Public Consultations

Closing Note to the Consultation on the Licensing Framework for Cybersecurity Service Providers

25 February 2026

CSA concludes public consultation on cybersecurity licensing framework updates. Key changes include mandatory certification requirements, extended 5-year licence validity, and streamlined notification processes. Implementation timeline provides adequate transition period for service providers to comply with new standards.

Introduction

1. The Cyber Security Agency of Singapore ("CSA") held a public consultation on the proposed changes to the Licensing Framework for Cybersecurity Service Providers from 22 September 2025 to 21 October 2025.

2. The licensing framework for cybersecurity service providers was first established in 2022 under Section 5 of the Cybersecurity Act 2018. The framework adopts a light-touch regulatory approach, targeting service providers that perform cybersecurity functions with significant access and potential impact on client systems. The proposed changes seek to a) raise baseline cybersecurity standards nationally and b) enhance clarity on the licensing requirements.

3. CSA received responses from 17 respondents, comprising cybersecurity service providers, industry associations, cloud service providers, and technology companies. The list of respondents is published in **Annex A**. CSA has considered the respondents' feedback, and this closing note seeks to address the key points of feedback received.

Overview of Feedback Received

4. Respondents generally expressed support for the intent to raise cyber hygiene assurance levels through mandatory certifications and appreciated the efforts to reduce regulatory friction through extended licence validity and simplified notification obligations.

Key Points of Feedback Received

Cyber Trust mark (CTM) and Data Protection Trustmark (DPTM) Certification Requirements

5. Feedback on the proposed certification requirements focused primarily on four areas:

a) Recognition of equivalent certifications;

b) Applicability of DPTM to cybersecurity service providers,

c) Certification requirements for resellers; and

d) Impact on smaller providers.

Recognition of Equivalent Certifications

6. Respondents appreciated the recognition of ISO/IEC 27001 as an equivalent to CTM. However, there were calls for CSA to recognise additional global standards as equivalents, including:

a) For cybersecurity: Service Organization Control 2 Type II (SOC 2 Type II).

b) For personal data protection: ISO/IEC 27701 Privacy Information Management System (PIMS) standard and General Data Protection Regulation (GDPR) compliance certifications.

7. Respondents suggested that CSA publish a list of equivalent certifications for both CTM and DPTM to avoid ambiguity during application and renewal.

8. CSA acknowledges the importance of providing clarity on equivalent certifications to reduce uncertainty for licensees. CSA assessed that ISO/IEC 27001 remains the only recognised equivalent for CTM for now, as it is an international information security standard. The other types of cybersecurity certification, such as SOC 2 Type II, rely on audit assessment which can vary in scope and rigour, thus making it challenging to ensure consistent regulatory compliance with the standards across all licensees. Nevertheless, CSA will progressively review additional certifications and add them to the list, if appropriate. We will adopt a balanced approach by referencing international standards to reduce regulatory duplication while maintaining robust cyber hygiene standards that are relevant to Singapore's cybersecurity landscape.

9. Licensees are advised to refer to www.csro.gov.sg ↗ where more details would be shared on the process for assessment of equivalent certifications in due course.

Applicability of DPTM to Certain Service Categories

10. Several respondents raised concerns over the relevance of DPTM for penetration testing services, citing limited interaction with personal data in the delivery of such services. Cloud service providers also highlighted that DPTM requirements do not align with their Shared Responsibility Model, where cloud service providers are to ensure the security of the cloud infrastructure while users are responsible for protecting the data stored in the cloud environment.

11. CSA wishes to clarify that the DPTM certification requirement is intended for licensed cybersecurity service providers, which are Managed Security Operations Centre (MSOC) monitoring service and penetration testing (PT) service providers only. The requirement is not intended for cloud service providers.

12. In recognition that CTM Promoter (Tier 3) certification already includes data protection measures and access to client's personal data may be limited for MSOC and PT service providers, CSA will not require licensees to achieve DPTM as a mandatory requirement. Licensees have the flexibility of achieving DPTM certification if it is needed for their business.

13. Notwithstanding, CSA assesses that MSOC and PT licensees providing these services may have access to privileged data in the course of their services and should therefore demonstrate their commitment to good data protection practices and compliance with the Personal Data Protection Act and/or other applicable data protection laws. This requirement is contained within paragraph 3.1 of the Conditions of Licence in **Annex B**.

Requirements for Resellers

14. Some respondents sought clarification on whether resellers would be required to obtain certifications for services performed entirely by third-party providers.

