TERMS OF REFERENCE
(TOR)

PROVISION OF DEVELOPMENT OF TECHNICAL DOCUMENTATIONS FOR INFORMATION SECURITY & DATA PRIVACY ASSESSMENT SUITE (ISDPAS) FOR CYBERSECURITY MALAYSIA

TABLE OF CONTENT

APPENDICES

1. BACKGROUND

1.1 CyberSecurity Malaysia is a national cyber security specialist center under the Ministry of Communications and Multimedia. Among the services offered to the government agencies and public sectors is related to information security and data privacy management and assurance.

1.2 CyberSecurity Malaysia plans to develop **Information Security & Data Privacy Assessment Suite (ISDPAS)**. ISDPAS is a web-based application with several assessment modules on information security & data privacy which consists of core engine for correlation & analysis on assessment findings. ISDPAS is targeted to various users depending on their subscription purpose.

1.3 With ISDPAS, it can help organizations to assess the current level of governance, readiness and compliance in context Information Security Management and Data Privacy. Organizations can also measure and identify current gaps of information security or data privacy implementation. Thus, organizations can plan appropriate activities to fill those gaps and focus on areas that need improvements. This, overall, helps to manage information security and or data privacy threats and challenges faced by the organizations.

1.4 Thus, several technical documents need to be produced prior development of ISDPAS (as stated in Section 3).

2. OBJECTIVE

2.1 To develop technical documentations as input for functional, information security and data privacy requirements during development stage of ISDPAS.

3. SCOPE OF WORK

Bidder is required to submit a proposal on technical documents for development of ISDPAS. The technical documents will be used during development stage of ISDPAS. Thus, the preparation of technical documentations MUST be based on contents in Appendix 1, 2 and 3 respectively.

The technical documents that are expected for development ISDPAS are as follows:

i) **User Requirement Specification** inclusive of:
   a) Functional Specification
   b) Software & Hardware Infrastructure
   c) System Flow
   d) Database Design

ii) **Concept Design** inclusive of:
   a) Enterprise Architecture Framework – inclusive of business architecture, data architecture, application architecture and technology architecture.
   b) Algorithm Application wherever is relevant.

iii) **System Description Design** inclusive of:
   a) Solution Design
   b) Interface Design

iv) **Application Design Specification.**

All the above four (4) technical documents must include the following requirements:

i. **Information Security Requirements**

   Bidder to document/include all relevant information security requirements on for ISDPAS development in order to preserve the confidentiality, integrity and availability of ISDPAS.

ii. **Data Privacy Requirements**

   Bidder to document/include all relevant data privacy requirements for ISDPAS development in order to preserve privacy of the personal identifiable information (PII) involved in ISDPAS.

3.1 Proposal shall comply with all the provisions of this Request for Proposal (RFP). Any proposal not complying therewith may be disregarded. The Bidder is required to submit a proposal that shall include the following:

--- **[THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]** ---

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
1.0	**GENERAL REQUIREMENTS**				
1.1	**SCOPE OF WORKS** Bidder MUST fully comply with the scope of works, which is development of technical documents as follows: i) **User Requirement Specification** inclusive of: a) Functional Specification b) Software & Hardware Infrastructure c) System Flow d) Database Design ii) **Concept Design** inclusive of: a) Enterprise Architecture Framework – inclusive of business architecture, data architecture, application architecture and technology architecture. b) Algorithm Application wherever is relevant. iii) **System Description Design** inclusive of: a) Solution Design b) Interface Design iv) **Application Design Specification**.	M			

