Information Security Management System
MS ISO/IEC 27001:2007

ASSET CLASSIFICATION & RISK ASSESSMENT PROCEDURE

KLASIFIKASI ASET & PROSEDUR PENILAIAN RISIKO

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
Pn. Ummi Naiemah Saraih Admin Officer	Pn. Rohazna Wahab Deputy Director ICT Centre	En. Nasrudin Abd. Shukor Director ICT Centre ISMR

For Dept Use Only

Date: 19th September 2013 **Version 1.1**

Revision History

No	Date of Change	Discription	Page	Version	Approved By
1.	19/09/2013	Deskripsi pada Bahagian 14 berhubung Kelulusan Pengurusan Sub Bahagian (v) ditukarkan daripada 'Sebarang risiko yang dikenalpasti selepas menggunakan kawalan yang perlu dianggap sebagai 'residual risks' dan diterima oleh pihak pengurusan' kepada 'Pengurusan tertinggi Pusat ICT UniMAP telah memutuskan bahawa semua risiko berbaki (risiko yang tinggal selepas menggunakan kawalan yang sesuai) hendaklah disifatkan sebagai 'Diterima' oleh pihak pengurusan'.	33	1.1	Nasrudin Abd Shukor

1. OBJECTIVE
OBJEKTIF

The purpose of this document is to provide an understanding for an information security risk assessment for UniMAP ICT Division based on MyRAM and ISO 27005 methodology.

Tujuan dokumen ini adalah untuk memberi pemahaman tentang penilaian risiko keselamatan maklumat untuk Pusat ICT UniMAP berdasarkan MyRAM dan kaedah ISO 27005 .

2. DEFINITIONS
DEFINISI

For the purposes of this risk assessment process, the glossary listed in General Circular Letter No. 5/2006: Public Sector Information Security Risk Assessment Guidelines and MS ISO/IEC 27001:2007 apply.

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 MS ISO/IEC 27001:2007 digunapakai.

GARIS PANDUAN UNTUK ASET KLASIFIKASI DAN PENILAIAN RISIKO

Bil .	Terma	Deskripsi
1.	Asset *Aset*	Anything of value for that may cause losses should it be lost or altered. In MyRAM assets are grouped into data/information, services, software, hardware and people. Refer to section 8, Description Of The Risk Assessment Steps: Identification of Asset (Step S3) for more details. *Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya hilang atau berubah. Berdasarkan MyRAM aset-aset tergolong kepada data/maklumat, perkhidmatan, perisian, perkakasan dan manusia. Sila rujuk seksyen 8, Deskripsi Langkah-Langkah Penilaian Risiko: Pengenalpastian Aset (Step S3) untuk maklumat lanjut.*
2.	Asset Depended On *Aset Yang Bergantung Kepada*	A subject state at the occasion of an event. It means other assets are needed to perform its functions. Refer to section 8, Description Of The Risk Assessment Steps: Valuation Of Assets And Establishment Of Dependencies Between Assets (Step S4) for more details. *Subjek yang dinyatakan ketika kejadian sesuatu peristiwa. Bermakna aset lain diperlukan untuknya berfungsi. Sila rujuk seksyen 8, Deskripsi Langkah-Langkah Penilaian Risiko: Penilaian Aset-aset Dan Penentuan Kebergantungan Antara Aset-aset (Step S4) untuk maklumat lanjut.*

3.	Custodian *Penjaga*	Immediate personnel who performs the act of keeping safe, maintaining or guarding an asset. Refer to section 8, Description Of The Risk Assessment Steps: Identification of Asset (Step S3) for more details. *Kakitangan terdekat yang memelihara keselamatan, menyelenggara, atau mengawal sesuatu aset. Sila rujuk Seksyen 8, Deskripsi Langkah- Langkah Penilaian Risiko: Pengenalpastian Aset (Step S3) untuk maklumat lanjut.*
4.	Owner *Pemilik*	Immediate legal possessor in-charge of an asset. Refer to section 8, Description Of The Risk Assessment Steps: Identification of Asset (Step S3) for more details. *Pemilik sah terdekat yang bertanggungjawab untuk sesuatu aset. Sila rujuk Seksyen 8, Deskripsi Langkah-Langkah Penilaian Risiko: Pengenalpastian Aset (Step S3) untuk maklumat lanjut.*
5.	Risk *Risiko*	In general is a possibility of meeting danger or suffering harm or loss, especially from lack of proper care. Refer to section 8, Description Of The Risk Assessment Steps: Calculation of Risk (Step S6) for more details. *Secara umum ia adalah kemungkinan berhadapan dengan bahaya atau menyebabkan mudarat atau kerugian, terutamanya dari kurang penjagaan yang sesuai. Sila rujuk Seksyen 8, Deskripsi Langkah-Langkah Penilaian Risiko: Pengiraan Risiko (Step S6) untuk maklumat lanjut.*