15. CSA wishes to clarify that the licensing framework applies to all entities providing the licensable services, regardless of their business model. Resellers who are licensed to provide licensable cybersecurity services are subject to the same certification requirements as other licensees. This is to ensure that cyber hygiene standards are consistent across the cybersecurity delivery chain to mitigate risks and provide assurance and accountability to customers.

Impact on Small Providers and Individual Licensees

16. Some respondents provided feedback on the administrative burden on small businesses and individual licensees in obtaining the required certifications. Respondents suggested introducing alternative compliance routes such as an "Independent Assurance Pack" for boutique firms and individual licensees, allowing them to demonstrate compliance through existing assurance mechanisms.

17. CSA notes the feedback and will study the possibility of introducing alternative compliance routes for smaller providers and individual licensees. However, CSA maintains that all licensees should achieve a minimum level of cyber hygiene posture regardless of firm size, and the CTM Promoter (Tier 3) certification was assessed to be proportionate to licensees' risk profile. CSA will also work with Certification Bodies to ensure that individual licensees can achieve the CTM Promoter (Tier 3) certification. CSA wishes to clarify that, for parity, the CTM certification scope is the same for business and individual licensees:

a) Certification must cover the environment (people, processes, and technology) supporting the delivery of licensed services.

b) Certification bodies must be accredited by SAC or equivalent national accreditation bodies.

Changes to Licence Validity, and Notification Timeframes

18. Feedback on the proposed administrative changes was positive. Respondents widely supported the proposed CSA extension of licence validity to 5 years as it reduces administrative burden on licensees. Respondents also welcomed the removal of requirements to report non-material changes and the extension of reporting window for key information changes from 14 to 30 calendar days.

19. Accordingly, CSA will proceed with the proposed extension of licence validity to 5 years, and the proposed simplification of notification obligations.

20. Suggestions were also made to automate updates using ACRA data and SingPass-based declarations to further streamline processes. CSA notes the suggestions on automation and will explore opportunities to streamline processes through integration with other government digital services where feasible.

Implementation Timeline

21. The proposed implementation timelines in phases for certifications (i.e. CTM by end 2026, DPTM by end 2027) were generally seen as reasonable for large providers. However, some respondents noted that boutique firms and individual licensees may face challenges to be certified within the proposed timeframe. There were suggestions for the implementation timeline to be further extended to account for certification bottlenecks and operational adjustments. CSA also noted that some respondents raised concerns about the need for DPTM.

22. CSA maintains that the proposed grace period is sufficient for licensees to obtain certifications. Licensees will have a grace period until 31 December 2026 to obtain CTM Promoter (Tier 3) certification. Thereafter, licensees would be required to have an active CTM certification during licence application and/or renewal. To reiterate, CSA will not mandate DPTM certification at this point and the proposed timeline to obtain DPTM certification by end 2027 will not be implemented.

Conclusion

23. CSA would like to thank all respondents for their feedback.

CSA will proceed to implement the proposed changes to the licensing framework, taking into account the feedback received. **Annex B** provides the updated licence conditions which will apply to all existing licensees, new licence applications and/or licence renewals following this review. For existing licensees, the licence conditions will be in effect 30 days from the publication of this Closing Note. Existing licensees will transition to the 5-year licence term upon renewal. The updated licence conditions will be published on the CSRO website.

24. CSA remains committed to engaging with industry stakeholders on technical and operational matters and welcomes continued collaboration to ensure the relevance of the licensing framework for cybersecurity service providers and contribute to the security of Singapore's cyberspace. For further enquiries, CSRO can be reached via contact@csro.gov.sg ↗.

Annex A – Respondents to the Consultation on the Licensing Framework for Cybersecurity Service Providers

1. Amazon Web Services (AWS)
2. Asia Pacific Carriers' Coalition (APCC)
3. Assurity Trusted Solutions Pte Ltd
4. Availabilit Pte Ltd
5. Business Software Alliance (BSA)
6. Centurion Information Security Pte Ltd
7. Cure53
8. Future Gen International Pte Ltd
9. Google
10. Hitachi Sunway Information Systems (S) Pte Ltd
11. Logicalis APAC
12. NTT Singapore
13. PSiDEO (Singapore) Pte Ltd
14. Rajah & Tann Cybersecurity Pte Ltd
15. SECASSURE LLP
16. Singtel
17. Tan Kiang Khiang

Annex B – Updated Conditions of Licence

CONDITIONS OF LICENCE

The following conditions are imposed under Section 27 of the Cybersecurity Act 2018 (the "**Act**") as conditions for the grant of a licence to provide licensable cybersecurity services. The conditions apply in addition to any requirements under the Act and the Cybersecurity (Cybersecurity Service Providers) Regulations 2022.