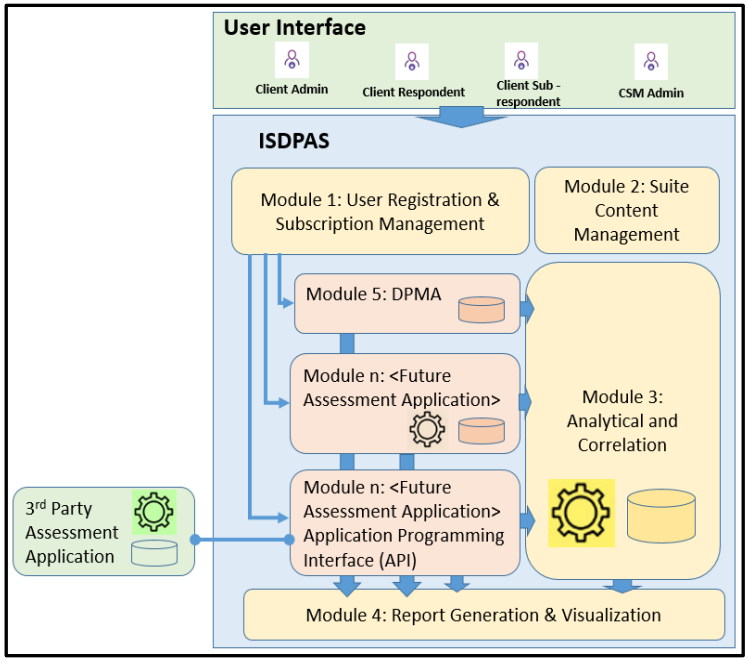
Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
1.2	All the above four (4) technical documents must include the following requirements: **i) Information Security Requirements** Bidder to document/include all relevant information security requirements for ISDPAS development in order to preserve the confidentiality, integrity and availability of ISDPAS. **ii) Data Privacy Requirements** Bidder to document/include all relevant data privacy requirements for ISDPAS development in order to preserve privacy of the personal identifiable information (PII) involved in ISDPAS.	M			
1.3	Bidder shall confirm that their proposal is based on development of the above scope of works. Bidder's partial compliance to the said scope of works shall be disqualified.	M			
2.0	**<u>BIDDER'S RESPONSIBILITY</u>**				
2.1	Bidder shall develop the technical documentations as stated in scope of work on an application namely 'Information Security & Data Privacy Assessment Suite (ISDPAS)'.	M			
2.2	Bidder is subjected to all existing government guidelines, procedures and regulations pertaining to the procurement and conduct of professional services.	M			
2.3	Bidder shall confirm that their proposal is based on the entire provision of the above scope of works/terms of reference. Bidder's partial compliance to the said scope of works/terms of reference shall be disqualified.	M			
2.4	Any of the outputs, findings and any other documents pertaining to the development of the Project shall not be abused or used by the Bidder for profit based or otherwise.	M			
2.5	In the interest of national security, all discussions and decisions made will remain confidential and should not be disclosed to any other person or organization.	**I**			
2.6	No media briefings can be undertaken or press releases issued by the Bidder or any of the Project team members.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that <u>MUST</u> be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
3.0	**BIDDER PAST EXPERIENCES**				
3.1	Bidder shall have at least two (2) years experiences in development of technical documentations.	M			
3.2	Bidder shall have involved in development of technical documentations for more than two (2) projects on application development or similar.	M			
3.3	Bidder shall have experiences in information security and data privacy.	M			
3.4	Bidder **MUST** have dedicated project team. Bidder shall provide curriculum vitae of project team members to be involved in the proposal.	M			
3.5	Bidder **MUST** have dedicated project team with relevant certification in information security and/or data privacy e.g. CISM or equivalent.	M			
4.0	**DOCUMENTATION REQUIREMENTS**				
4.1	All documentation shall be in English. Bidder shall be responsible for any translation cost incurred (if any) concerning the submission of the documentation required by this RFP.	M			
4.2	Bidder **MUST** provide timeline and documentation for all activities related to the development as specified in Scope of Work (SoW).	M			
4.3	CyberSecurity Malaysia reserves the right to reproduce all or part of the document submitted by the bidder for internal use.	M			
4.4	Bidder **MUST** provide documents as stated in Scope of Work (SoW).	M			
4.5	Bidder shall describe the project management methodology to be undertaken in the project planning document to ensure the time is met as scheduled as well as meeting the technical requirements of the project. The project management methodology shall include the tasks and activities involved as listed below: i) Project team structure; ii) Point of contact; iii) Implementation schedule based on proposed project delivery and timeline which indicating: a) Key milestones, dates and deliverables; B) Number of manpower involved and resumes.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
B	**TECHNICAL REQUIREMENTS**				
1.1	**PURPOSE** To develop technical documentations on "Information Security & Data Privacy Assessment Suite (ISDPAS)" application. ISDPAS is a web-based application and will be deployed on premise. Overall ISDPAS is as follows:  	M			
1.2	Bidder shall develop technical documentations that cover the following modules:	M			