6.	Risk Assessment *Penilaian Risiko*	Evaluation to the possibilities of meeting danger or suffering Harm or loss of ICT assets. *Penilaian bagi kemungkinan-kemungkinan bahaya atau mudarat atau kerugian/kehilangan aset ICT.*
7.	Threat *Ancaman*	Identification for any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental. Refer to section 8, Description Of The Risk Assessment Steps: Assessment of Threat (Step S5) for more details. *Mengenalpasti potensi 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. Sila rujuk Seksyen 8, Deskripsi Langkah-Langkah Penilaian Risiko: Penilaian Ancaman (Step S5) untuk maklumat lanjut.*

8.	Vulnerability *Kelemahan*	Characteristic of any asset which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability or integrity that may increases the severity of the effects of a threat event if it occurs. Refer to section 8, Description Of The Risk Assessment Steps: Assessment of Vulnerability (Step S6) for more details. *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. Sila rujuk Seksyen 8, Deskripsi Langkah- Langkah Penilaian Risiko: Penilaian Kelemahan (Step S6) untuk maklumat lanjut.*

3. RELATED DOCUMENTS
DOKUMEN BERKAITAN

This risk assessment exercise makes reference to the following general circular and guidelines:

Latihan Penilaian Risiko merujuk kepada pekeliling am dan garis panduan berikut:

a) MAMPU Risk Assessment guidelines (MyRAM)
b) ISO/IEC 27005:2008 Risk Assessment Guidelines for Information Security Management
c) Asset Register Template
d) Risk Assessment Template
e) Selection of Controls & Risk Treatment Plan

4. ABBREVIATION

SPSS	*Seksyen Pengurusan Serangan Siber*
SPS	*Seksyen Pemantauan Siber*
MyRAM	*Malaysian Public Sector Information Security Risk Assessment Methodology*
MAMPU	*Malaysian Administrative Modernisation and Management Planning Unit*

5. RISK ASSESSMENT METHODOLOGY
KAEDAH PENILAIAN RISIKO

Risk assessment is a method for determining what threats exists to a specific asset and the associated risk level of that threat. Establishing risk level provides organisation with the information required to select appropriate safeguards and control measures for lowering the risk to an acceptable level.

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 has developed the Malaysian Public Sector Information Security Risk Assessment Methodology or MyRAM to assist public sector organisations in identifying and managing ICT security risks. MAMPU will utilize MyRAM to ensure the integrity of Government information and assets in providing efficient and effective services to all customers. We have also taken ISO/IEC 27005 as a model.

MAMPU telah membangunkan Malaysian Public Sector Information Security Risk Assessment Methodology atau MyRAM bagi membantu organisasi sektor awam dalam mengenalpasti dan menguruskan risiko keselamatan ICT. MAMPU akan menggunakan MyRAM 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.

Refer the Risk Assessment Report that implements the methodology described in section 7. Risk Assessment Process.

Sila rujuk Laporan Penilaian Risiko yang melaksanakan kaedah yang diterangkan dalam seksyen 7. Proses Penilaian Risiko.

Risk Assessment Criteria:

Kriteria Penilaian Risiko

The risk assessment criterias for UniMAP ICT division are as follows:

Kriteria bagi penilaian risiko untuk Pusat ICT UniMAP adalah seperti berikut:

1. All risks assessed as “LOW” rating will be deemed as acceptable to the management.
1. *Semua risiko yang dinilaikan sebagai taraf “RENDAH” akan dianggap sebagai boleh diterima kepada pengurusan.*

2. Risks that do not affect the Vision, Mission and Values of UniMAP may be considered for acceptance.
2. *Risiko-risiko yang tidak menjejaskan Visi, Misi and Nilai-nilai UniMAP mungkin boleh dipertimbangkan untuk penerimaan.*

3. Risks that has no impact on the reputation, branding and image of UniMAP may be considered for acceptance.
3. *Risiko-risiko yang tidak mempunyai impak ke atas reputasi, penjenamaan dan imej UniMAP mungkin boleh dipertimbangkan untuk penerimaan.*

4. Risks that has no impact on the legal compliances may be considered for acceptance.
4. *Risiko-risiko yang tidak mempunyai impak ke atas pematuhan perundangan mungkin boleh dipertimbangkan untuk penerimaan.*

5. Risks that has negligible or no impact to end user may be considered for acceptance.

5. Risiko-risiko yang mempunyai sedikit impak atau tiada kepada pengguna akhir, mungkin boleh dipertimbangkan untuk penerimaan.

