingkungan sekitar** **Kontrol** Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan berbahaya harus dirancang dan diterapkan. **A.11.2.1 Penempatan dan perlindungan peralatan** **Kontrol** Peralatan harus ditempatkan pada tempat yang aman dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan kesempatan untuk akses yang tidak sah. **A.11.2.3 Keamanan kabel** **Kontrol** Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, gangguan atau kerusakan. **A.11.2.4 Pemeliharaan peralatan** **Kontrol** Peralatan harus dipelihara dengan benar untuk memastikan selalu siap guna dan tidak mengalami kegagalan fungsi **A.13.1.1 Kontrol jaringan** **Kontrol** Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi. **A.17.1.1 Merencanakan keamanan informasi yang berkelanjutan** **Kontrol** Organisasi harus menentukan persyaratannya untuk keamanan informasi dan keberlanjutan pengelolaan keamanan informasi dalam situasi yang merugikan, mis. Setelah bencana.
28	SW14	*Software* : Sistem Aplikasi	Sistem aplikasi di *hack*	• Kurangnya *security* terhadap sistem	**A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.9.4.1 Pembatasan akses informasi** **Kontrol** Akses terhadap informasi dan sistem aplikasi harus dibatasi sesuai dengan kebijakan pengendalian akses. **A.9.4.2 Prosedur keamanan *log-on*** **Kontrol**

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
					Bila diperlukan oleh kebijakan kontrol akses, akses terhadap sistem dan aplikasi harus dikendalikan oleh prosedur log-on yang aman/ prosedur *login* demi memperoleh keamanan terhadap sistem dan aplikasi **A.16.1.2 Melaporkan kejadian keamanan informasi** **Kontrol** Peristiwa keamanan informasi harus dilaporkan melalui jalur manajemen yang tepat secepat mungkin. **A.16.1.3 Melaporkan kelemahan keamanan informasi** **Kontrol** Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus mencatat dan melaporkan setiap kelemahan keamanan informasi yang teramati atau dicurigai dalam sistem atau layanan.
29	SW4	*Software* : *Operating System*	OS gagal booting	• Kesalahan konfigurasi dan instalasi tidak sesuai kebutuhan	**A.8.1.3 Prosedur penggunaan aset** **Kontrol** Prosedur dalam penggunaan aset informasi yang berhubungan dengan informasi serta fasilitas pengolah informasi harus diidentitifikasi, didokumentasikan dan diimplementasikan **A.8.2.3 Penanganan aset** **Kontrol** Prosedur penanganan aset harus dikembangkan dan dilaksanakan sesuai dengan skema klasifikasi informasi yang ditetapkan oleh organisasi. **A.12.5.1 Pemasangan perangkat lunak pada sistem operasional** **Kontrol** Prosedur harus diimplementasikan dengan jelas untuk mengendalikan pemasangan perangkat lunak pada sistem operasional. **A.12.6.2 Pembatasan instalasi perangkat lunak** **Kontrol** Aturan yang mengatur pemasangan perangkat lunak oleh pengguna harus dibuat dan diimplementasikan **A.9.4.4 Penggunaan program *utility*(program bawaan windows atau pemasangan program baru)** **Kontrol** Penggunaan program utilitas yang mungkin mampu mengesampingkan atau mempengaruhi sistem dan aplikasi harus dibatasi dan dikontrol dengan teliti.
30	DB4	Data : Database Sistem Informasi	Data tidak singkron	• Mahkamah Agung sedang melakukan maintenance terhadap server	**A.12.1.2 Pengelolaan Perubahan** **Kontrol** Perubahan pada organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi harus dikendalikan. **A.12.3.1 Melakukan *backup* informasi** **Kontrol** *backup* salinan informasi, perangkat lunak dan sistem aplikasi harus diambil dan dilakukan secara teratur sesuai dengan kebijakan cadangan yang disepakati.
31	JR1	Jaringan : Jaringan Internet Jaringan Komputer	Jaringan di hack (serangan : brute force and dictionary, DOS, IP Spoofing, Paket Sniffing)	• Kurangnya keamanan jaringan (password terlalu pendek dan kurang kuat)	**A.5.1.1 Kebijakan keamanan informasi** **Kontrol** Kumpulan kebijakan untuk keamanan informasi didefinisikan /diidentifikasi, disetujui oleh manajemen organisasi, dipublikasi dan dikomunikasikan kepada karyawan dan pihak eksternal terkait. **A.7.2.2 Kesadaran terhadap pengetahuan, dan pelatihan dalam melakukan keamanan informasi** **Kontrol** Semua karyawan pada PN. Slawi harus mengikuti atau menerima pendidikan dan pelatihan untuk meningkatkan kesadaran dalam kepedulian melakukan keamanan informasi sekaligus sebagai kegiatan berlanjut yang mana relevan dengan fungsi dan pekerjaan mereka. **A.9.3.1 Penggunaan informasi otentikasi rahasia (*password*)** **Kontrol**