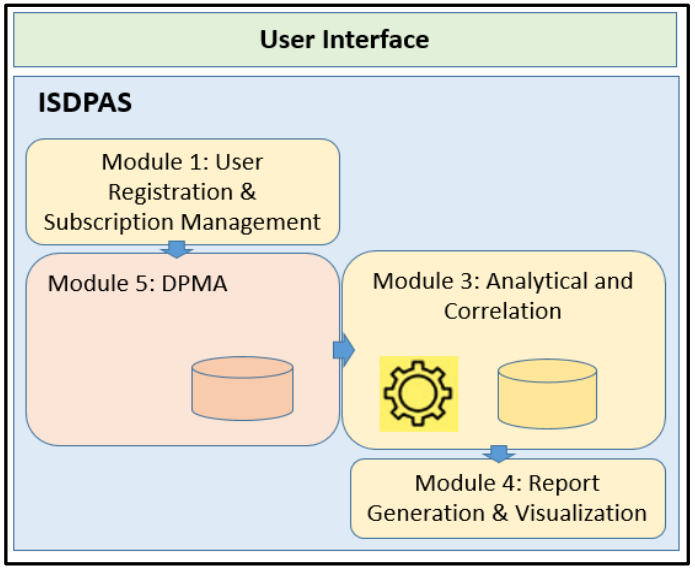
Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
1.3	**Module 1**: **User Registration & Subscription Management** i) Allow registration and module subscription by new user and existing user via 'Contact Us' form. ii) 'Contact Us' form allows verification and approval/rejection of an application by CSM admin. iii) CSM admin will create a unique user id for new user based on their organization's name and subscribed module(s). CSM admin will renew user id for existing user based on their organization's name and existing / newly subscribed module(s). iv) CSM admin will send an email to the approved application on their user id and password. v) ISDPAS store and process respondents' data for other purpose i.e., analytical study in future.	M			
1.4	**Module 2: Suite Content Management** i) Allow CSM administrator to perform maintenance on overall ISDPAS's feels and looks. ii) Allow bulk upload of questionnaires content in specific format i.e., MS Excel into assessment modules. iii) Provide suitable 'Online Help' based on each modules' requirements i.e., on mouse over	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
1.5	**Module 3: Analytical & Correlation** i) Core of ISDPAS where correlation and analysis will be performed to provide significant and meaningful findings based on assessment results; ii) Provide graphical user interfaces (GUI) to allow correlation & analysis been conducted; iii) Identify suitable platform or method for Machine Learning application to be executed in ISDPAS to perform analytical and correlation activities as follows: **a) Correlation and analysis for multiple assessment application** Results from multiple assessment application, for example, DPMA and results from other assessment applications will be correlated and analyzed to provide greater insight of organization's practices on inter-related domains and understanding on certain underlying issues. **b) Correlation and analysis on individual assessment application** Results from one (1) assessment application, for example, various domains in DPMA will be correlated and analyzed to provide better insight of organization's practices. iv) CSM admin will benefit from this module in order to get the landscape of organizational practices, governance and compliance in information security and data privacy. v) This module should allow customized correlation and analysis by CSM admin by selecting certain parameters and variables i.e., sector name, domains etc.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

1.6	**Module 4: Report Generation & Visualization** i) Consists of assessment questionnaires on data privacy domains. ii) Visualization in several graphical formats on (i) assessment results; and (ii) correlation and analysis findings. iii) Visualization is in several graphical formats and can downloaded into a few files format (i.e. CSV, PDF).	M			
1.7	**Module 5: DPMA** i) Under ISDPAS, there will be several assessment applications to be developed and added as separate module whenever they are ready for deployment. Features and functionality of Module 5 will be replicated to other assessment modules. ii) The first assessment application to be developed is DPMA as follows;  iii) Consists of assessment questionnaires on data privacy domains where access by client admin and respondents via the given user id. iv) Client admin and respondents with the access to this module will answer the respective questionnaires within specific timeframe.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
	v) Client admin and respondents will be alerted if the assessment is incomplete upon reaching specific timeframe. vi) Assessment application will have several questionnaires according to application's questionnaires structures. vii) Upon completion of the assessment, respondent will be able to view the result or score. viii) Correlation and analysis will be performed on assessment results (using engine in Module 3). ix) Client admin and respondent can view the (3) types of results which are linked to Module 4: **a) Assessment Results and Score** Overall score and level of compliance or readiness based on the defined matrix of the assessment. **b) Correlation and analysis findings on multiple assessment application** *(if subscribe more than one (1) assessment application)* Findings from multiple assessment application, for example, DPMA and results from other assessment applications will be correlated and analyzed to provide greater insight of organization's practices on inter-related domains and understanding on certain underlying issues. **c) Correlation and analysis findings on DPMA domains** Findings from correlation and analysis on domains in DPMA will provide better insight of organization's practices.				
1.8	**Module *n*: (Future Assessment Application)** i) Available slot for future assessment application where features and capabilities are similar as Module 5. ii) It able to perform correlation and analysis on assessment results (using engine on its own or in Module 3); or iii) Allow integration with third-party / external assessment application via API.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