6. ASSET CLASSIFICATION & ASSET COLOUR CODING
KLASIFIKASI ASET & KOD WARNA ASET

Four-Level Classification	Description	Type of Docs.
Highly Restricted ***(Sangat Terhad)***	The most sensitive information, intended strictly for Management and IT Director, is assigned this classification. The unauthorized disclosure of information of this type could seriously and unfavourably impact the organization, its shareholders, partners or clients. Reputation & Image could be effected. *Maklumat paling sensitif, klasifikasi ini bertujuan hanya untuk Pihak Pengurusan dan Pengarah IT. Pendedahan tanpa kelulusan maklumat jenis ini boleh memberi impak yang serius dan tidak diingini kepada organisasi, pemegang saham, rakan kongsi atau pelanggan. Reputasi & Imej boleh terjejas.*	Financial Records, Quotations, Service Records, Staff Files, Exco-Minutes, VC instructions & communications to IT Director, Back-up tapes, Source Codes of Applications, System Audit Logs, Firewall configuration data. *Rekod Kewangan, Sebutharga, Rekod Perkhidmatan, Fail Kakitangan, Minit-Exco, Arahan Naib Canselor & komunikasi dengan Pengarah IT, Pita Sokongan, Source Codes untuk Aplikasi, Logs Sistem Audit, Data konfigurasi Firewall.*
Confidential ***(Rahsia)***	This classification is assigned to information less sensitive, yet destined for IT Director and 'Authorised Staff'. The unauthorized disclosure of this type of information could unfavourably affect the organization, its shareholders, partners or clients. Reputation can be effected. *Klasifikasi ini diberi untuk maklumat yang kurang sensitif, bertujuan untuk*	Costing Sheet, Invoice, Debit Note, Credit Note, Agreements, AR, Infrastructure Diagram, Audited Accounts, IP addresses, Pen test results, Risk assessment summery, SOA, Asset Register & Selected SOP's, BCP & DR manuals. *Lembaran kos, Invois, Nota Debit, Nota Kredit ,*

	Pengarah IT dan 'Kakitangan Yang Dibenarkan'. Pendedahan tanpa kelulusan maklumat jenis ini boleh memberi kesan yang tidak diingini kepada organisasi, pemegang saham, rakan kongsi atau pelanggan. Reputasi boleh terjejas.	*Perjanjian, Register Aset, Diagram Infrastruktur, Akaun yang telah di audit, IP addresses, Keputusan Ujian Penembusan, Kesimpulan Penilaian Risiko, SOA, Register Aset & SOP's terpilih, Manual BCP & DR.*
Dept Use Only ***Untuk Kegunaan Bahagian Sahaja***	This classification is reserved for information used within the organization, and whose unauthorized disclosure could seriously and unfavourably affect the organization and its employees. *Klasifikasi ini dikhaskan untuk maklumat yang digunakan di dalam organisasi, dan pendedahan tanpa kelulusan boleh memberi kesan yang serius dan tidak diingini kepada organisasi dan kakitangan.*	Tape Storage and Retrieval Form, Tape Storage Inventory List, Customer Files, ISO docs, Maintenance File, Delivery Order, Customer Testing Bookings. *Storan pita dan Borang Retrieval, Senarai Inventori Pita Storan, Fail Pelanggan, Dokumen ISO, Fail Penyelenggaraan, Delivery Order, Tempahan Customer Testing.*
Unclassified ***Tidak Diklasifikasi***	This classification covers information not clearly fitting into any other classification. Although unauthorized disclosure of this type of information is against policy, it should not seriously or unfavourably affect the organization, its shareholders, partners or clients. *Klasifikasi ini merangkumi maklumat yang tidak dapat dimuatkan atau disesuaikan dengan jelas dalam mana-mana klasifikasi lain. Walaupun pendedahan tanpa kelulusan maklumat jenis ini bertentangan dengan dasar,namun ia tidak sepatutnya memberi kesan yang serius atau tidak diingini kepada organisasi, pemegang saham, rakan kongsi atau pelanggan.*	Not Classified as above. *Tidak Diklasifikasi Seperti Diatas*

All documents generated in UniMap ICT Center (effective Sep 2012) will be having one of the above classifications. Hardware Assets with information will be colour coded with lables to identify them based on the above classifications.

Semua dokumen yang dihasilkan dalam Pusat ICT UniMAP (efektif Sep 2012) akan mengandungi satu daripada klasifikasi di atas. Aset-aset perkakasan dengan maklumat akan dikod warna dengan label untuk dikenalpasti berdasarkan klasifikasi di atas.

RED	**signifies Highly Restricted**
MERAH	***menandakan Sangat Terhad***
BLUE	**signifies Confidential**
BIRU	***menandakan Rahsia***
GREEN	**signifies Dept Use Only** **No Colour Lable on Asset means its public use or not significant for the purpose of security.**
HIJAU	***menandakan untuk Kegunaan Bahagian Sahaja*** ***Tiada label warna pada mana-mana asset bermakna untuk kegunaan awam atau tidak mempunyai kepentingan yang ketara untuk tujuan keselamatan.***
No Colour	**signifies Unclassified**
No Color	***menandakan Tidak Diklasifikasi***

7. REQUIREMENT FOR RISK ASSESSMENT
KEPERLUAN UNTUK PENILAIAN RISIKO

The risk assessment shall be carried out to:

Penilaian risiko akan dilakukan untuk:

a) Take account of changes to organization structure and new assets;
Mengambilkira perubahan pada struktur organisasi dan aset baru;

b) Consider new threats and vulnerabilities; and
Mempertimbangkan ancaman baru dan kelemahan; dan

c) Confirm that controls remain effective and appropriate;
Mengesahkan bahawa kawalan tetap efektif dan bersesuaian;

d) Confirm the residual risk after the controls for the treatment of risk have been implemented;

Mengesahkan risiko yang masih ada setelah kawalan untuk rawatan risiko dilaksanakan;

e) Confirms the risk assessment criteria by the top management.

