Penentuan Kriteria Dampak Risiko Keamanan Informasi, Mutu, dan Layanan Pada Layanan Jaringan Komunikasi di BMKG

Nunik Lathifah Agustina Wicahyani *[1], Muhammad Salman [2]
[1,2]Program Studi Magister Manajemen Keamanan Jaringan Informasi, Departemen Teknik Elektro, Universitas Indonesia
E-mail: *[1] nunik.lathifah@ui.ac.id, [2]muhammad.salman@ui.ac.id

Abstrak

Abstract—Teknologi informasi menjadi aset yang sangat berharga bagi organisasi dikarenakan menjadi pendukung utama proses bisnis pada organisasi. Badan Meteorologi, Klimatologi, dan Geofisika (BMKG) sebagai Lembaga Pemerintah Non Departenen (LPND) yang memberikan pelayanan informasi cuaca, iklim, gempabumi dan tsunami perlu untuk menjaga keamanan informasi terutama aspek confidentiality, integrity, availability, maupun accountability dari informasi yang diberikan untuk masyarakat. Penilaian risiko organisasi menjadi salah satu syarat utama dalam proses pengamanan informasi. Dalam manajemen risiko perlu dilaksanakan proses penentuan kriteria dampak risiko.

Kata Kunci*— manajemen risiko, keamanan informasi, ISO 27005, ISO 31000, manajemen risiko SPBE*

1. PENDAHULUAN

Penggunaan teknologi informasi dan komunikasi dalam mendukung proses bisnis organisasi sangat lazim dilakukan seiring dengan laju perkembangan teknologi informasi dan komunikasi. Teknologi informasi menjadi sebuah aset yang sangat berharga bagi organisasi. Ketiadaan teknologi informasi dapat menyebabkan proses bisnis dalam organisasi terhenti.

Badan Meteorologi, Klimatologi, dan Geofisika merupakan Lembaga Pemerintah Non Departemen (LPND) yang bertugas untuk memberikan pelayanan informasi cuaca, iklim, gempa bumi dan tsunami kepada masyarakat dan para *stakeholder*. Proses diseminasi informasi dilakukan melalui berbagai macam media komunikasi.

Informasi yang dikirimkan kepada masyarakat dan para *stakeholder* merupakan informasi yang handal, akurat, cepat, tepat dan dapat dipertanggungjawabkan. Informasi yang didiseminasikan harus terjaga baik *confidentiality, integrity, availability,* maupun *accountability* dari informasi tersebut untuk menghindari terjadinya salah informasi yang dapat mengakibatkan kerugian materiil maupun kehilangan nyawa.

Untuk menjaga *confidentiality, integrity, availability,* maupun *accountability* dari informasi dari BMKG diperlukan pengamanan informasi pada aset yang dipergunakan dalam proses diseminasi informasi meteorologi, klimatologi, serta gempabumi dan tsunami.
Ada tiga syarat utama dalam pengamanan informasi seperti yang disebutkan dalam ISO/IEC 27002:2014[1], yaitu:

1. penilaian risiko terhadap organisasi, dengan mempertimbangkan strategi dan tujuan bisnis organisasi secara keseluruhan. Melalui penilaian risiko, ancaman terhadap aset diidentifikasi, kerentanan dan kemungkinan terjadinya dievaluasi dan dampak potensial diperkirakan;
2. persyaratan hukum, undang-undang, peraturan, dan kontrak yang harus dipenuhi oleh organisasi, mitra dagang, kontraktor, dan penyedia layanannya, dan lingkungan sosial budaya mereka;

3. sekumpulan prinsip, tujuan, dan kebutuhan bisnis untuk penanganan, pemrosesan, penyimpanan, komunikasi, dan pengarsipan informasi yang telah dikembangkan organisasi untuk mendukung operasinya.

Dapat dilihat bahwa penilaian risiko pada organisasi sangat penting karena menjadi salah satu persyaratan utama dalam pengamanan informasi.