2.0	**INFORMATION SECURITY REQUIREMENTS** Bidder's proposal **MUST** be able to comply with all the specifications below (but not limited to): **i) Secure Software Development Life- Cycle (SSDLC)** The preparation of technical documents MUST consider SSDLC at every development phases. **ii) Authentication** All users MUST be authenticated before access is granted to the ISDPAS. **iii) ID & Password Management** a) Enforce role-based access control b) CSM admin is responsible to generate unique user id to client admin based on organization's name and chosen module. c) Respondent to login to respective module and answer the assessment by using this user id. d) Using one login id, respondent is able to access the subscribed module(s). **iv) Input validation** a) Every data input MUST have input validation to prevent improperly formed data from entering ISDPAS; b) Error messages must be descriptive to allow user to rectify data input error. **v) Audit trail/log** a) Audit trails should be generated by ISDPAS and include the local date and time of the actions that alter the record; b) Data must be stored in a secure manner and must not be editable by any user. **vi) Subscription Period** a) Respondent to complete assessment on respective module within a predefined subscription period. b) The given user id will be invalid after the subscription period. Hence, new subscription application to be submitted to CSM admin. **vii) Backup and Redundancy (to avoid Single Point of Failure (SPoF))** o Design of ISDPAS must consider backup and redundancy components on i.e., secondary database to avoid SPoF.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
	viii) Application Programming Interfaces (APIs) o APIs developed for ISDPAS must apply relevant security schemes to prevent malicious attacks or misuse of APIs. **ix) Adopts OWASP Top 10 Web Application Security Risks** o Application is developed according to secure development practices to mitigate web application security risks. Refer OWASP Top Ten for most critical security risks to web applications.				
3.0	**DATA PRIVACY REQUIREMENTS** Bidder's proposal **MUST** be able to comply with all the specifications below (but not limited to): **i) Privacy by Design (PbD)** o Data protection to be taken into account throughout the system development process. Thus, the preparation of technical documents MUST consider relevant PbD concepts at every development phases. o The following data design strategies may need to suitably apply at the relevant stage: a) **Minimize** Limit as much as possible the processing of PII without compromising the function of ISDPAS. b) **Abstract** Limit as much as possible the detail in which personal data is processed, while still being useful. c) **Hide** Prevent PII from becoming public or known.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT)* IN SUPPORTING THEIR COMPLIANCE STATEMENT
	ii) Privacy Notice / Privacy Policy o Privacy Notice & Consent to include during data collection in Module 1. **iii) Data masking techniques** o Apply pseudonymization (or any suitable data masking technique) on the collected PII data to preserve the privacy of data used correlation. o Necessary data masking technique should be applied to protect sensitive data in database level. **iv) Encryption** o Apply during data collection in Module 1, during transit between modules and in processing stage. o The encryption algorithm MUST apply the listed algorithms by MySEAL (https://myseal.cybersecurity.my) only.				

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement :These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement :These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only :These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

4. PROJECT DELIVERABLES & TIMELINE

The Project should be successfully delivered not later than **2** (**two**) months from the date the Project is awarded to the successful bidder with the following details:

	Activity	*Timeline
1.	Letter of Award (LOA) is issued by CyberSecurity Malaysia	T1
2.	Signing of relevant contract & documents (including review of documents from Legal)	T2 = T1 + 2 w
3.	Phase 1 – Development of 'User Requirement Specification' & 'Concept design including algorithm development'	T3= T1 + a w
4.	Phase 2 – Development of 'System Description Design' & Application Design Specification	T4= T1 + b w

* Timeline by which activity shall be completed ('T1' is the date of LOA. 'w' means time period of a week, 'a', 'b', and 'c' is the proposed timeline)

5. PROJECT MANAGEMENT APPROACH

Bidder shall describe the project management methodology to be undertaken in the project planning document to ensure the time is met as scheduled as well as meeting the technical requirements of the project. The project management methodology shall include the tasks and activities involved as listed below:

i) Project team structure;
ii) Point of contact;
iii) Implementation schedule based on proposed project delivery and timeline which indicating:
   a) Key milestones, dates and deliverables;
   b) Number of manpower involved and resumes.

6. BIDDER RESPONSIBILITY

a) The Bidder is subjected to all existing government guidelines, procedures and regulations pertaining to the procurement and the conduct of the professional services.

b) The Bidder shall confirm that their proposal is based on the entire provision of the above scope of works/terms of reference. The Bidder's partial compliance with the said scope of works/terms of reference shall be disqualified.

c) The bidder shall review this document and take full responsibility for obtaining the necessary information from CyberSecurity Malaysia as may be required to meet the specifications and requirements.

d) The bidder shall review and fulfil all specifications and requirements before committing to sign the purchase agreement.

e) CyberSecurity Malaysia reserves the right to reproduce all, or part of the document submitted by the bidder for internal use.

7. POINT OF CONTACT

The Bidder shall nominate an executive within its organization, whom shall be a full-time employee of the organization to be working together with the Project Owner from CSM. The appointed person shall be the single point of contact between the Bidder and CSM.

