USULAN MANAJEMEN RISIKO BERDASARKAN STANDAR SNI ISO/IEC 27001:2009 MENGGUNAKAN INDEKS KAMI (KEAMANAN INFORMASI) STUDI KASUS: BADAN NASIONAL PENEMPATAN DAN PERLINDUNGAN TENAGA KERJA INDONESIA (BNP2TKI)

Indah Kusuma Dewi[1], Fitroh[2], Suci Ratnawati[3]
Fakultas Sains dan Teknologi
Universitas Islam Negeri Syarif Hidayatullah Jakarta
Email : indahkd21@gmail.com[1] , fitroh@uinjkt.ac.id [2], Sratnaw69@gmail.com[3]

ABSTRACT

National Agency for the Placement and Protection of Indonesian Overseas Workers (BNP2TKI) managing labor data are vital such as data placement and data arrival so required security information. At the Center for Research and Development Information (Puslitfo) are the head of information systems in charge of sub-areas of system development and maintenance of the system. Of the two sub-areas that many threats that occur as the incident that led to the demise of electricity damaged server so that services should be in real time was inhibited. The study began with a check (analysis of current conditions), Act (Self-assessment based index WE) is an evaluation of the role and the importance of ICT as well as V (five) the completeness of the information security area, namely governance, risk management, framework, asset management, and technology and information security, Plan (Creating Risk Management Plan) which has an output Inventory asset, threat list, list of potential weakness, value possible threats, the impact value, and the value of risk and level of risk. And the last one is Do (Implement controls planned). From the results, the role and the importance of ICT with a score of 31, which has a higher category. For completeness of information security level still needs to be improved, and the maturity level of information security is at the first level categories (initial conditions). Of V (five) area evaluation, information security risk management has not reached the minimum so that made the Risk Management Plan and the policies and controls in the Risk Management Plan.

Keywords: *Risk Management Plan, Assets, Threats, Weaknesses, Value Possible Threat, Impact Analysis, Risk Value.*

ABSTRAK

Badan Nasional Penempatan dan Perlindungan Tenaga Kerja Indonesia (BNP2TKI) mengelola data tenaga kerja penting seperti informasi keamanan penempatan data dan kedatangan data sehingga diperlukan. Di Pusat Penelitian dan Pengembangan Informasi (Puslitfo) adalah kepala sistem informasi yang bertanggung jawab atas sub-bidang pengembangan sistem dan pemeliharaan sistem. Dari dua sub-daerah yang banyak ancaman yang terjadi sebagai kejadian yang menyebabkan matinya listrik yang rusak server sehingga layanan harus dalam real time terhambat. Penelitian ini dimulai dengan cek (analisis kondisi saat ini), Undang-Undang (Self-assessment berdasarkan indeks WE) adalah evaluasi peran dan pentingnya ICT serta V (lima) kelengkapan area keamanan informasi, yaitu tata kelola , manajemen risiko, kerangka, manajemen aset, dan teknologi dan informasi keamanan, Rencana (Membuat Rencana manajemen risiko) yang memiliki aset keluaran Inventarisasi, daftar ancaman, daftar potensi kelemahan, nilai kemungkinan ancaman, nilai dampak, dan nilai risiko dan tingkat risiko. Dan yang terakhir adalah Do (Melaksanakan kontrol direncanakan). Dari hasil, peran dan pentingnya ICT dengan skor 31, yang memiliki kategori yang lebih tinggi. Untuk kelengkapan tingkat keamanan informasi masih perlu ditingkatkan, dan tingkat kematangan keamanan informasi adalah pada kategori tingkat pertama (kondisi awal). V (lima) evaluasi daerah, manajemen risiko keamanan informasi belum mencapai minimum sehingga membuat Rencana Manajemen Risiko dan kebijakan dan kontrol dalam Rencana Manajemen Risiko.

