MSP[3] Framework

General principle

The Managed Service Provider Partner Program (MSP[3]) aims to strengthen the cyber security of Managed Service Providers (MSPs) through partnership with the Australian Cyber Security Centre (ACSC).

Rationale

1. MSPs are targeted by malicious actors due to their unique access to multiple systems and sensitive information.
2. The ACSC established the MSP[3] to uplift MSPs' cyber security practices to help mitigate this threat.
3. MSP[3] provides an additional level of confidence to the ACSC and the Australian economy when procuring services from MSP[3] partners.
4. MSP[3] does not remove the requirement for government, business or academic organisations to undertake their own security risk assessments when procuring MSP services. All stakeholders are responsible for managing the security risks of their procured services when partnering with MSPs.

Expected outcomes

5. MSPs manage and mitigate cyber security risks for their systems and the systems of their customers aligned to ACSC advice.
6. Provide an effective and efficient mechanism for uplifting MSP's cyber security practices.
7. Enable increased access to information and security tools to strengthen MSPs cyber security practices.
8. Deliver a level of confidence when partnering with MSPs, underpinned by risk based oversight and self-assessment activities.

The Program

9. MSPs are attractive targets for malicious cyber actors, given their privileged access to the systems and networks of their customers. The impacts of this were recently realised in the large scale compromise of MSPs, known as Cloud Hopper.
10. The program objective is to uplift the cyber security posture across the MSP community to reduce the risk of and impact of future compromises.
11. To assist MSPs to lift their cyber security posture the ACSC has published the MSP Better Practice Principles. The better practice principles consist of 8 principles for MSPs to commit as part of joining the MSP3 program.
12. The ACSC acknowledges that the cyber security posture varies greatly across the MSP community and these principles will not apply uniformly across the MSP community.
13. Each principle is supported by actions that the ACSC recommends is implemented to improve the cyber security of an MSP. These recommended actions are based on ACSC's experience from responding to cyber security incidents and assessing IT systems.
14. MSPs should take a risk based approach when implementing the ACSC recommended actions in the Better Practice Principles. These actions are not intended to be a compliance standard that is mandatory for MSPs to implement. MSPs should assess their own cyber security posture against the better practice principles and

identify gaps. MSPs should then implement the most appropriate mitigations that meet the intent of the better practice principles.

15. It is not expected for MSPs to successfully implement all of the ACSC's advice immediately, each MSP should take a planned and considered approach to their cyber security and target their highest risk areas first.
16. MSPs and selected customers will undergo self-surveys at different milestones to measure improvements to the MSPs' cyber security posture and identify divergent results between MSPs and their customers.
17. MSP[3] membership provides MSPs with a range of benefits to help support, promote and manage MSP's cyber security posture in line with ACSC's security requirements. These include:
    a. MSP Partner Forum where the ACSC provides threat updates and discusses solutions where MSPs are not meeting Better Practice Principles.
    b. 24/7 Situational Awareness products.
    c. Provision of ACSC advice on cyber security best practice.
    d. List MSP[3] members on the cyber.gov.au website to promote MSPs' commitment to improving their cyber security posture.
    e. MSPs can advertise their partnership status via their website and associated media outlets.
18. MSP[3] membership supports government-industry partnerships and supply chain security.

Program Eligibility

19. To be eligible for MSP[3] membership an MSP must be:
    a. a managed service provider[1];
    b. registered as a legal business entity in Australia; and
    c. financially solvent.
20. The ACSC, through the First Assistant Director-General Protect, Assure and Enable, may deny, suspend or terminate MSP[3] membership if eligibility and criteria is not met or if it is determined that granting or continuing membership is not in ACSC's or the national interest.

Application

21. As part of the MSP[3] application process, MSPs will be required to:
    a. Submit the MSP[3] application form which will include:
        i. A signed Joint Cyber Security Centre Confidentiality Deed Poll.
        ii. A customer list sample, comprising of between two and six current customers across the public and private sector.
            - At least two Private Sector customer is required if applicable.
            - Participating customers will also be encouraged to sign the Confidentiality Deed Poll
    b. Once the ACSC reviews and approves the application, the MSP will be invited to co-sign the Managed Service Provider Commitment to Better Practice.

