

Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO/IEC 27005:2018 dan NIST SP 800-30 Revisi 1

Meilita Karendra Putri¹⁾, Arif Rahman Hakim²⁾

(1) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, meilita.karendra@bssn.go.id

(2) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, arif.rahman@bssn.go.id

Abstrak

Jaringan merupakan salah satu layanan internal yang dikelola oleh instansi MKP. Layanan ini termasuk salah satu yang kritikal dikarenakan hampir seluruh pertukaran informasi dan kegiatan perkantoran di lingkungan instansi tersebut membutuhkan koneksi jaringan. Apabila terjadi gangguan pada layanan jaringan maka gangguan tersebut dapat menyebabkan adanya penurunan reputasi dan kendala pada pelaksanaan proses bisnis instansi MKP. Oleh karena itu, perlu adanya metode manajemen risiko keamanan informasi yang dilakukan terhadap layanan jaringan instansi MKP. Berdasarkan hal tersebut, dilakukan perancangan manajemen risiko keamanan informasi pada layanan jaringan milik instansi MKP menggunakan kerangka kerja ISO/IEC 27005:2018 yang dikombinasikan dengan kerangka kerja NIST SP 800-30 Revisi 1 pada tahap penilaian risiko. Tahapan perancangan manajemen risiko yang dilakukan yaitu penetapan konteks, penilaian risiko, perlakuan risiko dan penerimaan risiko. Penilaian risiko dilakukan dengan menganalisis data yang diperoleh dari hasil wawancara, observasi, telaah dokumen, dan pemberian kuisioner penilaian risiko. Berdasarkan hasil penilaian risiko, telah teridentifikasi 23 aset dengan 59 skenario risiko yang diketahui. Dari 59 skenario risiko tersebut, 12 skenario diantaranya dapat diterima dan 47 skenario lainnya dimitigasi. Pada tahap perlakuan risiko dan penerimaan risiko, 47 skenario risiko tersebut diberikan strategi perlakuan modifikasi dan rekomendasi kontrol serta ditentukan penanggung jawab kontrol berdasarkan skenario risikonya. Hasil dari penelitian ini adalah perancangan manajemen risiko keamanan informasi yang disertakan dengan rekomendasi kontrol keamanan informasi yang mengacu pada kerangka kerja ISO/IEC 27002:2013.

Kata kunci : ISO/IEC 27002:2013, ISO/IEC 27005:2018, Manajemen Risiko, NIST SP 800-30 Revisi 1, Penilaian Risiko, Rekomendasi Kontrol Keamanan Informasi.

Abstract

Network service is one of the internal IT services managed by MKP Agency. This service is a kind of critical service because of that almost all office activities mainly information exchange through the network. If there is a disruption in network service, it causes damage of the agency's reputation as well as slow down the organization business processes. Therefore, it is necessary to have risk management on their network services due to information security risk. Based on those reasons, we design the information security risk management on MKP's network services by using the ISO / IEC 27005: 2018 framework. Moreover, we combined the framework with the NIST SP 800-30 Revision 1 framework mainly at the risk assessment stage. The stages of risk management design undertaken comprise of; the establishment of context, risk assessment, risk treatment, and risk acceptance. Risk assessment is done by analyzing data obtained from interviews, observations, document reviews, and the provision of risk assessment questionnaires. Based on the risk assessment results, 23 assets have been identified with 59 known risk scenarios. Of the 59 risk scenarios, 12 of them are acceptable, and 47 are reduced. In the stage of risk treatment and risk acceptance, 47 risk scenarios are given modifications to the treatment strategy and control recommendations, and the person-in-charge is determined based on the risk scenario. Finally, we provide security control recommendations based on the results from earlier steps that refer to the ISO / IEC 27002: 2013 framework.

Keywords : Information Security Control Recommendations, ISO/IEC 27002:2013, ISO/IEC 27005:2018, NIST SP 800-30 Revision 1, Risk Assessment, Risk Management.

1. PENDAHULUAN

Keamanan informasi (KAMI) merupakan salah satu upaya untuk melindungi aset informasi dari berbagai ancaman. Terdapat empat prinsip dari tujuan utama KAMI yaitu; mencegah pihak yang tidak berhak mengakses teknologi informasi (TI) milik organisasi, mencegah adanya pencurian data, melindungi keutuhan dan integritas data, dan menghindari adanya kerusakan sistem secara sengaja maupun tidak disengaja [1]. Hal pertama yang dapat dilakukan suatu organisasi untuk membangun dan menerapkan sistem KAMI adalah melakukan kajian

dan analisis terhadap risiko KAMI sesuai dengan skala prioritas [1]. MKP merupakan institusi pemerintahan yang memanfaatkan TI untuk menjalankan salah satu misinya yaitu menjamin keamanan informasi di sektor pemerintah, infrastruktur informasi kritikal nasional, dan ekonomi digital dalam mewujudkan keamanan nasional dan meningkatkan pertumbuhan ekonomi nasional [2]. Peran TI di lingkungan MKP merupakan hal yang sangat krusial sehingga perlu adanya pengelolaan dan perhatian khusus. Pengelola TI di lingkungan MKP adalah bagian ABC [2]. Dalam rangka mendukung pelaksanaan TI nya, ABC mengelola 11 layanan utama yang disediakan untuk

internal MKP [3]. Seiring dengan tingginya peran dan kebutuhan TI tersebut, menyebabkan munculnya potensi ancaman TI yang berada di lingkungan MKP, sehingga dapat mengganggu proses bisnis milik instansi. Belum dilakukannya penilaian risiko oleh ABC terhadap ketersediaan TI di lingkungan MKP juga meningkatkan terjadinya risiko ancaman yang tentunya dapat mengganggu stabilitas organisasi. Oleh karena itu, perlu adanya kajian dan analisis terhadap risiko dalam proses bisnis ABC agar pelaksanaan keamanan informasi di lingkungan MKP dapat berjalan dengan baik. Hal tersebut juga mendukung salah satu tugas ABC dalam melaksanakan penyiapan penyusunan, pelaksanaan, evaluasi dan pelaporan di bidang manajemen risiko teknologi informasi komunikasi untuk layanan internal MKP [4].