Kata kunci: *Risk Management Plan, Assets, Threats, Weaknesses, Value Possible Threat, Impact Analysis, Risk Value.*

1. Pendahuluan

Pada bidang sistem informasi di Puslitfo, terdapat dua sub bidang yaitu pengembangan sistem dan pemeliharaan sistem. Dua sub bidang inilah yang mengelola seluruh aplikasi dan *server* untuk kebutuhan data dan informasi baik internal maupun eksternal. Oleh karena itulah mereka memerlukan sebuah pengkajian risiko untuk tugas mereka yang berisiko tinggi bagi kelangsungan bisnis dan informasi di BNP2TKI.

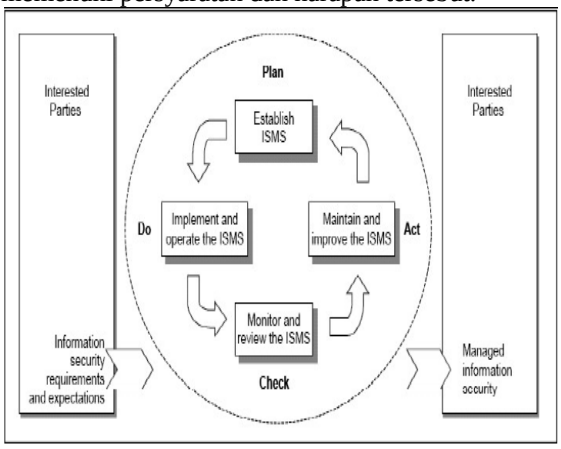
Setelah penulis melakukan observasi dan wawancara kepada kepala sub bidang pengembangan sistem, BNP2TKI ternyata tidak mempunyai pengkajian dan pengelolaan risiko, tidak ada kerangka kerja pengelolaan risiko yang mencakup klasifikasi aset informasi dan tingkat keamanan serta tidak melakukan pendefinisian kepemilikan dan pihak pengelola aset informasi. BNP2TKI hanya menjadi organisasi yang reaktif terhadap risiko ancaman yang terjadi. Contoh insiden yang pernah terjadi adalah saat aliran listrik yang tiba-tiba mati dan menyebabkan server menjadi rusak. Saat itu pelayanan yang biasanya *real time* pun tidak dapat diakses oleh para *user*. Apalagi BNP2TKI yang terletak di Jl. MT. Haryono ini adalah kantor pusat sehingga kasus itu pun berimbas pula ke kantor-kantor cabang di Indonesia. Kasus ini membuat BNP2TKI menderita kerugian baik dari segi bisnis maupun informasi.

2. Landasan Teori

A. SNI ISO/IEC 27001:2009

Merupakan susunan secara adopsi identik terhadap standar ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*. Standar yang merupakan standar nasional ini dibuat sebagai model untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan, dan perbaikan Sistem Manajemen Keamanan Informasi (SMKI). Desain dan penerapan SMKI dari suatu perusahaan dipengaruhi oleh kebutuhan dan sasaran perusahaan. Standar ini dan sistem pendukungnya diperkirakan akan berubah dari waktu ke waktu. Penerapan SMKI disesuaikan pula dengan kebutuhan perusahaan. Standar ini dapat digunakan untuk menilai kesesuaian oleh pihak terkait baik internal maupun eksternal (Badan Standardisasi Nasional SNI ISO/IEC 27001: 2005).

Standar SNI ISO/IEC 27001:2009 mengadopsi model "*Plan-Do-Check-Act*" (PDCA) yang diterapkan untuk membentuk seluruh proses SMKI. Gambar 2.1 memperlihatkan persyaratan keamanan informasi dan harapan dari pihak terkait menjadi masukan bagi SMKI, serta melalui tindakan dan proses yang diperlukan akan menghasilkan keluaran keamanan informasi yang memenuhi persyaratan dan harapan tersebut.



Gambar 2.1 Model PDCA

Tabel 2.1 Penjelasan Model PDCA

Plan (Penetapan SMKI)	Menetapkan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran perusahaan secara keseluruhan.
Do (Penerapan dan Pengoperasian SMKI)	Menerapkan dan mengoperasikan kebijakan pengendalian, proses dan prosedur SMKI.
Check (Pemantauan dan Pengkajian SMKI)	Mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.
Act (Peningkatan dan Pemeliharaan SMKI)	Mengambil tindakan korektif dan pencegahan berdasarkan hasil *internal* audit SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI.