IMPORTANT NOTE: Appendices 1, 2 and 3 provide information on ISDPAS's overview and relevant requirements for guidance on development of four (4) technical documents specify in Section 3 (Scope of Work). Bidder shall develop technical documentations that cover the ISDPAS's modules as per Appendix 1 & 3 and requirements as per Appendix 2.

APPENDIX 1 : OVERVIEW OF ISDPAS

This appendix provides overview of ISDPAS.

A. System Description

ISDPAS is a web-based application and will be deployed on premise. The overall ISDPAS consists of the following modules as depicted in Figure 1 (but not limited to).

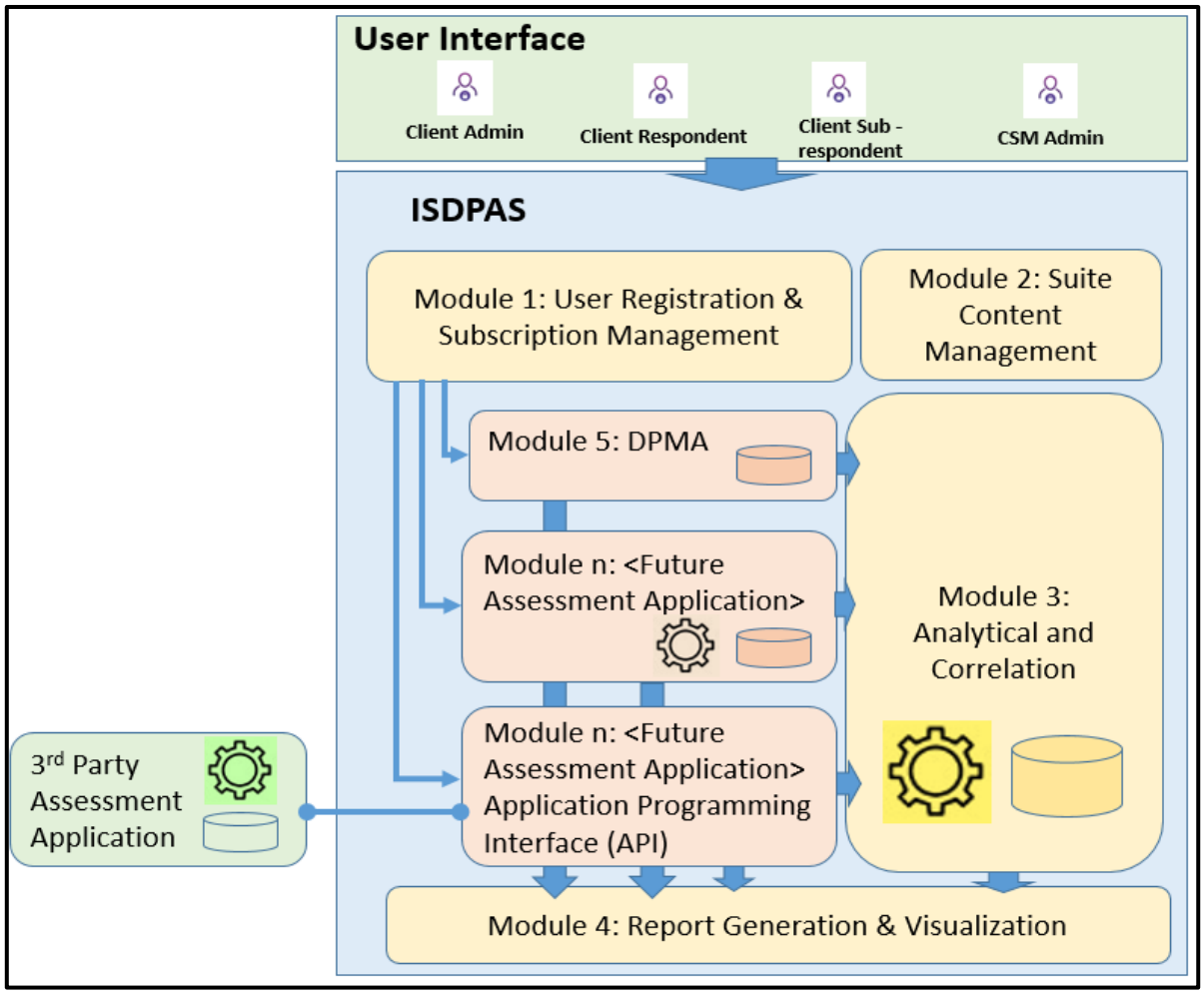


Figure 1 : Overview of ISDPAS

A) User interface:

a) Allow CSM Administrator to interact with ISDPAS and access its' modules based on the assigned access rights;

b) Allow the clients to interact with ISDPAS and access respective module(s) based on the assigned access rights.