Perancangan manajemen risiko dilakukan menggunakan kerangka kerja ISO/IEC 27005 sebagai kerangka kerja utama perancangan manajemen risiko dan *National Institute of Standards and Technology Special Publication 800-30 Revision 1* (NIST SP 800-30 Revisi 1) yang digunakan sebagai petunjuk pelaksanaan penilaian risiko yang dipilih berdasarkan rekomendasi pada dokumen rencana strategis ABC [5-6]. Penelitian sebelumnya dilakukan oleh Hermawan Setiawan *et.al.*, pada tahun 2017 yang membahas tentang kombinasi kerangka kerja ISO/IEC 27005 dan NIST SP 800-30 Revisi 1 untuk melakukan rancangan manajemen risiko keamanan informasi [7]. Lalu, penelitian tahun 2019 yang dilakukan oleh Irma Resha Lestari yang membahas tentang penerapan standar ISO/IEC 27005:2011 dalam perencanaan manajemen risiko dan menghasilkan daftar kontrol keamanan informasi yang dapat dijadikan rekomendasi untuk layanan pada instansi lokus [8].

Berdasarkan pembahasan di atas, maka perancangan manajemen risiko keamanan informasi pada layanan jaringan ABC yang disediakan untuk internal MKP dilakukan berdasarkan kerangka kerja ISO/IEC 27005:2018 dan NIST SP 800:30 Revisi 1. Hasil penelitian ini adalah perancangan manajemen risiko yang disertakan dengan rekomendasi kontrol keamanan informasi untuk menangani skenario risiko. Rekomendasi kontrol yang diberikan mengacu pada standar ISO/IEC 27002:2013 [9].

2. TELAAH KEPUSTAKAAN

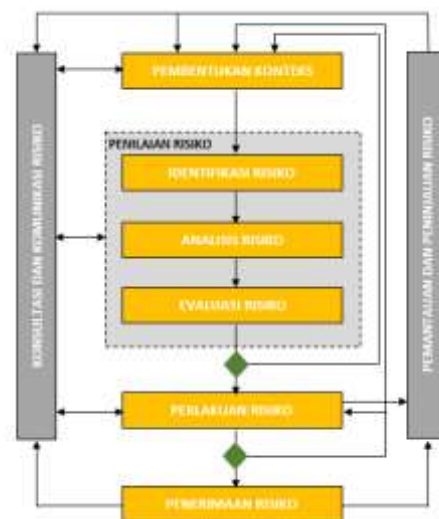
Bagian telaah kepustakaan menjelaskan tentang standar ISO/IEC 27005:2018 dan penelitian-penelitian terkait yang dijadikan sebagai acuan dalam penelitian ini.

2.1. Standar ISO/IEC 27005:2018

Perancangan manajemen risiko layanan jaringan ABC dilakukan berdasarkan standar ISO/IEC 27005:2018. Standar ini membahas tentang manajemen risiko keamanan informasi yang dirancang untuk membantu pelaksanaan konsep

keamanan informasi berdasarkan pendekatan manajemen risiko [5]. Standar ini dapat diterapkan pada semua jenis organisasi yang melakukan pengelolaan risiko untuk menghindari adanya bahaya yang mengancam keamanan informasi pada organisasi tersebut [5]. Di dalam standar ini, disertakan gambaran proses manajemen risiko yang dibagi ke dalam enam klausul, yaitu Penetapan konteks, Penilaian risiko, Perlakuan risiko, Penerimaan risiko, Komunikasi risiko, dan Pemantauan dan peninjauan risiko.

Setiap klausul proses manajemen risiko dapat diuraikan menjadi *input*, tindakan, panduan implementasi dan *output*. Pada klausul penilaian risiko dan perlakuan risiko dapat dilakukan perulangan agar mendapatkan efektivitas serta efisiensi waktu dan usaha dalam mengidentifikasi risiko. Pada penelitian ini, klausul yang digunakan dibatasi pada penetapan konteks, penilaian risiko, perlakuan risiko dan penerimaan risiko. Skema proses manajemen risiko berdasarkan standar ISO/IEC 27005:2018 ditunjukkan pada Gambar 1.

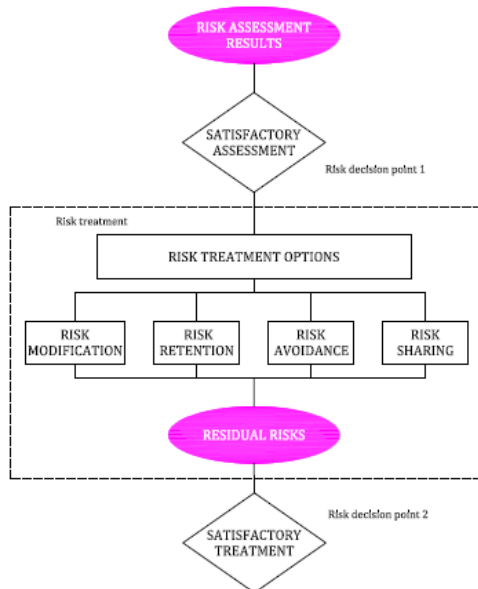


Gambar 1. Proses Manajemen Risiko Berdasarkan Kerangka Kerja ISO/IEC 27005:2018

Penetapan konteks dilakukan dengan menjelaskan profil organisasi lokus penelitian, menentukan kriteria dasar manajemen risiko yang dilakukan, menentukan batasan dan ruang lingkup pengerjaan, serta menentukan organisasi atau bagian yang bertanggung jawab dalam melakukan manajemen risiko yang bertujuan untuk menentukan sekaligus mempertegas tujuan dilakukannya manajemen risiko. Selanjutnya melakukan penilaian risiko yang diawali dengan mengidentifikasi risiko yang mungkin terjadi, menganalisis risiko berdasarkan hasil identifikasi, dan melakukan evaluasi risiko.

