KEMENTERIAN PERTAHANAN RI
PUSAT DATA DAN INFORMASI

PEDOMAN KERJA
REGISTRASI ASET DAN PENILAIAN RISIKO
PUSDATIN KEMHAN

Nomor : PK/02/VIII/2022/PUSDATIN

TAHUN 2022

BAB I
PEDOMAN REGISTRASI ASET (*ASSET REGISTER*)

1. Pedoman Registrasi Aset (*Asset Register*)

   a. Pendahuluan

      Pedoman ini memberikan panduan dalam pelaksanaan dan pengaturan registrasi aset di lingkungan Pusdatin Kemhan RI yang bertujuan untuk menentukan, mengklasifikasi, dan meng - identifikasi jenis aset serta melakukan penilaian terhadap level dari aset yang dimiliki oleh Pusdatin Kemhan RI.

      Jenis aset yang dimiliki dibedakan menjadi beberapa klasifikasi, diantaranya :

      1) Aset informasi berupa *database, file*, kontrak dan perjanjian, dokumentasi sistem, informasi, penelitian, buku petunjuk, bahan pelatihan, Pedoman atau pendukung operasional, rencan kelangsungan bisnis, hasil audit, dan informasi yang diarsipkan.

      2) Aset *software* berupa aplikasi perangkat lunak, system perangkat lunak, pengembangan perangkat dan utilitas.

      3) Aset fisik berupa peralatan komputer, peralatan komunikasi, removable media, dan peralatan lainnya.

      4) Aset jasa *(service)* berupa komputasi dan layanan komunikasi serta utilitas umum, misalnya pemanas, penerangan, listrik, telepon, genset, fotokopi, dll.

      5) Aset orang berupa kualifikasi, keterampilan, dan pengalaman.

      6) Aset tidak berwujud seperti reputasi dan citra organisasi.

   b. Registrasi Aset

      Pemilik aset untuk setiap Bagian/Bidang melakukan pendataan terhadap aset Pusdatin Kemhan RI yang di kelolanya. Seluruh aset yang di miliki diklasifikasikan dan diberi nilai untuk menentukan Risiko yang dimiliki aset tersebut. Penilaian tersebut dapat menentukan perlakuan yang akan dilakukan jika aset tersebut memiliki nilai yang tinggi. Secara garis besar metode penyusunan registrasi aset sebagai beikut:

1) Inventarisasi Aset

a) Detil inventaris aset terdiri dari. nama aset klasifikasi aset, kode aset, nomor seri asset/*business specific requirements*, mantra, status perawatan dll, tergantung dari jenis asetnya.

b) Setiap aset juga memiliki kepemilikan aset yang didetailkan dalam kolom pemilik (penaggung jawab) aset, pemeliharaan aset, Lokasi, detail penyimpangan, dll tergantung dari jenis asetnya.

c) Setiap aset harus dilakukan penilaian yang dihitung dari aspek *Confidentiality* (kerahasiaan), *Integrity (*keutuhan*)* dan *Availability* (ketersedian) dengan berpedoman pada tabel.

NAMA ASET	**Penilaian Terkait Confidentiality**	**Penilaian Terkait Integrity**	**Penilaian Terkait Availability**	**Kepemilikan**
Informasi	Mengikuti klasifikasi kerahasiaan informasi	Keutuhan dan kebenaran data	Ketersediaan ketika dibutuhkan oleh seluruh pihak yang memerlukan	Sesuai dengan dok/informasi /data yang dihasilkan oleh bidang terkait. (Surat - menyurat, Bidang Tata Usaha)
Perangkat Lunak	Terkait dengan informasi yang diproses mengguna kan software ini	Keterandalan (contoh: banyak bug/ problem, integritynya rendah)	Ketersediaan pada saat yang dibutuhkan	Sesuai dengan fungsi dan kegunaan software di bidang terkait. (Firewall – Pamsisinfo san, Infratik)
Aset Fisik	Terkait dengan informasi yang ada di dalamnya	Keterandalan (durability), keakuratan	Ketersediaan dalan kondisi yang disyaratakan terhadap aset tersebut.	Sesuai dengan keberadaan asset tersebut. (Server, Infrarik, Pamsosinfo san dan Banglola)

Layanan	Konfigurasi peratan yang menyediakan service	Keterandalan dari layanan yang diberikan	Ketersediaan dari layanan yang diberikan	Sesuai dengan layanan yang di berikan oleh masing masing bidang
Sumber Daya Manusia	Terkait dengan kerahasiaan informasi yang dimiliki oleh personel secara persorangan maupun kelompok	Karakter: Dapat diandalkan, dipercaya, dan memiliki kemampuan sesuai bidangnya	Keberadaannya di organisasi (tinggi: tidak dapat digantikan, sedang: dapat digantikan, rendah: mudah digantikan)	Sesuai dengan struktur organisasi
Aset tidak berwu jud	Kerahasiaan terkait hak cipta atau aset tidak berwujud lainnya	Pengaruh nya terhadap citra organisasi	Keberadaannya ketika digunakan (misalnya untuk promosi dsb)	Disesuaikan oleh asset masing masing bidang (Aplikasi, Desain, dll)

d) *Asset Valuation* didasarkan atas perhitungan sebagai berikut:

$$\frac{Confidentiality + Integrity + Availability}{3} = Asset\ Value$$

Di mana:

(1) Nilai, *integrity* dan a*vailability* adalah 3 untuk tinggi, 2 untuk sedang dan 1 untuk rendah. Dan

(2) Penilaian confidentiality khusus untuk asset informasi adalah sebagai berikut:

(a) 3 = *highly confidential.*

(b) 2 = *condifential*, dan

(c) 1 = *Internal Use Only.*

e) Untuk aset informasi, pada kolom *"Pembatasan Akses"* adalah membatasi akses hanya kepada orang yang berkepentingan, penentuan akses ini tergantung pada peraturan yang ada. Kolom *"Pembatasan Akses"* hanya perlu diisi untuk aset-aset informasi yang bernilai 2 atau 3.