B) Module 1: User Registration & Subscription Management

Allow registration and subscription for new user and existing user.

C) Module 2: Suite Content Management

Allow CSM administrator to perform maintenance on overall ISDPAS's feels and looks.

D) Module 3: Analytical and Correlation

i. Core of ISDPAS where correlation and analysis will be performed to reveal meaningful relationships between different domains or groups of domains and to provide significant findings based on assessment results;

ii. Provide an engine for correlation and analysis as follows;

- **Correlation and analysis for multiple assessment application**

  Results from multiple assessment application, for example, DPMA and results from other assessment applications will be correlated and analyzed to provide greater insight of organization's practices on inter-related domains and understanding on certain underlying issues.

- **Correlation and analysis on individual assessment application**

  Results from one (1) assessment application, for example, various domains in DPMA will be correlated and analyzed to provide better insight of organization's practices.

E) Module 4: Report Generation & Visualization

Visualization in several graphical formats on (i) assessment results; and (ii) correlation and analysis findings (from Module 3).

F) Module 5: DPMA

i. Consists of assessment questionnaires on data privacy domains;

ii. Perform correlation and analysis on assessment results (using engine on its own or in Module 3).

G) Module *n* (Future Assessment Applications)

i. Available slot for future assessment application where features and capabilities are similar as Module 5.

ii. Able to perform correlation and analysis on assessment results (using engine on its own or in Module 3); or

iii. Allow integration and interfaces with third-party / external assessment application via API.

B. System Users

The main users of ISDPAS are:

NO	TYPE OF USER	Description
1	CSM administrator	a) Review the submitted subscribtion application; b) Provide approval / rejection on subscribtion application; c) Provide access to organizations based on the chosen package by generate unique user id to the approved applicant and send notification via email; d) Responsible on maintenance of "Suite Content Management" (add, delete, update, review assessment contents); e) Adding / dropping / editing of organization's information; f) Adding / dropping / editing of organization's services on relevant assessment subscriptions; g) Adding / dropping / editing of questionnaires relevant to the assessment applications in Module 3; h) Manage change request;

NO	TYPE OF USER	Description
		i) Technical management such as hosting, maintenance and system support.
2	Client Administrator	a) Creating/ dropping/ updating list of respondents for organization; b) Grant access to respondents to answer questionnaires based on chosen package; c) Initiate new assessment cycle by completing the current organization's information, respondent and approver; d) Notify respondents on new assessment or incomplete assessment; and e) Adding / deleting/ editing of assessment that has been done.
3	Client Respondents	a) Answer the questionnaires based on provided components; b) Provide additional comments to related questionnaires; c) Able to see all questions but only permitted to answer questions based on their role and chosen package; and d) Delegate the questionnaires to sub-respondent (if any).
4	Client Sub - respondents	Answer the delegated questionnaires.

APPENDIX 2 : REQUIREMENTS

This appendix provides requirements on ISDPAS.

A. Functional Requirements

ISDPAS consists of modules as follows:

Main Modules	Description
Module 1: User Registration & Subscription Management	An organization representative or user can visit ISDPAS home page via a secure link (https://isdpas.cybersecurity.my). ***New User*** 1. If they are interested to subscribe any of the assessment modules, they need to fill in 'Contact Us' form for further action by CSM admin. 2. CSM admin will receive the submitted form and review the subscription application. 3. CSM admin will provide approval/rejection to the applicant. 4. CSM admin will allocate unique user id to the approved application. Refer *Appendix 2 – Part A on requirement for user id*. 5. CSM admin will send new user ID & password via email to approved user. ***Existing User*** 1. If user is an existing subscriber to ISDPAS, have an active subscription status and no intention to add new assessment module, user can proceed login to the respective module using existing user id.

Main Modules	Description
	2. If user is an existing subscriber to ISDPAS, but have an inactive subscription status, user need to fill in 'Contact Us' form for further action by CSM admin. 3. CSM admin will receive the submitted form from existing subscriber and review the subscription application. 4. CSM admin will provide approval/rejection to the applicant. 5. CSM admin will allocate new unique user id to the approved application. New user id will be emailed to respective user. Refer *Appendix 2 – Part A on requirement for user id*. 6. All communication via email must leverage on official CSM email infrastructure. 7. This module enables CSM Admin to perform the following user maintenance tasks: i) Add new user ii) Remove inactive / invalid user iii) Update/ edit user profile (via the info from 'Contact Us') form
Module 2: Suite Content Management	1. Allow CSM administrator to perform maintenance on overall ISDPAS's feels and looks. 2. Allow bulk upload of questionnaires content in specific format i.e., MS Excel into assessment modules. 3. Provide suitable 'Online Help' based on each modules' requirements i.e., on mouse over