BMKG telah menerapkan ISO/IEC 27001, ISO/IEC 20000-1, dan ISO 9001. Penerapan ketiga standar tersebut jika berdiri sendiri akan mengakibatkan pemborosan biaya administrasi, serta pelaksanaan operasional sistem yang rumit dan tidak efektif [2], oleh sebab itu dilakukan integrasi sistem manajemen dengan menggunakan standar Integrasi Sistem Manajemen PAS 99. integrasi sistem sekaligus juga mengintegrasikan manajemen risiko

2. METODE PENELITIAN

2.1. Manajemen Risiko

Dalam ISO Guide 73:2009[3] disebutkan bahwa risiko merupakan efek dari ketidakpastian pada suatu sasaran. Efek merupakan suatu penyimpangan dari apa yang diharapkan baik positif maupun negatif. Sedangkan sasaran merupakan penerapan yang dapat dilakukan pada berbagai tingkatan dan aspek. Risiko terjadi sebab adanya potensi atau kemungkinan dan konsekuensi dari suatu kejadian.

Manajemen risiko merupakan pendekatan sistematis yang mencakup proses, pengukuran, struktur dan budaya untuk menentukan tindakan terbaik terkait risiko[4]. Manajemen risiko pada awalnya sangat melekat dengan jasa asuransi, namun seiring berjalannya waktu manajemen risiko juga mulai digunakan untuk mengendalikan dan mengelola risiko secara luas[5]. Seperti yang disebutkan oleh Barafort et al, Manajemen risiko merupakan topik yang sangat penting dan menarik bagi organisasi. Manajemen risiko sangat berperan penting dalam sistem manajemen[2]. Manajemen risiko sebaiknya terintegrasi dengan semua proses dalam organisasi, baik saat pengembangan, perencanaan, tinjauan bisnis dan strategi maupun manajemen perubahan dan sebisa mungkin sebagai bagian dalam pengambilan keputusan[5], dikarenakan manajemen risiko merupakan fase yang sangat penting, yang memungkinkan dampak risiko terkadang sangat serius dan memastikan peningkatan dan optimisasi proses. Proses manajemen risiko harus diintegrasikan pada tiap siklus hidup yang akan memfasilitasi pemecahan masalah pada penelitian[6].

2.2. Proses Manajemen Risiko

Proses manajemen risiko dapat didefinisikan sebagai penerapan kebijakan manajemen, prosedur dan praktik kegiatan konsultasi, komunikasi, penetapan konteks, identifikasi, analisis, evaluasi, pemantauan, perlakuan dan tinjauan risiko secara sistematis seperti didefinisikan oleh[5]. Adapun ilustrasi proses manajemen risiko dapat dilihat pada gambar 1.

Dalam pelaksanaan proses manajemen risiko diperlukan kriteria dasar dari manajemen risiko seperti yang dijelaskan dalam[8], yaitu:

1. Pendekatan manajemen risiko

Pendekatan manajemen risiko dapat berubah sesuai dengan ruang lingkup dan tujuannya. Pendekatan manajemen risiko yang baik harus dikembangkan berdasarkan kriteria evaluasi risiko, kriteria dampak, dan kriteria penerimaan risiko.

2. Kriteria evaluasi risiko

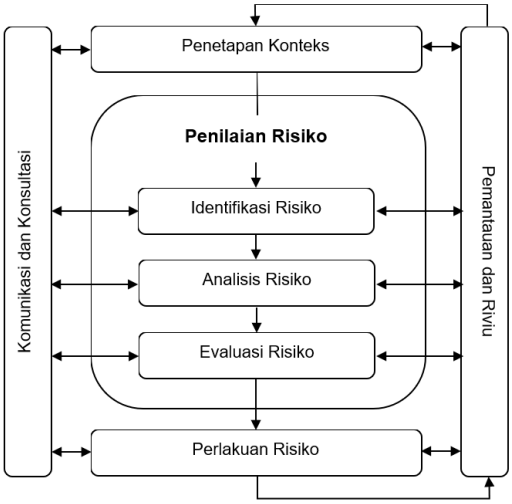
Kriteria evaluasi dikembangkan untuk mengevaluasi organisasi terkait nilai strategis proses bisnis, kritikalitas asset, kepentingan operasional dan bisnis terkait kerahasiaan, integritas dan ketersediaan.