NO	*ID Risk*	Aset Kritis	*Risk Event*	*Cause*	Strategi Mitigasi (ISO/IEC 27002:2013)
					Pengguna diharuskan mengikuti praktik organisasi dalam penggunaan informasi otentikasi rahasia (penggunaan *password).* **A.9.4.3 Manajemen *password*** **Kontrol** Pengelolaan *password* terhadap sistem harus interaktif dan harus memastikan kualitas *password* **A.13.1.1 Kontrol jaringan** **Kontrol** Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi. **A.17.1.1 Merencanakan keamanan informasi yang berkelanjutan** **Kontrol** Organisasi harus menentukan persyaratannya untuk keamanan informasi dan keberlanjutan pengelolaan keamanan informasi dalam situasi yang merugikan, mis. Setelah bencana.
32	JR3	Jaringan : Jaringan Internet	Jaringan internet down	• Bawaan dari perusahaan (speed koneksi internet lemah dan tidak stabil)	**A.13.1.2 Keamanan Layanan jaringan** **Kontrol** Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan termasuk di dalamnya perjanjian layanan jaringan, apakah layanan ini disediakan *in-house* atau *outsource*. **A.13.1.3 Pemisahan jaringan (segregasi jaringan)** **Kontrol** Kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan pada jaringan.
33	SW16	*Software : Antivirus*	Antivirus gagal fungsi	• Kurangnya control dan maintenance (jarang diupdate) sehingga fitur yang terbatas dan tidak mampu mendeteksi virus-virus baru	**A.12.5.1 Pemasangan perangkat lunak pada sistem operasional** **Kontrol** Prosedur harus diimplementasikan dengan jelas untuk mengendalikan pemasangan perangkat lunak pada sistem operasional. **A.12.6.2 Pembatasan instalasi perangkat lunak** **Kontrol** Aturan yang mengatur pemasangan perangkat lunak oleh pengguna harus dibuat dan diimplementasikan
34	DB2	Data : Database Sistem Informasi	Penyalahgunaan wewenang terhadap data (modification dan fabrication)	• Password sangat lemah dan password disimpan pada desktop komputer dan bahkan meminta data dan password secara langsung kepada pemilik (social engineering)	**A.7.2.2 Kesadaran terhadap pengetahuan, dan pelatihan dalam melakukan keamanan informasi** **Kontrol** Semua karyawan pada PN. Slawi harus mengikuti atau menerima pendidikan dan pelatihan untuk meningkatkan kesadaran dalam kepedulian melakukan keamanan informasi sekaligus sebagai kegiatan berlanjut yang mana relevan dengan fungsi dan pekerjaan mereka. **A.7.2.3 Proses disiplin dalam bekerja** **Kontrol** Diadakan penyampaian proses pendisiplinan formal dalam mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran dalam keamanan informasi **A.9.4.3 Manajemen *password*** **Kontrol** Pengelolaan *password* terhadap sistem harus interaktif dan harus memastikan kualitas *password*

4. KESIMPULAN

Berdasarkan penelitian yang dilakukan penulis, diperoleh kesimpulan sebagai berikut:

1. Berdasarkan hasil identifikasi risiko aset kritis IS/IT pada Pengadilan Negeri Slawi, diperoleh 75 kemungkinan risiko yang dibedakan berdasarkan faktor penyebab potensialnya.Dengan menggunakan metode penilaian *risk* FMEA, dilakukan pencarian nilai skor risiko dan nilai RPN.

Kemudian penentuan risiko kritis dimana memenuhi ketentuan garis batas yang diperoleh dari penetapan nilai kritis RPN yakni ≥ 205 dan nilai kritis skor risiko yakni ≥ 33. Sehingga diperoleh risiko kritis sejumlah 34 risiko kritis.
2. Penentuan strategi mitigasi risiko berdasarkan ISO/IEC 27002:2013 pada risiko kritis yang membutuhkan perhatian serius, berikut adalah klausul yang akan digunakan yakni, Klausul 5, Klausul 6, Klausul 7, Klausul 8, Klausul 9, Klausul 11, Klausul 12, Klausul 13, Klausul 14, Klausul 16, Klausul 17, Klausul 18.
3. Metode ini dapat mengurangi tingkat resiko sehingga pelayanan di PN Negeri Slawi dapat lebih efektif dan efesien.