Proses identifikasi dilakukan pada seluruh aset yang berkaitan dengan objek penelitian, ancaman, kontrol yang sudah ada dan kerentanan pada objek penelitian. Tahap selanjutnya adalah menganalisis risiko yang dapat dilakukan dengan tiga metodologi

yaitu kualitatif, kuantitatif maupun kombinasi keduanya. Tahap ini ditujukan untuk menentukan tingkat peluang dan dampak terhadap ancaman pada setiap aset. Kemudian dilakukan tahap evaluasi risiko untuk menghasilkan daftar prioritas risiko berdasarkan kriteria evaluasi risiko yang berhubungan dengan skenario risiko yang mengarah ke risiko tersebut.



Gambar 2. Alur Perlakuan Risiko yang Dilakukan

Berdasarkan Gambar 2, dapat dilihat alur perlakuan risiko yang dilakukan pada penelitian ini. Perlakuan risiko dilakukan setelah proses penilaian risiko selesai. Hasil dari proses penilaian risiko kemudian dikategorikan berdasarkan empat kondisi perlakuan yaitu risiko yang dimodifikasi (*risk modification*), risiko yang diterima (*risk retention*), risiko yang dihindari (*risk avoidance*) dan risiko yang dibagi (*risk sharing*).

2.2. Penelitian Terkait

- a. *Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Applications of XYZ Institute* [7]. Penelitian ini membahas tentang desain manajemen risiko keamanan informasi yang menggunakan standar ISO/IEC 27005 dan NIST SP 800-30 Revisi 1 sebagai *tools* untuk melakukan penilaian risiko [7]. Standar ISO/IEC 27005:2011 digunakan sebagai kerangka kerja utama dalam penetapan manajemen risiko, sedangkan standar NIST SP 800-30 Revisi 1 digunakan pada penentuan beberapa kriteria di proses penetapan konteks dan proses identifikasi risiko serta analisis risiko pada tahap penilaian risiko. Kemudian dijelaskan pula secara rinci penggunaan standar NIST SP 800-30 Revisi 1 dalam melakukan manajemen risiko. Contoh perancangan manajemen risiko keamanan informasi pada sampel institusi XYZ berdasarkan

kombinasi standar tersebut disertakan di dalam tulisan. Berdasarkan penelitian tahun 2017 ini, didapatkan kesimpulan bahwa ISO/IEC 27005 dapat dikombinasikan dan dilengkapi dengan standar lain, sedangkan NIST SP 800-30 Revisi 1 tidak memiliki petunjuk yang menjelaskan proses insiden pada skenario risiko sehingga standar ini dapat ditambahkan atau dikombinasikan dengan *tools* lain. Penelitian Setiawan *et.al* ini dijadikan referensi bagaimana standar ISO/IEC 27005 dikombinasikan dengan standar NIST SP 800-30 Revisi 1. Selain itu, digunakan pula sebagai pertimbangan dan acuan dalam tahap atau proses perancangan manajemen risiko.

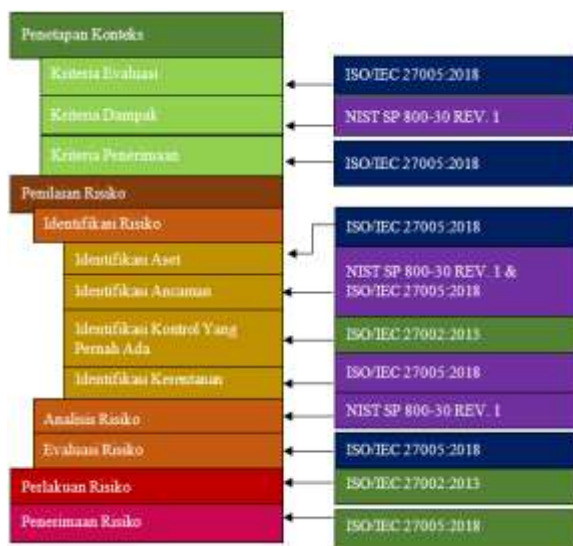
- b. *Perencanaan Manajemen Risiko Keamanan Informasi Layanan Mail MKP pada Bagian ABC Berdasarkan Kerangka Kerja ISO/IEC 27005:2011* [8]

Pada penelitian terkait ini telah dilakukan perencanaan manajemen risiko untuk layanan *email* di lokus ABC [8]. Manajemen risiko dilakukan dengan berdasarkan kerangka kerja dari standar ISO/IEC 27005:2011 dan menghasilkan daftar risiko yang telah dinilai dan diprioritaskan serta ditujukan sebagai rekomendasi kontrol keamanan informasi layanan *email* ABC. Pembatasan masalah pada penelitian tahun 2019 ini yaitu, tahapan ISO/IEC 27005:2011 hanya dilakukan hingga tahap perlakuan risiko, rekomendasi kontrol keamanan informasi mengacu pada ISO/IEC 27002:2013, metode penelitian yang digunakan adalah penelitian deskriptif kualitatif. Metode kualitatif diterapkan pada proses pengumpulan, penyajian dan analisis data. Sumber yang dibutuhkan pada proses pengumpulan data berasal dari data primer dan data sekunder. Selain itu, diterapkan pula metode *member checking* untuk melakukan validasi data. Penelitian dari Lestari digunakan sebagai bahan pertimbangan untuk menentukan narasumber dan kerangka kerja yang tepat pada perancangan manajemen risiko layanan jaringan ABC [8]. Selain itu, digunakan pula sebagai gambaran dan pertimbangan dalam menentukan objek dan *scope* yang diteliti, juga menentukan metode apa yang digunakan di setiap tahapan pengerjaan.