[1] **Managed Service Provider**

The ACSC defines an MSP as a third party engaged by organisations to manage their IT services and infrastructure, but does not include Cloud Services Providers. An MSP by this definition may, however, also offer Cloud Services to its clients.

Partner Status Review

22. The Partner Status Review will safeguard the Program's integrity, ensuring that committed MSPs remain as part of the program and are able to differentiate themselves from others in the market.
23. The ACSC will conduct analytics on the self-survey results and map the MSPs' results at different milestones to measure improvements to the MSPs' cyber security posture and identify divergent results between MSPs and their customers.
24. Where the ACSC identifies divergent results or becomes aware of significant deficiencies within the MSP's cyber security posture, the ACSC reserves the right to have the MSP undergo an independent assessment against their self-survey.

MSP Reports

25. The ACSC will, at its discretion, publish anonymised whole of market reports on the cyber security posture of the MSP industry at the end of each of the Partner Status Reviews.

Independent Assessment

26. If the ACSC finds that the MSP's self-survey results are significantly contrary to the independent assessment, or if MSPs refuse to undertake the independent assessment, the ACSC reserves the right to terminate the MSP's Partnership status.
27. The standard of the independent assessor will be determined by the ACSC in consultation with the respective MSP.
28. The MSP will meet the cost of the independent assessment.

Maintaining program membership

29. MSP[3] members, by the determination of the ACSC, must:
    a. take appropriate actions to work towards meeting the relevant Principles through a risk-based approach[2];
    b. report any changes to program eligibility changes;;
    c. meet ongoing reporting requirements within the designated timeframe for membership; and
    d. maintain the requirements of the Joint Cyber Security Centre Confidentiality Deed Poll.

Roles and Responsibilities

Australian Cyber Security Centre

30. The ACSC commits to:
    a. acting in good faith;
    b. assisting all eligible MSP's to join the MSP3 program through timely provision of information and support for joining the program;
    c. processing all membership applications in a timely manner;
    d. providing ongoing cyber security risk management advice; and

[2] The ACSC wants to see improvement in how MSPs manage their cyber security risks.

e. upholding all responsibilities as outlined in this document.

MSPs

31. MSPs are responsible for:
    a. Implementing the Principles through a risk based approach that demonstrates commitment to improving their cyber security posture;
    b. acting in good faith;
    c. ensuring information provided is not deceptive or misleading; and
    d. providing all relevant information required to assess their eligibility and suitability for MSP3 membership.

Ceasing Membership

32. MSP[3] membership will continue until such time as it is voluntarily ceased by the MSP or terminated by the ACSC.

Voluntary withdrawal or ceasing

33. MSPs can cease their membership at any time by notifying the ACSC in writing.
34. Upon receiving notification of request to cease membership:
    a. the ACSC will remove the member from the ACSC website list and remove the MSP from all other distribution and access products obtained due to MSP[3] membership; and
    b. MSPs are required to remove from their public facing website and documentation all reference to MSP[3] membership.

Terminating membership

35. Should an MSP be found to be non-compliant with MSP3 membership requirements the ACSC may terminate an MSP's membership.
36. With the exception of termination, the ACSC will not apply any other penalties associated with the failure to comply with MSPs' membership requirements under the MSP[3].
37. Prior to terminating a party's membership, the ACSC will provide that member with a 'show cause notice' indicating the ACSC's intention to suspend or terminate the membership and the reasons for that intention. The affected member will have 7 days to respond to the notice, after which the ACSC will make a final decision.
38. The decision to suspend or terminate an MSP's membership will be made, at minimum, by First Assistant Director General Protect, Assure and Enable and cannot be delegated down.
39. Upon terminating membership, the ACSC will remove the member from the ACSC website list and remove the MSP from all other distribution and access products obtained due to MSP[3] membership.

Feedback and Complaints

40. All feedback and/or complaints should be directed to the ACSC by email at asd.assist@defence.gov.au or by telephone on 1300 CYBER1 (1300 292 371).