Mengesahkan kriteria penilaian risiko oleh pihak pengurusan atasan.

8. RISK ASSESSMENT PROCESS
PROSES PENILAIAN RISIKO

The approached adopted strictly the risk assessment process outlined in MyRAM document, starting from Establishment of Team step until Step 10, which is Calculation of Risk. These steps are related to each other because input for one step of the risk assessment activity may be taken from the output of one of its previous steps. Figure 1 below shows the ten (10) steps in a risk assessment exercise.

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.

9. DESCRIPTION OF THE RISK ASSESSMENT STEPS
DESKRIPSI LANGKAH PENILAIAN RISIKO

Below is the overview of the steps in the risk assessment process, its description and the subtasks involved in each step.

Di bawah ialah tinjauan langkah-langkah dalam proses penilaian risiko, penghuraiannya dan subtasks yang terlibat dalam setiap langkah.

Table1: Description of Risk Assessment Steps
Jadual 1: Deskripsi Langkah Penilaian Risiko

Steps	Description	Task(s) Involved
Establishment of Team (S1) *Penubuhan Kumpulan (S1)*	Creates a basic component of a risk assessment exercise.The team members that possess vast knowledge of the organization are identified.The schedule and logistics are established to ensure the smoothness of the whole exercise. *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) Identify the assessment team members *a) Mengenalpasti ahli kumpulan penilaian* b) Draw upTasking Schedule List *b) Menyediakan senarai tugasan dan jadual*

Establishment of Review Boundary (S2) *Penubuhan Kajian Semula Sempadan (S2)*	Determines the scope of the risk assessment process. The final scope will be submitted to the senior management. Once it has received approval, the assessment team will collect all the relevant materials and information. Current Scope is the ICT operations of UniMAP. *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. Skop semasa ialah Operasi ICT UniMAP.*	a) Identify the scope of the risk assessment *a) Mengenalpasti skop penilaian risiko* b) Obtain approval from management *b) Mendapatkan kelulusan dari pihak pengurusan* c) Gather information related to the review boundary *c) Mengumpul maklumat berkenaan kajian semula batasan* d) Revisit Step1 as necessary *d) Kembali ke Langkah 1 jika perlu.*
Identification of Assets (S3) *Mengenalpasti Risiko (S3)*	Identifies all the assets which are within the scope of the risk assessment boundary. *Mengenalpasti semua aset yang terkandung didalam skop Batasan Penilaian Risiko.*	a) Identify related assets *a) Mengenalpasti asset berkenaan* b) Group and classify assets *b) Kumpul dan kelaskan aset* c) Identify assets owners *c) Mengenalpasti pemilik dan penjaga aset*

Valuation of Assets based on CIA (S4) *Penilaian Aset-aset berdasarkan CIA (S4)*	Assigns semi-quantitative values to the assets and determine values based on Confidentiality, Availability & Integrity of each Asset. See page 29. *Menentukan nilai-nilai semi-kuantitatif kepada aset-aset dan tentukan nilai berdasarkan Kerahsiaan, Ketersediaan & Kesahihan setiap aset. Rujuk mukasurat 29.*	a) Identify Asset Values based on CIA (See Asset Register Template) See page 29. *a) Mengenal pasti nilai asset berdasarkan CIA (Sila rujuk Template Aset Register) mukasurat 29* b) Assign a quantified value to each asset (CIA) *b) Menentukan nilai Kuantifikasi bagi setiap asset (CIA)*
Assessment of Threat (S5) *Penilaian Ancaman (S5)*	Determines types of threats associated with the assets, and their relative levels.(See sample of threats on page 23 & 24). *Menetapkan jenis-jenis ancaman berkaitan dengan aset-aset, dan tahap-tahap relatif mereka. (Rujuk muka surat 23 & 24).*	a) Identify all relevant threats to assets *a) Kenal pasti semua ancaman- ancaman kepada aset-aset*

Assessment of Vulnerability (S6) *Penilaian Kelemahan (S6)*	Identifies all potential vulnerabilities which may be exploited by threats.In addition, it will rate the relative vulnerability levels. (See examples of Vulnerabilities on Page 24 & 25). Mengenal pasti semua kelemahan yang berpotensi untuk dieksploitasikan oleh ancaman. Sebagai tambahan, ia akan menilai tahap pendedahan kelemahan relatif. (Rujuk contoh Kelemahan muka surat 24 & 25).	a) Identify potential vulnerabilities exploited by threats *a) Kenal pasti kelemahan-kelemahan yang berpotensi untuk dieksploitasikan oleh ancaman*
Identification of Existing & Planned controls (S7) *Mengenalpasti Perlindungan Yang Sedia Ada & Perancangan (S7)*	Identifies all types of existing & planned controls which have been or will be deployed to protect the assets. *Mengenalpasti semua jenis perlindungan yang sedia ada & dirancang yang telah diatur atau akan diatur untuk melindungi aset-aset.*	a) Review existing and planned controls for protecting the assets *a) Menyemak semula perlindungan sedia ada dan rancangan untuk melindungi aset*

