KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 3 TAHUN 2024

GARIS PANDUAN
PENGURUSAN RISIKO KESELAMATAN MAKLUMAT SEKTOR AWAM

JABATAN PERDANA MENTERI

21 MAC 2024

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI
PRIME MINISTER'S DEPARTMENT
Blok B8, Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
MALAYSIA

Tel. : 03-8000 8000
Fax : 03-8888 3904
Web : http://www.jpm.gov.my
Emel : jpm@jpm.gov.my

Ruj. Kami : MKN.10.700-8/151 JLD 3 (5)

Tarikh : 21 Mac 2024

Semua Ketua Setiausaha Kementerian

Semua Ketua Jabatan Persekutuan

Semua YB Setiausaha Kerajaan Negeri

Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri

Semua Pihak Berkuasa Tempatan

SURAT PEKELILING AM BILANGAN 3 TAHUN 2024

GARIS PANDUAN
PENGURUSAN RISIKO KESELAMATAN MAKLUMAT SEKTOR AWAM

1. TUJUAN

1.1 Garis Panduan Pengurusan Risiko Keselamatan Maklumat ini disediakan kepada organisasi sektor awam untuk dijadikan rujukan bagi pelaksanaan pengurusan risiko keselamatan maklumat.

1.2 Garis panduan ini menyenaraikan kaedah serta menerangkan langkah-langkah menguruskan risiko keselamatan maklumat secara bersistematik dan berkesan.

1.3 Garis panduan ini dibangunkan berdasar kepada beberapa garis panduan dan piawaian antarabangsa pengurusan risiko. Antaranya adalah ISO 31000, MS ISO 31000 dan ISO/IEC 27005.

2. LATAR BELAKANG

2.1 Transformasi digital adalah paksi perubahan dalam dunia masa kini, yang dipacu oleh perkembangan teknologi digital dalam pelbagai aspek kehidupan. Dengan kemajuan kecerdasan buatan, kecekapan jaringan telekomunikasi dan kepesatan pertumbuhan data, transformasi digital menjadi daya penggerak utama dalam perkembangan masyarakat, hubungan perniagaan dan penyampaian perkhidmatan.

2.2 Usaha kerajaan dalam menambah baik sistem penyampaian perkhidmatan awam melalui perkhidmatan pendigitalan menyaksikan kesan yang amat positif. Perkhidmatan pendigitalan ini membolehkan pelbagai perkhidmatan kerajaan dapat diakses dengan pantas, mudah dan efisien.

2.3 Namun, seiring dengan perkembangan perkhidmatan pendigitalan ini, sistem penyampaian perkhidmatan awam turut terdedah kepada pelbagai risiko. Serangan siber seperti penafian perkhidmatan, pencerobohan dan jangkitan perisian

hasad merupakan antara risiko yang boleh menyebabkan ketirisan dan kehilangan maklumat kerajaan.

2.4 Sehubungan dengan itu, bagi memastikan sistem penyampaian perkhidmatan awam berada dalam keadaan terbaik dan maklumat kerajaan sentiasa tersedia dan berintegriti, risiko keselamatan maklumat perlu dikenal pasti dan ditangani dengan sebaik mungkin. Risiko ini boleh dikurangkan melalui pengurusan risiko yang berkesan.

2.5 Pengurusan risiko keselamatan maklumat bertujuan membolehkan organisasi sektor awam mengenal pasti risiko, menganalisis risiko, menilai tahap risiko, dan seterusnya mengambil tindakan untuk mengawal risiko.

3. PELAKSANAAN

Garis Panduan ini menyediakan langkah-langkah pelaksanaan proses pengurusan risiko keselamatan maklumat untuk rujukan organisasi sektor awam.

4. TANGGUNGJAWAB ORGANISASI SEKTOR AWAM

4.1 Organisasi Sektor Awam perlu melaksana proses pengurusan risiko keselamatan maklumat secara berkala (sekurang-kurangnya sekali dalam setahun).

4.2 Proses pengurusan risiko boleh dibuat secara dalaman (*in-house)* atau melalui perkhidmatan pihak ketiga yang bertauliah.

4.3 Proses pengurusan risiko keselamatan maklumat yang melibatkan aktiviti penilaian risiko dan penguraian risiko boleh dilaksanakan secara berulang sehingga pengurusan atasan organisasi berpuas hati dengan maklumat dan hasil kedua-dua aktiviti tersebut.

5. PEMAKAIAN

5.1 Surat Pekeliling Am ini terpakai kepada semua organisasi Perkhidmatan Awam Persekutuan bermula dari tarikh pekeliling ini ditandatangani.

5.2 Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan Surat Pekeliling Am ini pada keseluruhannya dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Negeri dan Pihak Berkuasa Tempatan.

6. PEMBATALAN

Dengan berkuat kuasanya Surat Pekeliling Am ini, pekeliling dan surat pekeliling yang berikut adalah dibatalkan:

6.1 Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 Nov 2005.

6.2 Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Risiko Keselamatan Maklumat Menggunakan MyRAM App 2.0 di Agensi Sektor Awam bertarikh 12 Ogos 2015.

7. MAKLUMAT PERTANYAAN

Sebarang kemusykilan berkaitan dengan Surat Pekeliling Am ini hendaklah dirujuk kepada Agensi Keselamatan Siber Negara (NACSA) melalui maklumat perhubungan seperti di berikut:

Agensi Keselamatan Siber Negara (NACSA)
Majlis Keselamatan Negara
Aras LG & G, Blok Barat
Bangunan Perdana Putra
62502 PUTRAJAYA
No. Telefon: 03-8064 4888
E-mel: admin@nacsa.gov.my

8. TARIKH KUAT KUASA

Surat Pekeliling Am ini berkuat kuasa mulai dari tarikh ia dikeluarkan

"BERKHIDMAT UNTUK NEGARA"

(TAN SRI DATO' SERI MOHD ZUKI BIN ALI)
Ketua Setiausaha Negara

GARIS PANDUAN
PENGURUSAN RISIKO KESELAMATAN MAKLUMAT SEKTOR AWAM

AGENSI KESELAMATAN SIBER NEGARA (NACSA)

MAJLIS KESELAMATAN NEGARA

JABATAN PERDANA MENTERI

ISI KANDUNGAN

TAFSIRAN

Bagi tujuan Pekeliling Am ini, terma yang digunakan ditafsirkan seperti berikut:

i.	Analisis Risiko	Proses untuk memahami sifat risiko dan tahap risiko.
ii.	Ancaman	Kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah ke atas aset Teknologi Maklumat dan Komunikasi (ICT).
iii.	Aset	Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya berlaku kehilangan, kerosakan atau perubahan. Dalam konteks keselamatan maklumat, aset boleh dikategorikan kepada beberapa kumpulan antaranya proses kerja, data/maklumat, perisian, perkakasan, perkhidmatan, sumber manusia dan tapak / premis.

iv.	Baki risiko	Tahap risiko yang terkini selepas penguraian atau rawatan risiko.
v.	Kawalan	Langkah pengukuhan yang diambil untuk mengurus atau mengubahsuai risiko.
vi.	Kebarangkalian	Kemungkinan sesuatu peristiwa berlaku.
vii.	Kerentanan	Kelemahan / sifat mana-mana aset, proses atau aktiviti yang boleh meningkatkan kebarangkalian berlakunya ancaman dan menyebabkan mudarat dalam soal kerahsiaan, integriti dan ketersediaan maklumat.
viii.	Kerahsiaan Maklumat	Maklumat dilindungi daripada capaian yang tidak dibenarkan.
ix.	Ketersediaan Maklumat	Maklumat dapat dicapai pada bila-bila masa oleh pihak yang diberi kuasa.
x.	Komunikasi dan rundingan	Proses berterusan dan berulang yang dijalankan oleh organisasi

		untuk menyedia, berkongsi atau mendapatkan maklumat.
xi.	Impak	Akibat atau kesan daripada perkara atau peristiwa yang menjejaskan objektif.
xii.	Integriti Maklumat	Maklumat yang tepat dan lengkap serta hanya boleh diubahsuai dengan cara yang dibenarkan.
xiii.	Pemilik risiko	Personel yang mempunyai akauntabiliti dan kuasa untuk menguruskan risiko.
xiv.	Pentadbir Aset	Personel yang bertanggungjawab terhadap penggunaan dan pengurusan sesebuah aset ICT.
xv.	Risiko	Kecenderungan berlakunya sesuatu peristiwa yang memberi kesan kepada pencapaian objektif akibat dari pelaksanaan sesuatu tindakan.
xvi.	Tahap Risiko	Tahap risiko diperoleh dari gabungan impak dengan kebarangkalian.

1. PENGENALAN PENGURUSAN RISIKO

1.1 Pengurusan risiko merupakan penyelarasan aktiviti secara bersepadu melalui penetapan hala tuju dan kawalan dalam menghadapi risiko yang berkemungkinan berlaku di sesebuah organisasi. Organisasi perlu mengenal pasti, menganalisis dan menilai risiko dengan penggunaan sumber secara teratur bagi mengurangi, memantau dan mengawal kemungkinan serta kesan risiko tidak diingini.

