MANAJEMEN RISIKO KEAMANAN INFORMASI DALAM MEMINIMALISASI ANCAMAN SIBER PADA PUSAT DATA DAN TEKNOLOGI INFORMASI KOMUNIKASI BADAN SIBER DAN SANDI NEGARA GUNA MENINGKATKAN PERTAHANAN DAN KEAMANAN SIBER

INFORMATION SECURITY RISK MANAGEMENT IN MINIMIZING CYBER THREATS AT THE DATA CENTER AND COMMUNICATION INFORMATION TECHNOLOGY OF THE NATIONAL CYBER AND CRYPTO AGENCY TO IMPROVE CYBER DEFENSE AND SECURITY

Jefferson Benyamin[1], Much Mualim[2], Editha Praditya Duarte[3]

PRODI MANAJEMEN PERTAHANAN, FAKULTAS MANAJEMEN PERTAHANAN,
UNIVERSITAS PERTAHANAN REPUBLIK INDONESIA[123]

Email: jeffersonbenyamin@gmail.com[1], mualimdrt@gmail.com[2],
editha.duarte@yahoo.com[3]

Abstrak - Ancaman siber sekarang sudah sangat meresahkan semua pihak. Ancaman siber perlu diantisipasi agar tidak menimbulkan dampak buruk bagi kelangsungan proses bisnis suatu organisasi. Pusat Data dan Teknologi Informasi Komunikasi (Pusdatik) Badan Siber dan Sandi Negara (BSSN) mempunyai tugas perencanaan, pelaksanaan, evaluasi, dan pelaporan di bidang data dan teknologi informasi komunikasi. Kondisi saat ini penerapan manajemen risiko Pusdatik BSSN masih belum optimal dikarenakan aturan maupun pedoman yang ada saat ini masih minim, adanya insiden yang pernah terjadi seperti salah prosedur maintenance UPS, serta adanya insiden yang terjadi pada website JDIH disebabkan serangan siber. Oleh karena itu, diperlukan manajemen risiko yang baik terhadap aset dan layanan Pusdatik BSSN untuk meminimalisasi ancaman siber. Tujuan penelitian ini adalah untuk mengidentifikasi risiko, menganalisis risiko, serta merencanakan penanganan dan penerimaan risiko dalam meminimalisasi ancaman siber pada Pusdatik BSSN. Penelitian ini menggunakan metode analitis kualitatif dengan pendekatan ISO/IEC 27005 dan NIST 800-30 Revisi 1. Berdasarkan hasil penelitian, didapatkan bahwa 14 aset teridentifikasi sebanyak 13 potensi ancaman, serta terdapat 27 skenario risiko, dimana 14 skenario risiko dapat diterima dan 13 skenario risiko harus dimitigasi. Pada tahap penanganan risiko dan penerimaan risiko, 13 skenario risiko yang dimitigasi diberikan strategi penanganan risiko modifikasi dan 36 rekomendasi kontrol, serta terdapat tiga pihak yang terlibat dan bertangung jawab dalam pengelolaan risiko yaitu Bidang Manajemen Risiko dan Kelangsungan TIK, Bidang Infrastruktur, dan Vendor. Hasil dari penelitian ini adalah dokumen manajemen risiko keamanan informasi yang disertakan dengan rekomendasi kontrol keamanan informasi.
Kata Kunci: Ancaman Siber, ISO/IEC 27005, Manajemen Risiko, NIST 800-30 Revisi 1, Pusat Data dan Teknologi Informasi Komunikasi Badan Siber dan Sandi Negara

Abstract- *Cyber threats are now very troubling to all parties. Cyber threats need to be anticipated so that they do not have a negative impact on the continuity of an organization's business processes. The Center for Data and Communication Information Technology (Pusdatik) of the National Cyber and Crypto Agency (BSSN) has the task of planning, implementing, evaluating, and reporting in the field of data and communication information technology. The current condition of Pusdatik BSSN's risk management implementation is still not optimal due to the current rules and guidelines that are still minimal, the incidents that have occurred such as the wrong UPS maintenance procedures, and the incidents that occurred on the JDIH website due to cyber attacks. Therefore, good risk management is needed for the assets and services of Pusdatik BSSN to minimize cyber threats. The purpose of this research is to identify risks, analyze risks, and plan risk handling and acceptance in minimizing cyber*

threats at Pusdatik BSSN. This research uses a qualitative analytical method with the ISO/IEC 27005 and NIST 800-30 Revision 1 approaches. Based on the results of the study, it was found that 14 assets were identified as many as 13 potential threats, and there were 27 risk scenarios, where 14 risk scenarios were acceptable and 13 risk scenarios had to be mitigated. In the risk management and risk acceptance stage, 13 mitigated risk scenarios are given modified risk handling strategies and 36 control recommendations, and there are three parties involved and responsible for risk management, namely the ICT Risk Management and Continuity Division, the Infrastructure Division, and Vendors. The result of this research is an information security risk management document that is included with information security control recommendations.
Keywords: *Cyber Threats, Data Center and Communication Information Technology of the National Cyber and Crypto Agency, ISO/IEC 27005, NIST 800-30 Revision 1, Risk Management*

PENDAHULUAN

Teknologi informasi dan komunikasi, atau disingkat TIK, saat ini telah menjadi bagian dalam setiap aspek kehidupan masyarakat, baik dalam aspek ekonomi, sosial, budaya, pendidikan, dan kesehatan. Sektor TIK di Indonesia berkembang dengan sangat pesat, terutama dalam hal penggunaan internet. Pada kuartal kedua tahun 2020, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) memperkirakan 196,7 juta orang, atau 73,7 persen, dari populasi Indonesia akan menggunakan internet (Asosiasi Penyelenggara Jasa Internet Indonesia, 2020).