Analysis of Impact (S8) *Analisis Impak (Kesan) (S8)*	Quantifies the job impact as well as business impacts of the assets accordingly. (See page 29) *Mengukur impak kerja serta organisasi sesuatu asset sewajarnya. (Rujuk muka surat 29).*	a) Determine the job impact and businessimpact *a) Tentukan impak kerja dan impak bisnes* b) Determine theimpact levels *b) Tentukan tahap impak*
Analysis of Likelihood/Probibility (S9) *Analisis Kemungkinan/ Kebarangkalian (S9)*	Ascertains the likelihood/ Probibility of threats & vulnerabilities that may happen, with current controls in place. (See Page 29). *Memastikan kemungkinan/kebarangkalian ancaman-ancaman & kelemahan-kelemahan yang boleh berlaku, dengan kawalan yang sedia ada. (Rujuk muka surat 29).*	a) Determine the likelihood/ Probibility of threats & vulnerabilities that may happen *a) Tentukan kemungkinan/ kebarangkalian ancaman-ancaman & kelemahan-kelemahan yang boleh berlaku*

Calculation of Risk (S10) *Pengiraan Risiko (S10)*	Calculates the risk level for each asset, based on the impact value & likelihood results. Use the formula given on page 29. *Mengira tahap risiko untuk setiap aset, Berdasarkan keputusan nilai impak & kemungkinan. Rujuk muka surat 29.*	a) Calculate the risk level for each asset *a) Mengira tahap risiko untuk setiap aset*

10. RISK ASSESSMENT TEAM ROLES AND RESPONSIBILITIES
PERANAN DAN TANGGUNGJAWAB AHLI KUMPULAN PENILAIAN RISIKO

The roles and responsibilities for the RA Team are as follows:
Peranan dan tanggungjawab Pasukan Penilaian Risiko adalah seperti berikut:

a) Project Advisor (Consultant): *Penasihat Projek (Perunding)*
- Provide expert advice for the risk assessment activity.
  Memberi nasihat kepakaran untuk aktiviti penilaian risiko

b) Project Manager (ISMR): *Pengurus Projek (ISMR)*
- Manage the risk assessment activities;
  Mengurus aktiviti penilaian risiko
- Ensure timely completion; and
  Memastikan selesai tepat pada masa; dan
- Conduct reviews of all output and documents before they presented to Project Advisor.
  Melakukan semakan semula untuk semua output dan dokumen sebelum dibentangkan kepada penasihat projek

c) Team Leader (Department Representative): *Ketua Kumpulan (Wakil-wakil Bahagian)*
- Regularly ascertain the progress of work;
  Sentiasa menentukan progres kerja;

- Evaluate results, assess gaps and provide feedback; and
  Menilai keputusan-keputusan, jurang dan memberi maklum balas; dan
- Performs all tasks defined under each risk assessment step.
  Melakukan semua tugasan yang disebut dalam langkah-langkah penilaian risiko

d) Team Members: *Ahli Kumpulan*

- Perform all tasks defined under each risk assessment step.
  Melakukan semua tugasan yang disebut dalam langkah-langkah penilaian risiko

11. ASSETS VALUE RATING
TARAF NILAI ASET

The Risk Assessment team has to establish value rating for the requirements of ICT security, namely Confidentiality (C), Integrity (I) and Availability (A) base on the Table 1 given below. Levels of Low, Medium and High are stated in the table based on descriptions given against each score. In rating the sensitivity of each asset, RA Team shall use the following guidelines:

Berdasarkan Jadual 1 dibawah, kumpulan penilaian risiko perlu mewujudkan taraf nilai untuk keperluan Keselamatan ICT, iaitu Rahsia/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-garis panduan berikut:

a) **Confidentiality**. The impact of unauthorized disclosure of confidential information can result in loss of stakeholder confidence and embarrassment.
Rahsia. *Kesan pendedahan maklumat rahsia/sulit yang tidak diluluskan boleh mengakibatkan kehilangan keyakinan pemegang saham dan mengaibkan.*

b) **Integrity**. This is the impact on the system that would result from deliberate, unauthorized or inadvertent modification of the asset.

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

c) **Availability**. This is the impact as a result from deliberate or accidental denial of the asset's use.

Ketersediaan*. Ini ialah kesan daripada penafian pengunaan aset secara sengaja atau kebetulan.*

Each asset must be evaluated according to their respective confidentiality, integrity and availability levels.

Setiap aset mesti dinilai menurut tahap Confidentiality (Rahsia), Integrity (Kesahihan) dan Availability (Ketersediaan) masing-masing.

Risk Scoring Method

Kaedah Skor Untuk Risiko

Using the table 1 below, after the CIA values have been calculated and the asset value computed, now we have to calculate the levels of Risks these assets are exposed to. Risks exist due to the existence of ***Threats*** to these assets and the assets own ***Vulnerabilities***.