B. Manajemen Risiko

Manajemen risiko adalah proses untuk mengidentifikasi risiko, menganalisa risiko dan melakukan penanganan untuk mengurangi risiko sampai dampaknya terhadap proses bisnis di perusahaan ataupun organisasi pada level yang dapat diterima atau dibolehkan (Sarno&Iffano,

2009). Manajemen risiko meliputi aktifitas-aktifitas yaitu: identifikasi informasi, identifikasi ancaman

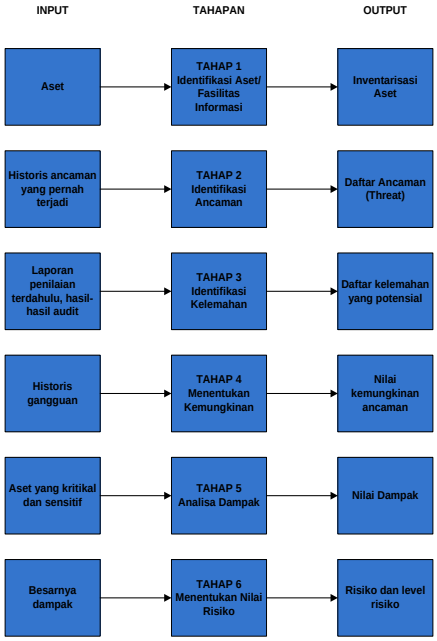
dan kelemahan, analisa dampak bisnis serta penilaian risiko (*risk assessment*).

Penilaian Risiko

Penilaian risiko (*risk assessment*) adalah langkah atau tahap pertama dari proses manajemen risiko dan bertujuan untuk mengetahui ancaman-ancaman (*threat*) dari luar yang berpotensi mengganggu keamanan informasi organisasi dan potensial kelemahan (*vulnerability*) yang mungkin dimiliki oleh informasi di perusahaan atau organisasi (Sarno&Iffano, 2009). Pada tahap ini, penulis mengadopsi dan mengadaptasikannya menjadi *Plan*, yaitu membuat *Risk Management Plan* dengan melakukan tahap-tahap pada metode dibawah ini.

Metode penilaian risiko terdiri dari 6 (enam) tahapan yaitu:

1. Identifikasi aset/Fasilitas Informasi
2. Identifikasi ancaman (*threat*)
3. Identifikasi kelemahan (*vulnerability*)
4. Menentukan kemungkinan ancaman (*probability*)
5. Analisa dampak (*impact analysis*)
6. Menentukan nilai risiko



Gambar 2.2 Tahapan Penilaian Risiko

C. Indeks KAMI (Keamanan Informasi)

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009. Hasil evaluasi indeks KAMI menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di instansi pemerintah (Direktorat Keamanan Informasi, 2012).

3. Metode Penelitian

A. Metodologi Penelitian

Metodologi penelitian yang akan digunakan dalam penelitian ini dibagi menjadi beberapa proses, yaitu menggunakan *Check-Act-Plan-Do* yang masing-masing mencakup analisis kondisi terkini, melaksanakan *self-assessment* berdasarkan Indeks KAMI (Keamanan Informasi), membuat perencanaan manajemen risiko, serta melakukan kebijakan yang akan dilakukan

B. Metode Pendekatan Proses

Berdasarkan teori yang ada, metode yang diterapkan oleh SNI ISO/IEC 27001: 2009 menggunakan model atau siklus *Plan-Do-Check-Act* (PDCA). Karena merupakan suatu siklus, PDCA ini juga dapat dilakukan dari siklus mana saja, baik itu dari *Do, Check*, maupun *Act*. Penulis melakukan penelitian ini dengan menggunakan *Check-Act-Plan-Do* (CAPD). Alasan penulis memilih model CAPD karena penulis melihat dari saran penelitian sebelumnya yang kebanyakan hanya melakukan *Plan* dan *Do* saja. Karena framework SNI ISO/IEC 27001: 2009 ini fleksibel, maka dapat disesuaikan dengan kondisi organisasinya. BNP2TKI belum pernah melakukan tata kelola teknologi informasi dan tidak memiliki pengkajian risiko untuk mengelola ancaman-ancaman yang ada maupun yang akan datang. Maka dengan melakukan *Check* terlebih dahulu, penulis dapat mengetahui apa kebutuhan sebenarnya dari BNP2TKI.