Jika dibandingkan dengan tahun 2018, angka ini naik 64,8%. Di satu sisi, meningkatnya kemampuan masyarakat untuk beradaptasi dengan kemajuan teknologi didukung oleh peningkatan pengguna internet. Namun, meningkatnya jumlah pengguna yang masih awam dengan keamanan siber juga meningkatkan risiko keamanan.

Pelaku kejahatan siber telah tertarik dengan peningkatan lalu lintas internet, yang menyebabkan banyaknya serangan siber di Indonesia. Menurut Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber pada tahun 2020 mencapai 495,3 juta, naik 41% dari tahun 2019 yang mencapai 290,3 juta (Badan Siber dan Sandi Negara, 2021).

Serangan siber adalah upaya untuk menguasai atau mendapatkan akses tidak sah ke sistem komputer atau jaringan komputer (Marshall & Saulawa, 2015). Sebaliknya, kejahatan siber adalah aktivitas ilegal yang memanfaatkan atau menargetkan jaringan atau sistem komputer (International Telecommunication Union, 2012). Menurut pernyataan yang berbeda, istilah "*cybercrime*" mengacu pada tindakan kriminal yang menggunakan komputer atau jaringan komputer sebagai alat, target, atau lokasi dan menimbulkan kerugian materiil maupun imateriil bagi pihak-pihak yang menjadi sasaran (Wilson, 2008).

Menurut laporan data anomali trafik BSSN, terdapat 495,3 juta serangan siber di Indonesia pada tahun 2020, meningkat 41% dari tahun sebelumnya yang berjumlah 290,3 juta (Badan Siber dan Sandi Negara, 2021). Dengan total 7.311.606 anomali, tanggal 10 Desember 2020 merupakan tanggal dengan anomali trafik terbanyak. Anomali dengan jumlah tertinggi adalah Trojan. Selama tahun 2020, negara dengan

jumlah serangan anomali terbanyak adalah Amerika Serikat, dan Indonesia juga menjadi negara dengan jumlah serangan anomali terbanyak yang berasal dari Indonesia sendiri (dengan alamat IP Indonesia). Laporan tersebut juga menemukan sebanyak 2.549 kasus email phishing, dengan peningkatan jumlah kasus email phishing pada bulan Maret sampai Mei 2020.

Ancaman cyber atau ancaman terhadap keamanan data di komputer sangat meresahkan semua pihak saat ini. Ketika berbicara tentang keamanan data dan informasi, tidak ada institusi atau organisasi yang dikecualikan. Tentu saja, hal ini membutuhkan banyak penelitian dan perhatian untuk mengukur daya tahan dan keamanan data komputer organisasi. Perlindungan data di komputer menjadi topik yang semakin populer di seluruh dunia. Hal ini tidak hanya berdampak negatif dalam bentuk malware atau virus, tetapi juga dapat berakibat fatal, seperti terbongkarnya rahasia negara dan lumpuhnya lembaga- lembaga penting negara (Czosseck, C. et al, 2013).

Menyusul terjadinya kebocoran data di sejumlah instansi, kasus kebocoran data akhir-akhir ini menjadi perhatian. Insiden kebocoran data yang pernah terjadi di Indonesia adalah sebagai berikut (Clinten, 2022): kebocoran data pengguna aplikasi e-HAC Kementerian Kesehatan, kebocoran data BPJS kesehatan, kebocoran data nasabah BRI Life, kebocoran data Daftar Pemilih Tetap (DPT) Pemilu KPU, kebocoran data pengguna Tokopedia, dan kebocoran data 26 juta riwayat pengguna IndiHome. Berdasarkan kasus kebocoran data tersebut diatas, maka pemanfaatan TI secara optimal menjadi hal yang penting dalam pelaksanaan Sistem Pemerintahan Berbasis Elektronik (SPBE) di instansi pemerintahan. Sesuai dengan Peraturan Presiden No. 95 Tahun 2018, SPBE adalah penyelenggaraan pemerintahan yang memberikan layanan kepada pengguna SPBE melalui pemanfaatan teknologi informasi dan komunikasi. Ketika instansi pemerintah menggunakan TI untuk mengimplementasikan SPBE, mereka harus mempertimbangkan keterbatasan sumber daya seperti data, teknologi, fasilitas, dan sumber daya manusia, serta fakta bahwa TI relatif mahal untuk digunakan. Kebutuhan akan tata kelola TI untuk mengendalikan bagaimana TI digunakan dalam organisasi pemerintah tumbuh sebagai akibat dari sumber daya yang terbatas.

Berdasarkan Peraturan Presiden No. 95 Tahun 2018, implementasi SPBE instansi pemerintah harus dipantau dan dievaluasi untuk mengukur dan meningkatkan kualitasnya. Menurut peraturan di atas, maka semua instansi pemerintahan yang memanfaatkan penggunaan TI dalam proses bisnisnya memiliki kewajiban untuk melakukan evaluasi pemanfaatan TI dalam pelaksanaan SPBE.

Salah satu kementerian di Indonesia yang memiliki urgensi untuk melakukan evaluasi pelaksanaan SPBE ialah Badan Siber dan Sandi Negara (BSSN). Sesuai dengan Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara, BSSN mempunyai tugas menyelenggarakan urusan pemerintahan di bidang keamanan siber dan persandian untuk membantu

Presiden dalam menyelenggarakan pemerintahan negara.

Sebagai bagian dari tanggung jawab utamanya, BSSN menyediakan sejumlah layanan publik elektronik dan aplikasi berbasis internet, seperti: Sistem Informasi Perencanaan dan Akuntabilitas Kinerja (SIPAK), Jaringan Dokumentasi dan Informasi Hukum (JDIH), Absensi Elektronis, Sistem Informasi Kepegawaian (SIMPEG), *Email, Website,* Portal, *Secure Electronic Document Management System* (SEDMS), dan Sistem Informasi Manajemen Aset (SIMAS). Pusat Data dan Teknologi Informasi dan Komunikasi (Pusdatik) bertanggung jawab untuk mengelola seluruh data dari aplikasi-aplikasi yang ada di BSSN secara terpusat.