2) Pengendalian Terhadap Aset *Register*

a) Registrasi Aset dapat dirubah jika ada penambahan atau pengurangan terhadap aset yang dimiliki oleh pemilik aset.

b) Registrasi aset harus dilakukan peninjauan setiap tahun, hal ini bertujuan agar akurasi dari registrasi aset dapat dipertanggungjawabkan.

c) Setiap perubahan komponen asset pada registrasi aset harus mengacu kepada Prosedur manajemen perubahan Pusdatin Kemhan RI.

BAB II
PEDOMAN PENILAIAN MANAJEMEN RISIKO

2. Pedoman Penilaian Manajemen Risiko

a. Pendahuluan

1) Istilah dan Definisi

Berikut adalah istilah dan definisi yang digunakan dalam pedoman manajemen Risiko pada dokumen pedoman ini, yaitu:

a) Risiko
Suatu peristiwa atau penyebab yang menimbulkan terjadinya ketidakpastian dalam mencapai sasaran. Risiko merupakan kombinasi probabilitas suatu peristiwa dan konsekuensinya.

b) Manajemen Risiko
Kegiatan terkoordinasi untuk mengarahkan dan mengendalikan organisasi terkait dengan Risiko.

c) Risiko Residual
Risiko yang tersisa setelah penanganan Risiko.

d) Penerimaan Risiko
Keputusan untuk menerima Risiko.

e) Analisis Risiko
Penggunaan informasi secara sistematis untuk mengidentifikasi sumber dan memperkirakan Risiko.

f) Penilaian Risiko
Keseluruhan proses analisis dan evaluasi Risiko.

g) Evaluasi Risiko
Proses membandingkan Risiko yang diperkirakan dengan kriteria Risikoyang diberikan untuk menentukan signifikansi risiko.

h) Perlakuan Risiko
Proses pemilihan dan penerapan tindakan untuk memodifikasi Risiko.

i) Pernyataan Penerapan *(Statement of Applicability)* Dokumen yang menjelaskan tujuan pengendalian dan kontrol yang relevan yang dapat diterapkan pada Pusdatin Kemhan RI, berdasarkan hasil dan kesimpulan dari Proses Penilaian Risiko dan Perlakuan Risiko.

j) Pemilik risiko *(Owner)* adalah unit kerja yang bertanggungjawab terhadap seluruh dampak dari Risiko yang diidentifikasi dan berwenang mengelola dan mengendalikan Risiko.

k) Ancaman *(Threat)* adalah suatu potensi insiden karena kelemahan kontrol yang dapat menimbulkan kerugian/bahaya terhadap penyelenggaraan layanan.

l) Dampak *(Impact)* adalah gangguan atau kerugian yang akan dialami jika risiko yang diidentifikasi terjadi.

m) Kemungkinan *(Likely hood)* adalah peluang terjadinya suatu risiko karena kelemahan yang ada.

n) Kerawanan *(Vulnerability)* adalah kelemahan dari suatu aset atau kontrol yang dimanfaatkan untuk menimbulkan satu atau lebih ancaman.

o) Kriteria Penerimaan Risiko *(Risk Acceptance Criteria)* adalah tingkat risiko yang diterima oleh organisasi.

p) Rencana Penanggulangan Risiko *(Risk Treatment Plan)* adalah rencana tindakan untuk menurunkan kemungkinan *(Likely hood)* terjadinya Risiko dan mengurangi dampak (*Impact*) Risiko dengan menetapkan kontrol, mengalokasikan sumber daya dan menetapkan jadwal.

q) Daftar Risiko *(Risk Register*) adalah dokumen tentang identifikasi kerawanan, ancaman, dampak, serta kontrol dan rencana penanggulangan Risiko terhadap penyelenggaraan layanan TIK.

r) Disaster Recovery (DR)
Rencana pemulihan awal operasi Bisnis jika terjadi insiden yang menyebabkan terganggunya operasional.

s) Keamanan Informasi
Menjaga Kerahasiaan, Integritas, dan Ketersediaan Informasi.

t) Peristiwa Keamanan Informasi
Kejadian yang teridentifikasi dari suatu sistem, layanan, atau status jaringan yang menunjukkan kemungkinan pelanggaran kebijakan keamanan informasi atau kegagalan pengamanan, atau situasi yang sebelumnya tidak diketahui yang mungkin terlibat dalam peristiwa tersebut.

u) Insiden Keamanan Informasi
Satu atau serangkaian peristiwa keamanan informasi yang tidak diinginkan atau tidak terduga yang memiliki kemungkinan signifikan untuk membahayakan operasi bisnis dan mengancam keamanan informasi.

v) Integritas
Menjaga keakuratan dan kelengkapan informasi dan metode pemrosesan.

w) Analisis Risiko kualitatif
Proses penilaian Risiko berdasarkan persepsi seseorang tentang tingkat keparahan dan kemungkinan konsekuensinya.

x) Analisis Risiko Kualitatif
Proses menghitung Risiko berdasarkan data yang dikumpulkan.

y) Nomor ID *(*Risk *ID)*
atau nama yang digunakan untuk mengidentifikasi suatu Risiko.

z) Tujuan Strategis
Tujuan yang didapatkan dari rencana strategis untuk pengidentifikasian Risiko.