Berikut ini adalah tabel model CAPD yang dilakukan oleh penulis beserta dengan penjelasannya:

Tabel 3.1 Model CAPD

Check (pemantauan dan pengkajian)	Mengobservasi profil, struktur organisasi dan SOP, serta kondisi organisasi saat ini untuk dijadikan analisis kondisi terkini.
Act (peningkatan dan pemeliharaan)	Peningkatan dan pemeliharaan dengan melaksanakan *self-assessment* berdasarkan Indeks KAMI (Keamanan Informasi). Penilaian yang dilakukan meliputi: **Peran dan tingkat kepentingan TIK, Tata kelola keamanan informasi Pengelolaan risiko keamanan informasi, Kerangka kerja pengelolaan keamanan informasi, Peengelolaan aset informasi**, serta **Teknologi dan keamanan informasi**. Hasil dari *assessment* ini untuk peningkatan dan pemeliharaan organisasi dari sisi manajemen
Plan (penetapan dan perencanaan)	Membuat *risk management plan* dari prosedur SMKI yang sesuai untuk perbaikan keamanan informasi. Perencanaan tersebut meliputi: 1. **Identifikasi aset, outputnya yaitu daftar aset utama dan aset pendukung.** 2. **Identifikasi ancaman, outputnya yaitu daftar ancaman.** 3. **Identifikasi kelemahan, outputnya yaitu daftar kelemahan yang potensial terjadi.** 4. **Menentukan nilai kemungkinan, outputnya yaitu nilai kemungkinan ancaman dan prioritas aset.** 5. **Analisa dampak, outputnya yaitu nilai dampak bisnis dan analisa mitigasi.** 6. **Menentukan nilai risiko, outputnya yaitu nilai risiko dan level risiko.**
Do (penerapan dan pengoperasian)	Melakukan kontrol yang direncanakan berupa kebijakan dan pengendalian dari usulan *risk management* pada tahap sebelumnya.

4. Analisis Dan Pembahasan

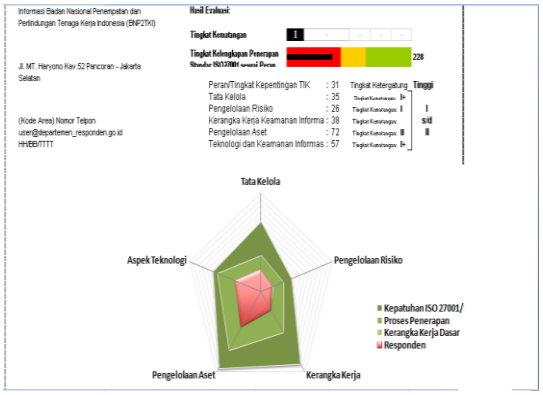
A. Check (Analisis Kondisi Terkini)

Penulis mengecek profil, visi, misi, arah, kebijakan, tujuan dan sasaran organisasi, logo, struktur organisasi baik pada organisasi maupun lingkup batasan masalah, serta proses bisnis yang ada pada Kepala Bidang Sistem Informasi Pusat Penelitian dan Pengembangan Informasi (Puslitfo).

B. Act (Melakukan *self-assessment*)

Self-assessment dilakukan untuk melakukan penilaian menggunakan indeks KAMI (Keamanan Informasi). Penilaian ini mencakup penilaian tingkat ketergantungan Teknologi Informasi dan Komunikasi (TIK) dan Penilaian V (lima) area tingkat kelengkapan keamanan informasi sebagai berikut:

1. Peran dan Tingkat Kepentingan TIK dalam instansi
2. Tata kelola keamanan informasi
3. Pengelolaan risiko keamanan informasi
4. Kerangka kerja pengelolaan keamanan informasi
5. Pengelolaan aset informasi
6. Teknologi dan keamanan informasi



Gambar 4.1 *Dashboard* dan *Radar Chart* Kantor Pusat BNP2TKI

Dari hasil evaluasi kelengkapan penerapan standar SNI ISO/IEC 27001: 2009 didapatkan bahwa kantor pusat BNP2TKI berada pada area merah dan memiliki nilai 228 sehingga masih dikategorikan dalam status kesiapan perbaikan. Sedangkan untuk tingkat kematangan keamanan informasi berada pada kategori tingkat I yaitu kondisi awal (Reaktif).

