	PANDUAN PENILAIAN RISIKO ASET **SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

1.0 TUJUAN

Panduan ini disediakan untuk menilai tahap risiko keselamatan maklumat supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas keselamatan maklumat UPM. Panduan ini merangkumi metodologi Penilaian Risiko Terperinci (*Malaysian Public Sector ICT Risk Assessment Methodology, MyRAM*) berpandukan kepada Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

2.0 DOKUMEN RUJUKAN

Kod Dokumen	Tajuk Dokumen
-	Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
ISO/IEC 27001:2013	*Information Technology – Security Techniques – Information Security Management Systems – Requirements*
ISO/IEC 27005:2008	*Risk Assessment Guidelines for Information Security Management*
-	Arahan Keselamatan Kerajaan Malaysia
-	*The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM)*

3.0 DEFINISI

Bagi tujuan proses penilaian risiko ini, glosari yang disenaraikan dalam Surat Pekeliling Am No. 5 / 2006: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam dan ISO/IEC 27001:2013 digunapakai.

BIL.	TERMA	DESKRIPSI
1.	Aset	Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya hilang atau berubah. Berdasarkan MyRAM aset-aset tergolong kepada data/maklumat, perkhidmatan, perisian, perkakasan dan manusia.
2.	Aset Yang bersandar	Subjek yang dinyatakan ketika kejadian sesuatu peristiwa. Bermakna aset lain diperlukan untuknya berfungsi
3.	Owner/Pentadbir Proses /Pemilik Risiko	Pentadbir Proses yang bertanggungjawab terhadap risiko untuk sesuatu aset atau proses.
4.	Custodian/ Pentadbir Sistem	Kakitangan Teknikal ICT yang memelihara keselamatan, menyelenggara, atau mengawal sesuatu aset.
5.	Risiko	Secara umum ia adalah kemungkinan berhadapan dengan bahaya atau menyebabkan mudarat atau kerugian, terutamanya dari kurang penjagaan yang sesuai.
6.	Penilaian Risiko	Penilaian bagi kemungkinan-kemungkinan bahaya atau mudarat atau kerugian/kehilangan aset
7.	Ancaman	sebarang kejadian atau perbuatan yang boleh menyebabkan satu atau lebih daripada perkara berikut berlaku: pendedahan yang tidak diluluskan, kemusnahan, penyingkiran, pengubahsuaian atau gangguan maklumat sensitif atau kritikal, aset-aset atau perkhidmatan. Sesuatu ancaman boleh berlaku dengan semula jadi, sengaja atau tidak sengaja.
8.	Kelemahan	Sifat mana-mana aset yang boleh meningkatkan kebarangkalian berlakunya ancaman dan menyebabkan mudarat dalam soal kerahsiaan, ketersediaan atau kesahihan yang mungkin boleh meningkatkan kesan-kesan kejadian ancaman jika berlaku menjadi bertambah teruk.
9.	Insiden	Apabila berlakunya kejadian ancaman. *Ancaman= rujuk kepada definisi ancaman dalam seksyen 4.0 Definisi :ancaman;

4.0 METODOLOGI PENILAIAN RISIKO

Penilaian risiko ialah satu kaedah untuk menentukan apakah ancaman-ancaman yang wujud untuk sesuatu aset dan tahap risiko yang berkaitan dengan ancaman tersebut. Penentuan tahap risiko menyediakan organisasi dengan maklumat yang diperlukan untuk memilih perlindungan-perlindungan dan langkah kawalan yang bersesuaian untuk mengurangkan risiko kepada satu tahap yang boleh diterima.

MAMPU telah membangunkan *Malaysian Public Sector Information Security Risk Assessment Methodology* atau MyRAM bagi membantu organisasi sektor awam dalam mengenalpasti dan menguruskan risiko keselamatan Maklumat. MyRAM digunakan untuk memastikan kesahihan maklumat dan aset Kerajaan dalam menyediakan perkhidmatan yang efektif dan efisien bagi semua pelanggan. Kami juga telah mengambil ISO/IEC 27005 sebagai contoh.

