IMDA Data Protection Certifications

INFORMATION KIT FOR APPLICATION TO BE ASSESSMENT BODIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The Infocomm Media Development Authority (IMDA) administers and issues three data protection (DP) certifications[1]:

- Data Protection Trustmark (DPTM)
- APEC Cross Border Privacy Rules (CBPR) System
- APEC Privacy Recognition for Processors (PRP) System

in which organisations are certified in accordance with the certification requirements.

1.2 The IMDA invites companies interested in being appointed as assessment bodies ("ABs") to submit proposals for its consideration. In brief, the role of an AB is to assess whether applicant organisations (AOs) satisfy the requirements for the relevant certifications that they have applied for.

1.3 The IMDA is the Certification Body for the three certifications and appoints, oversees and trains ABs on the certification requirements of the relevant certification schemes. IMDA will also review the assessment reports of ABs to ensure the quality of the assessment and to issue the relevant certifications to successful AOs.

2. ROLES AND RESPONSIBILITIES OF AN ASSESSMENT BODY

2.1 The roles of an AB primarily include:

i. assessing AOs for their compliance with the relevant certification requirements in accordance with the certification methodology approved by the IMDA;

ii. where gaps are found during the course of the assessment, advising on the best practices that AOs may adopt to rectify the non-compliance identified; and

iii. preparing and submitting assessment reports in the specified form, containing the AB's assessment findings and all relevant supporting information and documents, to the IMDA.

[1] Please refer to www.imda.gov.sg/dpcertifications for more information on the three data protection certifications

3. SCOPE OF WORK FOR ASSESSMENT BODIES

3.1 The AB shall provide assessment services for AOs for the DP certifications.

3.2 The AB shall be responsible for hiring (at least two) qualified assessors to provide the required assessment services. Such assessors must possess the qualifications and meet the requirements specified by the IMDA before being deployed to conduct assessments or prepare assessment reports. All the recruitment costs (e.g. advertisement costs), shall be borne by the AB.

3.3 The AB's services shall include, but are not limited to, the following:

(i) providing prompt confirmation to the IMDA that there are no conflicts of interest between the AO and itself;

(ii) briefing AOs on the assessment process for the relevant certification;

(iii) determining the scope of assessment[2];

(iv) conducting a desktop review[3] of the documents/evidence provided by the AO, followed by an onsite assessment[4];

(v) communicating to the AO the areas that do not meet the certification requirements, advising them on the best practices that may be taken to rectify the non-compliance identified, and verifying that the required changes have been properly implemented within the stipulated timeframe;

(vi) preparing an assessment report (template provided by the IMDA) within a stipulated timeframe with the AB's findings and recommendations to the IMDA;

(vii) implementing a dispute resolution procedure between the AB and AO; and

(viii) assisting the IMDA in investigating complaints against certified organisations assessed by them.

---

[2] Depending on the scope of an AO's business activities, not all the certification requirements will apply. The AB will therefore have to determine the scope of such requirements that will be applicable to the AO.

[3] An AO must self-assess their organisation's privacy policies and practices against the prescribed self-assessment form (SAF). The assessor is responsible for reviewing the completed form against the relevant certification requirements. The assessor is required to enter into a dialogue with the AO in relation to any follow-up questions arising from:

(i) the review of the AO's responses to the SAF;
(ii) requests for clarification; and
(iii) any supplementary documentation required from the AO.

[4] This is for the purposes of evaluating the implementation, including effectiveness, of the AO's privacy policies and practices against the respective certifications' requirements.

3.4 The ABs should support the IMDA in its publicity activities relating to the DP certifications. This includes, but is not limited to, being present at roadshows or events organised by the relevant organisations promoting these certifications, conducting general preparatory and training courses to educate the public and organisations on these certifications, and answering any queries regarding the assessment process.

3.5 The AB/Assessors must attend on-boarding training sessions and relevant training courses, as required by the IMDA. These are sessions conducted for the purposes of educating the appointed ABs on the certification requirements for the respective certifications.

4. REQUIREMENTS FOR ASSESSMENT BODIES AND ASSESSORS

4.1 Mandatory requirements

(i) Companies that are currently debarred from participating in government tenders are not eligible to be appointed as ABs. If a proposal is submitted without explicitly mentioning that the interested company is currently so debarred, the IMDA shall treat the submission of the proposal as an express continuing declaration by the company that the company is eligible. If it is discovered to be false, the IMDA shall be entitled to rescind any contracts entered into pursuant to such a proposal, without the IMDA being liable for damages or compensation of whatever nature or howsoever arising, and to claim any damages suffered as a result from the company.