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.*

Threats **:** Some examples of threats are as below:

Ancaman ***:*** *Di bawah ialah beberapa contoh ancaman:*

1. Virus

   Virus

2. Theft

   Kecurian

3. Damage due to wear “n” tear

   Kerosakan disebabkan wear “n” tear
4. Accidental Deletion of data

   Memadam data secara tidak sengaja
5. Hardware failure (Mechanical Fault)

   Perkakas gagal berfungsi (Kerosakan Mekanikal)
6. Power Fluctuation

   Power Fluctuation
7. Improper usage of Assets (User Error)

   Penyalahgunaan asset (Kesalahan Pengguna)
8. Incompetency of the user

   Pengguna yang tidak cekap
9. Sabotage & Malicious intent

   Sabotaj & Niat yang tidak baik
10. Espionage due to business competition

    Pengintipan kerana persaingan dalam perniagaan
11. Fire

    Kebakaran
12. Weather and Natural Disasters

    Cuaca dan Bencana Alam

Vulnerabilities:

Kelemahan:

1. Lack of proper inspection

   Kurang pemeriksaan yang sesuai
2. Not updated AV solution

   AV yang tidak dikemaskini
3. Poor Patch management

   Pengurusan Patch yang kurang baik
4. Lack of capacity plan for systems

   Kurang pelan keupayaan untuk sistem
5. Lack of User training & awareness

   Kurang latihan/kursus dan kesedaran pengguna

6. No back-ups
   Tiada sokongan
7. Inaccurate user information
   Maklumat pengguna yang tidak tepat
8. Lack of User security policies
   Kurang Polisi Keselamatan untuk Pengguna
9. Badly maintained fire suppression systems
   Sistem memadam api yang tidak diselenggara dengan baik
10. Citing and location of assets inadequate
    Tempat atau lokasi aset yang tidak sesuai
11. No access controls
    Tiada control akses
12. Assets not tagged and classified
    Aset tidak ditag dan diklasifikasi
13. No procedures for system maintenance
    Tiada prosedur untuk sistem penyelenggaraan
14. Poor source codes security
    Keselamatan kod sumber yang kurang baik

Please note that these examples are not complete and can be more depending on the activities and functions of each department. The users must work as a team in brainstorming and identifying the correct threats and vulnerabilities for each asset and record the findings in the "Risk Register".

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".*

Probability & Impact

Kebarangkalian & Impak

The risk identified based on the threats and vulnerabilities may or may not happen in real environment. There is a "chance" of the risk happening depending on the situation. Hence risk assessment is based on the "Probability of the occurrence" and the "Impact" due to the occurrence. Impact is measured to the asset directly as well as the impact to business.
Probability and Impact can be selected based on the table 1 below and rated from 3~1 based on the description in the table.

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 3~1 berdasarkan huraian dalam Jadual.

Table 1

ASSET VALUE

CONFIDENTIALITY (C)		
Rating	**Description**	**Points**
High (H)	Confidential, Real problem if disclosed to external parties, Loss of Image and Reputation, Legal action.	3
Medium (M)	Restricted, should not happen, minor problem if disclosed. Loss of Reputation but can be recovered.	2
Low (L)	Public, does not matter if disclosed. No impact to image.	1

INTEGRITY (I)		
Rating	**Description**	**Points**
High (H)	Serioius problem, accuracy and completeness Is critical for service delivery and customers. May have permanent impact on ICT sevice.	3
Medium (M)	Noticeable problem, Can effect the service but service can be restored quickly.	2
Low (L)	Negligible or minor problem, no influential or critical effect on the business. Can be restored within 2 hours	1

RISK VALUE

PROBABILITY (P)		
Probability of Event	**Description**	**Points**
High (H)	High Likely, Almost Certain, Common Occurance (Eg: Once every month or less)	3
Medium (M)	Most Likely, Probable to Occure, (Eg: Once every 2 months)	2
Low (L)	Unlikely, Infrequently, Rarely Happens (Eg: Once in 6 months or more)	1

IMPACT / HARM (I)		
Impact / Harm of Event	**Description**	**Points**
High (H)	Serious to grave harm	3
Medium (M)	Significant to damaging harm	2
Low (L)	No to minor Harm	1

GARIS PANDUAN UNTUK ASET KLASIFIKASI DAN PENILAIAN RISIKO

AVAILABILITY (A)		
Rating	**Description**	**Points**
High (H)	Mission critical, non-availability is a real problem. Can permanently impact ICT service & Reputation	3
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.	2
Low (L)	No or minor problem, extended outage is tolerable. Outage is only a few hours. No impact to Image & Reputation	1

Business Impact (BI)		
Impact / Harm of Event	**Description**	**Points**
High (H)	Serious to grave impact on business. Loss of customer. Can shut down business operations due to Legal breech.	3
Medium (M)	Significant to damaging impact on business. Penalties may be levied but can be tolerated. Financial loss to Business	2
Low (L)	Negligible Impact on business.	1

SCORE = (C x I x A)

SCORE = P x [[I + BI]/2] x AV 1

ASSET VALUE (AV) - based on CIA		
Rating	**Description**	**Value**
High (H)	19 - 27 points	**H**
Medium (M)	8 - 18 points	**M**
Low (L)	1 - 7 points	**L**

RISK LEVEL		
Rating	**Description**	**Points**
High (H)	122 - 243 points	**H**
Medium (M)	61 - 121 points	**M**
Low (L)	1 - 60 points	**L**

13. GUIDELINES ON DECISION WITH RISK IDENTIFIED

GARIS PANDUAN UNTUK KEPUTUSAN BAGI RISIKO YANG DIKENALPASTI

The output of the risk assessment process is input to a decision-making process which determines whether to accept, reduce, transfer or avoid risks identified. This will be done in the Selection of Controls and reflected in the Risk Treatment Plan (RTP).