å) Proses Bisnis
Aktivitas atau serangkaian aktivitas yang mencapai tujuan organisasi tertentu.

ä) Kategori Risiko
Pengelompokkan Risiko berdasarkan sumbernya, area yang terkena dampak dan kelompok lainnya yang berkaitan.

ö) Kejadian Risiko
Realisasi konkret *(manifestasi)* dari Risiko yang abstrak.

aa) Penyebab Risiko
Suatu sumber atau penyebab yang dapat mengakibatkan terjadinya suatu kejadian/peristiwa risiko.

bb) Gejala Risiko
Pengidentifikasian pemicu Risiko dapat membantu kita mengantisipasi saat Risiko akan terjadi.

cc) Faktor Positif
Suatu kendali yang sudah ada atau sudah diimplementasikan dan dijalankan sejak lama, yang dapat menghambat atau menanggulangi terjadinya suatu Risiko.

dd) Dampak Kualitatif
Hasil dari persepsi orang atau masyarakat.

ee) Dampak kuantitatif
Hasil dari monetisasi atau perhitungan keuangan suatu risiko yang telah terjadi. Dan

ff) Risiko bawaan
Tingkat risiko alami dalam suatu proses yang belum dikendalikan atau dimitigasi.

2) Tujuan dan Manfaat

a) Tujuan

Adapun tujuan penerapan manajemen risiko di lingkungan Pusdatin Kemhan RI adalah sebagai berikut:

(1) Meningkatkan kemungkinan pencapaian tujuan dan kinerja.

(2) Mendorong manajemen yang proaktif.

(3) Memberikan dasar yang kuat dalam pengambilan keputusan dan perencanaan.

(4) Meningkatkan efektivitas alokasi dan efisiensi penggunaan sumber daya organisasi.

(5) Meningkatkan kepatuhan kepada ketentuan peraturan yang berlaku.

(6) Meningkatkan kepercayaan para pemangku kepentingan di lingkungan Kementerian Pertahanan RI. Dan

(7) Meningkatkan ketahanan organisasi Pusat Data dan Informasi Kementerian Pertahanan RI.

b) Manfaat

Adapun manfaat penerapan manajemen risiko di lingkungan Pusdatin Kemhan RI adalah sebagai berikut:

(1) Dapat melakukan pengendalian kejadian yang tidak diinginkan.

(2) Pengelolaan risiko yang sistematis.

(3) Meningkatnya perencanaan, kinerja, dan efektivitas unit kerja di Pusdatin Kemhan RI.

(4) Meningkatnya hubungan dengan para pemangku kepentingan.

(5) Meningkatnya mutu informasi untuk pengambilan keputusan.

(6) Meningkatnya reputasi di antara satuan kerja lain di lingkungan Kemhan RI.

(7) Meningkatnya kesadaran akan risiko di lingkungan Pusdatin Kemhan RI. Dan

(8) Meningkatnya akuntabilitas dan tata Kelola Pusdatin Kemhan RI.

3) Manajemen Risiko

a) Prinsip manajemen risiko

Manajemen di lingkungan Pusat Data dan Informasi Kementerian Pertahanan RI memiliki tanggung jawab utama untuk manajemen Risiko dan pengendalian internal, termasuk untuk penentuan sifat dan tingkat Risiko utama yang diambil untuk mencapai tujuan strategis dan untuk memastikan bahwa budaya yang sesuai telah tertanam di lingkungan Pusdatin Kemhan RI. Pedoman ini memberikan gambaran tingkat tinggi tentang beberapa faktor yang harus dipertimbangkan oleh manajemen Pusdatin Kemhan RI terkait dengan desain, implementasi, pemantauan, dan tinjauan manajemen Risiko serta sistem pengendalian internal.

b) Proses manajemen risiko

Proses manajemen Risiko adalah penerapan sistematis kebijakan, prosedur, dan teknik manajemen untuk kegiatan komunikasi dan konsultasi, pengaturan konteks, identifikasi Risiko, analisis Risiko, penilaian Risiko, mitigasi Risiko, serta pemantauan dan tinjauan. Proses manajemen Risikodilakukan oleh seluruh jajaran manajemen dan seluruh staf di lingkungan Pusdatin Kemhan RI. Proses manajemen Risikoharus menjadi bagian yang terintegrasi dari keseluruhan proses manajemen, budaya organisasi, dan konsisten dengan proses bisnis yang berlaku di lingkungan Kemhan RI.
Adapun proses manajemen Risiko dilaksanakan melalui tahapan sebagai berikut:

(1) Komunikasi dan konsultasi baik kepada para pemangku kepentingan internal maupun pemangku kepentingan eksternal.

(2) Penetapan konteks untuk mendeskripsikan tujuan, parameter internal dan eksternal yang akan dipertimbangkan dalam mengelola Risiko yang ada.