C. *Plan* (Membuat *Risk Management Plan*)

Dari hasil evaluasi *self-assesment* yang telah didapatkan, pengelolaan risiko pada kantor pusat BNP2TKI memang belum sampai pada tahap minimal. Risiko keamanan informasi adalah potensi bahwa ancaman yang diberikan akan mengeksploitasi kerentanan aset yang dimiliki oleh organisasi ataupun kelompok aset lainnya. Organisasi yang memberikan layanan untuk publik, sangat rentan akan keamanan informasi. Semakin tinggi teknologi suatu organisasi, maka makin tinggi pula risiko keamanan informasinya. Untuk menjadikan organisasi yang preventif, *Risk Management Plan* dapat menjadi solusi. Penulis menggabungkan ISO 27001 dengan ISO 27005 mengenai manajemen risiko yang merupakan prasyarat untuk membuat Sistem Manajemen Keamanan Informasi (SMKI).

1. Identifikasi Aset/Fasilitas Informasi

Jenis aset dapat dibedakan menjadi 2 (dua):

1. Aset utama

   Aset utama biasanya merupakan proses dan informasi inti kegiatan dalam lingkup organisasi. Aset utama lainnya seperti proses organisasi juga dapat diperhitungkan, yang akan lebih tepat untuk menyusun kebijakan keamanan informasi atau rencana kelangsungan bisnis.

   Aset utama terdiri dari dua jenis:

   a. Proses bisnis (sub-proses) dan kegiatan
   b. Informasi

2. Aset pendukung

   Aset pendukung merupakan dimana unsur-unsur utama dari ruang lingkup bergantung. Ruang lingkup terdiri dari aset yang harus diidentifikasikan dan dijelaskan. Aset-aset ini mempunyai kerentanan yang dapat dieksploitasi oleh ancaman yang bertujuan untuk merusak aset utama. Yang termasuk aset pendukung antara lain:

   a. *Hardware*
   b. *Software*/Aplikasi
   c. Jaringan
   d. Personel
   e. Tempat
   f. Struktur organisasi

2. Identifikasi Ancaman

Threat atau ancaman adalah suatu potensi yang disebabkan oleh insiden yang tidak diinginkan yang mungkin membahayakan jalannya proses bisnis organisasi. Tujuan dari mengidentifikasi ancaman adalah agar diketahui ancaman yang mungkin terjadi dan membahayakan sistem dalam organisasi. Sumber ancaman dapat berasal dari alam (*natural threat*), lingkungan (*environmental threat*), dan manusia (*human threat*).

Pada ISO 27005: 2008, diberikan daftar contoh ancaman yang khas. Daftar tersebut memberikan gambaran ancaman yang mungkin disengaja, tidak disengaja atau lingkungan alam dan dapat mengakibatkan kerusakan atau kehilangan layanan yang penting. Daftar ini menunjukkan untuk setiap jenis ancaman yang diklasifikasikan sebagai berikut:

Tabel 4.1 Daftar klasifikasi ancaman

A	Tidak disengaja	Digunakan untuk semua tindakan manusia yang tidak sengaja dapat merusak aset informasi
D	Disengaja	Digunakan untuk semua tindakan sengaja yang ditujukan untuk aset informasi
E	Lingkungan	Digunakan untuk semua insiden yang tidak didasarkan pada tindakan manusia

3. Identifikasi Kelemahan

Kelemahan yang dimaksud dalam mengidentifikasi kelemahan ini adalah yang di dalam

prosedur kemanan informasi, perencanaan, implementasi atau kontrol internal di dalam organisasi terhadap penjagaan informasi yang dimiliki, dimana kelemahan ini dapat menimbulkan atau memicu ancaman. Tujuan utama dari tahap ini adalah organisasi memahami kelemahan yang dimiliki dalam sistem manajemen keamanan informasinya.