3. Kriteria dampak

Dalam penentuan kriteria dampak harus disesuaikan dengan tingkat kerugian dan biaya yang dikeluarkan

4. Kriteria penerimaan risiko

Penerimaan risiko bergantung pada kebutuhan organisasi.



Gambar 1. Proses manajemen risiko[7]

2.3. Penetapan Konteks

Penetapan konteks dimaksudkan untuk menetapkan kriteria mendasar seperti kriteria dampak, kriteria kemungkinan, dan kriteria penerimaan risiko serta penentuan ruang lingkup, batasan, organisasi serta sumber ancaman dan kerawanan yang dapat terjadi terhadap setiap sasaran dalam proses manajemen risiko

2.3.1 Identifikasi sasaran

Pengidentifikasian sasaran dilakukan dalam penentuan sasaran risiko, indikator dan target sasaran. Sasaran risiko ditentukan berdasarkan layanan yang diberikan oleh Pusat Jaringan Komunikasi BMKG.

2.3.2 Penetapan kategori risiko

Tujuan penetapan kategori risiko adalah untuk memastikan bahwa proses identifikasi, analisis dan penilaian risiko dapat dilakukan secara menyeluruh. Kategori Risiko di Pusat Jaringan Komunikasi ditetapkan sesuai dengan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi No. 5 Tahun 2020 Tentang Pedoman Manajemen Risiko SPBE.

1. Arsitektur, yaitu risiko terkait dengan pembuatan dan penggunaan arsitektur yang menggambarkan integrasi proses bisnis, data dan informasi, infrastruktur, dan keamanan lembaga;
2. Peta Rencana, yaitu risiko terkait dengan pembuatan dan pelaksanaan rencana kerja lembaga;
3. Proses Bisnis, yaitu risiko yang terkait dengan penyiapan dan pelaksanaan proses bisnis lembaga;
4. Rencana dan Anggaran, yaitu risiko yang terkait dengan penyusunan program dan anggaran lembaga;
5. Inovasi, yaitu risiko yang terkait dengan ide-ide baru atau gagasan kreatif yang memberi nilai tambah pada lembaga;
6. Ketaatan terhadap Peraturan, yaitu risiko terkait dengan kepatuhan unit kerja di lingkungan BMKG terhadap peraturan perundang-undangan, perjanjian internasional, dan peraturan lain yang berlaku;
7. Pengadaan Barang dan Jasa, yaitu risiko yang terkait proses penyediaan barang dan jasa;
8. Proyek Pembangunan/Pengembangan Sistem, yaitu risiko terkait pekerjaan pembangunan maupun pengembangan sistem pada lembaga;
9. Data dan Informasi, yaitu risiko yang terkait dengan seluruh data dan informasi milik BMKG;
10. Infrastruktur, yaitu risiko yang terkait dengan pusat data, jaringan LAN, WAN, perangkat keras, perangkat lunak, dan fasilitas pendukung utama operasional lembaga;
11. Aplikasi, yaitu risiko yang terkait dengan program komputer yang digunakan dalam pelaksanaan tugas dan fungsi layanan;
12. Keamanan, yaitu risiko yang terkait dengan kerahasiaan, integritas, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya pendukung;
13. Layanan, yaitu risiko yang terkait dengan layanan yang diberikan kepada Pengguna;
14. Sumber Daya Manusia, yaitu risiko yang terkait dengan pegawai yang bekerja di BMKG; dan
15. Bencana Alam, yaitu risiko yang terkait dengan kejadian yang disebabkan oleh alam

2.3.3 Penetapan Area Dampak Risiko

Tujuan dari Penetapan Area Dampak Risiko adalah untuk mengetahui area yang terkena dampak dari risiko di BMKG dengan terlebih dahulu menentukan dampak risiko. Area Dampak Risiko dalam penerapan Manajemen Risiko di BMKG meliputi:

1. Finansial, yaitu dampak risiko terkait dengan segi keuangan;
2. Reputasi, yaitu dampak risiko terkait dengan tingkat kepercayaan para pemangku kepentingan;
3. Kinerja, yaitu dampak risiko terkait dengan pencapaian sasaran organisasi;
4. Layanan Organisasi, yaitu dampak risiko terkait dengan terpenuhinya kebutuhan atau layanan kepada pemangku kepentingan;
5. Operasional dan Aset TIK, yaitu dampak risiko terkait dengan aktivitas operasional TIK dan manajemen aset TIK;
6. Hukum dan Regulasi, yaitu dampak risiko terkait dengan peraturan perundang-undangan dan kebijakan; dan
7. Sumber Daya Manusia, yaitu dampak risiko terkait dengan aspek fisik dan mental pegawai.
8. Area Dampak Risiko terdiri atas area dampak positif dan/atau negatif[4].

2.3.4 Penerapan Kriteria Risiko

Penetapan Kriteria Risiko ditujukan untuk mengukur dan menentukan seberapa besar kemungkinan terjadinya risiko dan dampak yang dapat terjadi. Kriteria Risiko ini dipantau secara berkala dan harus disesuaikan jika terjadi perubahan.

Penetapan Kriteria Risiko ini terdiri atas:

a) Kriteria Kemungkinan

Kriteria Kemungkinan Risiko ditetapkan berdasarkan pada tingkat kemungkinan dan kriteria dari setiap tingkat kemungkinan terhadap risiko. BMKG menggunakan 5 tingkat kemungkinan, yang diuraikan sebagai berikut:

1) Hampir Tidak Terjadi;
2) Jarang Terjadi;
3) Kadang-Kadang Terjadi;
4) Sering Terjadi;
5) Hampir Pasti Terjadi.

Penetapan kriteria kemungkinan disesuaikan dengan jumlah frekuensi terjadinya risiko dalam satuan waktu yang ditentukan seperti tercantum pada tabel 1.

Tabel 1. Kriteria Kemungkinan Risiko

Level Kemungkinan	Persentase Kemungkinan Terjadinya dalam Satu Tahun	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
Hampir Tidak Terjadi	X ≤ 5%	X < 2 kali
Jarang Terjadi	5% < X ≤ 10%	2 ≤ X ≤ 5 kali
Kadang-kadang terjadi	10% < X ≤ 20%	6 ≤ X ≤ 9 kali
Sering Terjadi	20% < X ≤ 50%	10 ≤ X ≤ 12 kali
Hampir Pasti Terjadi	X ≥ 10%	>12 kali

b) Kriteria Dampak

Kriteria dampak risiko merupakan kombinasi antara area dampak dan tingkat dampak risiko. Pusat Jaringan Komunikasi BMKG menggunakan 5 tingkat dampak risiko sebagai berikut:

1) Tidak Signifikan;
2) Kurang Signifikan;
3) Cukup Signifikan;
4) Signifikan;
5) Sangat Signifikan.

Kriteria Dampak Risiko dapat ditentukan berdasarkan hasil FGD, data periode sebelumnya, analisis subyektif, dan atau *benchmarking*[9]

3. KRITERIA DAMPAK RISIKO

Kriteria dampak risiko di BMKG ditentukan melalui FGD berdasarkan analisis dari para pemangku kepentingan yang dijabarkan sebagai berikut:

3.1 Kinerja

Tabel 2. Kriteria dampak risiko aspek kinerja

Dampak	Positif	Negatif
Tidak Signifikan	Mempercepat layanan <20% dari jam operasional harian	Gangguan layanan <3% dari jam operasional harian