1.2 Berdasarkan ISO 31000 dan MS ISO 31000, proses pengurusan risiko melibatkan penggunaan dasar, prosedur dan amalan yang sistematik terhadap enam (6) perkara:

a. Komunikasi dan Rundingan

b. Skop, Konteks dan Kriteria

c. Penilaian Risiko

d. Penguraian Risiko

e. Pemantauan dan Penyemakan

f. Perekodan dan Pelaporan

1.3 Rajah 1 menunjukkan kitaran hayat proses pengurusan risiko seperti yang ditakrifkan dalam piawaian MS ISO 31000.

Rajah 1. Proses Pengurusan Risiko
(Sumber: ISO 31000, MS ISO 31000)

1.3.1 Komunikasi dan Rundingan (*Communication & Consultation*)

1.3.1.1 Komunikasi dan rundingan adalah penting dalam proses pengurusan risiko bagi memastikan pelaksanaan yang berkesan.

1.3.1.2 Objektif komunikasi dan rundingan adalah untuk membantu pihak berkepentingan dalaman dan luaran organisasi seperti pengurusan atasan, kakitangan, pembekal, pelanggan dan pemegang taruh dalam memahami risiko, asas

keputusan risiko dibuat dan sebab tindakan tertentu diperlukan.

1.3.1.3 Komunikasi bertujuan untuk menggalakkan kesedaran dan pemahaman tentang risiko, manakala rundingan melibatkan pengumpulan maklum balas dan maklumat untuk menyokong dalam membuat keputusan.

1.3.1.4 Komunikasi dan rundingan adalah berkait rapat antara satu sama lain bagi memudahkan pertukaran maklumat yang berfakta, relevan, tepat dan boleh difahami, dengan mengambil kira kerahsiaan dan integriti maklumat.

1.3.1.5 Komunikasi dan rundingan dengan pihak berkepentingan luaran dan dalaman organisasi sewajarnya dilakukan disepanjang proses pengurusan risiko.

1.3.2 Skop, Konteks dan Kriteria (*Scope, Context, Criteria*)

1.3.2.1 Sebelum risiko dinilai, organisasi perlu terlebih dahulu menentukan skop, konteks dan kriteria penerimaan risiko.

1.3.2.2 Tujuan menentukan skop, konteks dan kriteria penerimaan risiko adalah untuk membolehkan

proses pengurusan risiko direka dan dilaksana dengan berkesan dan bersesuaian.

1.3.2.3 Penentuan skop harus jelas dan sejajar dengan konteks objektif organisasi. Kajian terhadap kedua-dua konteks luaran dan dalaman diperlukan pada permulaan perancangan penilaian risiko. Kajian ini melibatkan pengenalpastian kekuatan, kelemahan, peluang dan ancaman dalam persekitaran dalaman dan luaran organisasi.

1.3.2.4 Kriteria penerimaan risiko juga perlu ditentukan untuk menilai kepentingan risiko bagi menyokong proses membuat keputusan. Kriteria penerimaan risiko membolehkan organisasi mentakrifkan dengan jelas tahap risiko yang boleh diterima atau tidak boleh diterima.

1.3.3 Penilaian Risiko (*Risk Assessment*)

1.3.3.1 Penilaian risiko ialah proses keseluruhan mengenal pasti risiko (*risk identification*), menganalisis risiko (*risk analysis*) dan menilai tahap risiko (*risk evaluation*). Penilaian risiko hendaklah dijalankan secara sistematik, berulang dan kolaboratif, berdasarkan

pengetahuan dan pandangan pihak berkepentingan.

1.3.3.2 Mengenal pasti risiko bertujuan untuk mencari, mengenali dan menerangkan risiko yang mungkin membantu atau menghalang organisasi mencapai objektifnya. Maklumat yang relevan, sesuai dan terkini adalah penting dalam mengenal pasti risiko.

1.3.3.3 Menganalisis risiko pula bertujuan untuk memahami sifat risiko dan ciri-cirinya. Menganalisis risiko melibatkan pertimbangan terperinci tentang sumber risiko, akibat risiko, kemungkinan risiko dan kesan risiko.

1.3.3.4 Menganalisis risiko turut menyediakan input kepada proses menilai risiko dan kepada pembuat keputusan sama ada risiko perlu dirawat atau tidak, strategi dan kaedah rawatan risiko yang paling sesuai.

1.3.3.5 Manakala menilai tahap risiko pula adalah untuk menyokong pembuatan keputusan. Ia melibatkan perbandingan antara hasil analisis risiko yang diperoleh dengan kriteria penerimaan risiko yang telah ditetapkan bagi menentukan tindakan tambahan yang diperlukan.

1.3.3.6 Hasil penilaian risiko perlu direkod, dikomunikasi, dibentang dan kemudian disahkan oleh peringkat atasan.

1.3.4 Penguraian Risiko (*Risk Treatment*)

1.3.4.1 Penguraian risiko merupakan proses menangani dan mengubahsuai risiko yang melibatkan pemilihan opsyen mitigasi.

1.3.4.2 Pemilihan opsyen mitigasi penguraian risiko hendaklah dibuat mengikut objektif organisasi, kriteria penerimaan risiko dan sumber yang ada.

1.3.4.3 Organisasi harus menyedia pelan penguraian risiko dan melaksana pelan tersebut. Butiran dalam pelan penguraian adalah seperti:

i. Rasional untuk memilih opsyen penguraian.

ii. Personel yang bertanggungjawab meluluskan dan melaksanakan rancangan penguraian.

iii. Tindakan yang dicadangkan untuk dilaksanakan.

iv. Sumber dan anggaran kos pelaksanaan yang diperlukan.

v. Jangkaan tempoh tindakan yang perlu diambil dan diselesaikan.

1.3.5 Pemantauan dan Penyemakan (*Monitoring & Review*)

1.3.5.1 Pemantauan dan penyemakan merupakan aktiviti menambah baik kualiti dan keberkesanan keseluruhan proses pengurusan risiko.

1.3.5.2 Pemantauan dan penyemakan harus dilakukan dalam semua peringkat proses pengurusan risiko. Aktiviti pemantauan dan penyemakan merangkumi merancang, mengumpul maklumat, menganalisis maklumat, merekod keputusan dan memberi maklum balas.

1.3.5.3 Hasil pemantauan dan penyemakan hendaklah disepadukan dalam keseluruhan aktiviti pengurusan prestasi, pengukuran dan pelaporan organisasi.

1.3.6 Perekodan dan Pelaporan (*Recording & Reporting*)

1.3.6.1 Proses pengurusan risiko dan hasilnya perlu didokumen dan dilapor melalui mekanisme yang teratur dan bersesuaian.

1.3.6.2 Perekodan dan pelaporan bertujuan untuk:

i. Menyampaikan aktiviti dan hasil pengurusan risiko di seluruh organisasi.

ii. Menyediakan maklumat untuk membuat keputusan.

iii. Menambah baik aktiviti pengurusan risiko.

iv. Membantu interaksi dengan pihak berkepentingan, termasuk pihak yang mempunyai tanggungjawab dan akauntabiliti untuk aktiviti pengurusan risiko.

2. PENGURUSAN RISIKO KESELAMATAN MAKLUMAT (PRKM)

2.1 Pengurusan risiko dalam konteks keselamatan maklumat merupakan satu pendekatan bersistematik yang diperlukan untuk mengenal pasti keperluan keselamatan organisasi bagi

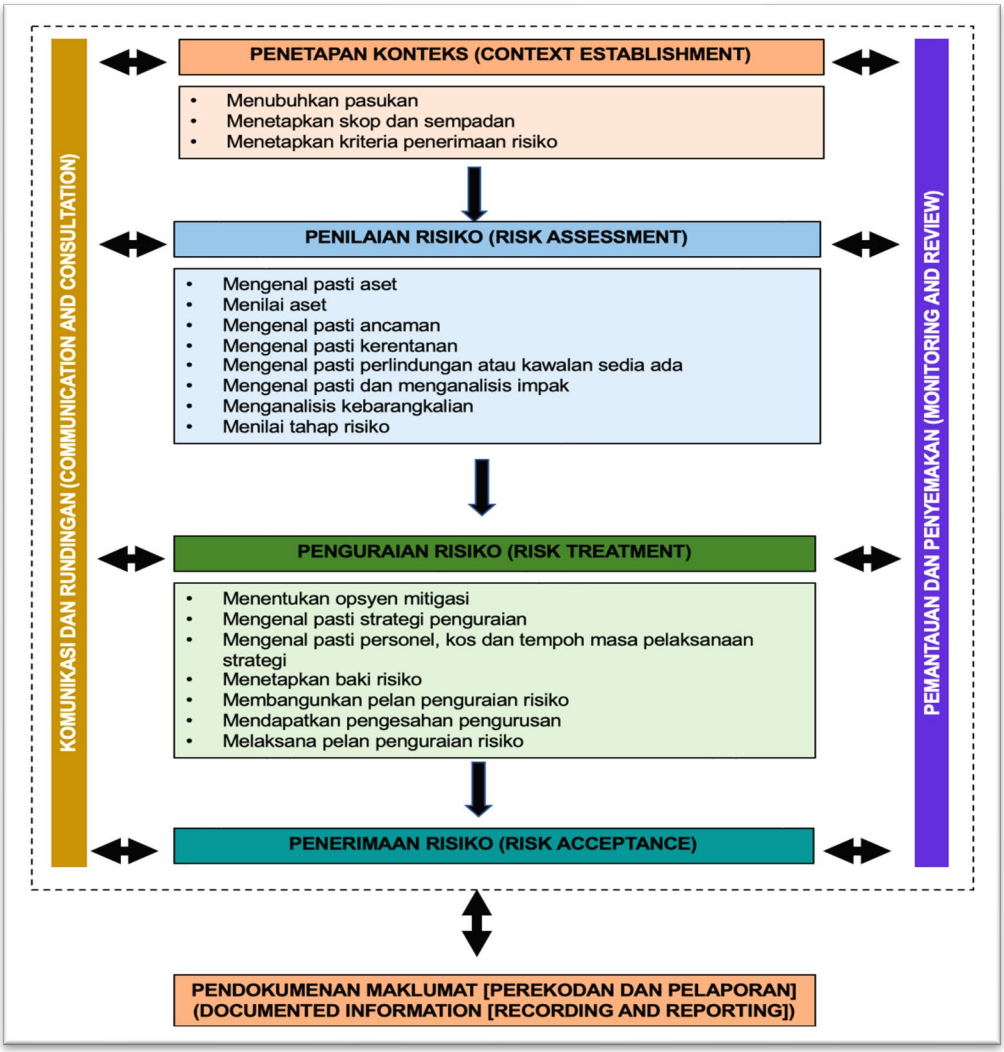
memastikan keberkesanan sistem pengurusan keselamatan maklumat.