5. SARAN

Saran berdasarkan penelitian yang dilakukan oleh penulis sebagai bentuk perbaikan penelitian tugas akhir ini antara lain:
1. Melakukan evaluasi atau penilaian kembali terhadap perolehan risiko kritis setelah menerapkan rekomendasi strategi berdasarkan ISO/IEC 27002:2013 pada PN.Slawi.Menggunakan standart keamanan yang berbeda terutama pada standart keamanan proses bisnis terhadap perilaku kinerja sumber daya manusia.
2. Memperhatikan kemungkinan tingkat kerugian secara finansial yang diperoleh berdasarkan risiko yang telah terjadi.Melakukan mitigasi risiko terhadap aset teknologi dan sistem informasi terhadap seluruh bagian yang terdapat pada PN Slawi.

DAFTAR PUSTAKA

[1] U. Salim, "MANAJEMEN RISIKO BERBASIS SPIRITUAL ISLAM," *Ekuitas J. Ekon. dan Keuang.*, vol. 16, no. 2, pp. 184–208, 2012.

[2] I. Gamayanto, "Porter S Five Forces Model Scott Morton S Five Forces Model Bakos Treacy Model Analyzes Strategic Information Systems Management," *J. Inform.*, vol. 5, no. 2, p. pp.127-134, 2004.

[3] A. Awalianti and J. Isgiyarta, "PENERAPAN DAN FUNGSI MANAJEMEN RISIKO FLUKTUASI HARGA BATU BARA BERDASARKAN ISO 31000 (Studi Kasus pada Perusahaan Distributor Alat Berat PT X)," *DIPONEGORO J. Account.*, vol. 3, no. 1, pp. 1–13, 2014.

[4] A. Kinerja, N. Tambah, D. A. N. Mitigasi, and R. Rantai, "Analisis kinerja, nilai tambah dan mitigasi risiko rantai pasok agroindustri bawang merah," *J. Teknol. Ind. Pertan.*, vol. 28, no. 1, pp. 61–74, 2018.

[5] B. R. Kristanto, "APLIKASI MODEL HOUSE OF RISK (HOR) UNTUK MITIGASI RISIKO PADA SUPPLY CHAIN," *JITI*, vol. 13, no. 2, pp. 149–157, 2014.

[6] N. Awang *et al.*, "Risk Assessment using Big Data Analytics Approach : A Review," *Open Int. J. Informatics*, vol. 6, no. 4, pp. 1–12, 2018.

[7] N. U. Handayani, M. A. Wibowo, D. P. Sari, and Y. Satria, "Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001," *TEKNIK*, vol. 39, no. 2, pp. 78–85, 2018.

[8] D. L. Trenggonowati, "MENGGUNAKAN METODE HOUSE OF RISK PADA DIVISI PENGADAAN," *J. Ind. Serv.*, vol. 3, no. 1, pp. 1–7, 2017.

[9] L. Pan, "Application of a Financial Quantitative Risk Model to Information Security Risk Assessment," 2018.

[10] R. M. Harahap, "Information Technology Risk Measurement : Octave-S Method,"

CommIT, vol. 5, no. 1, pp. 27–29, 2011.

[11] S. M. Sulaman and M. Höst, "Risk Analysis and Management of IT Systems : Practice and Challenges," in *ISCRAM Conference*, 2018, no. May.

[12] Y. E. Pertiwi and A. Susanty, "SURYA CIP DENGAN HOUSE OF RISK MODEL."

[13] A. Nafasari, W. S. Sari, J. S. Informasi, U. D. Nuswantoro, and A. Kritis, "Analisis dan Mitigasi Risiko Aset Kritis Terhadap Kegagalan Proses Produksi Penyiaran Di TVKU Semarang Menggunakan Metode OCTAVE Dan FMEA Analysis and Mitigation of Critical Asset Risk on The Failure of Process of," *J. Inf. Syst.*, vol. 3, no. 2, pp. 171–179, 2018.

[14] K. Properti, O. Aditya, and P. Naomi, "Penerapan Manajemen Risiko Perusahaan dan Nilai Perusahaan di Sektor Konstruksi dan Properti Oka," *Esensi J. Bisnis dan Manaj.*, vol. 7, no. April, pp. 167–180, 2017.

[15] P. I. Setiasih, "Effectiveness of Failure Modes Effect Analysis (FMEA) to Reduce Medical Error," *J. Indones. Heal. POLICY Adm.*, vol. 2, no. 2, pp. 25–29, 2017.