Main Modules	Description
Module 3: Analytical & Correlation	1. Center of ISDPAS where correlation and analysis will be performed to provide significant and meaningful findings based on assessment results; 2. Provide graphical user interfaces (GUI) to allow correlation & analysis been conducted; 3. Identify suitable platform or method for Machine Learning application to be executed in ISDPAS to perform analytical and correlation activities as follows: **a) Correlation and analysis for multiple assessment application** Results from multiple assessment application, for example, DPMA and results from other assessment applications will be correlated and analyzed to provide greater insight of organization's practices on inter-related domains and understanding on certain underlying issues. **b) Correlation and analysis on individual assessment application** Results from one (1) assessment application, for example, various domains in DPMA will be correlated and analyzed to provide better insight of organization's practices. 4. CSM admin will benefit from this module in order to get the landscape of organizational practices, governance and compliance in information security and data privacy.

Main Modules	Description
	5. This module should allow customized correlation and analysis by CSM admin by selecting certain parameters and variables i.e., sector name, domains etc.
Module 4: Report Generation & Visualization	1. Visualization in several graphical formats on (i) assessment results; and (ii) correlation and analysis findings. 2. Visualization is in several graphical formats and can downloaded into a few files format (i.e., CSV, PDF).
Module 5: DPMA	1. Consists of assessment questionnaires on data privacy domains. 2. Access by client admin and respondents via the given user id. 3. Client admin and respondents with the access to this module will answer the respective questionnaires within specific timeframe. Refer *Appendix 2 – Part A on requirement for subscription period*. 4. Client admin and respondents will be alerted if the assessment is incomplete upon reaching specific timeframe. 5. Assessment application will have several questionnaires according to application's questionnaires structures. 6. Upon completion of the assessment, respondent will be able to view the result or score. 7. Correlation and analysis will be performed on assessment results (using engine in Module 3).

Main Modules	Description
	8. Client admin and respondent can view the (3) types of results which are linked to Module 4: **a) Assessment Results and Score** Overall score and level of compliance or readiness based on the defined matrix of the assessment. **b) Correlation and analysis findings on multiple assessment application** (*if subscribe more than one (1) assessment application)* o Findings from multiple assessment application, for example, DPMA and results from other assessment applications will be correlated and analyzed to provide greater insight of organization's practices on inter-related domains and understanding on certain underlying issues. **c) Correlation and analysis findings on DPMA domains** o Findings from correlation and analysis on domains in DPMA will provide better insight of organization's practices.
Module *n*: (Future Assessment Application)	1. Available slot for future assessment application where features and capabilities are similar as Module 5. 2. Able to perform correlation and analysis on assessment results (using engine on its own or in Module 3); or

Main Modules	Description
	3. Allow integration and interfaces with third-party / external assessment application via API.

B. Information Security & Data Privacy Requirements

Requirement	Description
A) Information Security Requirements	**1) Secure Software Development Life- Cycle (SSDLC)** The preparation of technical documents MUST consider SSDLC at every development phases. **2) Authentication** All users MUST be authenticated before access is granted to the ISDPAS. **3) ID & Password Management** i) Enforce role-based access control ii) CSM admin is responsible to generate unique user id to client admin based on organization's name and chosen module. iii) Respondent to login to respective module and answer the assessment by using this user id. iv) Using one login id, respondent is able to access the subscribed module(s). **4) Input validation** i) Every data input MUST have input validation to prevent improperly formed data from entering ISDPAS. ii) Error messages must be descriptive to allow user to rectify data input error. **5) Audit trail/log**

Requirement	Description
	i) Audit trails should be generated by ISDPAS and include the local date and time of the actions that alter the record. ii) Data must be stored in a secure manner and must not be editable by any user. **6) Subscription Period** i) Respondent to complete assessment on respective module within a predefined subscription period. ii) The given user id will be invalid after the subscription period. Hence, new subscription application to be submitted to CSM admin. **7) Backup and Redundancy (to avoid Single Point of Failure (SPoF))** Design of ISDPAS must consider backup and redundancy components on i.e., secondary database to avoid SPoF. **8) Application Programming Interfaces (APIs)** APIs developed for ISDPAS must apply relevant security schemes to prevent malicious attacks or misuse of APIs. **9) Adopts OWASP Top 10 Web Application Security Risks** Application is developed according to secure development practices to mitigate web application security risks. Refer OWASP Top Ten for most critical security risks to web applications.
B) Data Privacy	**1. Privacy by Design (PbD)** Data protection to be taken into account throughout the system development process. Thus, the