Berdasarkan Peraturan Kepala BSSN No. 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN, Pusdatik merupakan unsur pendukung tugas dan fungsi BSSN yang berada di bawah dan bertanggung jawab kepada Kepala melalui Sekretaris Utama. Perencanaan, pelaksanaan, evaluasi, dan pelaporan teknologi informasi dan komunikasi menjadi tanggung jawab Pusdatik

Pelaksanaan manajemen risiko keamanan informasi pada Pusat Data dan Pusdatik tentunya dibutuhkan dalam rangka mengidentifikasi, menilai, dan mengatasi risiko-risiko yang mungkin terjadi pada saat melakukan kegiatan operasional. Organisasi yang tidak memiliki prosedur manajemen risiko sendiri dapat mengacu pada standar nasional atau internasional yang ada dalam pedoman penerapan tata kelola keamanan informasi untuk penyedia layanan publik (Tim Direktorat Keamanan Informasi, 2011). Kondisi Pusdatik saat ini didasarkan pada hasil observasi awal yang telah dilakukan yaitu masih belum memiliki sertifikasi ISO/IEC 27001, belum memiliki dokumen prosedur mitigasi serangan siber yang baku, serta personil yang ada di Pusdatik masih belum bekerja secara optimal dikarenakan aturan maupun pedoman terkait tata kelola TIK yang ada saat ini sangat minim sehingga menyebabkan hasil kinerja personil belum maksimal.

Kemudian adanya insiden yang pernah terjadi seperti salah prosedur maintenance UPS dikarenakan kecerobohan personil Pusdatik sehingga menyebabkan layanan yang ada di Pusdatik berjalan tidak optimal serta insiden yang terjadi pada website JDIH yang terkena serangan siber, seperti serangan DDos yang dilakukan oleh pihak yang tidak berkepentingan sehingga website tidak dapat diakses oleh masyarakat dan pegawai BSSN, serta berdampak pada data center yang harus dimatikan dan menyebabkan proses bisnis Pusdatik berjalan belum optimal.

Berdasarkan kondisi saat ini yang telah dijelasakan diatas, maka diperlukan manajemen risiko keamanan informasi yang baik untuk keberlangsungan proses bisnis Pusdatik. Manajemen risiko perlu dilakukan agar dapat mengetahui dan menangani risiko yang memungkinkan terjadi terhadap sistem yang ada di Pusdatik.

Manajemen risiko secara umum terdiri dari beberapa tahap yaitu tahap analisis/penilaian risiko, penyusunan tindakan mitigasi, dan kontrol pelaksanaan strategi mitigasi yang telah disusun sebelumnya. Tujuan dari manajemen risiko

keamanan informasi adalah untuk mengetahui seberapa besar dampak atau risiko yang dihadapi organisasi jika terjadi kegagalan keamanan informasi dan menemukan cara untuk mengelola risiko tersebut (Sarno & Iffano, 2009).

Penelitian ini menggunakan kerangka kerja ISO/IEC 27005 yang dilengkapi pada tahap penilaian risiko oleh NIST SP 800-30 revisi 1. Di mana tahap penentuan konteks, penilaian risiko, perlakuan risiko, dan penerimaan risiko pada ISO/IEC 27005 adalah tahap manajemen risiko. Tahap pemantauan dan tinjauan risiko tidak dilakukan karena melibatkan penerapan hasil manajemen risiko oleh pihak Pusdatik dan keterbatasan waktu penelitian.

Prosedur manajemen risiko keamanan informasi ISO/IEC 27005 dapat digunakan baik untuk aspek yang baru maupun yang sudah ada, serta organisasi secara keseluruhan. Gambaran umum proses manajemen risiko keamanan informasi disediakan dalam ISO/IEC 27005, dengan referensi ke ISO/IEC 27001 dan ISO/IEC 27002. ISO/IEC 27005 dirancang untuk membantu penerapan keamanan informasi berdasarkan pendekatan manajemen risiko dan mendukung konsep umum yang didefinisikan dalam ISO/IEC 27001 (ISO/IEC, 2018).

Peneliti tertarik untuk menyelidiki manajemen risiko keamanan informasi di Pusdatik BSSN sehubungan dengan masalah-masalah yang disebutkan di atas. Hasil yang diharapkan dari penelitian ini adalah rekomendasi untuk meningkatkan efisiensi proses bisnis Pusdatik BSSN.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah kualitatif melalui pendekatan deskriptif analisis. Metode ini memiliki tujuan utamanya adalah untuk memberikan gambaran dengan menggunakan kata-kata dan angka serta untuk menyajikan profil (persoalan), klasifikasi jenis, atau garis besar tahapan guna menjawab pertanyaan seperti siapa, kapan, dimana, dan bagaimana (Neuman, 2014) dan bukan hanya digunakan untuk mencari jawaban dari pertanyaan 'bagaimana', tetapi juga 'mengapa' dari topik yang diangkat melalui informasi acak yang dijadikan sebagai data, seperti transkrip dan rekaman wawancara, email, video, gambar, dan catatan. Pendekatan kualitatif juga menyediakan pemaparan komprehensif terkait apa yang menjadi kesenjangan dari das sein dan das sollen yang timbul pada objek penelitian berdasarkan teori dan data yang diperoleh di lapangan. Untuk memperoleh data yang absah dilakukan uji kredibilitas dengan cara triangulasi data, sumber dan metode.