2.2 Pengurusan Risiko Keselamatan Maklumat merupakan sebuah proses yang berterusan. Proses pengurusan risiko terdiri daripada satu siri langkah yang apabila dijalankan mengikut urutan, membolehkan penambahbaikan berterusan dalam membuat keputusan.

2.3 Proses Pengurusan Risiko Keselamatan Maklumat berdasarkan ISO/IEC 27005 melibatkan proses yang hampir sama dengan proses pengurusan risiko ISO 31000. Proses Pengurusan Risiko Keselamatan Maklumat merangkumi:

i. Penetapan Konteks (*Context Establishment*)
ii. Penilaian Risiko (*Risk Assessment*)
iii. Penguraian Risiko (*Risk Treatment*)
iv. Penerimaan Risiko (*Risk Acceptance*)
v. Komunikasi dan Rundingan (*Communication & Consultation*)
vi. Pemantauan dan Penyemakan (*Monitoring and Review*).
vii. Pendokumenan Maklumat [Perekodan dan Pelaporan] (*Documented Information* [*Recording and Reporting*])

2.4 Proses Pengurusan Risiko Keselamatan Maklumat digambarkan seperti Rajah 2.



Rajah 2. Proses Pengurusan Risiko Keselamatan Maklumat

(Adaptasi: ISO / IEC 27005)

2.4.1 Penetapan Konteks

a. Penetapan konteks menganalisis latar belakang dan persekitaran organisasi. Segala maklumat organisasi yang relevan kepada pengurusan risiko keselamatan maklumat perlu ditetapkan.

b. Aktiviti yang diperlukan dalam penetapan konteks adalah sebagaimana berikut:

i. Menubuhkan pasukan.

ii. Menetapkan skop dan sempadan.

iii. Menetapkan kriteria penerimaan risiko.

2.4.1.1 Menubuhkan Pasukan

a. Organisasi harus menubuhkan Pasukan Pengurusan Risiko Keselamatan Maklumat bagi melancarkan keseluruhan proses pengurusan risiko keselamatan maklumat.

b. Kakitangan yang terlibat dalam pengurusan risiko perlu dikenal pasti dan peranan mereka dalam Pasukan Pengurusan Risiko Keselamatan Maklumat perlu ditakrifkan.

c. Pasukan Pengurusan Risiko Keselamatan Maklumat yang ditubuhkan perlu mendapat kelulusan dan dilantik oleh pengurusan atasan.

d. Contoh struktur Pasukan Pengurusan Risiko Keselamatan Maklumat serta peranan dan tanggungjawab adalah seperti di **Lampiran A**.

2.4.1.2 Menetapkan Skop dan Sempadan

a. Organisasi hendaklah menetapkan skop dan sempadan bagi pengurusan risiko.

b. Skop perlu ditakrifkan untuk memastikan semua aset yang berkaitan diambil kira dalam penilaian risiko.

c. Manakala sempadan perlu dikenalpasti bagi memastikan risiko yang diambil kira hanya melibatkan sempadan yang ditetapkan sahaja.

d. Skop dan sempadan yang dipilih perlu dimaklumkan kepada pengurusan atasan organisasi untuk kelulusan.

e. Penilaian risiko hanya akan dilaksana terhadap aset yang dinyatakan dalam skop dan sempadan yang terlibat sahaja.

2.4.1.3 Menetapkan Kriteria Penerimaan Risiko

a. Kriteria penerimaan risiko perlu ditetapkan sebelum melaksanakan proses penilaian risiko.

b. Kriteria penerimaan risiko digunakan sebagai rujukan bagi menentukan sama ada risiko boleh diterima, tidak boleh diterima atau perlu dikurangkan.

c. Penetapan kriteria penerimaan risiko adalah bergantung kepada polisi, objektif dan matlamat organisasi. Antara yang boleh dipertimbangkan semasa penetapan kriteria penerimaan risiko adalah aspek reputasi perniagaan/perkhidmatan, undang-undang, teknologi, kewangan, operasi dan faktor sosial.

d. Contoh kriteria penerimaan risiko adalah seperti di **Lampiran B**.

2.4.2 Penilaian Risiko

a. Penilaian Risiko Keselamatan Maklumat adalah proses mengenal pasti, menganalisis dan menilai tahap risiko aset yang mungkin terjejas oleh serangan atau insiden keselamatan.

b. Penilaian risiko boleh dilaksana dengan menggunakan sebarang kaedah atau metodologi penilaian mengikut kesesuaian organisasi.

c. Aktiviti yang diperlukan dalam pelaksanaan penilaian risiko adalah sebagaimana berikut:

i. Mengenal pasti aset

ii. Menilai aset

iii. Mengenal pasti ancaman

iv. Mengenal pasti kerentanan

v. Mengenal pasti perlindungan sedia ada

vi. Mengenal pasti dan menganalisis impak

vii. Menganalisis kebarangkalian

viii. Menilai tahap risiko

d. Hasil penilaian risiko perlu direkod, dibentang dan disahkan oleh pengurusan atasan.

2.4.2.1 Mengenal Pasti Aset

a. Pasukan Pengurusan Risiko Keselamatan Maklumat harus mengenal pasti aset yang terlibat dalam skop pengurusan risiko.

b. Setiap aset dikategorikan mengikut kumpulan seperti yang ditunjukkan dalam Jadual 1.

Kategori Aset	Penerangan	Contoh
i. Proses Kerja	Proses kerja utama dan sokongan.	Proses pembayaran gaji; Proses perlesenan pembekal; Proses pendaftaran pelajar.
ii. Maklumat	Mengandungi data (salinan digital atau salinan cetak) yang telah diproses, disusun dan mempunyai makna kepada penerima.	Data pelajar; Laporan gaji; Profil pelanggan.
iii. Perkakasan	Diguna untuk menyokong pemprosesan dan penyimpanan maklumat.	Komputer; Komputer riba; Pelayan, Pencetak .

Kategori Aset	Penerangan	Contoh
iv. Perisian	Perisian aplikasi atau sistem yang menyediakan kemudahan pemprosesan maklumat.	Perisian sistem operasi; Perisian pakej / standard; aplikasi perkhidmatan
v. Perkhidmatan	Perkhidmatan sokongan dan perkhidmatan capaian yang menyokong aset lain untuk melaksana fungsinya.	Penghawa dingin; Bekalan elektrik; *Fire Suppresion System*, LAN, WAN, VPN, WIFI
vi. Sumber manusia	Individu yang terlibat dalam proses kerja atau / dan pemprosesan maklumat.	Ketua Penolong Pengarah; Penolong Pengarah; Juruteknik komputer; Pembekal
vii. Premis	Premis yang diguna untuk menempatkan perkara i – vi.	Bangunan pejabat

Jadual 1. Kategori aset dan contohnya

c. Setiap aset perlu mempunyai butiran terperinci seperti nombor siri aset, kategori aset, penerangan ringkas, pemilik dan lokasi aset tersebut berada.

d. Contoh maklumat aset adalah seperti di **Lampiran C**.

2.4.2.2 Menilai Aset

a. Pasukan Pengurusan Risiko Keselamatan Maklumat perlu melaksana penilaian terhadap aset yang telah dikenal pasti.

b. Aset dinilai berdasarkan prinsip keselamatan maklumat iaitu perlindungan terhadap kerahsiaan, integriti dan ketersediaan maklumat.

c. Antara perkara yang boleh diambil kira dalam penilaian aset adalah dengan melihat kesan daripada kehilangan perlindungan kerahsiaan, integriti dan ketersediaan maklumat seperti gangguan terhadap operasi organisasi, hilang keyakinan pelanggan, pelanggaran kontrak dan kerugian kewangan.

d. Setiap aset dinilai mengikut skala yang tertentu. Antara skala yang biasa digunakan dalam menilai aset adalah skala tiga tahap (Rendah, Sederhana, Tinggi) dan Skala lima tahap (Sangat Rendah, Rendah, Sederhana, Tinggi, Sangat Tinggi).

e. Pasukan Pengurusan Risiko Keselamatan Maklumat bebas untuk membangunkan atau memilih skala penilaian mengikut kesesuaian organisasi.

f. Contoh skala penilaian dan pengiraan nilai aset adalah seperti di **Lampiran D**.