(ii) Companies shall be located and incorporated in Singapore and accredited by the Singapore Accreditation Council (SAC) for compliance with ISO/IEC 17021-1 (Conformity assessment – requirements for bodies providing audit and certification of management systems).

(iii) Companies shall have at least two (2) assessors who meet the mandatory criteria specified in 4.4.

4.2 Companies shall have a proven track record in performing management systems audit and certification services. Companies shall demonstrate the internal processes that they have established and actively implemented in connection with the performance of such audit and certification services. Such processes include, but are not limited to, certification, on-going monitoring and compliance review, re-certification, dispute resolution, enforcement and complaint handling processes.

4.3 ABs shall demonstrate impartiality and independence. This includes not placing themselves in situations where allegations of actual or perceived conflicts of interest may arise. Companies shall therefore demonstrate that they have established and actively implement internal processes to eliminate conflicts of interest.

4.4 ABs shall appoint qualified assessors to conduct the assessment for the certifications. ABs shall have processes to ensure that their personnel have appropriate knowledge and skills relevant for performing all the activities related to the assessment. The assessors shall meet the mandatory criteria[5] as follows:

Criteria	Auditor	Lead Auditor
(1) Qualifications and Experience	At least a degree/diploma with at least FOUR (4) years full time working experience which includes minimum of THREE (3) years full time professional work experience in Data Privacy, Information Systems auditing, control or security work experience	
(2) Audit Experience	Performed a minimum of five (5) Information Security Management System **or** Data Privacy audits within a two (2)-year period with a minimum of ten (10) auditor days on site **OR** Successfully completed at least five days of training, the scope of which covers Data Privacy or Information Security Management System audits and audit management, **AND** Gained experience in the entire process of assessing Data Privacy or Information Security prior to assuming responsibility for performing as an auditor. This experience should have been gained by participating in a minimum of three (3) Data Privacy or Information Security certification audits (including both stage 1 and stage 2), for a total of at least 10 audit days.	Performed a minimum of five (5) Information Security Management System **or** Data Privacy audits within a two (2)-year period with a minimum of ten (10) auditor days on site **AND** Performed an additional minimum of three (3) audits as a Lead Auditor within a two (2)-year period
(3) Maintenance of qualification (once every	Performed at least five (5) Data Privacy audits by the end of	Performed at least five (5) Data Privacy audits by the end of

[5] Subject to changes by the IMDA depending on the relevant certification requirements.

Criteria	Auditor	Lead Auditor
three (3) years)	every three (3)-year cycle	every three (3)-year cycle **AND** At least two (2) of these audits performed shall be in the capacity as the Lead Auditor
(4) Auditor Training	Successfully completed and passed: (i) any of the following: (a) Certified Information Privacy Professional/Asia (CIPP/A[6]); (b) Certified Information Privacy Manager (CIPM[6]); (c) Recognised Auditor / Lead Auditor course for information security management systems (ii) a "Fundamentals of the Personal Data Protection Act" course[7] (iii) a "Practitioner Certificate in Personal Data Protection (Singapore)" course[8]	

4.5 Companies shall show that at least two (2) assessors currently meet the foregoing mandatory criteria.

5. APPOINTMENT PERIOD

5.1 The appointment of ABs will be for a period of THIRTY-SIX (36) months.

[6] CIPP/A and CIPM are certification programmes offered by International Association of Privacy Professionals (IAPP).
[7] This course is developed under the SkillsFuture Singapore (SSG) Business Management Workforce Skills Qualifications (BM WSQ) framework.
[8] This is an intermediate course that complements the "Fundamentals of the Personal Data Protection Act" course under the SSG BM WSQ framework.

6. HOW TO BE APPOINTED AS ASSESSMENT BODY

a) Expression of Interest

Interested companies to submit an email application to IMDA (data_protection_certifications@imda.gov.sg) and provide details on meeting the mandatory requirements stated in Clause 4.1.

b) Submission of proposal

Eligible companies that meet the mandatory requirements will be notified by IMDA and invited to submit a proposal as outlined in Section 7 – Submission Requirements. Kindly note that only complete proposals written in the prescribed format and bearing all required information will be processed.

c) Appointment as AB

Successful companies that met all the necessary criteria will be appointed as an AB and be required to sign a formal written agreement.