Dampak	Positif	Negatif
Kurang Signifikan	Mempercepat layanan 20% s.d <40% dari jam operasional harian	Gangguan layanan 3% s.d <4% dari jam operasional harian
Cukup Signifikan	Mempercepat layanan 40% s.d <60% dari jam operasional harian	Gangguan layanan 4% s.d <5% dari jam operasional harian
Signifikan	Mempercepat layanan 60% s.d <80% dari jam operasional harian	Gangguan layanan 5% s.d <6% dari jam operasional harian
Sangat Signifikan	Mempercepat layanan >80% dari jam operasional harian	Gangguan layanan >6% dari jam operasional harian

3.2 Reputasi

Tabel 3. Kriteria dampak risiko aspek reputasi

Dampak	Positif	Negatif
Tidak Signifikan	Kredibilitas tidak terpengaruh	Kredibilitas tidak terpengaruh
Kurang Signifikan	Peningkatan kredibilitas di tingkat lokal dan perorangan	Kredibilitas terpengaruh secara lokal dan perorangan
Cukup Signifikan	Peningkatan kredibilitas di tingkat regional/daerah	Kredibilitas terpengaruh dengan munculnya kritik public dari berbagai pihak di tingkat regional/daerah
Signifikan	Peningkatan kredibilitas di tingkat nasional	Kredibilitas terpengaruh secara signifikan dengan kritik public dari berbagai pihak yang menyebar sampai tingkat nasional
Sangat Signifikan	Kredibilitas meningkat di tingkat internasional	Kredibilitas diragukan dengan adanya kecaman dan penolakan dari berbagai pihak terhadap organisasi

3.3 Finansial

Tabel 4. Kriteria dampak risiko aspek finansial

Dampak	Positif	Negatif
Tidak Signifikan	Tidak ada peningkatan finansial	Tidak ada kerugian finansial
Kurang Signifikan	Peningkatan anggaran sampai dengan 100 juta rupiah	Kerugian finansial antara di bawah 100 juta rupiah
Cukup Signifikan	Peningkatan anggaran di atas 100 juta rupiah	Kerugian finansial diatas 100 juta rupiah

Dampak	Positif	Negatif
Signifikan	Peningkatan anggaran di atas satu milyar rupiah	Kerugian finansial diatas satu milayar rupiah
Sangat Signifikan	Peningkatan anggaran di atas satu trilyun rupiah	Kerugian finansial diatas satu trilyun rupiah

3.4 Layanan organisasi

Tabel 5. Kriteria dampak risiko aspek layanan organisasi

Dampak	Positif	Negatif
Tidak Signifikan	Tidak berpengaruh terhadap hubungan dengan stakeholder	Tidak berpengaruh terhadap hubungan dengan stakeholder
Kurang Signifikan	Hubungan dengan 1 stakeholder meningkat	Melemahnya hubungan dengan 1 stakeholder yang dapat dipulihkan dalam waktu singkat
Cukup Signifikan	Hubungan dengan beberapa stakeholder meningkat	Melemahnya hubungan dengan beberapa stakeholder, pemulihan memerlukan perlakuan khusus
Signifikan	Hubungan dengan mayoritas stakeholder meningkat	Rusaknya hubungan dengan mayoritas stakeholder
Sangat Signifikan	Naiknya kepercayaan seluruh stakeholder	Hilangnya kepercayaan seluruh stakeholder

3.5 Operasional dan Aset TIK

Tabel 6. Kriteria dampak risiko aspek operasional TIK

Dampak	Positif	Negatif
Tidak Signifikan	Tidak ada gangguan operasional	Aktivitas terhenti selama < 2 jam
Kurang Signifikan	Gangguan operasional di bawah 1 hari berkurang	Aktivitas terhenti 2- 4 jam
Cukup Signifikan	Gangguan operasional di bawah 1 minggu berkurang	Aktivitas terhenti >4 jam – 1 hari
Signifikan	Gangguan operasional di atas 1 minggu berkurang	Aktivitas terhenti selama 1-3 hari
Sangat Signifikan	Tidak pernah terjadi gangguan operasional	Aktivitas terhenti selama >3 hari