HASIL DAN PEMBAHASAN

Penelitian terkait Manajemen Risiko Keamanan Informasi Dalam Meminimalisasi Ancaman Siber pada Pusat Data dan Teknologi Informasi Komunikasi dalam Meningkatkan Pertahanan dan Keamanan Siber ini dilakukan dengan metode pengumpulan data melalui kegiatan wawancara, observasi, dan studi dokumen. Peneliti melakukan wawancara kepada sejumlah informan dari Pusdatik BSSN. Selain itu, pengumpulan data dilakukan dengan observasi langsung dengan mengunjungi lokasi Pusdatik BSSN.

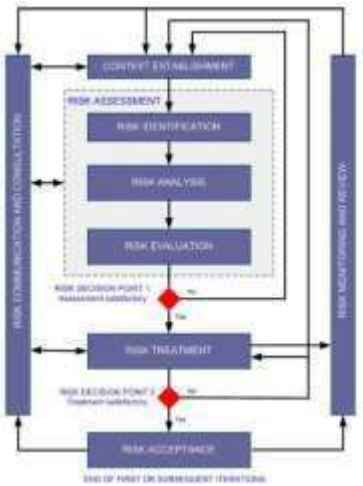
Peneliti juga mengumpulkan dokumentasi pada saat proses wawancara dan observasi berlangsung. Berikut adalah hasil pengumpulan data melalui wawancara, observasi, dan studi dokumen yang telah dilakukan.

Identifikasi Risiko pada Pusat Data dan Teknologi Informasi Komunikasi BSSN Dalam Meminimalisasi Ancaman Siber

Risiko merupakan peluang terjadinya suatu ancaman yang dapat memberikan dampak atau mengakibatkan proses bisnis dari suatu organisasi menjadi terganggu sehingga menyebabkan kegagalan organisasi dalam mencapai visi dan misinya (Sarno & Iffano, 2009). Risiko berhubungan dengan ketidakpastian, ini terjadi karena kurang atau tidak tersedianya cukup informasi tentang apa yang akan terjadi. Sesuatu yang tidak pasti dapat berakibat menguntungkan atau merugikan (Nuriah, Rois, & Risnaeni, 2021).

Peraturan Menteri Komunikasi dan Informatika Nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI) menyatakan bahwa penyelenggara sistem elektronik wajib menerapkan manajemen pengamanan informasi berdasarkan asas risiko. Teori/standar ISO/IEC 27005:2018 merupakan pedoman manajemen risiko keamanan informasi pada organisasi dan dirancang untuk membantu pelaksanaan proses keamanan informasi berdasarkan pendekatan manajemen risiko pada aset teknologi informasi (ISO/IEC, 2018). Standar ini dapat diimplementasikan untuk setiap jenis organisasi, seperti instansi pemerintah maupun organisasi nonprofit yang ingin mengelola risiko terhadap keamanan informasi pada organisasinya.

Peneliti memandang bahwa Pusdatik telah menerapkan manajemen risiko namun masih belum optimal mulai dari tahap identifikasi risiko, analisis risiko, serta penanganan dan penerimaan risko dalam kegiatan operasional sesuai dengan teori/standar ISO/IEC 27005:2018 yang diilustrasikan sesuai dengan gambar berikut ini:



Gambar 1 Proses Manajemen Risiko ISO/IEC 27005

Sumber: (ISO/IEC 27005,2018)

Proses ini menjadi landasan Peneliti dalam menemukan jawaban atas persoalan manajemen risiko keamanan informasi dalam meminimalisasi ancaman siber pada Pusdatik BSSN. Peneliti mengidentifikasi risiko-risiko yang mungkin dihadapi dan dapat menghambat keberlangsungan kegiatan operasional di Pusdatik BSSN. Tahapan identifikasi risiko yang dilakukan yaitu dengan melakukan identifikasi aset, identifikasi ancaman, identifikasi kontrol yang sudah ada/pernah dilakukan, dan identifikasi kerentanan pada aset di Pusdatik.

Berdasarkan hasil analisis dapat dinyatakan bahwa penerapan manajemen risiko yang ada di Pusdatik masih belum optimal dikarenakan masih terdapat 13 jenis peristiwa ancaman pada aset Pusdatik. Berikut ini merupakan 13 jenis peristiwa ancaman pada aset Pusdatik yaitu:

1) Penyalahgunaan hak (Contoh: penyalahgunaan komputer, akses PC yang tidak sah)
2) Terjadinya kerusakan/kehilangan data (Contoh: file berkas yang tersimpan rusak/hilang, terdapat virus pada PC)
3) Server tidak bisa diakses (Contoh: server tidak tersambung/terdapat gangguan koneksi, server mati)
4) Layanan tidak berjalan (Contoh: UPS tidak aktif/berfungsi saat terjadi pemadaman listrik)
5) Terjadi kegagalan konfigurasi
6) Terjadi kesalahan saat set-up jaringan
7) Peretasan (Contoh: adanya pihak yang tidak berhak masuk ke dalam jaringan, informasi dicuri/dimodifikasi).
8) Koneksi ke perangkat mengalami gangguan (Contoh: terputusnya koneksi LAN, akses jaringan tidak berfungsi, adanya perangkat jaringan rusak)
9) Manipulasi Data (Contoh: laporan diubah/tidak sesuai dengan kondisi sebenarnya)
10) Penyalahgunaan otoritas (Contoh: proses tidak sesuai prosedur/juknis, menyalahgunakan komputer, mengubah sistem secara tidak sah)
11) Terdapat laporan yang salah/tidak tercatat (Contoh: kesalahan mencatat laporan masuk/keluar)
12) Pelanggaran ketersediaan Personel (Contoh: personel tidak bertugas sesuai prosedur seperti adanya panggilan pimpinan/terdapat tugas di luar tupoksinya)
13) Adanya permasalahan dalam pengoperasian perangkat dan aplikasi (Contoh: terdapat bug yang menyebabkan aplikasi error/tidak berfungsi)

Kemudian masih terdapat beberapa kerentanan/kelemahan yang ada pada aset Pusdatik walaupun sudah terdapat kontrol yang sudah dilakukan. Berikut merupakan aset Pusdatik yang masih terdapat kerentanan yaitu:

1) Tidak digunakan sistem login dengan password pada beberapa PC/Desktop
2) Penggunaan default password/password lemah pada database server, router, aplikasi Zimbra, dan firewall yang ada di Pusdatik
3) Tidak melakukan update OS windows secara berkala
4) Tidak melakukan update antivirus secara berkala
5) Kurangnya security awareness

Oleh sebab itu, perlunya dokumen dan penerapan manajemen risiko yang baik di Pusdatik agar potensi risiko/ancaman yang ada saat ini dapat diminimalisasi supaya tidak menimbulkan dampak buruk terhadap kelangsungan proses bisnis Pusdatik.