(3) Identifikasi Risiko untuk mengidentifikasi kejadian, penyebab, dan konsekuensi setiap peristiwa Risikoyang dapat menghalangi, menurunkan, atau menunda pencapaian tujuan Organisasi sebagaimana yang telah ditetapkan di renstra.

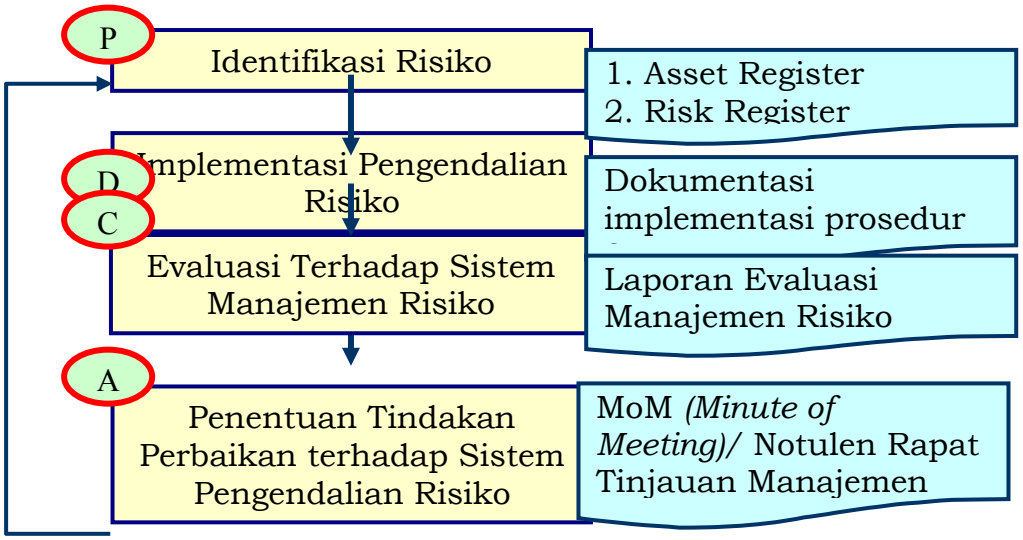
(4) Analisis Risiko dilakukan dengan cara menentukan tingkat konsekuensi dan tingkat kemungkinan terjadinya Risiko.

(5) Evaluasi Risiko untuk membantu upaya penanganan Risikoserta penentuan prioritas penanganan.

(6) Mitigasi Risiko dilakukan dengan mengidentifikasi berbagai opsi mitigasi Risiko yang akan diterapkan. Dan

(7) Pemantauan dan peninjauan dilakukan secara berkala setidaknya satu (1) tahun sekali terhadap seluruh aspek dari proses pengelolaan risiko.

Berdasarkan petunjuk umum (*general guideline*) dari Kementerian terkait (Kominfo) dan ketentuan dari Standar ISMS ISO 27001:2013, Pusdatin Kemhan RI menetapkan pedoman yang berisi kerangka (*framework*) manajemen Risiko, sebagai pedoman dalam pengendalian Risiko terkait informasi.
Secara garis besar, kerangka (*framework*) manajemen Risiko informasi di Pusdatin Kemhan RI adalah mengikuti kaidah Plan-Do-Check-Action (PDCA), yang digambarkan sebagai berikut:



b. *Plan* "Identifikasi Risiko"

1) Pendekatan Identifikasi Risiko

Tim Satgas SMKI beserta perwakilan dari setiap bidang/bagian diharuskan melakukan identifikasi Risiko terhadap segala potensi ancaman yang dapat menggangu kondisi organisasi dan pencapaian sasaran strategis Pusdatin Kemhan RI dengan pendekatan dijelaskan dalam diagram di

bawah ini. Hasil dari Penilaian Risiko adalah berupa Risk Register (Register Risiko) yang secara ringkasan dituangkan dalam Risk Assessment Report untuk kemudian disetujui oleh Kepala Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia (Kapusdatin Kemhan RI).

Identifikasi Risiko Terhadap Pencapaian IKU Pimpinan

a. Lakukan pendataan semua potensi ancaman terhadap pencapaian IKU Kabid/Kabag dari aspek Infrastruktur TIK, pengoperasian sistem aplikasi, keamanan informasi dan tata kelola layanan.

b. Tuliskan seluruh potensi ancaman yang berdampak di Risk Register sesuai prosedur Registrasi Asset, Penilaian Risiko dan Tindak lanjut Nomor: SOP/18/VIII/2022/PUSDATIN.

c. Identifikasi kemungkinan serta dampak terhadap setiap IKU pada risk register.

Penilaian Risiko Inherent

a. Tentukan tingkat dampak dan kemungkinan, dengan berpedoman pada ketentuan pada prosedur tersebut diatas. Masukkan nilai besaran Risiko di *Risk Register*.

b. Hitung nilai Risiko *inherent* berdasarkan perkalian: kemungkinan x dampak

c. Ketua Tim Satgas SMKI (Kabid Pamsisinfosan) menentukan tingkat akseptabilitas dari nilai Risiko yang mungkin terjadi.

Penentuan Opsi Pengendalian Risiko

a. Untuk setiap nilai Risiko inherent yang *unacceptable* (tidak diterima) maka ditentukan opsi pengendalian Risiko yang mencakup salah satu dari Eskalasi Risiko, Mitigasi Risiko, Transfer Risiko, Penghindaran Risiko atau Penerimaan Risiko.

b. Penjelasan mengenai opsi diatas dapat dibaca pada prosedur Registrasi Aset, Penilaian Risiko dan Tindak lanjut Nomor: SOP/18/VIII/2022/PUSDATIN.