3. METODOLOGI PENELITIAN

Penelitian ini dilakukan menggunakan metode kualitatif deskriptif dengan mengacu pada standar ISO/IEC 27005:2018 yang dikombinasikan dengan NIST SP 800-30 Revisi 1. Penggunaan masing-masing standar di setiap tahap pengerjaan manajemen risiko pada penelitian ini dapat dilihat pada Gambar 3. Penetapan konteks yang dilakukan adalah menjelaskan profil organisasi lokus penelitian dan objek penelitian, juga merancang kriteria dasar untuk melakukan manajemen risiko [5]. Kriteria dampak

dibentuk berdasarkan standar NIST SP 800-30 Revisi 1, dengan mempertimbangkan salah satu Dokumen Pedoman Kepala MKP tentang Pelaksanaan Penyelenggaraan SPIP MKP sebagai substansi penelitian [10]. Penilaian risiko terdiri dari tiga tahap, yaitu identifikasi risiko, analisis risiko dan evaluasi risiko. Pada tahap identifikasi risiko, dilakukan identifikasi pada aset, ancaman, kontrol yang sudah ada serta kerentanan berdasarkan objek penelitian. Selanjutnya dilakukan analisis risiko untuk mendapatkan hasil penilaian risiko dan tingkat kemungkinan risiko yang dilakukan dengan mengacu pada NIST SP 800-30 Revisi 1. Pada proses evaluasi risiko ditentukan prioritas terhadap skenario risiko yang didapatkan pada proses analisis risiko, hal ini ditujukan untuk memudahkan lokus dalam mengenali risiko mana yang perlu ditangani terlebih dahulu. Skenario risiko yang dimaksud adalah pemetaan setiap kejadian ancaman terhadap aset yang telah diidentifikasi [11]. Pada tahap penilaian risiko diberikan kuisioner kepada pihak lokus untuk mengetahui nilai-nilai pada masing-masing parameter penilaian yang dibutuhkan pada tahap ini. Hasil dari penilaian risiko selanjutnya diberikan perlakuan dan ditentukan penanggung jawab risiko sebagai hasil dari tahap penerimaan risiko. Pada tahap perlakuan risiko, skenario risiko yang mendapat selera risiko dimitigasi dan diprioritaskan mendapat perlakuan berupa rekomendasi kontrol keamanan informasi yang diberikan berdasarkan ISO/IEC 27002:2013 dan strategi perlakuan risiko. Selanjutnya, pada tahap penerimaan risiko ditentukan penanggung jawab masing-masing risiko. Hasil dari rangkaian tahap perancangan manajemen risiko dikomunikasikan kepada pihak lokus untuk mengonfirmasi terkait kesesuaiannya.



Gambar 3. Penggunaan Standar pada Tahap Manajemen Risiko

4. HASIL DAN PEMBAHASAN

Pembahasan pada penelitian ini berfokus pada hasil perancangan manajemen risiko berdasarkan standar yang digunakan sebagai acuan yaitu, pembentukan konteks, penilaian risiko, perlakuan risiko dan penerimaan risiko.

4.1. Penetapan Konteks

Penelitian ini dilakukan pada layanan jaringan ABC yang dibatasi pada:

- Manajemen risiko dilakukan pada layanan Jaringan ABC.
- Pembatasan area manajemen risiko layanan jaringan dilakukan pada :
 - Bagian XXX
 - Deputi YYY
 - Ruang Meet Me Room
 - ABC
- Tahapan manajemen risiko yang dilakukan mengacu pada kerangka kerja ISO/IEC 27005:2018 di tahap penetapan konteks, penilaian risiko, perlakuan risiko dan penerimaan risiko. Tahap pemantauan dan tinjauan risiko tidak dilakukan karena melibatkan penerapan hasil manajemen risiko oleh pihak ABC dan keterbatasan waktu penelitian.
- Pemberian rekomendasi kontrol risiko pada tahap perlakuan risiko dilakukan dengan mengacu pada standar ISO/IEC 27002:2013.

4.2. Kriteria dasar

Kriteria dasar digunakan sebagai acuan dalam melakukan proses manajemen risiko. Penetapan kriteria dasar penting dilakukan agar dapat memberikan hasil manajemen risiko yang sesuai dengan kondisi lokus. Kriteria dasar tersebut yaitu kriteria evaluasi risiko, kriteria dampak risiko, dan kriteria penerimaan risiko.

- Kriteria evaluasi risiko yang ditetapkan adalah sebagai berikut :
 - Nilai strategis dari proses bisnis layanan jaringan ABC.
 - Tingkat urgensi dari keterlibatan aset informasi yang dimiliki oleh organisasi.
 - Operasional dan kepentingan bisnis dari unsur kerahasiaan (*confidentiality*), ketersediaan (*availability*), dan integritas (*integrity*).
 - Persepsi dan harapan dari pemegang kepentingan (*stakeholder*)
 - Dampak negatif terhadap reputasi suatu organisasi
- Kriteria dampak risiko yang ditetapkan yaitu dampak ancaman, kemungkinan terjadinya ancaman, kemungkinan terjadinya dampak buruk dan penerimaan risiko. Kriteria-kriteria tersebut dapat dilihat pada Tabel 1, 2, 3, dan 4.