2.4.2.3 Mengenal Pasti Ancaman

a. Pasukan Pengurusan Risiko Keselamatan Maklumat perlu mengenal pasti ancaman yang mungkin berlaku terhadap aset.

b. Ancaman mungkin datang secara tidak sengaja atau disengajakan. Ancaman juga mungkin timbul dari dalam atau luar organisasi.

c. Sesetengah ancaman boleh menjejaskan lebih daripada satu aset dan setiap aset pula boleh mempunyai satu atau lebih ancaman.

d. Panduan ringkas berikut boleh digunakan untuk mengenal pasti ancaman:

    i. Ancaman yang telah berlaku sebelum ini.

    ii. Ancaman yang mungkin berlaku sekiranya tiada tindakan pencegahan proaktif diambil.

    iii. Ancaman yang mungkin berlaku walaupun pencegahan proaktif telah diambil.

e. Ancaman juga boleh dikenal pasti melalui penyemakan dokumen, log serta aduan pelanggan; dan pertanyaan kepada pemilik atau pengguna aset, kakitangan organisasi serta pakar pengurusan keselamatan maklumat dalam dan luar organisasi.

f. Contoh ancaman yang mungkin berlaku adalah seperti di **Lampiran E.**

2.4.2.4 Mengenal Pasti Kerentanan

a. Semua potensi kerentanan yang mungkin dieksploitasi oleh ancaman perlu dikenal pasti.

b. Kerentanan boleh dikenal pasti melalui pelbagai aspek seperti:

i Organisasi

ii Proses dan prosedur

iii Rutin pengurusan

iv Kakitangan

v Persekitaran fizikal

vi Konfigurasi sistem maklumat

vii Perkakasan, perisian atau peralatan komunikasi

viii Kebergantungan kepada pihak luar

c. Aset yang tergolong dalam kategori yang sama berkemungkinan mempunyai kerentanan yang sama.

d. Contoh kerentanan yang mungkin berlaku adalah seperti di **Lampiran F.**

2.4.2.5 Mengenal Pasti Perlindungan atau Kawalan Sedia Ada

a. Berdasarkan daripada ancaman dan kerentanan yang telah dikenal pasti, Pasukan Pengurusan Risiko Keselamatan Maklumat

seterusnya perlu mengenal pasti perlindungan atau kawalan sedia ada yang telah atau sedang dilaksana.

b. Pengenalpastian perlindungan atau kawalan sedia ada perlu dibuat bagi mengelakkan pertindihan tugas atau pengeluaran kos yang tidak perlu.

c. Semasa mengenal pasti perlindungan atau kawalan sedia ada, semakan perlu dibuat untuk memastikan bahawa perlindungan atau kawalan yang dilaksana berfungsi dengan berkesan.

d. Aktiviti berikut boleh digunakan untuk mengenal pasti perlindungan atau kawalan sedia ada:

    i Menyemak dokumen yang mengandungi maklumat tentang kawalan keselamatan maklumat.

    ii Menyemak dengan pihak yang bertanggungjawab dalam keselamatan maklumat tentang kawalan keselamatan maklumat yang telah dilaksanakan.

iii Membuat semakan di tapak kawalan fizikal.

2.4.2.6 Mengenal Pasti dan Menganalisis Impak

a. Setiap insiden keselamatan maklumat yang berlaku boleh memberi impak kepada sesebuah aset.

b. Impak yang mungkin terhasil daripada aset yang terjejas perlu dikenal pasti dan dianalisis.

c. Pasukan Pengurusan Risiko Keselamatan Maklumat boleh mengenal pasti impak berdasar kepada nilai kerugian melalui skala kerugian yang dirujuk atau yang dihasilkan.

d. Seterusnya nilai impak di analisis berdasarkan dari pendaraban nilai aset (para 2.4.2.2) dengan nilai kerugian yang diperoleh.

e. Contoh skala kerugian dan pengiraan nilai impak terdapat dalam **Lampiran G**.

2.4.2.7 Menganalisis Kebarangkalian

a. Pasukan Pengurusan Risiko Keselamatan Maklumat perlu menganalisis kebarangkalian berlakunya ancaman.

b. Output daripada aktiviti mengenal pasti ancaman, mengenal pasti kerentanan dan mengenal pasti perlindungan sedia ada boleh digunakan dalam menganalisis kebarangkalian berlakunya ancaman.

c. Semasa menganalisis kebarangkalian, pasukan pengurusan risiko bebas merujuk kepada skala kebarangkalian yang bersesuaian.

d. Contoh skala kebarangkalian berlakunya ancaman ditunjukkan seperti **Lampiran H**.

2.4.2.8 Menilai Tahap Risiko

a. Pasukan Pengurusan Risiko Keselamatan Maklumat seterusnya perlu menilai tahap risiko.

b. Tahap risiko dinilai dengan menggunakan matriks penilaian risiko yang bersesuaian.

c. Contoh matriks penilaian tahap risiko boleh dirujuk di **Lampiran I**.

d. Pasukan Pengurusan Risiko Keselamatan Maklumat seterusnya perlu mengenalpasti pemilik risiko. Pemilik risiko merupakan

personel atau entiti yang bertanggungjawab dalam mengurus risiko.

e. Hasil dari keseluruhan aktiviti penilaian risiko perlu direkodkan. Contoh perekodan hasil penilaian risiko adalah seperti di **Lampiran J**.

2.4.3 Penguraian Risiko

a. Berdasarkan hasil penilaian tahap risiko yang diperoleh, Pasukan Pengurusan Risiko Keselamatan Maklumat hendaklah melaksana penguraian risiko.

b. Aktiviti yang diperlukan semasa penguraian risiko adalah sebagaimana berikut:

i. Menentukan opsyen mitigasi.

ii. Mengenal pasti strategi penguraian.

iii. Mengenal pasti personel, kos dan tempoh masa pelaksanaan strategi.

iv. Menetapkan baki risiko.

v. Membangunkan pelan penguraian risiko.

vi. Mendapatkan pengesahan pengurusan.

vii. Melaksana pelan penguraian risiko.

2.4.3.1 Menentukan Opsyen Mitigasi

a. Secara umumnya, terdapat empat opsyen mitigasi risiko seperti di Jadual 2.

Bil	Opsyen Mitigasi	Penerangan
1.	Menerima risiko	Menerima risiko tanpa melaksanakan sebarang perlindungan atau kawalan.
2.	Mengurang risiko	Melaksanakan perlindungan atau kawalan untuk mengurangkan risiko.
3.	Memindah risiko	Memindahkan risiko kepada entiti lain.
4.	Mengelak risiko	Mengelakkan risiko apabila tiada pilihan lain yang tersedia.

Jadual 2. Opsyen strategi pemulihan

b. Pasukan pengurusan risiko perlu terlebih dahulu menentukan sama ada tahap risiko yang diperoleh pada langkah di para 2.4.2.8 boleh diterima atau tidak. Penentuan ini dibuat dengan merujuk kepada kriteria penerimaan

risiko yang telah ditetapkan seperti para 2.4.1.3.

c. Sekiranya tahap risiko menepati kriteria penerimaan risiko, maka risiko adalah diterima dan dicadang untuk tidak perlu melaksana kawalan tambahan.

d. Sekiranya tahap risiko tidak menepati kriteria penerimaan risiko, maka pasukan pengurusan risiko perlu menilai sama ada risiko tersebut perlu dikurangkan, dipindahkan atau dielakkan.

e. Bagaimanapun keputusan muktamad sama ada untuk menerima, mengurang, memindah atau mengelak risiko adalah berdasarkan kelulusan pengurusan atasan.

2.4.3.2 Mengenal Pasti Strategi Penguraian

a. Setelah memilih opsyen mitigasi, pasukan pengurusan risiko perlu membangunkan strategi penguraian atau rawatan untuk dibentangkan kepada pengurusan atasan.

b. Dalam memilih strategi penguraian, ahli pasukan perlu melihat sama ada perlindungan atau kawalan sedia ada mencukupi ataupun tidak dalam mengurangi risiko.

c. Sekiranya perlindungan atau kawalan sedia ada tidak mencukupi, pasukan pengurusan risiko hendaklah mengenal pasti strategi penguraian yang melibatkan perlindungan atau kawalan tambahan.

2.4.3.3 Menentukan Personel, Kos dan Tempoh Masa Pelaksanaan Strategi

a. Langkah seterusnya selepas mengenal pasti strategi penguraian adalah menentukan personel yang bertanggungjawab untuk melaksanakan strategi yang dipilih.

b. Sekiranya penguraian memerlukan kos, anggaran kos bagi pelaksanaan penguraian tersebut hendaklah diperolehi.

c. Tempoh masa yang merangkumi tarikh mula dan tarikh tamat pelaksanaan strategi juga perlu ditentukan.

2.4.3.4 Menetapkan Baki Risiko

a. Pasukan Pengurusan Risiko Keselamatan Maklumat kemudiannya perlu menetapkan baki risiko.

b. Baki risiko merujuk kepada nilai risiko setelah penguraian risiko dilaksana.