Berdasarkan pada ISO 27001, input dari identifikasi kelemahan ini adalah dari laporan penilaian terdahulu dan hasil-hasil audit

4. Menentukan Kemungkinan / Nilai Kemungkinan Ancaman

Tujuan dari tahap ini adalah untuk mengetahui kemungkinan ancaman yang akan timbul sesuai dengan identifikasi ancaman yang telah didefinisikan. Nilai aset, dan tingkat ancaman dan kerentanan, relevan untuk setiap jenis konsekuensi dan dicocokkan dalam matriks berdasarkan ISO/IEC 27005: 2008.

5. Analisa Dampak

Analisa dampak adalah kegiatan untuk menentukan seberapa besar dampak atau pengaruhnya suatu risiko yang diakibatkan oleh ancaman atau kelemahan terhadap organisasi atau jalannya proses bisnis organisasi. Jika analisa dampak ditujukan atau difokuskan kepada proses bisnis organisasi diistilahkan dengan analisa dampak bisnis yang disingkat BIA (*Business Impact Analysis*).

6. Menentukan Nilai Risiko

Nilai risiko adalah gambaran dari seberapa besar akibat yang akan diterima organisasi jika ancaman yang menyebabkan kegagalan keamanan informasi terjadi.

Tabel 4.2 Nilai kemungkinan skenario risiko

Kemungkinan Ancaman	Rendah (R)			Sedang (S)			Tinggi (T)		
Level Kerentanan	R	S	T	R	S	T	R	S	T
Nilai kemungkinan dari skenario insiden	0	1	2	1	2	3	2	3	4

Tabel 4.3 Matriks nilai aset dan nilai kemungkinan

Nilai Aset	0	1	2	3	4
Nilai Kemungkinan					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Penulis membuat penilaian risiko dari aplikasi data *warehouse* yang memiliki 3 (tiga) aset utama yaitu Data Penempatan (A1), Data Kedatangan (A2), serta Data Pengaduan (A3). Ancaman yang terjadi pada BNP2TKI adalah data dari sumber yang tidak dapat dipercaya (T1).

Tabel 4.4 Nilai Risiko Aplikasi Data *Warehouse* BNP2TKI

Aset/Nilai Aset	T1	Jumlah
A1/4	7	7
A2/4	6	6
A3/4	7	7
Nilai Risiko Data Warehouse		20

Dapat dilihat bahwa aplikasi data warehouse yang merupakan salah satu aplikasi penting untuk pengambilan keputusan pada level *top management* memiliki nilai risiko 20 dikarenakan aset-aset yang ada memiliki kemungkinan ancaman yang sedang dan tinggi. Dengan nilai ancaman yang masing-masing 7, 6 dan 7 termasuk dalam kategori risiko yang tinggi dan diperlukan mitigasi prioritas menengah bagi manajemen atas.

D. *Do* (Melaksanakan kontrol yang direncanakan)

Dalam menerapkan Keamanan Informasi dua aspek tersebut tidak dapat dipisahkan. Artinya sebaiknya suatu organisasi tidak hanya menerapkan Teknologi Keamanan Informasi saja tanpa menerapkan Sistem Manajemen Keamanan Informasi (SMKI). Berdasarkan perbandingan (*benchmarking),* jika dihitung perbandingan kontribusi maka Sistem Manajemen Keamanan Informasi (SMKI) berperan lebih besar (60%) dalam Keamanan Informasi dibandingkan dengan Teknologi Keamanan Informasi.