Tabel 1. Kriteria Dampak Ancaman

| No. | Nilai Kualitatif | Nilai Angka | Deskripsi NIST SP 800-30 Revisi 1 | Kriteria Dampak Ancaman |
|-----|------------------|-------------|--|---|
| 1. | Sangat Tinggi | 98-100 | Kejadian ancaman memiliki efek samping besar yang beragam dan ekstrem terhadap jalannya operasional organisasi, aset organisasi, secara individu, maupun terhadap organisasi lain atau negara. | <ul style="list-style-type: none"> Pencapaian target kinerja $\leq 25\%$ Proses bisnis tertunda lebih dari 24 jam Terdapat pemberitaan negatif di media massa internasional Terdapat kebocoran atau kehilangan data pada MKP Terdapat pelanggaran peraturan dan hukum berat dengan sanksi hukum Jumlah kerugian mencapai lebih dari Rp 500 Juta |
| 2. | Tinggi | 80-97 | Kejadian ancaman memiliki efek samping yang besar terhadap jalannya operasional organisasi, aset organisasi, secara individu, maupun terhadap organisasi lain atau negara. | <ul style="list-style-type: none"> Pencapaian target kinerja $> 25\%$ namun $< 50\%$ Proses bisnis tertunda selama 12-24 jam Adanya pemberitaan negatif di media massa nasional Terdapat kebocoran atau kehilangan data pada lingkup eselon 2 Terdapat pelanggaran peraturan atau hukum sedang dengan sanksi administratif Jumlah kerugian mencapai lebih dari Rp 100 Juta namun kurang Rp 500 Juta |
| 3. | Sedang | 21-79 | Kejadian ancaman memiliki efek samping yang sedang terhadap jalannya operasional organisasi, aset organisasi, secara individu, maupun terhadap organisasi lain atau negara. | <ul style="list-style-type: none"> Pencapaian target kinerja $> 50\%$ namun $< 80\%$ Proses bisnis tertunda selama 2-12 jam Terdapat pemberitaan negatif di media massa lokal Terdapat kebocoran atau kehilangan data di lingkup unit kerja eselon 3 Terdapat pelanggaran peraturan atau hukum ringan dengan surat peringatan Jumlah kerugian mencapai lebih dari Rp 50 Juta namun kurang dari Rp 100 Juta |
| 4. | Rendah | 5-20 | Kejadian ancaman memiliki efek samping yang rendah terhadap jalannya operasional organisasi, aset organisasi, secara individu, maupun terhadap organisasi lain atau negara. | <ul style="list-style-type: none"> Pencapaian target kinerja $> 80\%$ namun $< 100\%$ Proses bisnis tertunda selama 1-2 jam Terdapat keluhan dari pemangku kepentingan secara langsung atau tertulis > 3 kali dalam 1 tahun Terdapat kebocoran atau kehilangan data di lingkup unit kerja eselon 4 Terdapat pelanggaran peraturan atau hukum ringan dengan teguran Jumlah kerugian lebih dari Rp 10 Juta namun kurang dari Rp 50 Juta |
| 5. | Sangat Rendah | 0-4 | Kejadian ancaman memiliki efek samping yang sangat rendah terhadap jalannya operasional organisasi, aset organisasi, secara individu, maupun terhadap organisasi lain atau negara, sehingga dapat diabaikan. | <ul style="list-style-type: none"> Pencapaian target kinerja $\geq 100\%$ Proses bisnis tertunda ≤ 1 jam Terdapat keluhan dari pemangku kepentingan secara langsung atau tertulis sebanyak ≤ 3 kali dalam 1 tahun Jumlah kerugian yang dihasilkan \leq Rp 10 Juta Dampak kerugian yang dihasilkan sangat kecil sehingga dapat diabaikan |

Tabel 2. Kemungkinan Terjadinya Ancaman

| No. | Nilai Kualitatif | Nilai Angka | Deskripsi NIST SP 800-30 Revisi 1 | Kriteria Kemungkinan Terjadinya Ancaman |
|-----|------------------|-------------|--|--|
| 1. | Sangat Tinggi | 98-100 | Subjek hampir pasti menginisiasi kejadian ancaman. | Subjek hampir selalu memulai kejadian ancaman |
| 2. | Tinggi | 80-97 | Subjek sangat mungkin menginisiasi kejadian ancaman. | Subjek berpotensi tinggi memulai kejadian ancaman |
| 3. | Sedang | 21-79 | Subjek terkadang mungkin menginisiasi kejadian ancaman. | Subjek terkadang mungkin memulai kejadian ancaman |
| 4. | Rendah | 5-20 | Subjek tidak mungkin menginisiasi kejadian ancaman. | Subjek tidak mungkin memulai kejadian ancaman |
| 5. | Sangat Rendah | 0-4 | Subjek sangat tidak mungkin menginisiasi kejadian ancaman. | Subjek sangat tidak mungkin memulai kejadian ancaman |

Tabel 3. Kemungkinan Terjadinya Dampak Buruk

| No. | Nilai Kualitatif | Nilai Angka | Deskripsi NIST SP 800-30 Revisi 1 | Kriteria Kemungkinan Terjadinya Dampak Buruk |
|-----|------------------|-------------|--|---|
| 1. | Sangat Tinggi | 98-100 | Jika ancaman diinisiasi atau terjadi, hampir pasti menyebabkan dampak buruk. | Pasti menyebabkan dampak yang merugikan |
| 2. | Tinggi | 80-97 | Jika ancaman diinisiasi atau terjadi, sangat mungkin menyebabkan dampak buruk. | Sangat mungkin menyebabkan dampak yang merugikan |
| 3. | Sedang | 21-79 | Jika ancaman diinisiasi atau terjadi, terkadang mungkin menyebabkan dampak buruk. | Mungkin menyebabkan dampak yang merugikan |
| 4. | Rendah | 5-20 | Jika ancaman diinisiasi atau terjadi, tidak mungkin menyebabkan dampak buruk. | Kemungkinan kecil dapat menyebabkan dampak yang merugikan |
| 5. | Sangat Rendah | 0-4 | Jika ancaman diinisiasi atau terjadi, sangat tidak mungkin menyebabkan dampak buruk. | Sangat tidak mungkin menyebabkan dampak yang merugikan |