2.4.3.5 Membangunkan Pelan Penguraian Risiko Keselamatan Maklumat

a. Pasukan Pengurusan Risiko Keselamatan Maklumat perlu membangunkan Pelan Penguraian Risiko Keselamatan Maklumat.

b. Maklumat opsyen mitigasi, strategi penguraian, personel, tempoh masa dan baki risiko perlu direkod dan dimasukkan dalam pelan penguraian risiko.

c. Pelan Penguraian Risiko Keselamatan Maklumat ini seterusnya perlu dibawa kepada pemilik risiko dan pengurusan atasan untuk persetujuan pelaksanaan.

2.4.3.6 Mendapatkan Pengesahan Pengurusan

a. Pasukan Pengurusan Risiko Keselamatan Maklumat perlu membentangkan Pelan Penguraian Risiko Keselamatan Maklumat kepada pengurusan atasan untuk kelulusan pelaksanaan.

b. Keputusan kelulusan pelaksanaan pelan penguraian risiko perlu direkodkan.

c. Contoh pelan penguraian risiko adalah seperti di **Lampiran K**.

2.4.3.7 Melaksana Pelan Penguraian Risiko Keselamatan Maklumat

a. Seterusnya Pelan Penguraian Risiko Keselamatan Maklumat yang telah dibangunkan boleh dilaksana seperti yang dirancang.

b. Personel yang telah dikenal pasti dalam strategi penguraian risiko perlu melaksana, memantau dan melapor status pelaksanaan dari semasa ke semasa.

c. Hasil daripada pelaksanaan pelan penguraian risiko perlu direkodkan.

2.4.4 Penerimaan Risiko

a. Aktiviti penerimaan risiko perlu memastikan bahawa baki risiko yang diperoleh selepas melaksana penguraian risiko diterima pengurusan atasan organisasi.

b. Keputusan penerimaan risiko perlu direkodkan.

2.4.5 Komunikasi dan Rundingan

a. Komunikasi dan rundingan merupakan aktiviti penting bagi mencapai persetujuan tentang tata cara mengurus risiko yang melibatkan perkongsian pandangan dan maklumat antara pengurusan atasan, pasukan pengurusan risiko dan pihak berkepentingan lain.

b. Komunikasi dan rundingan akan memastikan semua pihak memahami asas sesebuah keputusan dibuat dan mengapa tindakan tertentu diperlukan.

2.4.6 Pemantauan dan Penyemakan

a. Ancaman, kerentanan, kebarangkalian dan kesan risiko sentiasa berubah. Oleh yang demikian, pemantauan berterusan adalah perlu untuk mengesan perubahan ini.

b. Pasukan Pengurusan Risiko Keselamatan Maklumat harus memastikan bahawa proses Pengurusan Risiko Keselamatan Maklumat dan aktiviti berkaitan kekal sesuai dalam keadaan semasa dan sentiasa dipatuhi.

c. Sebarang penambahbaikan yang dipersetujui kepada proses atau tindakan hendaklah dimaklumkan kepada pengurus pasukan dan pengurusan atasan sebagai jaminan bahawa tiada risiko atau elemen risiko yang diabaikan.

d. Selain itu, Pasukan Pengurusan Risiko Keselamatan Maklumat harus sentiasa mengesahkan bahawa kriteria yang digunakan untuk mengukur risiko dan elemennya masih sah dan konsisten dengan objektif, strategi dan dasar organisasi.

e. Pasukan Pengurusan Risiko Keselamatan Maklumat perlu sentiasa bersedia mengkaji semula risiko, ancaman, kerentanan dan perlindungan atau kawalan sedia ada dari semasa ke semasa.

2.4.7 Pendokumenan Maklumat (Perekodan dan Pelaporan)

a. Semua maklumat yang diperoleh semasa proses pengurusan risiko dan hasil yang diperoleh perlu direkodkan dan dilaporkan dengan sebaiknya.

3. RUJUKAN

I. Proza, A. 2022. ISO 27005:2022 *Overview*.

II. CSA, Singapore. 2019. *Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure*.

III. ISO/IEC 27000. 2018. *Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*.

IV. ISO/IEC 27001. 2013. *Information Technology - Security Techniques – Information Security Management Systems – Requirements*.

V. ISO/IEC 27001. 2022. *Information Security, cybersecurity and privacy protection - Information Security Management Systems – Requirements*.

VI. ISO/IEC 27005. 2018. *Information Technology - Security techniques - Information security risk management.*

VII. ISO/IEC 27005. 2022. *Information Security, cybersecurity and privacy protection – Guidances on managing information security risks.*

VIII. ISO 31000. 2018. *Risk Management — Guidelines.*

IX. MS ISO/IEC 27005. 2012. *Information Technology - Security Techniques - Information Security Risk Management (First Revision)*.

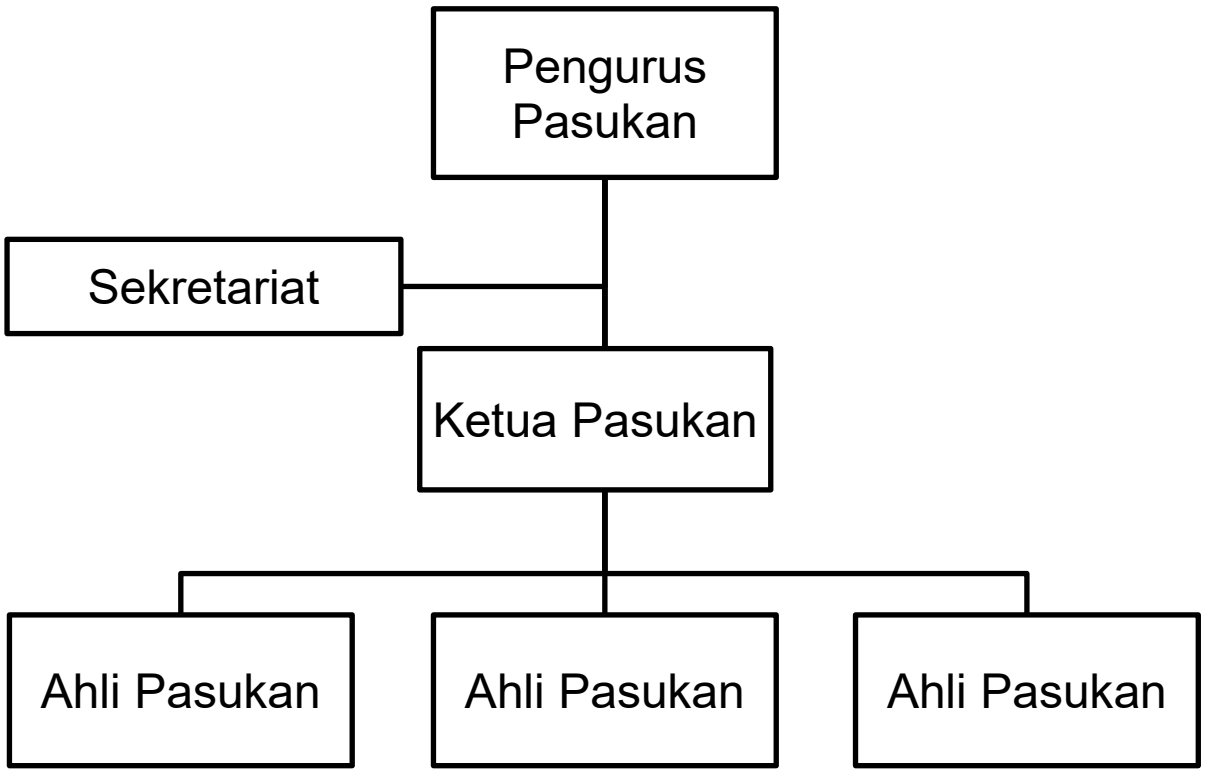
X. MS ISO 31000. 2020. *Risk Management - Guidelines (First Revision)*

XI. MAMPU. 2005. *The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM) Handbook*

XII. New Zealand Government. 2014. *Risk Assessment Process Information Security*.

Lampiran A

Contoh Struktur Pasukan Pengurusan Risiko Keselamatan Maklumat Serta Peranan dan Tanggungjawab



Rajah 1 – Lampiran A: Contoh struktur pasukan pengurusan risiko

Peranan	Tanggungjawab
Pengurus Pasukan	1. Mengurus dan memantau aktiviti pengurusan risiko. 2. Memastikan proses dan prosedur yang berkaitan dipatuhi. 3. Menyelesaikan sebarang isu berbangkit. 4. Membuat penilaian dan semakan output serta dokumen sebelum ia dibentangkan kepada pengurusan atasan.
Ketua Pasukan	1. Mengetuai aktiviti penilaian dan penguraian risiko. 2. Memastikan skop kerja dilaksanakan oleh semua ahli. 3. Menilai keputusan, menilai jurang dan memberikan maklum balas.
Ahli Pasukan	1. Melaksanakan semua tugas yang ditakrifkan di bawah setiap langkah penilaian dan penguraian risiko.
Sekretariat	1. Melaksana kerja-kerja keurusetiaan 2. Mengumpul dan menyelaras semua maklumat yang diperlukan dan mengkompilasi semua dokumen.