3.6 Hukum dan Regulasi

Tabel 7. Kriteria dampak risiko aspek hokum dan regulasi

Dampak	Positif	Negatif
Tidak Signifikan	Mendapatkan penghargaan dari perorangan	Patuh terhadap peraturan/perundang -undangan yang berlaku
Kurang Signifikan	Mendapatkan penghargaan dari Lembaga	Patuh terhadap peraturan/perundang -undangan yang berlaku
Cukup Signifikan	Mendapatkan penghargaan tingkat regional/daerah	Patuh terhadap peraturan/perundang -undangan yang berlaku
Signifikan	Mendapatkan penghargaan tingkat nasional	Ketidakpatuhan berdampak penghentian layanan atau dikenakan denda
Sangat Signifikan	Mendapatkan penghargaan tingkat internasional	Ketidakpatuhan yang menyebabkan hukuman pidana

3.7 Sumber Daya Manusia

Tabel 8. Kriteria dampak risiko aspek sumber daya manusia

Dampak	Positif	Negatif
Tidak Signifikan	sebagian kecil pegawai merasa bahagia, operasional stagnan	Sebagian kecil pegawai resah, tidak mengganggu operasional
Kurang Signifikan	sebagian pegawai merasa bahagia, produktivitas sedikit meningkat	Sebagian pegawai resah, produktivitas menurun
Cukup Signifikan	sebagian pegawai merasa bahagia, produktivitas sedikit meningkat, operasional meningkat	Sebagian pegawai resah, produktivitas menurun, operasional terganggu
Signifikan	sebagian pegawai merasa bahagia, produktivitas meningkat, operasional meningkat	Sebagian pegawai resah, produktivitas menurun, operasional terganggu dan berdemontrasi
Sangat Signifikan	Pegawai merasa bahagia, produktivitas meningkat, operasional meningkat, prestasi pegawai meningkat	Pemogokan pegawai operasional terhenti >1 hari

4. KESIMPULAN

Kriteria dampak risiko keamanan informasi, mutu, dan layanan ini disesuaikan dengan penerapan integrasi manajemen sistem di Pusat Jaringan Komunikasi BMKG. Penentuan kriteria dampak risiko ini mempermudah *Risk Manager* dalam proses pengeloaan Manajemen risiko dalam Lembaga.

DAFTAR PUSTAKA

[1] S. N. I. Iso, "Teknologi informasi – Teknik keamanan – Panduan praktik kendali keamanan informasi," 2014.
[2] B. Barafort, A. L. Mesquida, and A. Mas, "Integrating risk management in IT settings from ISO standards and management systems perspectives," *Comput. Stand. Interfaces*, vol. 54, pp. 176–185, 2017, doi: 10.1016/j.csi.2016.11.010.
[3] B. S. Nasional, "Standar Nasional Indonesia SNI ISO Guide 73:2016 Manajemen risiko-Kosakata Risk management-Vocabulary (ISO Guide 73:2009, IDT)."
[4] Pemerintah Republik Indonesia, *Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik*, vol. 5, no. 261. 2020, pp. 1689–1699.
[5] C. R. Vorst, D. S. Priyarsono, and A. Budiman, *Manajemen Risiko Berbasis SNI ISO 31000*, Pertama. Jakarta: Badan Standardisasi Nasional, 2018.
[6] I. Akkiyat and N. Souissi, "Modelling risk management process according to ISO standard," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2, pp. 5830–5835, 2019, doi: 10.35940/ijrte.B3751.078219.
[7] "iso-iec-27005-2018-pdf-download.pdf." .
[8] ISO/IEC, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and," *ACM Work. Form. Methods Secur. Eng. DC, USA*, vol. 34, no. 19, pp. 45–55, 2018, [Online]. Available: http://www.worldcat.org/title/service-operation/oclc/254028066&referer=brief_results%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf%0Ahttp://k504.kh.
[9] D. Rachmina, "Ruang Lingkup, Konteks, Kriteria Manajemen Risiko – Kriteria Risiko." https://irmapa.org/ruang-lingkup-konteks-kriteria-manajemen-risiko-kriteria-risiko/.