4.1 Kriteria Penilaian Risiko:

Kriteria bagi penilaian risiko UPM adalah seperti berikut:

(i) Semua risiko yang dinilaikan sebagai taraf "RENDAH" akan dianggap Sebagai boleh diterima kepada pengurusan.
(ii) Risiko-risiko yang tidak menjejaskan Visi, Misi and Nilai-nilai UPM mungkin boleh dipertimbangkan untuk penerimaan.
(iii) Risiko-risiko yang tidak mempunyai impak ke atas reputasi, penjenamaan dan imej UPM mungkin boleh dipertimbangkan untuk penerimaan.
(iv) Risiko-risiko yang tidak mempunyai impak ke atas pematuhan perundangan mungkin boleh dipertimbangkan untuk penerimaan.
(v) Risiko-risiko yang mempunyai sedikit impak atau tiada kepada pengguna akhir, mungkin boleh dipertimbangkan untuk penerimaan.

5.0 KEPERLUAN UNTUK PENILAIAN RISIKO

Penilaian risiko akan dilakukan untuk:

(i) Mengambilkira perubahan pada struktur organisasi dan aset baru;
(ii) Mempertimbangkan ancaman baru dan kelemahan; dan
(iii) Mengesahkan bahawa kawalan tetap efektif dan bersesuaian.
(iv) Mengesahkan risiko yang masih ada setelah kawalan untuk rawatan risiko dilaksanakan;
(v) Mengesahkan kriteria penilaian risiko oleh pihak pengurusan atasan.

6.0 PROSES PENILAIAN RISIKO

Pendekatan yang diambil adalah mengikut garis panduan proses penilaian risiko dalam dokumen MyRAM, bermula dari langkah Penubuhan Ahli Kumpulan sehingga Langkah 10, yang merupakan Pengiraan Risiko. Langkah-langkah ini berkaitan antara satu sama lain kerana input untuk satu aktiviti penilaian risiko boleh diambil daripada output langkah-langkah terdahulu. Jadual 1 dibawah, menunjukkan sepuluh (10) langkah latihan penilaian risiko.

LANGKAH	KETERANGAN	TINDAKAN YANG TERLIBAT
Penubuhan Kumpulan (S1)	Mewujudkan satu komponen asas latihan penilaian risiko. Kenalpasti ahli kumpulan yang memiliki pengetahuan luas tentang organisasi. Jadual dan logistik ditubuhkan untuk memastikan kelancaran keseluruhan latihan.	(a) Mengenalpasti ahli kumpulan penilaian (b) Menyediakan senarai tugasan dan jadual
Penubuhan Kajian Semula Sempadan (S2)	Menetapkan skop proses penilaian risiko. Skop akhir akan diserahkan kepada pengurusan kanan. Sebaik sahaja kelulusan diterima, pasukan penilaian akan mengumpul semua bahan-bahan dan maklumat berkaitan.	(a) Mengenalpasti skop penilaian risiko (b) Mendapatkan kelulusan dari pihak pengurusan (c) Mengumpul maklumat (d) berkenaan kajian semula batasan (e) Kembali ke Langkah 1 jika perlu.
Mengenalpasti Risiko (S3)	Mengenalpasti semua aset yang terkandung didalam skop Batasan Penilaian Risiko.	(a) Mengenalpasti asset berkenaan (b) Kumpul dan kelaskan aset (c) Mengenalpasti pemilik dan penjaga aset
Penilaian Aset-aset berdasarkan CIA (S4)	Menentukan nilai-nilai semi-kuantitatif kepada aset-aset dan tentukan nilai berdasarkan Kerahsiaan, Ketersediaan & Kesahihan setiap aset	(a) Mengenal pasti nilai asset berdasarkan CIA (b) Menentukan nilai Kuantifikasi bagi setiap asset (CIA)
Penilaian Ancaman (S5)	Menetapkan jenis-jenis ancaman berkaitan dengan aset-aset, dan tahap-tahap relatif mereka.	Kenal pasti semua ancaman-ancaman kepada aset-aset