Rencana Pengendalian

a. Untuk setiap opsi pengendalian yang telah dipilih, maka harus ditentukan tindakan pengendalian dan rencana tindakan pengendaliannya, sebagai berikut:

b. Buatkan dokumen Laporan Penanganan Risiko sebagai implementasi dari rencana Tindakan.

Penilaian Risiko Residual

a. Jika hasil pengendalian dibawah tingkat akseptabilitas, Risiko tersebut harus ditangani lebih lanjut sebagai Risiko residual.

b. Identifikasikan tingkat dampak dan kemungkinan yang masih tersisa walaupun pengendalian sudah diterapkan secara efektif, dengan berpedoman pada ketentuan pada prosedur Registrasi Asset, Penilaian Risiko dan Tindak lanjut Nomor: SOP/18/VIII/2022/PUSDATIN.

c. Hitung nilai Risiko residual berdasarkan perkalian: *value* x *severity* x *probability*

d. Dapatkan persetujuan manajemen atas nilai Risiko yang masih tersisa ini.

2) Pedoman Mengenali Identifikasi Risiko

Didalam menetukan identifikasi Risiko harus berdasarkan penilaian yang telah dilakukan pada registrasi aset sebelumnya. Berikut adalah ketetapan yang harus ada untuk menentukan identifikasi Risiko, yaitu :

Risk ID	*Value* (Nilai)	*Vulnerability* (Kerentanan)	*Threat* (Ancaman)	*Impact* (Dampak)

a) Risk ID No.

Penentuan nomor identitas Risiko (risk no.) berdasarkan urutan penilaian dari registrasi pada daftar Risiko (Risk Register) yang di identifikasi.

b) Value

Jumlah nilai yang ditetapkan untuk ancaman yang berpotensi menyebabkan kerusakan pada sistem teknologi informasi sehingga menghambat pencapaian sasaran strategis Pusdatin Kemhan RI. Didalam penentuan identifikasi Risiko hanya Risiko yang memiliki nilai diatas 3 yang akan di identifikasikan Risikonya (artinya kemungkinannya jarang = 2 dan dampaknya sangat kecil = 1.). Cara penentuan nilai lihat poin 3.1.1 Peta Inherent yang dijelaskan dibawah.

c) Vulnerability

Analisa ancaman terhadap sistem teknologi informasi harus mencakup analisa *vulnerability* yang berhubungan dengan sistem lingkungan. Tujuan dari langkah ini adalah untuk mengembangkan daftar kelemahan (kerentanan) sistem yang bisa di ungkapkan oleh sumber-sumber ancaman potensial.

d) Threat

Tahapan ini mengenai permasalahan ancaman yang berasal dari sumber tertentu, supaya dapat diatasi dengan melakukan *vulnerability assessment*. *Vulnerability* (kerentanan) adalah faktor kelemahan yang dapat tanpa sengaja diungkapkan. Ancaman tidak dapat menimbulkan Risiko jika ada *vulnerability* yang dieksekusi. Dalam menentukan kemungkinan ancaman perlu mempertimbangkan ancaman/sumber dari potensi

vulnerability. Sumber ancaman didefinisikan sebagai keadaan atau peristiwa yang berpotensi menyebabkan kerusakan pada sistem teknologi informasi. Umumnya bersumber dari alam, manusia dan lingkungan.
Berikut contoh sumber ancaman :

(1) Sumber ancaman dari alam

Alam dapat menjadi sumber ancaman yang tak terduga seperti banjir, gempa bumi, ataupun badai. Hal tersebut dapat mengganggu aktivitas usaha bila sistem teknologi informasi mengalami kerusakan.

(2) Sumber ancaman dari manusia

Manusia dapat menjadi sumber ancaman dari tindakan yang di sengaja, seperti tindakan berbahaya yang dilakukan dengan sengaja oleh orang atau karyawan yang tidak puas dan tindakan yang tidak sengaja dilakukan seperti kelalaian atau kesalahan. Contoh tindakan yang sengaja dilakukan adalah upaya jahat untuk mendapatkan akses teknologi informasi secara tidak sah ke dalam sistem (misalnya, melalui menebak *password*). Tindakan dalam upaya menghindari sistem keamanan lainnya adalah melalui serangan yang sengaja di tulis programer yaitu Program *Trojan Horse.*

(3) Sumber ancaman dari lingkungan

Walaupun letak *server* IT berada di lantai atas dan tidak dapat terkena banjir alami, tetapi banjir bisa berasal dari kebocoran pipa air yang ada di dekat area server. Banjir tersebut dapat menyebabkan kerusakan pada kegiatan organisasi teknologi informasi dan sumber daya.

e) Impact

Tahapan ini merupakan penentuan dampak negatif yang di hasilkan dari pengungkapan *vulnerability*. Dampak merugikan dari peristiwa keamanan dapat digambarkan dalam hal kehilangan atau kerugian apapun, tiga dampak negatif adalah:

(1) Hilangnya kerahasiaan *(Loss of Confidential)* adalah dampak dari pengungkapan yang tidak

sah/pencurian informasi yang sensitif. Sistem dan kerahasiaan data mengacu pada perlindungan informasi dari pengungkapan yang tidak sah. Dampak dari pengungkapan yang tidak sah terhadap informasi rahasia dapat membahayakan keamanan nasional sehingga pengungkapan data aktual yang bersifat sangat pribadi. Pengungkapan tidak sah, tidak terduga, atau tidak disengaja bisa mengakibatkan hilangnya kepercayaan publik, rasa malu, maupun tindakan hukum terhadap organisasi.