Tabel 4. Kriteria Penerimaan Risiko

| Persyaratan ISO/IEC 27005:2018 | Kriteria Penerimaan Risiko |
|---|---|
| 1. Mencakup beberapa batas penerimaan dengan target tingkat risiko yang diinginkan namun tetap mempertimbangkan ketentuan manajer senior. | 1. Risiko diterima jika tingkat risiko tidak memberi dampak signifikan atau tingkat dampak rendah |
| 2. Dapat dinyatakan sebagai rasio pendapatan yang diperkirakan terhadap risiko yang telah diperkirakan. | 2. Risiko diterima apabila pihak yang memiliki risiko dapat memastikan dengan tingkat keyakinan 90% bahwa tidak akan terjadi kegagalan pada sumber daya manusia, proses, maupun sistem yang ada |
| 3. Mencakup persyaratan untuk perlakuan tambahan selanjutnya. | |
| 4. Mempertimbangkan aspek hukum dan peraturan, kriteria bisnis, operasi, teknologi, finansial, faktor sosial dan faktor kemanusiaan | |

4.3. Penilaian Risiko

Pada tahap ini telah dilakukan penilaian terhadap risiko yang sudah diidentifikasi serta telah dilakukan evaluasi pada masing-masing skenario risiko dan didapatkan hasil sebagai berikut:

a. Identifikasi risiko

Tahap yang dilakukan pada identifikasi risiko yaitu identifikasi aset, ancaman, dan kontrol yang sudah ada kerentanannya. Hasil identifikasi risiko adalah sebagai berikut:

- Sebanyak 23 aset teridentifikasi yang terdiri dari 10 aset utama dan 13 aset pendukung.
- Berdasarkan hasil identifikasi sumber ancaman didapatkan 8 sumber termasuk *adversarial*, 10 sumber ancaman termasuk *non-adversarial*. Kemudian, hasil identifikasi menunjukkan bahwa terdapat 28 jenis ancaman dengan total sebanyak 59 ancaman. Sebanyak 14 kejadian ancaman dikategorikan *confirmed*, 4 kejadian ancaman dikategorikan *expected*, 14 kejadian ancaman dikategorikan *anticipated*, 6 kejadian ancaman dikategorikan *predicted*, 18 kejadian ancaman dikategorikan *possible*, dan 3 kejadian ancaman dikategorikan *N/A*
- Terdapat 28 jenis kontrol dengan total 63 kontrol yang sudah ada atau telah digunakan,

namun masih terdapat dua aset yang tidak memiliki kontrol.






- Sebanyak 23 jenis kerentanan yang telah teridentifikasi dengan total 48 kerentanan. Seluruh kerentanan bernilai SEDANG.

4.4. Analisis Risiko

Tahap analisis risiko dilakukan dengan mengolah hasil identifikasi dan kuisioner untuk mengetahui tingkat kemungkinan risiko yang didapat dari kombinasi nilai kualitatif kemungkinan terjadinya ancaman dan kemungkinan terjadinya ancaman yang memberikan dampak buruk menggunakan matriks kemungkinan risiko. Berdasarkan analisis menggunakan matriks kemungkinan risiko, didapatkan hasil 47 ancaman bernilai SEDANG dan 12 ancaman bernilai RENDAH. Selanjutnya hasil tersebut dikombinasikan dengan dampak kejadian ancaman menggunakan matriks selera risiko dan didapatkan daftar selera risiko dengan rincian 47 skenario risiko dimitigasi dan 12 lainnya diterima. Matriks-matriks yang digunakan pada penelitian dibuat berdasarkan NIST SP 800-30 Revisi 1. Matriks-matriks tersebut dapat dilihat pada Tabel 5 dan 6.

Tabel 5. Matriks Kemungkinan Risiko

| Kemungkinan Terjadinya Ancaman | Kemungkinan Terjadinya Ancaman Yang Memberikan Dampak Buruk | | | | |
|--------------------------------|---|---------------------|---------------------|---------------------|----------------------------|
| | Sangat Rendah ₁ | Rendah ₂ | Sedang ₃ | Tinggi ₄ | Sangat Tinggi ₅ |
| Sangat Tinggi ₁ | Sangat Rendah | Sedang | Tinggi | Sangat Tinggi | Sangat Tinggi |
| Tinggi ₂ | Sangat Rendah | Sedang | Sedang | Tinggi | Sangat Tinggi |
| Sedang ₃ | Sangat Rendah | Rendah | Sedang | Sedang | Tinggi |
| Rendah ₄ | Sangat Rendah | Rendah | Rendah | Sedang | Sedang |
| Sangat Rendah ₅ | Sangat Rendah | Sangat Rendah | Sangat Rendah | Rendah | Rendah |

-  : Sangat Tinggi (b₁₄, b₁₅, b₂₅) → berpotensi sangat tinggi mengancam pencapaian tujuan organisasi sehingga memiliki prioritas untuk direspon.
-  : Tinggi (b₁₃, b₂₄, b₃₅) → berpotensi tinggi mengancam pencapaian tujuan organisasi sehingga memiliki prioritas untuk direspon.
-  : Sedang (b₁₂, b₂₂, b₂₃, b₃₃, b₃₄, b₄₄, b₄₅) → berpotensi sedang mengancam pencapaian tujuan organisasi sehingga akan direspon setelah area b₁₄, b₁₅, b₁₃, b₂₄, b₃₅ berjalan.
-  : Rendah (b₃₂, b₄₂, b₄₃, b₅₄, b₅₅) → berpotensi rendah mengancam pencapaian tujuan organisasi sehingga dapat direspon jika ada sumber daya tersisa.
-  : Sangat Rendah (b₁₁, b₂₁, b₃₁, b₄₁, b₅₁, b₅₂, b₅₃) → berpotensi sangat rendah mengancam pencapaian tujuan organisasi sehingga dapat diabaikan.