Analisis Risiko pada Pusat Data dan Teknologi Informasi Komunikasi BSSN Dalam Meminimalisasi Ancaman Siber

Analisis Risiko adalah kegiatan menentukan tingkat kemungkinan /frekuensi terjadinya risiko serta tingkat dampaknya terhadap pencapaian tujuan/sasaran dengan mempertimbangkan aktivitas pengendalian yang sudah dilakukan. Tingkat kemungkinan/frekuensi terjadinya risiko dan tingkat konsekuensi/dampaknya terhadap pencapaian tujuan/sasaran selanjutnya dikombinasikan mendapatkan suatu tingkat risiko yang diestimasi.

Berdasarkan teori/standar ISO/IEC 27005:2018, terdapat lima tingkatan dampak dan peluang, dikarenakan tingkatan dampak dan peluang yang dianalisis pada penelitian ini memiliki lima tingkatan, oleh karena itu proses analisis risiko menggunakan teori/standar NIST SP 800-30 revisi 1. Teori/standar NIST SP 800-30 revisi 1 digunakan di dalam kerangka kerja ISO/IEC 27005:2018. Hal ini dikarenakan pada NIST SP 800-30 revisi 1 memberikan panduan dan identifikasi yang rinci dalam penilaian risiko keamanan informasi (Prasetyo, 2014).

Berdasarkan hasil analisis dapat dinyatakan bahwa analisis risiko menggunakan matriks kemungkinan risiko, didapatkan sebanyak 15 ancaman berada di tingkat kemungkinan risiko yang RENDAH dan 12 ancaman berada di tingkat kemungkinan risiko yang SEDANG. Berikut daftar tingkat kemungkinan risiko yang rendah dan sedang tertera pada tabel 1 dan tabel 2.

Tabel 1 Daftar Tingkat Kemungkinan Risiko yang Rendah

No	Skenario Risiko (Aset – Peristiwa Ancaman)
1	Laporan Insiden dan Monitoring Keamanan Jaringan - Terjadinya kerusakan/kehilangan data
2	Laporan Insiden dan Monitoring Keamanan Jaringan - Manipulasi Data
3	UPS - Layanan tidak berjalan
4	*Router* - Penyalahgunaan hak
5	*Router* - Layanan tidak berjalan
6	*Switch* - Penyalahgunaan hak
7	*Switch* - Layanan tidak berjalan
8	Aplikasi Zimbra - Penyalahgunaan hak
9	Aplikasi Zimbra - Layanan tidak berjalan
10	Aplikasi Zimbra - Terjadi permasalahan dalam pengoperasian perangkat dan aplikasi
11	Administrator Aplikasi dan Jaringan - Penyalahgunaan otoritas
12	Operator - Terdapat laporan yang salah/tidak tercatat
13	Operator - Pelanggaran ketersediaan Personel
14	Personel Pusdatik - Penyalahgunaan otoritas
15	Personel Pusdatik - Pelanggaran ketersediaan Personel

Sumber: Diolah oleh Peneliti (2022)

Tabel 2 Daftar Tingkat Kemungkinan Risiko yang Sedang

No	Skenario Risiko (Aset – Peristiwa Ancaman)
1	Layanan Wifi Internal dan Publik - Peretasan
2	Layanan Wifi Internal dan Publik - Koneksi ke perangkat mengalami gangguan
3	Layanan Konfigurasi Jaringan – Terjadi kegagalan konfigurasi
4	Layanan Konfigurasi Jaringan – Terjadi kesalahan saat *set-up* jaringan
5	PC/Desktop – Penyalahgunaan hak
6	PC/Desktop – Terjadinya kerusakan /Kehilangan data

7	Database Server – Penyalahgunaan hak
8	Database Server – Terjadinya kerusakan / kehilangan data
9	Database Server – Server tidak bisa diakses
10	Antivirus – Terjadinya kerusakan /kehilangan data
11	Firewall - Penyalahgunaan hak
12	Firewall - Layanan tidak berjalan

Sumber: Diolah oleh Peneliti (2022)

Selanjutnya analisis risiko menggunakan matriks tingkat risiko untuk mengetahui tingkat risiko dari masing-masing skenario risiko. Tingkat risiko tersebut didapatkan dengan cara mengombinasi nilai kualitatif tingkat kemungkinan risiko dengan nilai kualitatif dampak kejadian ancaman sehingga didapatkan hasil tingkat risiko. Hasil analisis didapatkan ada 13 skenario risiko yang harus DIMITIGASI dan 14 skenario risiko dapat DITERIMA. Berikut tingkat risiko masing-masing skenario risiko yang harus dimitigasi dan diterima tertera pada tabel 3 dan tabel 4.