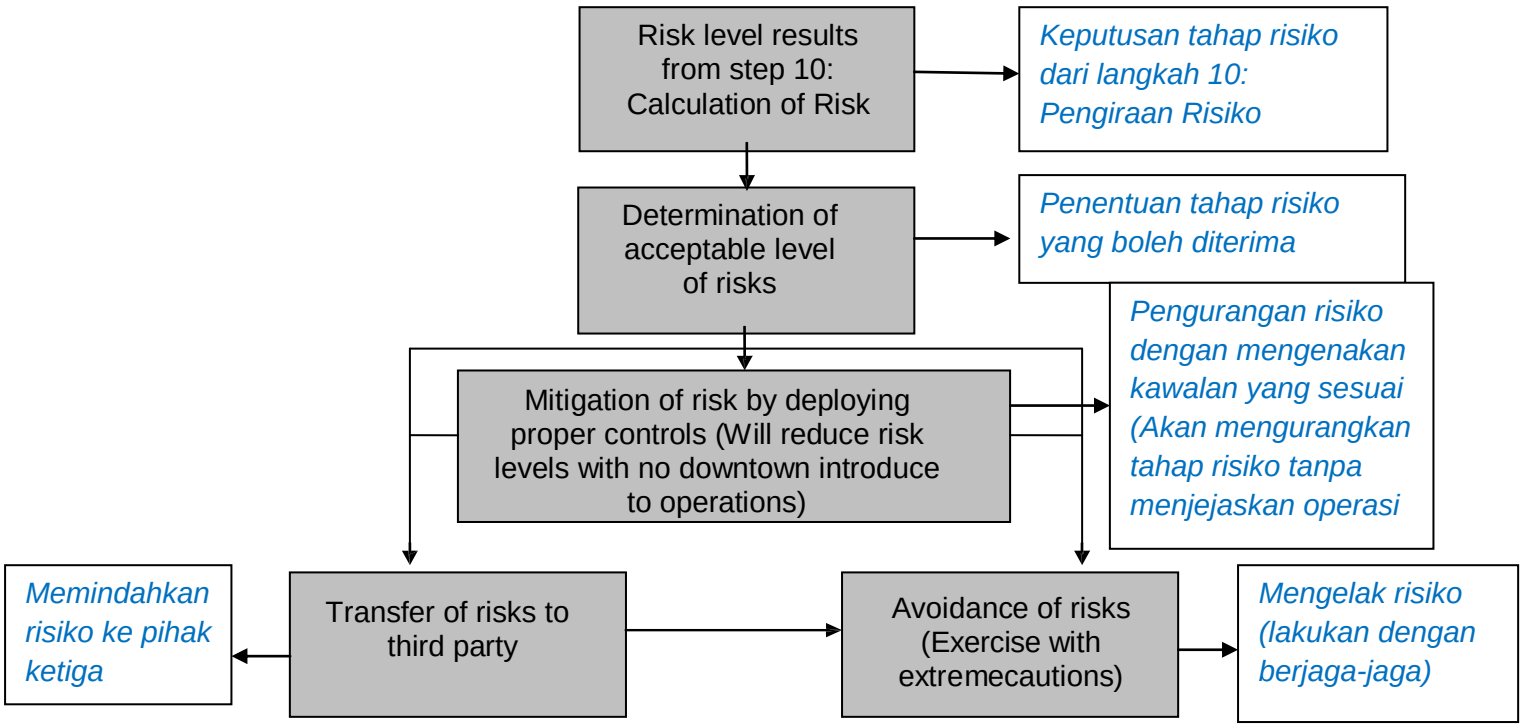
Output proses penilaian risiko adalah input bagi proses membuat keputusan yang menetapkan sama ada menerima, mengurangkan, memindahkan atau mengelakkan risiko yang sudah dikenalpasti. Ini akan dilakukan dalam Selection of Controls (Pemilihan Kawalan) dan ditunjukkan dalam Risk Treatment Plan (RTP) (Pelan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

The RA Team shall establish the High-Level Recommendation to obtain written approval or acknowledgement from the ISMS Sponsor (ICT Director) in handling risks. At this point the RA team will define in the RTP what is to be done after obtaining the risk level for all identified assets. During this stage, decisions of whether to accept, reduce, transfer, or avoid risks that have identified must be made only after the risk assessment exercise has been completed. This has to be finalized by the ICT Director.