Tabel 6. Matriks Selera Risiko

| Kemungkinan Terjadinya Ancaman | Kemungkinan Terjadinya Ancaman Yang Memberikan Dampak Buruk | | | | |
|--------------------------------|---|---------------------|---------------------|---------------------|----------------------------|
| | Sangat Rendah ₁ | Rendah ₂ | Sedang ₃ | Tinggi ₄ | Sangat Tinggi ₅ |
| Sangat Tinggi ₁ | Sangat Rendah | Sedang | Tinggi | Sangat Tinggi | Sangat Tinggi |
| Tinggi ₂ | Sangat Rendah | Sedang | Sedang | Tinggi | Sangat Tinggi |
| Sedang ₃ | Sangat Rendah | Rendah | Sedang | Sedang | Tinggi |
| Rendah ₄ | Sangat Rendah | Rendah | Rendah | Sedang | Sedang |
| Sangat Rendah ₅ | Sangat Rendah | Sangat Rendah | Sangat Rendah | Rendah | Rendah |

4.5. Evaluasi Risiko

Berdasarkan hasil analisis, didapatkan 47 skenario risiko yang dimitigasi dan diprioritaskan untuk diberikan perlakuan risiko pada tahap selanjutnya.

4.6. Perlakuan dan Penerimaan Risiko

Rekomendasi kontrol diberikan berdasarkan ISO/IEC 27002:2013 dan strategi perlakuan risiko. Tahap ini diawali dengan penentuan kriteria perlakuan risiko yang dapat dilihat pada Tabel 7. Kemudian, Ke-47 skenario yang telah ditentukan prioritasnya diberikan strategi perlakuan *modification* dan diberikan rekomendasi sebanyak 97 kontrol. Rekapitulasi klausul kontrol yang diberikan ditunjukkan pada Tabel 8. Selanjutnya ditentukan penanggung jawab pada masing-masing skenario sehingga didapatkan tiga pihak yang terlibat yaitu, bidang A sebanyak 32 skenario, Bidang B sebanyak 4 skenario, dan Bidang C sebanyak 27 skenario risiko.

5. KESIMPULAN

Berdasarkan hasil penelitian, dapat diambil kesimpulan sebagai berikut :

- Penanggung jawab manajemen risiko diampu oleh Kepala ABC. Pada tahap penetapan konteks ditetapkan instrumen kriteria sebagai dasar dalam melakukan perancangan manajemen risiko layanan jaringan ABC.

- Berdasarkan hasil identifikasi risiko, didapatkan sebanyak 23 aset layanan jaringan ABC yang terdiri dari 10 aset utama dan 13 aset pendukung. Dari 23 aset tersebut teridentifikasi sebanyak 59 ancaman yang disebabkan oleh 8 sumber ancaman *adversarial* dan 10 sumber ancaman *non-adversarial*. Aset-aset yang telah diidentifikasi tersebut memiliki 28 kontrol, namun masih terdapat 23 jenis kerentanan yang teridentifikasi. Dari 59 skenario risiko tersebut, sebanyak 47 skenario dinyatakan "Sedang", dan 12 skenario dinyatakan "Rendah". Hasil dari tingkat kemungkinan risiko tersebut dikombinasikan dengan dampak kejadian ancaman menggunakan matriks selera risiko, sehingga didapatkan 47 skenario "Dimitigasi" dan 12 skenario "Diterima".
- Pada tahap penentuan strategi perlakuan risiko, sebanyak 97 rekomendasi kontrol keamanan informasi diberikan untuk menangani risiko berdasarkan ISO/IEC 27002:2013 dengan 47 skenario mendapat strategi perlakuan *modification*.
- Pada tahap penerimaan risiko, ditentukan penanggung jawab kontrol untuk memastikan kontrol-kontrol tersebut dapat diterapkan dan dilakukan secara tepat sasaran. Terdapat tiga pihak yang terlibat dan bertanggung jawab dalam pengelolaan risiko yaitu Bidang A sebanyak 32 skenario, Bidang B sebanyak 4 skenario, dan Bidang C sebanyak 27 skenario.

Tabel 7. Kriteria Perlakuan Risiko

| No | Kriteria Perlakuan | Deskripsi ISO/IEC 27005:2018 | Kriteria Perlakuan Risiko |
|----|--------------------|--|--|
| 1 | Risk Modification | Risiko dihilangkan, dihilangkan atau mengubah kontrol sehingga risiko dapat diterima | <ul style="list-style-type: none"> Risiko diintervensi dengan melakukan upaya pengendalian yang dapat mengurangi tingkat risiko Pemilihan kontrol yang dilakukan tidak mengganggu proses bisnis yang sedang berjalan Manfaat yang didapatkan dalam pemilihan kontrol harus lebih besar daripada biaya yang dikeluarkan ABC memiliki sumber daya yang memadai untuk melakukan modifikasi risiko |
| 2 | Risk Retention | Risiko diputuskan untuk diterima tanpa adanya suatu aksi apapun tergantung pada hasil evaluasi risiko | <ul style="list-style-type: none"> Risiko dipertahankan dan tidak melakukan intervensi apapun terhadap risiko Selera risiko memiliki tingkat residual risiko yang rendah dan terdiri dari tingkat dampak rendah serta peluang yang rendah Tidak ada alternatif |
| 3 | Risk Avoidance | Kondisi ketika risiko harus dihindari | <ul style="list-style-type: none"> Risiko dihindari dengan tidak melakukan kegiatan apapun yang terkait Political will |
| 4 | Risk Sharing | Risiko dibagi dengan pihak lain sehingga dapat lebih efektif dalam manajemen risiko tersebut tergantung pada hasil evaluasi risiko | <ul style="list-style-type: none"> Risiko didistribusikan kepada pihak lain Residual risiko memiliki nilai dampak dengan tingkat yang tidak dapat diterima sesuai penerimaan risiko ABC tidak memiliki sumberdaya yang memadai dalam melakukan modifikasi/mitigasi risiko |