7. SUBMISSION REQUIREMENTS (ONLY FOR ELIGIBLE COMPANIES THAT ARE INVITED BY THE IMDA TO SUBMIT A PROPOSAL)

7.1 Eligible companies that are invited by IMDA to submit a proposal shall use the below proposal format (prepared in the English language), include the relevant supporting documents and submit to data_protection_certifications@imda.gov.sg:

(i) Management Summary

This shall contain an overview of the proposal, the services and support proposed to be offered, relevant supporting documentation, prices and any major assumptions made by the company. Tables, charts, schematic diagrams and other graphic representations should be used to summarise the information whenever possible.

(ii) Company Information

This shall contain the background information of the company, including at least a brief history, scope of operations and expertise (including, if relevant, information about its affiliates and its regional and/or international offices and affiliates), track record of work undertaken in Singapore (and, if relevant, regionally and/or internationally), staff size and distribution, and financial standing.

Please provide the latest ACRA Business Company Profile of not more than 6 months from date of submission and the following:

1. Contact Information

Contact Name	
Designation	
Contact Number	
Contact Facsimile Number	
Contact Email Address	

2. Principal Activities and Interests of the company

No.	Principal Activities and Interests

3. Affiliates, Subsidiaries and Joint Ventures

No.	Name of Affiliates, Subsidiaries and Joint Ventures	Registration Number	Country of Incorporation

4. Financial Capacity

Capitalisation of firm and present issued and paid-up capital	
Annual turnover for last three years	2021:
	2020:
	2019:
Financial Statements	Please attach the following documents: (a) Audited financial statements for the preceding three (3) financial years; (b) If available, provide the latest credit rating report from established credit rating agencies such as Standard & Poor's, Dun & Bradstreet or Moody's etc.

(iii) Personnel Information

Please describe the company structure of the team that will be managing the DP certifications, clearly indicating the process, responsibilities of each member and time commitment each individual will be giving to the project.

Please provide the detailed Curriculum Vitae (CV) of the assessors (at least 2) who will be assessing the DP certifications and team members who will be managing the DP certifications, clearly setting out their relevant experience in handling projects of a similar nature and scope.

The assessors shall possess qualifications in data privacy and/or relevant work experience in the field of data protection (refer to clause 4.4). Details of such qualifications and experience should be provided in the table below. Each assessor is to fill up one table.

Questions	Response
Does the assessor have a degree/diploma?	i. Yes or No ii. Provide supporting documentation
Number of years of working experience in Data Privacy, Information Systems auditing, control or security work experience	iii. No. of years of working experience iv. Provide supporting documentation
Has the assessor completed and passed any of the following: (a) Certified Information Privacy Professional/Asia (CIPP/A); (b) Certified Information Privacy Manager (CIPM); (c) Recognised Auditor / Lead Auditor course for information security management systems	Provide supporting documentation
Has the assessor completed and passed any of the following: (a) "Fundamentals of the Personal Data Protection Act" course (b) "Practitioner Certificate in Personal Data Protection (Singapore)" course	Provide supporting documentation

(iv) Statement of Compliance to Requirement Specifications

The company shall include in its proposal a paragraph-by-paragraph statement of compliance according to the paragraph references of this document and state whether the specified requirements can be complied with in the format below.

Clause	**Compliance***	**Explanatory Notes / Remarks** (Please provide alternatives/reasons ONLY if "U/C")
4.1 (i)		
4.1 (ii)		
4.1 (iii)		
4.2		
4.3		
4.4		
4.5		

*Only the following symbols shall be used to indicate due compliance or otherwise:

C - Able to fully comply

U/C - Unable to fully comply

(v) Additional Information

(a) User References: The company must submit at least two (2) user references whom IMDA can contact, preferably related to relevant certifications similar to DP certifications.

(b) Proposed Assessment Methodology: The company should elaborate on its processes for conducting the desktop review and onsite assessment.

(c) Promotion of the DP Certifications: The company shall elaborate on how it can further support the promotion and increase the take-up rate of the respective DP certifications to organisations in Singapore. Companies are encouraged to propose activities to promote and increase awareness of the DP certifications.

(d) Dispute Resolution Process: The Company shall elaborate on its mechanism to receive and investigate complaints relating to the assessment services provided.

The company may include any additional information that is relevant to its proposal. **Kindly ensure all required information is furnished, as only complete submissions will be processed.**

8. CONTACT

8.1 If you need more information, you can send an email to data_protection_certifications@imda.gov.sg.