Tabel 3 Tingkat Risiko dari Skenario Risiko yang Dapat Diterima

No	Skenario Risiko (Aset – Peristiwa Ancaman)
1	Layanan Wifi Internal dan PubliK - Peretasan
2	Layanan Wifi Internal dan Publik - Koneksi ke perangkat mengalami gangguan
3	Layanan Konfigurasi Jaringan - Terjadi kegagalan konfigurasi
4	Layanan Konfigurasi Jaringan - Terjadi kesalahan saat set-up jaringan
5	PC/Desktop - Penyalahgunaan hak
6	PC/Desktop - Terjadinya kerusakan/kehilangan data
7	Database Server - Penyalahgunaan hak
8	Database Server - Terjadinya kerusakan/kehilangan data
9	Database Server - *Server* tidak bisa diakses
10	UPS - Layanan tidak berjalan
11	Antivirus - Terjadinya kerusakan/kehilangan data
12	*Firewall* - Penyalahgunaan hak
13	*Firewall* - Layanan tidak berjalan

Sumber: Diolah oleh Peneliti (2022)

Tabel 4 Tingkat Risiko dari Skenario Risiko yang Dapat Diterima

No	Skenario Risiko (Aset – Peristiwa Ancaman)
1	Laporan Insiden dan Monitoring Keamanan Jaringan - Terjadinya kerusakan/kehilangan data
2	Laporan Insiden dan Monitoring Keamanan Jaringan - Manipulasi Data
3	*Router* - Penyalahgunaan hak
4	*Router* - Layanan tidak berjalan
5	*Switch* - Penyalahgunaan hak
6	*Switch* - Layanan tidak berjalan
7	Aplikasi Zimbra - Penyalahgunaan hak
8	Aplikasi Zimbra - Layanan tidak berjalan
9	AplikasI Zimbra – Terjadi permasalahan dalam pengoperasian perangkat dan aplikasi
10	Administrator Aplikasi dan Jaringan - Penyalahgunaan otoritas
11	Operator - Terdapat laporan yang salah/tidak tercatat
12	Operator - Pelanggaran ketersediaan Personel
13	Personel Pusdatik - Penyalahgunaan otoritas
14	Personel Pusdatik – Pelanggaran Ketersediaan Personel

Sumber: Diolah oleh Peneliti (2022)

Oleh sebab itu, perlu dilakukan evaluasi lebih lanjut terhadap 13 skenario risiko yang harus dimitigasi guna mengantisipasi atau meminimalisasi adanya potensi ancaman/risiko yang dapat mengakibatkan dampak buruk bagi

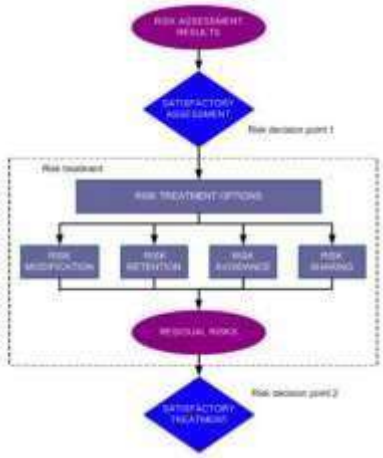
kelangsungan kegiatan operasional di Pusdatik.

Penanganan Risiko dan Penerimaan Risiko pada Pusat Data dan Teknologi Informasi Komunikasi BSSN Dalam Meminimalisasi Ancaman Siber

Penanganan Risiko

Penanganan risiko merupakan perencanaan atas mitigasi risiko-risiko untuk mendapatkan alternatif solusinya sehingga penanganan risiko dapat diterapkan secara efektif dan efisien. Berdasarkan teori/standar ISO/IEC 27005, terdapat empat macam penanganan risiko yaitu kontrol untuk memodifikasi (*modification*), mempertahankan (*retention*), menghindari (*avoidance*), untuk rencana dalam menangani risiko yang terjadi. Berikut penjabaran dari macam penanganan risiko (ISO/IEC, 2018):

a. Risk Modification merupakan penanganan risiko dengan tindakan pengelolaan dengan memperkenalkan, memindahkan, atau mengubah kontrol sehingga residual risk dapat ditetapkan lagi untuk dapat diterima.
b. Risk Retention merupakan penanganan risiko dengan keputusan untuk mempertahankan risiko tanpa adanya tindakan lebih lanjut yang harus diambil. Keputusan ini diambil tergantung dari hasil penilaian risiko. Jika level risiko memenuhi kriteria penerimaan risiko, maka tidak perlu menerapkan kontrol tambahan dan risiko dapat dipertahankan.
c. Risk Avoidance merupakan penanganan risiko dengan tindakan penghindaran terhadap risiko yang berasal dari kondisi tertentu. Risk Avoidance dipilih ketika risiko yang teridentifikasi dianggap terlalu tinggi, atau biaya pelaksanaan pilihan penanganan risiko melebihi manfaatnya. Organisasi menghindari atau membagikan (*sharing*) risiko (ISO/IEC, 2018). Kontrol tersebut dipilih risiko dengan cara menghilangkan penyebab timbulnya risiko yakni menghentikan aktivitas jika gejala risiko muncul.
d. Risk Sharing merupakan penanganan risiko dengan tindakan membagi risiko ke pihak lain yang paling memungkinkan untuk mengelola risiko tersebut. Keputusan ini tergantung dari hasil penilaian risiko. Dalam membagi risiko, dimungkinkan bahwa pengalihan tanggung jawab untuk mengelola risiko biasanya tidak mungkin membagi tanggung jawab terhadap dampak yang dihasilkan dari risiko. Dalam penanganan risiko yang dipilih, dilakukan proses pada risiko residual (*residual risk*). Risiko residual perlu ditetapkan setelah penentuan penanganan risiko. Gambar 2 merupakan tahapan pada penanganan risiko keamanan informasi berdasarkan ISO/IEC 27005.