Kebijakan yang penulis rekomendasikan untuk dilakukan oleh kantor pusat BNP2TKI berdasarkan referensi dari SNI ISO/IEC 27001: 2009 yang mencakup dari tahapan penilaian risiko yang sudah direncanakan

5. Kesimpulan Dan Saran

A. Kesimpulan

1. Badan Nasional Penempatan dan Perlindungan Tenaga Kerja Indonesia (BNP2TKI) telah melakukan *self-assessment* pada Pusat Penelitian

2. dan Pengembangan Informasi pada bidang sistem informasi dengan menggunakan indeks KAMI (Keamanan Informasi) berdasarkan SNI ISO/IEC 27001: 2009.
3. Hasil evaluasi peran dan tingkat kepentingan Teknologi Informasi dan Komunikasi (TIK) termasuk dalam kategori TINGGI yaitu dengan skor 31, yang berarti BNP2TKI membutuhkan keamanan ekstra untuk melindungi aset atau informasi yang dimiliki.
4. Hasil evaluasi kelengkapan penerapan keamanan informasi pada kantor pusat BNP2TKI berada pada area merah sehingga masih dikategorikan dalam status kesiapan tidak layak. Sedangkan untuk tingkat kematangan keamanan informasi berada pada kategori tingkat I yaitu kondisi awal (reaktif).
5. Perencanaan manajemen risiko telah menghasilkan daftar aset, daftar ancaman, daftar kelemahan yang potensial, nilai kemungkinan ancaman, nilai dampak dan risiko serta level risiko

B. Saran

1. Evaluasi penilaian dilakukan di semua deputi atau unit yang ada di kantor pusat BNP2TKI, tidak hanya pada Pusat Penelitian dan Pengembangan Informasi (Puslitfo).
2. Model *Plan-Do-Check-Act* (PDCA) terus dilakukan berkelanjutan membentuk siklus sehingga Sistem Manajemen Keamanan Informasi (SMKI) dapat berjalan optimal.
3. Dapat memberikan laporan dari hasil evaluasi tingkat kepentingan, kelengkapan informasi dan kematangan keamanan informasi kepada *top management* serta melakukan Business Impact Analysis (BIA) yang lebih mendalam.
4. Dapat melakukan *desktop assessment* dan *on site assessment* langsung oleh auditor atau *assessor* SNI ISO/IEC 27001: 2009.
5. Usulan manajemen risiko dapat diimplementasikan dan dilanjutkan untuk dibuat pengendalian sesuai dengan kebutuhan organisasi

6. Referensi

[1] Direktorat Keamanan Informasi. 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*. Jakarta: Penerbit Kementerian Komunikasi dan Informatika.

[2] Sarno, Riyanarto. 2009. *Audit Sistem dan Teknologi Informasi*. Surabaya: Penerbit ITS Press

[3] Sarno R, Iffano I. 2009. *Sistem Manajemen Keamanan Informasi berbasis ISO 27001*. Surabaya: Penerbit ITS Press.

[4] Surendro, Kridanto. 2009. *Implementasi Tata Kelola Teknologi Informasi*. Bandung: Penerbit: Informatika.

[5] Direktorat Keamanan Informasi. 2012. *Penerapan Standard SNI-27001 Dibidang Keamanan Informasi*. Jakarta: Penerbit Kementerian Komunikasi dan Informatika.

[6] ISO/IEC 27005. 2008. International Standard ISO/IEC 27005 *Information Technology - Security Techniques – Information Security Risk Management*.

[7] Direktorat Keamanan Informasi. 2012. *Bimbingan Teknis Sistem Manajemen Keamanan Informasi – Pendahuluan*. Jakarta: Kementerian Komunikasi dan Informatika.

[8] Direktorat Keamanan Informasi. 2012. *Bimbingan Teknis Sistem Manajemen Keamanan Informasi – Persyaratan Keamanan Informasi*. Jakarta: Kementerian Komunikasi dan Informatika.

[9] Direktorat Keamanan Informasi. 2012. *Bimbingan Teknis Sistem Manajemen Keamanan Informasi – Risk Management Information Security Management System*. Jakarta: Kementerian Komunikasi dan Informatika.

[10] Direktorat Keamanan Informasi. 2012. *Indeks KAMI Versi 2.3*. Jakarta: Kementerian Komunikasi dan Informatika.

[11] SNI ISO/IEC 27001: 2009. Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan. Badan standardisasi Nasional Indonesia.

[12] Sugiyono. 2012. *Memahami Penelitian Kualitatif*. Bandung: ALFABETA.

[13] Sugiyono. 2010. *Metode Penelitian Kuantitatif Kualitatif & RND*. Bandung: Alfabeta.