Requirement	Description
	preparation of technical documents MUST consider relevant PbD's concepts at every development phases. The following data design strategies may need to suitably apply at the relevant stage: i) **Minimize** Limit as much as possible the processing of PII without compromising the function of ISDPAS. ii) **Abstract** Limit as much as possible the detail in which personal data is processed, while still being useful. iii) **Hide** Prevent PII from becoming public or known. **2. Privacy Notice / Privacy Policy** Privacy Notice & Consent to be included during data collection stage **3. Data masking techniques** ○ Apply on the collected PII data i.e. pseudonymization to preserve the privacy of data used for correlation (refer description for Module 3). ○ In Database level, necessary data masking technique should be applied to protect sensitive data. **4. Encryption** ○ During data collection in Module 1, during transit between modules and in processing stage. ○ The encryption algorithm MUST apply the listed algorithms by MySEAL (https://myseal.cybersecurity.my) only.

APPENDIX 3 : MODULE 5: ASSESSMENT APPLICATION - DPMA

Under ISDPAS, there will be several assessment applications to be developed and added as separate module whenever they are ready for deployment. Features and functionality of Module 5 will be replicated to other assessment modules.

The first assessment application to be developed is DPMA as depicted in Figure 2.

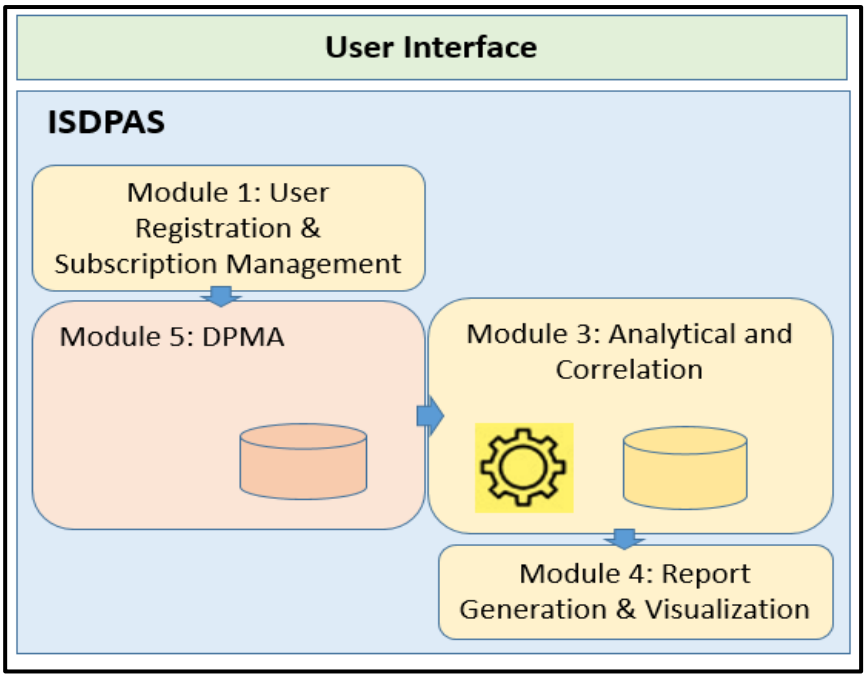


Figure 2 : Overall flow on DPMA

A. Functional Requirement for DPMA

DPMA consists of requirements as follows:

Requirement	Description
User Registration & Subscription Management **(Link to Module 1)**	Details are in Appendix 1.
Questionnaires	1. Consists of several assessment questionnaires. 2. Client admin and respondents can access this section via the given user id. 3. Respondents will answer the respective questionnaires within specific time. Refer *Appendix 2*

Requirement	Description
	– Part A on requirement-on-requirement subscription period. ***Delegation to sub-respondent(s)*** 1. Respondent can delegate the questionnaires to sub-respondent(s); 2. Sub-respondent(s) can answer the questionnaires without need to login to the suite or DPMA; and 3. Upon completion of the assessment, respondent will be able to view the result or score.
Analytical & Correlation **(Link to Module 3)**	Allow correlation and analysis on individual assessment application various domains in DPMA will be correlated and analyzed to provide better insight of organization's practices.
Report Generation & Visualization **(Link to Module 4)**	1. Visualization in several graphical formats on (i) assessment results; and (ii) correlation and analysis findings. 2. Respondent can view and download the result report into different file format (i.e., CSV, PDF) 3. Provide flexibilities for respondent to select variables for report printing (i.e., able to select certain data field, sorting in alphabetical, by certain field)
Content Maintenance	1. Allow CSM administrator to perform maintenance of the DPMA content (add, delete, update, review of domains and questionnaires). 2. Allow bulk upload of questionnaires content in specific format i.e., MS Excel. 3. Allow CSM administrator to perform maintenance on assessment content as follows: a) update new report template. b) revise of score/calculation matrix.

--- [THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK] ---