Gambar 2 Risk Treatment Activity

Sumber: (ISO/IEC 27005,2018)

Berdasarkan hasil analisis dan interpretasi data di atas, dapat dinyatakan bahwa dari 13 skenario risiko yang memiliki tingkat risiko dimitigasi, telah diputuskan bahwa strategi penanganan risiko untuk 13 skenario risiko tersebut adalah modification, dimana risiko dikenalkan, dihilangkan atau mengubah kontrol sehingga risiko dapat diterima. Pada proses penanganan risiko menghasilkan 36 jenis rekomendasi kontrol yang mengacu pada standar ISO/IEC 27002 dengan mempertimbangkan hasil penilaian risiko. Berikut merupakan 36 jenis rekomendasi kontrol yang dilakukan untuk mengantisipasi 13 skenario risiko yang memiliki tingkat risiko dimitigasi yang tertera pada tabel 5.

Tabel 5 Rekomendasi Kontrol 13 Skenario Risiko yang Dimitigasi

No	Rekomendasi Kontrol
1	Membatasi dan mengendalikan alokasi penggunaan *user privileged*
2	Memperbarui *password* secara berkala dengan mewajibkan kekuatan dan kualitas *password* tinggi
3	Memeriksa keamanan sistem secara rutin
4	Membuat dan menerapkan kontrol khusus untuk menjamin kerahasiaan dan integritas data saat melakukan akses ke sistem informasi yangdikelola Pusat Data dan Teknologi Informasi Komunikasi
5	Menerapkan kebijakan penggunaan layanan dengan membatasi akses pengguna
6	Melakukan sistem *login* dengan *password* pada setiap PC
7	Menerapkan manajemen keamanan *password*
8	Memberikan pengamanan berupa enkripsi/*lock file* pada berkas yang tersimpan
9	Melakukan *maintain* dan *update windows* secara periodik
10	Melakukan *upgrade windows* terbaru atau beralih ke OS Linux berbayar
11	Berlangganan *renewal antivirus*
12	Melakukan *maintain* dan *update* antivirus secara periodik
13	Menerapkan *password* pada *localhost* atau *root* pada pengguna dan disertai dengan penggunaan fungsi *hash* pada *database*
14	Memantau akses pengguna *database* dengan *log*
15	Melakukan *monitoring* pada *database* secara berkala
16	Membatasi jaringan publik yang dapat diakses oleh pengguna
17	Menerapkan *role authorization* (otorisasi peran) pada *server*
18	Menerapkan keamanan pada *storage* dengan cara enkripsi *storage*
19	Melakukan *screening* penggunaan aplikasi pada PC secara periodik
20	Membuat *back-up server*
21	Melakukan akses *remote* terhadap perangkat secara berkala
22	Meningkatkan pelayanan pada fungsi keamanan informasi dan kriptografi
23	Membuat kebijakan pengguanaan layanan *wifi public* untuk *user*
24	Melakukan pengujian pada sistem dan perangkat penyedia layanan *wifi public* untuk memastikan sistem dan perangkat dapat berfungsi dengan baik

25	Membuat dan menerapkan dokumentasi SOP dalam penggunaan layanan
26	Menerima dan menindaklanjuti pelaporan kegagalan oleh *user*
27	Membuat dokumentasi prosedur konfigurasi secara resmi dan konsisten
28	Melakukan tinjauan pada kontrol yang sudah ada untuk memastikan kontrol tersebut masih relevan atau tidak
29	Melakukan penyimpanan pada log aktivitas *user*
30	Menerapkan fungsi *hash* pada penyimpanan Password
31	Meningkatkan pengelolaan *Network Management System*
32	Membuat proses *logout* otomatis pada aplikasi dengan sesi *timeout*
33	Melakukan pemeliharaan perangkat secara rutin, dan sesuai dengan ketentuan pemeliharaan dari pabrik
34	Meningkatkan *awareness* keamanan informasi
35	Melakukan batasan penggunaan pada fasilitas proses informasi
36	Menerapkan kebijakan *clear desk* dan *clear screen*

Sumber: Diolah oleh Peneliti (2022)

Oleh karena itu, untuk mengatasi terjadinya potensi risiko/ancaman pada aset Pusdatik perlu dilakukan/diterapkan rekomendasi kontrol yang tepat supaya kegiatan operasional atau proses bisnis di Pusdatik berjalan dengan optimal.

Penerimaan Risiko

Berdasarkan teori/standar ISO/IEC 27005:2018, penerimaan risiko merupakan tahapan dalam menerima risiko dan bertanggung jawab terhadap keputusan yang diambil manajer dalam mengelola risiko yang dihadapi (ISO/IEC, 2018). Proses penerimaan risiko meliputi penetapan keputusan penanganan risiko dan penetapan penanggung jawab penanganan risiko.

Berdasarkan hasil analisis dan interpretasi data di atas, dapat dinyatakan bahwa terdapat 13 skenario risiko dimodifikasi yang telah diberikan rekomendasi kontrol pada tahap penanganan risiko. Dalam upaya memodifikasi risiko dengan menerapkan kontrol yang telah direkomendasikan, dibutuhkan penanggung jawab bagi setiap kontrol pada masing-masing skenario risiko. Dari hasil penerimaan risiko terdapat tiga pihak yang terlibat dan bertangung jawab dalam pengelolaan risiko pada aset Pusdatik. Penanggung jawab setiap kontrol pada masing-masing skenario risiko meliputi:

a. Bidang Manajemen Risiko dan Kelangsungan TIK sebanyak 4 skenario risiko yaitu Layanan Wifi Internal dan Publik - Peretasan, Layanan Wifi Internal dan Publik - Koneksi ke perangkat mengalami gangguan, Layanan Konfigurasi Jaringan - Terjadi kegagalan konfigurasi, Layanan Konfigurasi Jaringan - Terjadi kesalahan saat set-up jaringan.
b. Bidang Infrastruktur sebanyak 9 skenario risiko yaitu PC/Desktop - Penyalahgunaan hak, PC/Desktop - Terjadinya kerusakan/kehilangan data, Database Server - Penyalahgunaan hak, Database Server - Terjadinya kerusakan/kehilangan data, Database Server - Server tidak bisa diakses, UPS - Layanan tidak berjalan, Antivirus - Terjadinya kerusakan/kehilangan data, Firewall - Penyalahgunaan hak, Firewall - Layanan tidak berjalan.

c. Vendor sebanyak 2 skenario risiko yaitu Layanan Wifi Internal dan Publik - Peretasan, Layanan Wifi Internal dan Publik - Koneksi ke perangkat mengalami gangguan.