Penilaian Kelemahan (S6)	Mengenal pasti semua kelemahan yang berpotensi untuk dieksploitasikan oleh ancaman. Sebagai tambahan, ia akan menilai tahap pendedahan kelemahan relatif.	Kenal pasti kelemahan- kelemahan yang berpotensi untuk dieksploitasikan oleh ancaman
Mengenalpasti Perlindungan Yang Sedia Ada & Perancangan (S7)	Mengenalpasti semua jenis perlindungan yang sedia ada & dirancang yang telah diatur atau akan diatur untuk melindungi aset-aset.	Menyemak semula perlindungan sedia ada dan rancangan untuk melindungi aset
Analisis Impak (Kesan) (S8)	Mengukur impak kerja serta organisasi sesuatu asset sewajarnya.	(a) Tentukan impak kerja dan impak bisnes (b) Tentukan tahap impak
Analisis Kemungkinan/ Kebarangkalian (S9)	Memastikan kemungkinan/kebarangkalian ancaman-ancaman & kelemahan-kelemahan yang boleh berlaku, dengan kawalan yang sedia ada.	Tentukan kemungkinan/kebarangkalian ancaman- ancaman & kelemahan-kelemahan yang boleh berlaku
Pengiraan Risiko (S10)	Mengira tahap risiko untuk setiap aset, Berdasarkan keputusan nilai impak & kemungkinan.	Mengira tahap risiko untuk setiap aset

Jadual 1: Deskripsi Langkah Penilaian Risiko

7.0 PERANAN DAN TANGGUNGJAWAB AHLI KUMPULAN PENILAIAN RISIKO

(i) Memberi nasihat kepakaran untuk aktiviti penilaian risiko;
(ii) Mengurus aktiviti penilaian risiko;
(iii) Memastikan selesai tepat pada masa;
(iv) Melakukan semakan semula untuk semua output dan dokumen sebelum dibentangkan kepada penasihat projek;
(v) Sentiasa menentukan progres kerja;
(vi) Menilai keputusan-keputusan, jurang dan memberi maklum balas; dan
(vii) Melakukan semua tugasan yang disebut dalam langkah-langkah penilaian risiko.

8.0 TARAF NILAI ASET

Berdasarkan Jadual 1 dibawah, kumpulan penilaian risiko perlu mewujudkan taraf nilai untuk keperluan Keselamatan Maklumat, iaitu Kerahsiaan/*Confidentiality* (C), Kesahihan/*Integrity* (I) dan Ketersediaan/*Availability* (A). Tahap-tahap *Low* (Rendah), *Medium* (Pertengahan)dan *High* (Tinggi) di Jadual 1 adalah berpandukan huraian yang diberi mengikut setiap skor. Dalam menilai sensitiviti setiap aset, Pasukan Penilaian Risiko akan menggunakan garis panduan berikut:

(a) **Kerahsiaan (*Confidentiality*)**

Kesan pendedahan maklumat rahsia/sulit yang tidak diluluskan boleh mengakibatkan kehilangan keyakinan pemegang saham dan mengaibkan.

(b) **Kesahihan (*Integrity*)**

Kesan kepada sistem yang disebabkan dari pengubahsuaian aset secara sengaja, tanpa mendapat kelulusan atau tidak sengaja.

(c) **Ketersediaan (*Availability*)**

Ini ialah kesan daripada penafian pengunaan aset secara sengaja atau kebetulan. Setiap aset mesti dinilai menurut tahap Confidentiality (Rahsia), Integrity (Kesahihan) dan Availability (Ketersediaan) masing-masing.

8.1 Kaedah Skor Untuk Risiko

Menggunakan Jadual 1 di bawah, selepas mengira nilai-nilai CIA dan nilai aset, sekarang kita perlu menghitung tahap risiko yang terdedah kepada aset-aset tersebut. Risiko-risiko wujud disebabkan kewujudan **Ancaman** kepada aset dan **Kelemahan** aset-aset itu sendiri.