1. Definitions and interpretation

1.1. In these conditions, unless the context otherwise requires:

“Cybersecurity Services Regulation Office” (hereinafter referred to as “CSRO”) means the office through which the Licensing Officer administers Part 5 of the Act;

“Officer” refers to “officer of a business entity” as defined in Section 26(10) of the Act, namely, any director or partner of the business entity or other person who is responsible for the management of the business entity;

“Licence” means the licence granted or renewed by the Licensing Officer to the Licensee to provide the relevant Service as stated therein;

“Licensee” means the holder of a Licence;

“Licensing Officer” means the Commissioner of Cybersecurity appointed under section 4(1)(a) of the Act; and

“Service” means the licensable cybersecurity service that the Licensee is licensed to provide under the Licence, and refers EITHER to penetration testing service OR managed security operations centre (SOC) monitoring service, as respectively defined in paragraph 2 of the Second Schedule of the Act.

1.2. Apart from the definitions in paragraph 1.1 above, any other word or expression used in these conditions shall have the same meaning as in the Act unless the context otherwise requires.

1.3. This Licence is subject to the provisions of the Act and of any law amending, modifying or replacing the same. Any reference to the Act shall include any subsidiary legislation, rules, regulations and directions or orders made pursuant thereto.

1.4. For the avoidance of doubt, the Licensee shall comply with all obligations under the Act and this Licence at its own costs, unless otherwise specified in writing by the Licensing Officer.

2. Licence Period

2.1. The Licence is valid for the period stated therein, unless revoked or suspended by the Licensing Officer in accordance with Section 30 of the Act.

2.2. Any application to renew the Licence shall be made in accordance with the requirements and timelines prescribed in the Act.

2.3. Where an application to renew the Licence is made after the time prescribed by the Act, the application will be treated as a fresh application for grant of a licence.

3. Professional Conduct of Licensee

3.1. In relation to the Service it provides, the Licensee shall:

(a) Not make any false representation in the course of advertising or providing the Service;

(b) Comply with all applicable laws in the course of providing the Service, including, but not limited to, the Computer Misuse Act 1993 (Cap. 50A) and all obligations relating to confidentiality and data protection, including, but not limited to, the Personal Data Protection Act;

(c) Exercise due care and skill, and act with honesty and integrity in the course of providing the Service;

(d) Not act in a manner where there is a conflict between its interests and that of the person procuring or receiving the Service (the “Customer”); and

(e) Collect, use, or disclose any information about (i) a computer or computer system of any Customer, or (ii) the business, commercial or official affairs of any Customer, only for the purposes of providing the Service to the relevant Customer. The Licensee shall not collect, use or disclose any such information for other purposes, unless appropriate written consent has been obtained from the relevant customer, or such collection, use, or disclosure is lawfully required by any court, or lawfully required or allowed under law.

3.2. The Licensee shall also take all reasonable steps in the circumstances to ensure that its Officers, employees and/ or contractors also comply with the matters listed in paragraphs 3.1(a) to (e) above, with all references to the Licensee to be read as references to such persons.

4. Changes to Information

4.1. The Licensee shall notify the Licensing Officer, in the manner described in CSRO's website at www.csro.gov.sg ↗, of any change or inaccuracy in the information and particulars that the Licensee and/or its Officers submitted to the Licensing Officer in relation to this Licence, within thirty (30) calendar days of such change or knowing of such inaccuracy (exclusive of the day such change or knowledge occurs). Such information and particulars include, but are not limited to:

(a) The appointment of any Officer;

(b) When an Officer ceases to hold such office;

(c) Changes to or inaccuracies in the Licensee's and/or its Officers' names;

(d) Criminal convictions or civil judgments entered against the Licensee and/or its Officers for offences or proceedings involving fraud, dishonesty, breach of fiduciary duty, or moral turpitude, or any offences under the Act; or

(e) Where the Licensee and/or its Officers have been declared bankrupt or have gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction.

5. Other Licences

5.1. Nothing in this Licence affects the requirement to obtain any other licence that may be required under the Act or any other written law.

6. Duty to Maintain Active Certification

6.1. The Licensee shall maintain an active Cyber Trust mark Promoter (Tier 3) certification or equivalent, as listed on the CSRO website (https://www.csro.gov.sg ↗) for the delivery of the Service(s) for the duration of the Licence.

↑ Back to top