Dengan adanya penerimaan risiko, maka bisa mengantisipasi maupun meminimalisasi adanya potensi ancaman/risiko pada aset Pusdatik dikarenakan adanya pemantauan yang dilakukan oleh penanggung jawab terhadap rekomendasi kontrol yang diterapkan pada masing-masing skenario risko yang harus dimitigasi.

KESIMPULAN

Adapun kesimpulan dar penelitian sebagai berikut:

a. Berdasarkan hasil identifikasi risiko yang telah dilakukan, didapatkan sebanyak 14 aset pada Pusdatik BSSN yang terdiri dari 3 aset utama dan 11 aset pendukung. Dimana dari 14 aset tersebut teridentifikasi sebanyak 13 potensi ancaman.
b. Analisis risiko perlu dilakukan oleh Pusdatik BSSN untuk menentukan tingkat peluang dan tingkat dampak atas ancaman yang mungkin terjadi pada aset Pusdatik. Berdasarkan hasil analisis risiko yang telah dilakukan penilaian terhadap 27 skenario risiko, didapatkan bahwa masih terdapat 13 skenario risiko harus "Dimitigasi" guna mengantisipasi adanya potensi ancaman/risiko yangdapat mengakibatkan dampak buruk bagi kelangsungan kegiatan operasional di Pusdatik BSSN.
c. Proses penanganan risiko keamanan informasi pada aset Pusdatik BSSN dihasilkan sebanyak 36 rekomendasi kontrol keamanan informasi untuk menangani risiko berdasarkan ISO/IEC 27002 dan sebanyak 13 skenario risiko yang dimitigasi mendapat strategi penanganan modification. Pada tahap penerimaan risiko, ditentukan penanggung jawab kontrol untuk memastikan kontrol-kontrol tersebut dapat diterapkan dan dilakukan secara tepat sasaran. Dari hasil penerimaan risiko terdapat tiga pihak yang terlibat dan bertangung jawab dalam pengelolaan risiko yaitu Bidang Manajemen Risiko dan Kelangsungan TIK sebanyak 4 skenario risiko, Bidang Infrastruktur sebanyak 9 skenario risiko, dan Vendor sebanyak 2 skenario risiko.

Rekomendasi

Berdasarkan hasil dari penelitian ini, maka peneliti memberikan beberapa saran yang dapat digunakan sebagai bahan pertimbangan sebagaimana berikut ini:

a. Perlu menyusun SOP maupun pedoman terkait pelaksanaan kegiatan operasional secara menyeluruh agar tiap personil melaksanakan tugasnya sesuai dengan prosedur yang berlaku.
b. Perlu melakukan pengembangan implementasi kontrol keamanan terutama pada aspek prosedur operasional dan pemanfaatan penerapan keamanan terhadap

spesifikasi teknologi informasi yang dimiliki Pusdatik BSSN.

c. Perlu melakukan evaluasi, pengawasan, dan koordinasi terhadap setiap proses penanganan risiko yang telah ditetapkan, seperti melakukan pencatatan dalam laporan pengawasan risiko.
d. Perlu membuat jadwal untuk menerapkan kontrol-kontrol yang telah diidentifikasi agar risiko keamanan informasi dapat segera terkelola dengan baik.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia. (2020). Laporan Survey Internet Asosiasi Penyelenggara Jasa Internet Indonesia 2019-2020 (Q2). Jakarta: Indonesia Survey Data Center.

Badan Siber dan Sandi Negara. (2021). Laporan Tahunan: Monitoring Keamanan Siber 2020. Jakarta: Badan Siber dan Sandi Negara.

Clinten, Bill. (2022). Kasus Data Bocor di Indonesia Sepanjang 2022, dari PLN, Pertamina, hingga Aksi Bjorka. Indonesia

Czosseck, C., Ottis, R., & Talihärm, A. M. (2013). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. Case Studies in Information Warfare and Security: For Researchers, Teachers and Students, 72.

ISO/IEC 27005. (2018). "ISO/IEC 27002:2013 Information Technology–Security Techniques – Code of Practice for Information Security Controls".

International Telecommunication Union. (2021). Global Cybersecurity Index (GCI) 2020. International Telecommunication Union.

Marshall, J., & Saulawa, M. (2015). Cyberattack: the legal response. International Journal of International Law, 1 (2).

Neuman, W. Laurence (2015). Metodologi Penelitian Sosial: Pendekatan Kualitatif Dan Kuantitatif. Jakarta: PT Indeks.

Nuriah, S., Rois, B., & Risnaeni, U. S. J. M. J. A. S. (2021). Efektivitas manajemen risiko dan hasil. Indonesia

Peraturan Kepala Badan Siber dan Sandi Negara No. 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.

Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.

Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Prasetyo, S. (2014). Perencanaan Manajemen Risiko Keamanan Informasi: Studi Kasus Aplikasi Modul Kekayaan Negara Direktorat Jenderal Kekayaan Negara Kementerian Keuangan. Universitas Indonesia.

Sarno, R., & Iffano, I. (2009). Sistem Keamanan Informasi Berbasis ISO 27001. Surabaya: ITSPress.

Tim Direktorat Keamanan Informasi. (2011). Panduan Penerapan Tata Kelola Keamanan Informasi Bagi

Penyelenggara Pelayanan Publik (2nd ed.). Indonesia.

Wilson, C. (2008). Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for Congress. Congressional Research Service.http://etd.respository.ugm.ac.id.