ANCAMAN	KELEMAHAN
Di bawah ialah beberapa contoh ancaman: *(a) Virus* *(b) Theft* *(c) Damage due to wear "n" tear* *(d) Accidental Deletion of data* *(e) Hardware failure (Mechanical Fault)* *(f) Power Fluctuation* *(g) Improper usage of Assets (User Error)*	Di bawah ialah beberapa contoh ancaman: *(a) Lack of proper inspection* *(b) Not updated AV solution* *(c) Poor Patch management* *(d) Lack of capacity plan for systems*

Sila Ambil Perhatian bahawa contoh-contoh di atas adalah tidak lengkap dan boleh ditambah bergantung pada aktiviti-aktiviti dan fungsi-fungsi bahagian. Pengguna-pengguna mesti bekerjasama dan berbincang untuk mengenal pasti ancaman-ancaman dan kelemahan- kelemahan yang tepat untuk setiap aset dan mencatatkan penemuan-penemuan dalam Register Risiko "Risk Register"

8.2 Kebarangkalian & Impak

Dalam persekitaran sebenar, risiko yang dikenalpasti berdasarkan ancaman-ancaman dan kelemahan-kelemahan mungkin boleh berlaku atau tidak. Kemungkinan "peluang" risiko terjadi boleh bergantung kepada situasi. Oleh itu penilaian risiko adalah berdasarkan kepada "KebarangkalianTerjadi" dan "Impak" disebabkan sesuatu kejadian. Impak diukur kepada aset secara langsung, begitu juga impak kepada bisnes.

Kebarangkalian dan Impak boleh dipilih berdasarkan Jadual 1 di bawah dan ditarafkan dari *Low, Medium* dan *High* berdasarkan huraian dalam Jadual 1.

Table 1

ASSET VALUE

CONFIDENTIALITY (C)	
Rating	**Description**
High (H)	Confidential, Real problem if disclosed to external parties, Loss of Image and Reputation, Legal action.
Medium (M)	Restricted, should not happen, minor problem if disclosed. Loss of Reputation but can be recovered.
Low (L)	Public, does not matter if disclosed. No impact to image.

INTEGRITY (I)	
Rating	**Description**
High (H)	Serious problem, accuracy and completeness is critical for service delivery and customers. May have permanent impact on ICT service.
Medium (M)	Noticeable problem. Can effect the service but service can be restored quickly.
Low (L)	Negligible or minor problem, no influential or critical effect on the business. Can be restored within 2 hours.

AVAILABILITY (A)	
Rating	**Description**
High (H)	Mission critical, non-availability is a real problem. Can permanently impact ICT service & Reputation.
Medium (M)	Serious problem, short outage is tolerable and can be restored but takes more than 1 day. Small impact to Image & Reputation but can be restored.
Low (L)	No or minor problem, extended outage is tolerable. Outage is only a few hours. No impact to Image & Reputation.

RISK VALUE

PROBABILITY (P)	
Probability of Event	**Description**
High (H)	High Likely, Almost Certain, Common Occurance (Eg: Once every month or less)
Medium (M)	Most Likely, Probable to Occure, (Eg: Once every 2 months)
Low (L)	Unlikely, Infrequently, Rarely Happens (Eg: Once in 6 months or more)

IMPACT / HARM (I)	
Impact / Harm of Event	**Description**
High (H)	Serious to grave harm.
Medium (M)	Significant to damaging harm
Low (L)	No to minor harm

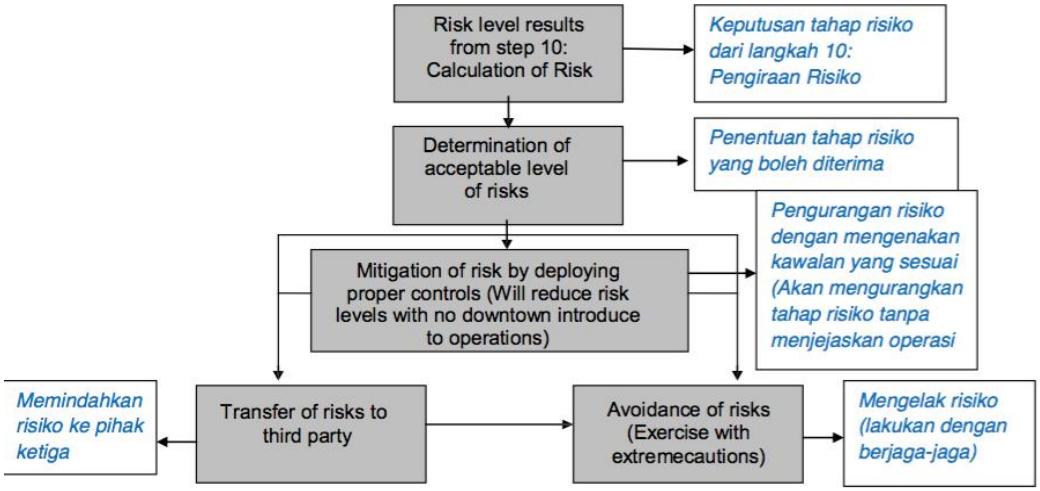
BUSINESS IMPACT (BI)	
Impact / Harm of Event	**Description**
High (H)	Serious to grave impact on business. Loss of customer. Can shut down business operations due to Legal breech.
Medium (M)	Significant to damaging impact on business. Penalties may be levied but can be tolerated. Financial loss to Business.
Low (L)	Negligible Impact on Business.