(2) Hilangnya keutuhan *(Loss of Integrity)* adalah dampak jika sistem atau integritas data hilang oleh perubahan tidak sah/pencurian terhadap data atau sistem. Sistem dan integritas data mengacu pada persyaratan bahwainformasi harus dilindungi dari modifikasi yang tidak benar. *Loss of Integrity* adalah penghilangan secara tidak sah perubahan yang dilakukan terhadap data atau sistem TI baik oleh tindakan disengaja atau tidak disengaja. Jika hilangnya integritas sistem atau data tidak diperbaiki, maka kelanjutan penggunaan sistem yang terkontaminasi atau data yang rusak bisa mengakibatkan ketidakakuratan, penipuan, atau keputusan yang salah terhadap penggunaan data.

(3) Hilangnya ketersediaan *(Loss of Availability)* adalah dampak bagi fungsi dan efektivitas operasional sistem. Jika sistem teknologi informasi tidak menyediakan tujuan tentang kriktikal sistem untuk pengguna akhirnya, maka tujuan organisasi akan terpengaruh. Kehilangan fungsi dan efektivitas operasional, misalnya dapat mengakibatkan hilangnya waktu produktif, sehingga menghambat kinerja pengguna akhir yaitu fungsi mereka dalam mendukung tujuan organisasi,

3) Pedoman Penilaian Risiko (*Inherent Risk* maupun Residual Risk)

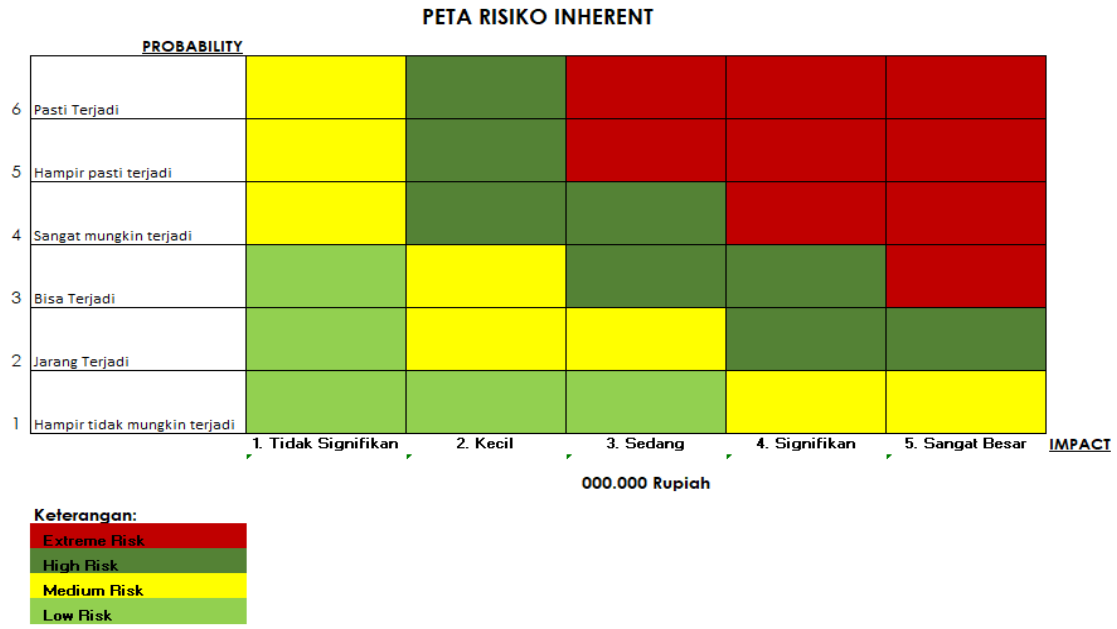
Penilaian penerapan manajemen risiko berupa penilaian profil risiko meliputi penilaian dan penetapan tingkat risiko inheren dan tingkat risiko residual. Berikut adalah cara penentuan penilaian risiko melalui pemetaan tingkat risiko yang dapat ditentukan berdasarkan nilai tingkat ancaman.

a) Peta Risiko

Secara umum, peta risiko risiko Pusdatin Kemhan RI terbagi menjadi dua, yaitu peta risiko inherent dan peta risiko residual. Secara detail dijelaskan pada tabel berikut:

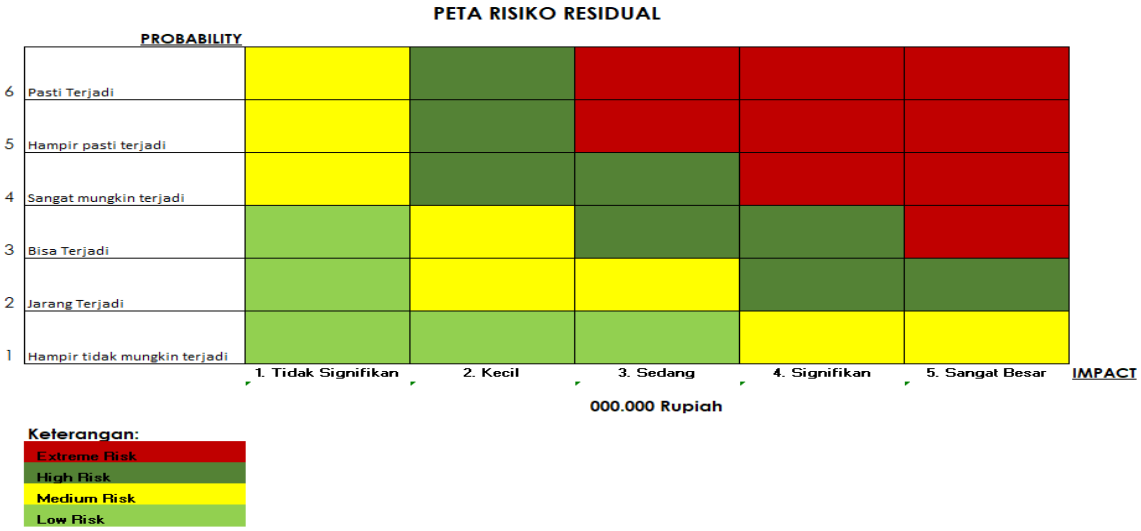
(1) Peta Risiko *Inherent*

Peta risiko inherent adalah sebagai berikut:



(2) Peta Risiko Residual

Peta risiko residual adalah sebagai berikut:



(3) Tabel Acuan

Tabel.1 Tabel Acuan Dampak

Indeks	Tipe Dampak	Dampak Reputasi	Dampak Keselamatan
5	Sangat Besar	Hancurnya reputasi secara nasional	Kematian karyawan atau masyarakat
4	Besar (signifikan)	Hilang reputasi secara propinsi	Luka besar pada beberapa orang
3	Sedang	Reputasi buruk dalam tingkat kota/kabupaten	Luka besar pada satu orang
2	Kecil	Reputasi buruk tingkat internal organisasi	Luka kecil
1	Sangat kecil (tidak signifikan)	Tidak ada dampak pada reputasi	Tidak menyebabkan dampak pada keselamatan

Tabel. 2 Tabel Acuan Kemungkinan

Indeks	Deskripsi	Kemungkinan
6	Pasti Terjadi	90% < X ≤ 100%
5	Hampir pasti terjadi	70% < X ≤ 90%
4	Sangat mungkin terjadi	50% < X ≤ 70%
3	Bisa Terjadi	30% < X ≤ 50%
2	Jarang Terjadi	10% < X ≤ 30%
1	Hampir tidak mungkin terjadi	0% ≤ X ≤ 10%

(4) Daftar Risiko *(Risk Register)*

Daftar risiko *(risk register)* adalah dokumen yang berisi catatan informasi tentang risiko yang telah teridentifikasi di lingkungan Pusdatin Kemhan RI. Proses ini bertujuan untuk secara kolektif mengidentifikasi, menganalisis, dan memecahkan risiko sebelum terjadinya masalah dan melakukan mitigasi. Berikut di bawah ini adalah table daftar risiko beserta penjelasan masing-masing kolom.

No	Risk ID	Strategic Objective	Proses Bisnis	Kategori Risiko	Kejadian Risiko	Penyebab Risiko	Gejala Risiko	Faktor Positif	Dampak Kualitatif	**Inherent**				**Residual**									
										Dampak Kuantitatif (Juta Rupiah)	Kemungkinan	Dampak	Risk Priority Number (RPN)	Rencana Mitigasi	Biaya Mitigasi (Juta Rupiah)	PIC	Tlp/ Email	Tgl Mulai	Tgl Selesai	Dampak Kuantitatif (Juta Rupiah)	Kemungkinan	Dampak	Risk Priority Number (RPN)

1) Analisis risiko kualitatif
Proses penilaian risiko berdasarkan persepsi seseorang tentang tingkat keparahan dan kemungkinan konsekuensinya.

2) Analisis Risiko Kualitatif
Proses menghitung risiko berdasarkan data yang dikumpulkan.

3) Risk ID
Atau nama yang digunakan untuk mengidentifikasi suatu risiko.

4) Tujuan Strategis
Tujuan yang didapatkan dari rencana strategis untuk pengidentifikasian Risiko.

5) Proses Bisnis
Aktivitas atau serangkaian aktivitas yang mencapai tujuan organisasi tertentu.

6) Kategori Risiko
Pengelompokkan risiko berdasarkan sumbernya, area yang terkena dampak dan kelompok lainnya yang berkaitan.

7) Kejadian Risiko
Realisasi konkret (manifestasi) dari Risiko yang abstrak.

8) Penyebab Risiko
Suatu sumber atau penyebab yang dapat mengakibatkan terjadinya suatu kejadian/peristiwa risiko

9) Gejala Risiko
Pengidentifikasian pemicu risiko dapat membantu kita mengantisipasi saat risiko akan terjadi.

10) Faktor Positif
Suatu kendali yang sudah ada atau sudah diimplementasikan dan dijalankan sejak lama, yang dapat menghambat atau menanggulangi terjadinya suatu risiko.

11) Dampak Kualitatif
Hasil dari persepsi orang atau masyarakat.

12) Dampak Kuantitatif
Hasil dari monetisasi atau perhitungan keuangan suatu risiko yang telah terjadi.

13) Risiko Bawaan (*Inherent Risk*)
Tingkat risiko alami dalam suatu proses yang belum dikendalikan atau dimitigasi.