Jadual 1 – Lampiran A: Contoh peranan dan tanggungjawab pasukan pengurusan risiko keselamatan maklumat

Lampiran B

Contoh Kriteria Penerimaan Risiko

Tahap Risiko		Penerangan	Penerimaan risiko
Tinggi	3	Risiko yang memberi implikasi besar dan serta merta terhadap fungsi, perkhidmatan dan reputasi organisasi dan melibatkan pertambahan kos yang besar.	Risiko tidak boleh diterima dan perlu dibuat penguraian risiko bagi menurunkan risiko ke tahap sederhana / rendah
Sederhana	2	Risiko yang memberi implikasi sederhana serta kos tambahan terhadap fungsi, perkhidmatan dan reputasi organisasi.	Risiko boleh diterima namun digalakkan membuat penguraian risiko bagi menurunkan risiko ke tahap rendah
Rendah	1	Risiko yang tidak / kurang menjejaskan fungsi, perkhidmatan dan reputasi organisasi.	Risiko diterima

Jadual 1 - Lampiran B: Contoh 1 kriteria penerimaaan risiko tiga tahap

Tahap Risiko		Penerangan Penerimaan risiko
Sangat Tinggi	5	Risiko tidak boleh diterima dan akan menimbulkan kesan yang sangat teruk sehingga aktiviti yang berkaitan perlu dihentikan serta-merta. Sebagai alternatif, strategi mitigasi atau pemindahan perlu diambil segera.
Tinggi	4	Risiko ini tidak boleh diterima. Strategi rawatan yang bertujuan untuk mengurangkan tahap risiko perlu dibangunkan dan dilaksanakan dalam tempoh 3-6 bulan akan datang.
Sederhana	3	Risiko ini tidak boleh diterima. Strategi rawatan yang bertujuan untuk mengurangkan tahap risiko perlu dibangunkan dan dilaksanakan dalam tempoh 6-12 bulan akan datang.
Rendah	2	Risiko ini boleh diterima sekiranya tiada strategi rawatan yang boleh dilaksanakan dengan mudah dan menjimatkan. Bagaimanapun, risiko perlu juga dipantau untuk memastikan sebarang perubahan dapat dikesan dan diambil tindakan sewajarnya.
Sangat Rendah	1	Risiko ini boleh diterima dan tidak memerlukan sebarang strategi rawatan tambahan dalam keadaan dikesan dan diambil tindakan sewajarnya.

Jadual 2 - Lampiran B: Contoh 2 kriteria penerimaaan risiko lima tahap

Lampiran C

Contoh Maklumat Aset

Nama Aset	No. Siri Aset	Kuantiti Aset	Penerangan Ringkas Aset	Kategori Aset	Pemilik Aset	Lokasi Aset

Jadual 1 – Lampiran C: Contoh maklumat aset

Lampiran D

Contoh Skala Penilaian dan Pengiraan Nilai Aset

TAHAP	PRINSIP KESELAMATAN		
	KERAHSIAAN	**INTEGRITI**	**KETERSEDIAAN**
RENDAH (1)	Status maklumat adalah "Terbuka"	Kehilangan / kerosakan maklumat akibat pengubahsuaian tidak memberi kesan kepada operasi organisasi.	Maklumat yang tidak tersedia tidak akan menyebabkan sebarang kesan kepada operasi organisasi.
	(1)	(1)	(1)
SEDERHANA (2)	Status maklumat adalah "Terhad"	Kehilangan / kerosakan maklumat akibat pengubahsuaian memberi kesan kepada operasi organisasi, namun maklumat boleh diperbetulkan dalam tempoh 24 jam.	Maklumat yang tidak tersedia memberi kesan kepada operasi organisasi, namun maklumat yang tidak tersedia ini boleh dicapai dalam tempoh 24 jam.
	(2)	(2)	(2)
TINGGI (3)	Status maklumat adalah '"Sulit" dan ke atas'	Kehilangan / kerosakan maklumat akibat pengubahsuaian akan memberi kesan besar kepada operasi organisasi. Maklumat hanya boleh diperbetulkan selepas tempoh 24 jam.	Maklumat yang tidak tersedia memberi kesan besar kepada operasi organisasi. Maklumat yang tidak tersedia hanya boleh dicapai selepas tempoh 24 jam.
	(3)	(3)	(3)

Jadual 1 – Lampiran D: Contoh skala tiga tahap penilaian aset berdasarkan prinsip kerahsiaan, integriti dan ketersediaan maklumat

TAHAP	PRINSIP KESELAMATAN		
	KERAHSIAAN	INTEGRITI	KETERSEDIAAN
SANGAT RENDAH (1)	Status maklumat adalah “Terbuka”	Kehilangan / kerosakan maklumat akibat pengubahsuaian tidak memberi kesan kepada perkhidmatan organisasi.	Maklumat yang tidak tersedia tidak memberi kesan kepada perkhidmatan organisasi.
	(1)	(1)	(1)
RENDAH (2)	Status maklumat adalah “Terhad”	Kehilangan / kerosakan maklumat akibat pengubahsuaian memberi sedikit kesan kepada perkhidmatan organisasi.	Maklumat yang tidak tersedia memberi sedikit kesan kepada perkhidmatan organisasi.
	(2)	(2)	(2)
SEDERHANA (3)	Status maklumat adalah ‘Sulit”	Kehilangan / kerosakan maklumat akibat pengubahsuaian memberi kesan buruk kepada organisasi.	Maklumat yang tidak tersedia memberi kesan buruk kepada organisasi.
	(3)	(3)	(3)
TINGGI (4)	Status maklumat adalah “Rahsia”	Kehilangan / kerosakan maklumat akibat pengubahsuaian memberi kesan buruk yang serius kepada organisasi.	Maklumat yang tidak tersedia memberi kesan buruk yang serius kepada organisasi.
	(4)	(4)	(4)
SANGAT TINGGI (5)	Status maklumat adalah “Rahsia Besar”	Kehilangan / kerosakan maklumat akibat pengubahsuaian menyebabkan kesan buruk yang luar biasa kepada organisasi.	Maklumat yang tidak tersedia memberi kesan buruk yang luar biasa kepada organisasi.
	(5)	(5)	(5)

Jadual 2 – Lampiran D: Contoh skala lima tahap penilaian aset berdasarkan prinsip kerahsiaan, integriti dan ketersediaan maklumat

JUMLAH NILAI ASET [NILAI KERAHSIAAN + NILAI INTEGRITI + NILAI KETERSEDIAAN]	NILAI ASET		PENERANGAN
1-3	RENDAH	1	Aset bernilai rendah dan tidak memberi kesan kepada operasi organisasi.
4-6	SEDERHANA	2	Aset bernilai sederhana dan memberi kesan sederhana kepada operasi organisasi.
7-9	TINGGI	3	Aset bernilai tinggi dan memberi kesan besar kepada operasi organisasi.

Jadual 3 - Lampiran D: Contoh pengiraan nilai aset bagi skala tiga tahap

JUMLAH NILAI ASET [NILAI KERAHSIAAN + NILAI INTEGRITI + NILAI KETERSEDIAAN]	NILAI ASET		PENERANGAN
1-3	SANGAT RENDAH	1	Aset bernilai sangat rendah dan tidak memberi kesan langsung ke atas perkhidmatan atau operasi organisasi.
4-6	RENDAH	2	Aset bernilai rendah dan merupakan aset asas dalam perkhidmatan atau operasi organisasi.
7-9	SEDERHANA	3	Aset bernilai sederhana dan merupakan aset yang digunakan bagi memudahkan perkhidmatan atau operasi organisasi.
10-12	TINGGI	4	Aset bernilai tinggi dan merupakan aset penting kepada perkhidmatan dan operasi organisasi.

JUMLAH NILAI ASET [NILAI KERAHSIAAN + NILAI INTEGRITI + NILAI KETERSEDIAAN]	NILAI ASET		PENERANGAN
13-15	SANGAT TINGGI	5	Aset bernilai sangat tinggi dan merupakan aset yang sangat penting kepada perkhidmatan dan operasi organisasi.

Jadual 4 - Lampiran D: Contoh pengiraan nilai aset bagi skala lima tahap

Nota:

Andaian untuk penilaian aset termasuk:

a. Nilai aset bergantung pada sensitiviti data dan potensi kesannya terhadap kerahsiaan, integriti dan ketersediaan maklumat.

b. Nilai tahap untuk kerahsiaan, integriti dan ketersediaan maklumat adalah seperti berikut:

i. Bagi skala tiga tahap:

- Penarafan 3 adalah tinggi.
- Penarafan 2 adalah sederhana.
- Penarafan 1 adalah rendah.

ii. Bagi skala lima tahap:

- Penarafan 5 adalah sangat tinggi.
- Penarafan 4 adalah tinggi.
- Penarafan 3 adalah sederhana.
- Penarafan 2 adalah rendah.
- Penarafan 1 adalah sangat rendah.

c. Nilai aset ditentukan oleh jumlah keseluruhan nilai ketiga-tiga atribut (kerahsiaan + integriti + ketersediaan).

d. Bagi skala tiga tahap, aset adalah bernilai rendah apabila jumlah keseluruhan antara 1 – 3; aset adalah bernilai sederhana apabila jumlah keseluruhan antara 4 – 6; manakala aset adalah bernilai tinggi apabila jumlah keseluruhan antara 7 – 9.

e. Bagi skala lima tahap, aset adalah bernilai sangat rendah apabila jumlah keseluruhan antara 1 – 3; aset bernilai rendah apabila jumlah keseluruhan antara 4-6; aset bernilai sederhana apabila jumlah keseluruhan antara 7-9; aset bernilai tinggi apabila jumlah keseluruhan antara 10-12 dan aset bernilai sangat tinggi apabila jumlah keseluruhan antara 13-15.