9.0 PANDUAN UNTUK KEPUTUSAN BAGI RISIKO YANG DIKENALPASTI

Output proses penilaian risiko adalah input bagi proses membuat keputusan yang menetapkan sama ada menerima, mengurangkan, memindahkan atau mengelakkan risiko yang sudah dikenalpasti. Ini akan dilakukan dalam *Selection of Controls* (Pemilihan Kawalan) dan ditunjukkan dalam Risk Treatment Plan (RTP) (Pelan Pemulihan Risiko).

Pasukan Penilaian Risiko akan menubuhkan *High-Level-Recommendation* (HLR) untuk memperoleh kelulusan bertulis atau pengakuan daripada Jawatankuasa Kerja ISMS yang akan menentukan di dalam RTP apa yang mesti dilakukan selepas mendapat tahap risiko untuk semua aset-aset yang dikenalpasti. Di peringkat ini, keputusan sama ada menerima, mengurangkan, memindahkan, atau mengelakkan risiko yang telah kenalpasti mestilah dibuat hanya setelah latihan penilaian risiko selesai. Perlu mendapat pengesahan muktamad Timbalan Wakil Pengurusan ISMS.

Secara asasnya membuat keputusan sama ada menerima, mengurangkan, memindahkan, atau mengelakkan tahap risiko adalah berdasarkan faktor-faktor masa, wang, tenaga kerja dan peralatan. Ketentuan pilihan untuk mengendali risiko boleh dilakukan dengan mengikuti langkah-langkah dalam Rajah 2 di bawah.



If the above is not possible, then the management shall accept the risk providing it does not conflict with the Risk Assessment Criteria set by the management.

In this case, all risks that fall in the "LOW Risk" category is considered as "Acceptable"

Jika senarai di atas tidak boleh digunapakai, pihak pengurusan akan menerima risiko dengan syarat ianya tidak mendatangkan konflik dengan Kriteria Penilaian Risiko yang ditetapkan oleh pengurusan.

Untuk kes begini, semua risiko yang jatuh dalam kategori "Risiko RENDAH" dianggap sebagai "boleh diterima"

Figure 2 : Decision on Options in Handling Risk
Rajah 2: Keputusan berkenaan Pilihan Dalam Menangani Risiko

Seperti yang digambarkan dalam Rajah 2 di atas, langkah pertama untuk membuat cadangan-cadangan High-Level ialah dengan mendapatkan keputusan tahap risiko-risiko dari Langkah 10. Kemudian tentukan apakah tahap risiko yang boleh diterima oleh Pasukan Penilaian Risiko. Rujuk Seksyen 4: Kriteria untuk menerima Risiko-risiko.
Untuk Cadangan High-Level, terdapat dua (2) output iaitu:

(a) Keputusan atas pilihan; dan
(b) Strategi Perlindungan

9.1 Keputusan atas Pilihan

Dalam Keputusan atas Pilihan, Kumpulan Penilaian Risiko akan mencadangkan kepada JawatanKuas Kerja ISMS sama ada untuk menerima, mengurangkan, memindahkan, atau mengelak tahap risiko ancaman yang wujud dalam sesuatu aset. Huraian-huraian untuk setiap pilihan keputusan ialah seperti berikut:

(a) **Menerima**:

untuk menerima risiko-risiko berkaitan dengan aset-aset tanpa melaksanakan sebarang perlindungan atau kawalan

(b) **Mengurangkan**:
melaksanakan kawalan untuk mengurangkan risiko. Mengurangkan tahap risiko adalah perlu apabila risiko tinggi.