Pasukan Penilaian Risiko akan menubuhkan High-Level-Recommendation untuk memperoleh kelulusan bertulis atau pengakuan daripada Penaja ISMS (Pengarah ICT) dalam mengendalikan risiko. Kumpulan Penilaian Risiko 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 dari Pengarah ICT.

Basically decision making of whether to accept, reduce, transfer, or avoid risks level are based on the factors of time, money, manpower and equipment. Determination of option on handling the risk can be done by following the steps in Figure 2 below.

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

As shown in Figure 2 above, **the first step to make high-level recommendations is by getting the result of the risks levels from Step 10**. Then determine what level of risk that is acceptable by RA Team. **Refer Section 4: Criteria for Accepting Risks.**

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.

In the High-Level Recommendations, there are two (2) outputs:

Untuk Cadangan High-Level, terdapat dua (2) output iaitu:

i) Decision on Option; and
Keputusan atas pilihan; dan

ii) Protection Strategy.
Strategi Perlindungan

Decision on Options

Keputusan atas Pilihan

In the "Decision on Option", the RA team will propose to the management of ICT Compliance Division whether to accept, reduce, transfer, or avoid the risk level of a particular threat that exists in a specific asset. The descriptions for each decision options are as follows:

Dalam Keputusan atas Pilihan, Kumpulan Penilaian Risiko akan mencadangkan kepada pengurusan Bahagian Pematuhan ICT 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) **Accept**: to accept risks associated with the assets without implementing any safeguards or controls.
Menerima: *untuk menerima risiko-risiko berkaitan dengan aset-aset tanpa melaksanakan sebarang perlindungan atau kawalan*

b) **Reduce**: to implement controls to mitigate risks. When risks are high, it is essential to reduce the risk levels.

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

c) **Transfer**: to transfer risks to another entity.

Pemindahan: *Memindahkan risiko kepada entiti yang lain.*

d) **Avoid**:to avoid risks when thereisno other available options.

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

The RA Team shall accept, reduce, transfer or avoid risk for the following criteria:

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

a) Check and assess whether the risk can be accepted or not. The RA team could propose to the management to accept all assets with risk levels of Low and there is no immediate action taken to protect the asset; and

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; dan

b) If the risks cannot be accepted, then check and assess whether they should be reduced, transferred or avoided.

Jika risiko-risiko tidak boleh diterima, maka semak dan nilaikan sama ada ianya patut dikurangkan, dipindahkan atau dielakkan.

i. If the implication of the risks is catastrophic and critical (High), then the risks should be reduced. Risk reduction shall be achieved through the implementation of the following components: operational, procedural, physical, personnel, and technical security to ensure that critical operations continue with no downtime; and

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

ii. If the implication of the risks is of an average criticality (Medium), then the risks may also be transferred on the following conditions.

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

- Risks must be transferred fairly. Risks can be shared by the asset owners and third parties. For example, if a communication line breaks down, and the Service Level Agreement (SLA) with the provider of the line states that the line will be available within 24 hours; unforeseen disasters that may strike the third party is a shared risk the agency is prepared to take; and

  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

- The risks should be avoided altogether if there are no reasonable controls that can be implemented for risk mitigation. Example, to avoid risks is to totally disconnect the system.

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

Protection Plan (RTP) (*Pelan Perlindungan*)

The RA Team now develops a protection plan called “Risk Treatment Plan” (RTP) to be presented to the management. For the RTP,the RA team needs to look whether the current controls are sufficient to protect the assets or not. If the current controls are not sufficient, the affected team or the risk owner team shall select appropriate control objectives and controls available in Annex A, ISO/IEC 27001:2005 ISMS Requirements.Justification must be elaborated to support reasoning to implement the controls. This can be found in the Statement of Applicability or SOA document.

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 27001:2005 ISMS Requirements.Ini boleh didapati dalam Statement of Applicability atau Dokumen SOA.

Refer to Risk Treatment Plan document for more details.

Rujuk Dokumen Risk Treatment Plan untuk maklumat lanjut.

14. MANAGEMENT APPROVAL
KELULUSAN PENGURUSAN

The document presented to ISMS Committee for approval on risk analysis information has the following items:

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

a) Any terms and concepts that may be new or different - for example, assets, threats, risk and risk profile - are explained.

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

b) The following data should be presented to and summarized for the ICT Director:

b) Data berikut perlu dikemukakan dan dirumuskan untuk Pengarah ICT:

i. Threat, risk and vulnerability information for each critical asset;
Maklumat ancaman, risiko dan kelemahan untuk setiap asset kritikal;

ii. Composite, analyzed results of the risk analysis. These should be presented in a table or graphical easy-to-read information. Each identified level of risk should also state clear implications;
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;

iii. Protection strategy practices and organisational vulnerabilities grouped by practice areas; and

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

iv. Justification on planned safeguards.

Justifikasi untuk rancangan pelindungan

v. The top management of UniMAP ICT Centre has decided that all residual risks (Risks remaining after applying the suitable controls) shall be deemed as 'Acceptable' to the management.

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

RISK ASSESSMENT FRAMEWORK