Lampiran E

Contoh Ancaman

Category	*No.*	*Threat description*	*Type of risk source* [a]
Physical threats	TP01	*Fire*	A, D, E
	TP02	*Water*	A, D, E
	TP03	*Pollution, harmful radiation*	A, D, E
	TP04	*Major accident*	A, D, E
	TP05	*Explosion*	A, D, E
	TP06	*Dust, corrosion, freezing*	A, D, E
Natural threats	TN01	*Climatic phenomenon*	E
	TN02	*Seismic phenomenon*	E
	TN03	*Volcanic phenomenon*	E
	TN04	*Meteorological phenomenon*	E
	TN05	*Flood*	E
	TN06	*Pandemic/epidemic phenomenon*	E
Infrastructure failures	TI01	*Failure of a supply system*	A, D
	TI02	*Failure of cooling or ventilation system*	A, D
	TI03	*Loss of power supply*	A, D, E
	TI04	*Failure of a telecommunications network*	A, D, E
	TI05	*Failure of telecommunication equipment*	A, D
	TI06	*Electromagnetic radiation*	A, D, E
	TI07	*Thermal radiation*	A, D, E
	TI08	*Electromagnetic pulses*	A, D, E
Technical failures	TT01	*Failure of device or system*	A
	TT02	*Saturation of the information system*	A, D
	TT03	*Violation of information system maintainability*	A, D
Human actions	TH01	*Terror. attack, sabotage*	D
	TH02	*Social Engineering*	D
	TH03	*Interception of radiation of a device*	D
	TH04	*Remote spying*	D
	TH05	*Eavesdropping*	D
	TH06	*Theft of media or documents*	D
	TH07	*Theft of equipment*	D
	TH08	*Theft of digital identity or credentials*	D
	TH09	*Retrieval of recycled or discarded media*	D
	TH10	*Disclosure of information*	A, D
	TH11	*Data input from untrustworthy sources*	A, D
	TH12	*Tampering with hardware*	D
	TH13	*Tampering with software*	A, D
	TH14	*Drive-by-exploits using web-based communication*	D
	TH15	*Replay attack, man-in-the-middle attack*	D

Category	*No.*	*Threat description*	*Type of risk source* [a]
	TH16	*Unauthorized processing of personal data*	A, D
	TH17	*Unauthorized entry to facilities*	D
	TH18	*Unauthorized use of devices*	D
	TH19	*Incorrect use of devices*	A, D
	TH20	*Damaging devices or media*	A, D
	TH21	*Fraudulent copying of software*	D
	TH22	*Use of counterfeit or copied software*	A, D
	TH23	*Corruption of data*	D
	TH24	*Illegal processing of data*	D
	TH25	*Sending or distributing of malware*	A, D
	TH26	*Position detection*	D
Compromise of functions or ser- vices	TC01	*Error in use*	A
	TC02	*Abuse of rights or permissions*	A, D
	TC03	*Forging of rights or permissions*	D
	TC04	*Denial of actions*	D
Organizatio nal threats	TO01	*Lack of staff*	A, E
	TO02	*Lack of resources*	A, E
	TO03	*Failure of service providers*	A, E
	TO04	*Violation of laws or regulations*	A, D
a D = *deliberate*; A = *accidental*; E = *environmental*.			

Jadual 1 – Lampiran E: Contoh ancaman terhadap aset

(Sumber: ISO/IEC27005:2022)

Lampiran F

Contoh Kerentanan

Category	*No.*	*Examples of vulnerabilities*
Hardware	VH01	*Insufficient maintenance/faulty installation of storage media*
	VH02	*Insufficient periodic replacement schemes for equipment*
	VH03	*Susceptibility to humidity, dust, soiling*
	VH04	*Sensitivity to electromagnetic radiation*
	VH05	*Insufficient configuration change control*
	VH06	*Susceptibility to voltage variations*
	VH07	*Susceptibility to temperature variations*
	VH08	*Unprotected storage*
	VH09	*Lack of care at disposal*
	VH10	*Uncontrolled copying*
Software	VS01	*No or insufficient software testing*
	VS02	*Well-known flaws in the software*
	VS03	*No "logout" when leaving the workstation*
	VS04	*Disposal or reuse of storage media without proper erasure*
	VS05	*Insufficient configuration of logs for audit trail's purposes*
	VS06	*Wrong allocation of access rights*
	VS07	*Widely-distributed software*
	VS08	*Applying application programs to the wrong data in terms of time*
	VS09	*Complicated user interface*
	VS10	*Insufficient or lack of documentation*
	VS11	*Incorrect parameter set up*
	VS12	*Incorrect dates*
	VS13	*Insufficient identification and authentication mechanisms (e.g. for user authentication)*
	VS14	*Unprotected password tables*
	VS15	*Poor password management*
	VS16	*Unnecessary services enabled*
	VS17	*Immature or new software*
	VS18	*Unclear or incomplete specifications for developers*
	VS19	*Ineffective change control*
	VS20	*Uncontrolled downloading and use of software*
	VS21	*Lack of or incomplete back-up copies*
	VS22	*Failure to produce management reports*
Network	VN01	*Insufficient mechanisms for the proof of sending or receiving a message*
	VN02	*Unprotected communication lines*
	VN03	*Unprotected sensitive traffic*
	VN04	*Poor joint cabling*
	VN05	*Single point of failure*
	VN06	*Ineffective or lack of mechanisms for identification and authentication of sender and receiver*
	VN07	*Insecure network architecture*
	VN08	*Transfer of passwords in clear*

Category	No.	Examples of vulnerabilities
	VN09	*Inadequate network management (resilience of routing)*
	VN10	*Unprotected public network connections*
Personnel	VP01	*Absence of personnel*
	VP02	*Inadequate recruitment procedures*
	VP03	*Insufficient security training*
	VP04	*Incorrect use of software and hardware*
	VP05	*Poor security awareness*
	VP06	*Insufficient or lack of monitoring mechanisms*
	VP07	*Unsupervised work by outside or cleaning staff*
	VP08	*Ineffective or lack of policies for the correct use of telecommunications media and messaging*
Site	VS01	*Inadequate or careless use of physical access control to buildings and rooms*
	VS02	*Location in an area susceptible to flood*
	VS03	*Unstable power grid*
	VS04	*Insufficient physical protection of the building, doors and windows*
Organization	VO01	*Formal procedure for user registration and de-registration not developed, or its implementation is ineffective*
	VO02	*Formal process for access right review (supervision) not developed, or its implemen- tation is ineffective*
	VO03	*Insufficient provisions (concerning security) in contracts with customers and/or third parties*
	VO04	*Procedure of monitoring of information processing facilities not developed, or its implementation is ineffective*
	VO05	*Audits (supervision) not conducted on a regular basis*
	VO06	*Procedures of risk identification and assessment not developed, or its implementation is ineffective*
	VO07	*Insufficient or lack of fault reports recorded in administrator and operator logs*
	VO08	*Inadequate service maintenance response*
	VO09	*Insufficient or lack of Service Level Agreement*
	VO10	*Change control procedure not developed, or its implementation is ineffective*
	VO11	*Formal procedure for ISMS documentation control not developed, or its implemen- tation is ineffective*
	VO12	*Formal procedure for ISMS record supervision not developed, or its implementation is ineffective*
	VO13	*Formal process for authorization of publicly available information not developed, or its implementation is ineffective*
	VO14	*Improper allocation of information security responsibilities*
	VO15	*Continuity plans do not exist, or are incomplete, or are outdated*
	VO16	*E-mail usage policy not developed, or its implementation is ineffective*
	VO17	*Procedures for introducing software into operational systems not developed, or their implementation is ineffective*
	VO18	*Procedures for classified information handling not developed, or their implementa- tion is ineffective*
	VO19	*Information security responsibilities are not present in job*

Category	No.	Examples of vulnerabilities
		descriptions
	VO20	*Insufficient or lack of provisions (concerning information security) in contracts with employees*
	VO21	*Disciplinary process in case of information security incident not defined, or not functioning properly*
	VO22	*Formal policy on mobile computer usage not developed, or its implementation is ineffective*
	VO23	*Insufficient control of off-premise assets*
	VO24	*Insufficient or lack of "clear desk and clear screen" policy*
	VO25	*information processing facilities authorization not implemented or not functioning properly*
	VO26	*Monitoring mechanisms for security breaches not properly implemented*
	VO27	*Procedures for reporting security weaknesses not developed, or their implementation is ineffective*
	VO28	*Procedures of provisions compliance with intellectual rights not developed, or their implementation is ineffective*

Jadual 1 – Lampiran F: Contoh kerentanan (Sumber: ISO/IEC27005:2022)

Lampiran G

Contoh Skala Nilai Kerugian dan Matrik Nilai Impak

NILAI KERUGIAN	SKALA NILAI KERUGIAN	PENERANGAN
Rendah	1	• Aset yang terjejas kurang / tidak membawa kepada implikasi kewangan. • Aset yang terjejas kurang / tidak menyebabkan gangguan untuk menjalankan operasi harian organisasi.
Sederhana	2	• Aset yang terjejas membawa kepada implikasi kewangan yang sederhana. • Aset yang terjejas mengakibatkan gangguan separa untuk menjalankan operasi harian organisasi.
Tinggi	3	• Aset yang terjejas membawa kepada implikasi kewangan yang tinggi. • Aset yang terjejas mengakibatkan sepenuhnya gangguan untuk menjalankan operasi harian organisasi.