(c) **Pemindahan**:
Memindahkan risiko kepada entiti yang lain.

(d) **Mengelakkan**:
untuk mengelak risiko-risiko apabila tiada pilihan lain.

Pasukan Penilaian Risiko akan menerima, mengurangkan, memindahkan atau mengelakkan risiko bagi kriteria berikut:

(a) Memeriksa dan menilai sama ada risiko dapat diterima atau tidak. Kumpulan Penilaian Risiko boleh mencadangkan kepada pengurusan untuk menerima semua aset dengan tahap risiko Low (Rendah) dan tiada tindakan serta-merta diambil bagi melindungi aset;

(b) Jika risiko-risiko tidak boleh diterima, maka semak dan nilaikan sama ada ianya patut dikurangkan, dipindahkan atau dielakkan;

(c) Jika implikasi risiko-risiko membawa kepada bencana dan kritikal (High), risiko-risiko tersebut patut dikurangkan. Pengurangan Risiko akan dicapai melalui pelaksanaan komponen-komponen berikut: operasi, prosedur, fizikal, Kakitangan dan keselamatan teknikal untuk memastikan bahawa operasi kritikal tidak terjejas; dan

(d) Jika implikasi risiko-risiko adalah sederhana kritikal (Medium), risiko-risiko tersebut boleh juga dipindahkan berdasarkan syarat-syarat berikut:

(i) Risiko-risiko mesti dipindahkan dengan adil. Risiko boleh dikongsi oleh pemilik-pemilik aset dan pihak ketiga. Misalnya, talian komunikasi bermasalah, dan *Service Level Agreement (SLA)* dengan penyedia talian menyatakan bahawa talian boleh didapati dalam 24 jam; bencana yang tidak dapat diketahui yang mungkin dialami pihak ketiga merupakan satu risiko yang dikongsi bersama dimana agensi bersediauntuk terima; dan

(ii) Risiko-risiko sepatutnya dielakkan sama sekali sekiranya tiada kawalan munasabah yang boleh dilaksanakan untuk mengurangkan risiko. Contoh, mengelak risiko-risiko ialah dengan memutuskan sistem.

Pasukan Penilaian Risiko perlu membangunkan pelan perlindungan "*Risk Treatment*

Plan" untuk dibentangkan kepada pengurusan. Bagi *Risk Treatment Plan,* kumpulan Penilaian Risiko perlu melihat samada kawalan yang sedia ada adalah cukup untuk melindungi aset-aset atau tidak. Jika kawalan yang sedia ada tidak mencukupi, kumpulan yang terbabit atau kumpulan pemilik risiko akan memilih objektif-objektif kawalan sesuai dan kawalan boleh didapati dalam *Annex A, ISO / IEC 27001:2013 ISMS Requirements*. Ini boleh didapati dalam *Statement of Applicability* atau Dokumen SOA.

10.0 KELULUSAN PENGURUSAN

Dokumen yang dibentangkan kepada Jawatankuasa Kerja ISMS untuk kelulusan maklumat analisis risiko mempunyai perkara-perkara berikut:

(a) Sebarang syarat dan konsep-konsep yang baru atau berbeza – misalnya, aset-aset, ancaman-ancaman, risiko dan profil risiko - perlu dijelaskan.

(b) Maklumat ancaman, risiko dan kelemahan untuk setiap asset kritikal;

(c) Komposit, analisa keputusan-keputusan analisis risiko. Maklumat tersebut perlu dikemukakan dalam bentuk jadual atau grafik yang mudah dibaca. Implikasi mesti turut dijelaskan pada setiap tahap risiko yang sudah dikenal pasti;

(d) Amalan-amalan strategi perlindungan dan kelemahan-kelemahan organisasi dikumpulkan mengikut bidang amalan; dan

(e) Justifikasi untuk rancangan pelindungan

(f) Pengurusan tertinggi telah memutuskan bahawa semua risiko berbaki (risiko yang tinggal selepas menggunakan kawalan yang sesuai) hendaklah disifatkan sebagai 'Diterima' oleh pihak pengurusan.