14) Risiko Residual (*Residual Risk*)
Risiko yang tersisa setelah menerapkan pengendalian yang direkomendasikan.

15) *Risk Priority Number* (RPN)
Suatu indikator untuk mengukur risiko dari moda kegagalan dan menentukan tingkat skala prioritas perbaikan yang harus dilakukan terlebih dahulu. Skor RPN didapatkan dari hasil perkalian nilai dampak (*severity*), kemungkinan (*occurrence*) dan deteksi (*detection*). Nilai deteksi adalah peringkat seberapa telitinya alat deteksi yang digunakan. Deteksi berupa angka dari 1 hingga 10 dimana 1 menunjukkan sistem deteksi dengan kemampuan tinggi atau hampir dipastikan suatu mode kegagalan dapat terdeteksi. Dalam hal ini nilai deteksi diasumsikan 1.

b. Do ”Implementasi Pengendalian Risiko”

Setelah register Risiko/risk register (sebagai hasil dari kegiatan analisis Risiko) disetujui oleh Kapusdatin, selanjutnya dilakukan hal-hal sebagai berikut:

1) Ketua Tim Satgas SMKI mengkoordinasikan implementasi dari rencana-rencana pengendalian Risiko yang telah ditetapkan dalam register Risiko. Hal ini mencakup:

   a) Pembuatan pedoman, prosedur dan instruksi kerja terkait Sistem Keamanan Informasi

   b) Melakukan penyempurnaan terhadap kebijakan dan peraturan terkait Sistem Keamanan Informasi

2) Ketua Tim Satgas SMKI mengordinasikan agar pihak-pihak terkait mengimplementasikan Sistem Keamanan Informasi, sesuai dengan yang diindentifikasikan dalam pedoman/prosedur/instruksi kerja.

3) Ketua Tim Satgas SMKI memastikan bahwa semua dokumentasi yang diperlukan sebagai hasil dari implementasi Sistem Keamanan Informasi dipelihara oleh pihak-pihak terkait, sesuai dengan yang ditetapkan dalam pedoman/prosedur/instruksi kerja

c. Check ”Evaluasi Terhadap Sistem Manajemen Risiko”

Minimal satu tahun satu kali, terhitung dari register Risiko/ perubahan register ditetapkan, Ketua Tim Satgas SMKI beserta perwakilan dari Bagian/Bidang, melakukan evaluasi terhadap sistem manajemen Risiko yang telah diterapkan, Hasil dari evaluasi

dituangkan dalam Laporan Evaluasi Manajemen Risiko yang memuat hal-hal sebagai berikut:

1) Rangkuman hasil dari *Technical Vulnerability Assessment* seperti kegiatan *patching* perangkat lunak dan OS, *penetration test*, dsb.

2) Rangkuman hasil pelaporan deteksi kelemahan oleh pegawai, internal audit, *assessment* pihak ketiga, *assessment* dari grup, dsb.

3) Hasil analisis yang menggambarkan poin-poin untuk perbaikan *risk register*, prosedur-prosedur terkait implementasi pengendalian risiko dan jika diperlukan juga mencakup usulan atas perbaikan dokumen Kerangka Penilaian Risiko Informasi.

Laporan Evaluasi Manajemen Risiko dapat dipresentasikan pada saat Rapat Tinjauan Manajemen berikutnya atau rapat evaluasi lainnya terkait masalah keamanan informasi.

Oleh karena suatu keadaan yang cukup penting, seperti setelah insiden kritis, audit, *vulnerability test* yang menghasilkan temuan-temuan kritis, *risk register* dapat dievaluasi dan diperbaharui. Apabila hal ini terjadi, *risk register* baru perlu ditetapkan kembali oleh Kepala Pusdatin Kemhan RI. Untuk hal ini, tidak perlu dibuatkan Laporan Evaluasi Manajemen Risiko

d. Action ”Penentuan Tindakan Perbaikan Terhadap Sistem Pengendalian Risiko”

Tindakan perbaikan terhadap Sistem Pengendalian Risiko, baik terhadap risk register, implementasi pengendalian Risiko, maupun Kerangka Penilaian Risiko Informasi ini dituangkan dalam Risalah Rapat Tinjauan Manajemen. Lebih jauh tentang mekanisme ini merujuk kepada Prosedur Rapat Tinjauan Manajemen.

BAB III
PENUTUP

3. Penutup

a. Demikian Pedoman Kerja Registrasi Aset dan Penilaian Resiko ini di buat, sebagai acuan dalam pengamanan informasi di Pusdatin.

b. Pedoman ini berlaku sejak di tandatangani dan ketentuan yang belum tercantum dalam pedoman ini akan diatur lebih lanjut dengan

memperhatikan perkembangan Sistem Manajemen Keamanan Informasi.

c. Dokumen asli dari prosedur ini dipelihara dan dikendalikan oleh Dokumen Kontrol di Bidang Pamsisinfosan Pusdatin Kemhan RI.

d. Penggunaan dokumen asli ataupun dokumen salinan harus mengikuti aturan yang tertulis pada Dokumen Prosedur Pengendalian Dokumen Nomor: SOP/22/VIII/2022/PUSDATIN.

Dikeluarkan di Jakarta
Pada tanggal Agustus 2022

Kepala Pusat Data dan Informasi,

Rionardo
Brigadir Jenderal TNI