Jadual 1 - Lampiran G: Contoh skala nilai kerugian tiga tahap

NILAI KERUGIAN	SKALA NILAI KERUGIAN	PENERANGAN
Sangat Rendah	1	• Aset yang terjejas tidak membawa kepada implikasi kewangan. • Aset yang terjejas tidak menyebabkan gangguan untuk menjalankan operasi harian organisasi.
Rendah	2	• Aset yang terjejas membawa kepada implikasi kewangan yang rendah. • Aset yang terjejas mengakibatkan sedikit gangguan untuk menjalankan operasi harian organisasi.
Sederhana	3	• Aset yang terjejas membawa kepada implikasi kewangan yang sederhana. • Aset yang terjejas mengakibatkan gangguan separa untuk menjalankan operasi harian organisasi.
Tinggi	4	• Aset yang terjejas membawa kepada implikasi kewangan yang tinggi. • Aset yang terjejas mengakibatkan gangguan besar untuk menjalankan operasi harian organisasI.
Sangat Tinggi	5	• Aset yang terjejas membawa kepada implikasi kewangan yang sangat tinggi. • Aset yang terjejas mengakibatkan gangguan secara keseluruhan untuk menjalankan operasi harian organisasi.

Jadual 2 - Lampiran G: Contoh skala nilai kerugian lima tahap

	NILAI KERUGIAN		
NILAI ASET	**Rendah** **1**	**Sederhana** **2**	**Tinggi** **3**
Rendah **1**	Kecil 1	Kecil 2	Sederhana 3
Sederhana **2**	Kecil 2	Sederhana 4	Besar 6
Tinggi **3**	Sederhana 3	Besar 6	Besar 9

Jadual 3 – Lampiran G: Contoh matrik nilai impak tiga tahap

Nota:

Nilai Impak = Nilai Aset * Nilai Kerugian

Nilai Impak (Nilai Aset * Nilai Kerugian)	Tahap Impak	Nilai Tahap Impak
1-2	Kecil	1
3-4	Sederhana	2
> 4	Besar	3

Jadual 4 – Lampiran G: Contoh tahap impak tiga tahap

	NILAI KERUGIAN				
NILAI ASET	**Sangat rendah**	**Rendah**	**Sederhana**	**Tinggi**	**Sangat tinggi**
	1	**2**	**3**	**4**	**5**
Sangat Rendah	Sangat kecil	Sangat kecil	Sangat kecil	Sangat kecil	Kecil
1	1	2	3	4	5
Rendah	Sangat kecil	Sangat kecil	Kecil	Kecil	Sederhana
2	2	4	6	8	10
Sederhana	Sangat kecil	Kecil	Kecil	Sederhana	Besar
3	3	6	9	12	15
Tinggi	Sangat kecil	Kecil	Sederhana	Besar	Sangat besar
4	4	8	12	16	20
Sangat Tinggi	Kecil	Sederhana	Besar	Sangat besar	Sangat besar
5	5	10	15	20	25

Jadual 5 – Lampiran G: Contoh matrik nilai impak lima tahap

Nota:

Nilai Impak = Nilai Aset * Nilai Kerugian

Nilai Impak (Nilai Aset * Nilai Kerugian)	Tahap Impak	Nilai Tahap Impak
1-4	Sangat kecil	1
5-9	Kecil	2
10-14	Sederhana	3
15-19	Besar	4
20-25	Sangat besar	5

Jadual 6 – Lampiran G: Contoh tahap impak lima tahap

Lampiran H

Contoh Skala Kebarangkalian Berlakunya Ancaman

KEBARANGKALIAN		PENERANGAN
Besar kemungkinan tidak berlaku	1	Ancaman mungkin berlaku hanya dalam keadaan yang luar biasa atau sekali dalam setahun.
Sekali - sekala	2	Ancaman mungkin berlaku sekurang-kurangnya sekali dalam tempoh 6 bulan.
Hampir pasti	3	Ancaman mungkin berlaku hampir setiap bulan

Jadual 1 - Lampiran H: Contoh skala kebarangkalian ancaman tiga tahap

KEBARANGKALIAN		PENERANGAN
Besar kemungkinan tidak berlaku	1	Besar kemungkinan tidak berlaku ancaman; atau lebih dari 3 tahun sekali.
Jarang- Jarang	2	Ancaman mungkin berlaku dalam tempoh 3 tahun sekali.
Sekali-sekala	3	Ancaman mungkin berlaku dalam tempoh sekali setahun.
Kemungkinan tinggi	4	Ancaman mungkin berlaku dalam tempoh 6 bulan sekali.
Hampir pasti	5	Ancaman yang kerap. Mungkin berlaku setiap bulan.

Jadual 2 - Lampiran H: Contoh skala kebarangkalian ancaman lima tahap

Lampiran I

Contoh Matrik Penilaian Tahap Risiko Keselamatan Maklumat

	KEBARANGKALIAN		
TAHAP IMPAK	Besar kemungkinan tidak berlaku	Sekali - sekala	Hampir pasti
	1	2	3
Kecil	Rendah	Rendah	Sederhana
1	1	2	3
Sederhana	Rendah	Sederhana	Tinggi
2	2	4	6
Besar	Sederhana	Tinggi	Tinggi
3	3	6	9

Jadual 1 - Lampiran I: Contoh matrik penilaian tahap risiko tiga tahap

Nota:

Tahap Risiko = Nilai Impak * Nilai Kebarangkalian

Nilai Risiko (Tahap Impak * Kebarangkalian)	Tahap Risiko	
1-2	Rendah	1
3-4	Sederhana	2
> 4	Tinggi	3

Jadual 2 – Lampiran I: Contoh tahap risiko tiga tahap

	KEBARANGKALIAN				
TAHAP IMPAK	Besar Kemungkinan tidak berlaku	Jarang-jarang	Sekali - sekala	Kemungkinan tinggi	Hampir Pasti
	1	2	3	4	5
Sangat kecil	Sangat rendah	Sangat rendah	Sangat rendah	Sangat rendah	Rendah
1	1	2	3	4	5
Kecil	Sangat rendah	Sangat rendah	Rendah	Rendah	Sederhana
2	2	4	6	8	10
Sederhana	Sangat rendah	Rendah	Rendah	Sederhana	Tinggi
3	3	6	9	12	15
Besar	Sangat rendah	Rendah	Sederhana	Tinggi	Sangat Tinggi
4	4	8	12	16	20
Sangat besar	Rendah	Sederhana	Tinggi	Sangat Tinggi	Sangat Tinggi
5	5	10	15	20	25

Jadual 3 - Lampiran I: Contoh matrik penilaian tahap risiko lima tahap

Nota: Tahap Risiko = Nilai Impak * Nilai Kebarangkalian

Nilai Risiko (Tahap Impak * Kebarangkalian)	Tahap Risiko	
1-4	Sangat rendah	1
5-9	Rendah	2
10-14	Sederhana	3
15-19	Tinggi	4
20-25	Sangat tinggi	5

Jadual 4 – Lampiran I: Contoh tahap risiko lima tahap

Lampiran J

Contoh Hasil Penilaian Risiko Keselamatan Maklumat

NAMA ASET	NILAI ASET	ANCAMAN	KELEMAHAN	PERLINDUNGAN / KAWALAN SEDIA ADA	NILAI KERUGIAN	NILAI / TAHAP IMPAK	KEBARANGKALIAN BERLAKUNYA ANCAMAN	TAHAP RISIKO	PEMILIK RISIKO

PENGESAHAN

Disediakan oleh:	Disemak oleh:	Diluluskan oleh:
.....	.....	.....
(Ketua Pasukan)	(Pengurus Pasukan)	(Pengurusan Atasan / Ketua Jabatan)

Lampiran K

Contoh Pelan Penguraian Risiko

NAMA ASET	NILAI ASET	ANCAMAN	KELEMAHAN	PERLINDUNGAN / KAWALAN SEDIA ADA	NILAI KERUGIAN	NILAI IMPAK	KEBARANGKALIAN BERLAKU ANCAMAN	TAHAP RISIKO	PEMILIK RISIKO	OPSYEN MITIGASI	STRATEGI PENGURAIAN	PERSONEL	ANGGARAN KOS (SEKIRANYA ADA) RM	TEMPOH MASA		BAKI NILAI / TAHAP RISIKO
														MULA	AKIHR	

PENGESAHAN

Disediakan oleh:

.....
(Ketua Pasukan)

Disemak oleh:

.....
(Pengurus Pasukan)

Diluluskan oleh:

.....
(Pengurusan Atasan / Ketua Jabatan)