Tabel 8. Rekapitulasi Hasil Rekomendasi

| No | Klausul | Kategori | Kontrol | Jumlah Rekomendasi |
|----|--|--|--|--------------------|
| 1 | 7 Human Resource security | 7.2 During Employment | 7.2.1 Management responsibilities | 1 |
| | | | 7.2.2 Information security awareness, education and training | 1 |
| | | | 7.2.3 Disciplinary process | 3 |
| 2 | 8 Aset Management | 8.2 Information Classification | 8.2.2 Labelling of information | 1 |
| | | | 8.2.3 Handling of assets | 1 |
| 3 | 9 Access Control | 9.1 Business Requirements of Access Control | 9.1.2 Access to networks and network services | 1 |
| | | 9.2 User Access Management | 9.2.3 Management of privileged access rights | 5 |
| | | 9.4 System and Application Access Control | 9.4.1 Information access restriction | 3 |
| | | | 9.4.2 Secure log-on procedures | 6 |
| | | | 9.4.3 Password management system | 10 |
| 4 | 10 Cryptography | 10.1 Cryptographic Control | 10.1.1 Policy on the use of cryptographic controls | 1 |
| 5 | 11 Physical and Environmental Security | 11.1 Secure Areas | 11.1.2 Physical entry controls | 3 |
| | | | 11.1.3 Securing offices, rooms and facilities | 1 |
| | | 11.2 Equipment | 11.2.1 Equipment siting and protection | 1 |
| | | | 11.2.2 Supporting utilities | 2 |
| | | | 11.2.3 Cabling security | 1 |
| | | | 11.2.4 Equipment maintenance | 6 |
| | | | 11.2.9 Clear desk and clear screen policy | 2 |
| 6 | 12 Operations Security | 12.1 Operational procedures and responsibilities | 12.1.1 Documented operating procedures | 10 |
| | | 12.2 Protection from malware | 12.2.1 Controls against malware | 7 |
| | | 12.3 Backup | 12.3.1 Information backup | 3 |
| | | 12.4 Logging and monitoring | 12.4.1 Event logging | 2 |
| | | | 12.4.2 Protection of log information | 1 |
| | | 12.5 Control of operational software | 12.5.1 Installation of software on operational systems | 4 |
| 7 | 13 Communications security | 13.1 Network security management | 13.1.1 Network controls | 4 |
| | | | 13.1.2 Security of network services | 2 |
| 8 | 14 System acquisition, development and maintenance | 14.2 Security in development and support processes | 14.2.8 System security testing | 5 |
| 9 | 16 Information security incident management | 16.1 Management of information security incidents and improvements | 16.1.1 Responsibilities and procedures | 3 |
| 10 | 18 Compliance | 18.1 Compliance with legal and contractual requirements | 18.1.3 Protection of records | 2 |
| | | 18.2 Information security reviews | 18.2.3 Technical compliance review | 5 |

REFERENSI

- [1] R. E. Indrajit, *Pengantar Konsep Keamanan Informasi di Dunia Siber*. Jakarta: APTIKOM, 2011.
- [2] MKP, Keputusan Kepala MKP Nomor 571.1 Tahun 2018 Tentang Peta Proses Bisnis MKP. 2018, p. 97.
- [3] Kepala Bidang C, "Katalog Layanan (*Service Catalogue*) ABC Versi 0.0." ABC, Sep. 2019.
- [4] MKP, Peraturan MKP Nomor 2 Tahun 2018 Tentang Organisasi dan Tata Kerja MKP. 2018, p. 89.
- [5] ISO/IEC, "ISO/IEC 27005: 2018 Information Technology-Security Techniques-Information Security Risk Management." ISO/IEC, 2018.
- [6] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-30r1.
- [7] H. Setiawan, F. A. Putra, and A. R. Pradana, "Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute," presented at the International

- Conference on Information Technology Systems and Innovation (ICITSI), Bandung, 2017.
- [8] I. R. Lestari, "Perencanaan Manajemen Risiko Keamanan Informasi Layanan Mail MKP pada ABC Berdasarkan Kerangka Kerja ISO/IEC 27005:2011," *Sekolah Tinggi Sandi Negara*, p. 158, 2019.
- [9] ISO/IEC, "ISO/IEC 27002:2013 Information Technology - Security Techniques - Code of Practice for Information Security Controls." 2013.
- [10] MKP, Pedoman Kepala MKP Nomor 2 Tahun 2019 tentang Pelaksanaan Pengendalian Intern Pemerintah MKP. 2019, p. 43.
- [11] F. A. Putra, "Perancangan Manajemen Risiko Keamanan Informasi Menggunakan Framework ISO/IEC 27005:2011 pada Sistem Jaring Komunikasi Berita (Jarkombra) Dinas Komunikasi dan Elektronika TNI Angkatan Laut," *Sekolah Tinggi Sandi Negara*, p. 280, 2017.