DISP Readiness Working Checklist

A practical preparation aid for Australian defence suppliers. Use it alongside current Defence guidance and your contract requirements. It is not an official Defence checklist, a complete control assessment, certification or a guarantee of DISP membership.

Download and save a local copy, then use a PDF reader that supports forms. Keep entries brief and save again after editing. Status means Not checked, Gap open, In progress, Evidence ready or Not applicable. Evidence ready is an internal working status, not Defence approval. Record a reason for Not applicable. Use controlled record references rather than attaching evidence. Do not enter passwords, classified information or sensitive personnel details. Store and share the completed file through your approved process.

Entity or business name

Review date

Checklist coordinator

Controlled scope record reference

Requested levels

Security governance

Personnel security

Physical security

ICT and cyber security

Use with the official sources

[1] Defence eligibility, membership levels and CSO/SO roles

[2] Defence application process and conditional pathway

[3] Defence cyber assurance and Cyber Security Questionnaire

[4] Defence ongoing membership responsibilities

[5] Defence membership requirements checklist (PDF)

Sources checked on 22 September 2026. Older Defence downloads contain legacy wording. Use current Defence web guidance for the cyber and screening baseline, and confirm any conflict with Defence. This worksheet does not replace official application documents.

Set the scope and responsibilities

01 Confirm eligibility and contract needs

Check entity details, ABN/ACN, eligibility and foreign ownership, control or influence. Confirm whether membership is required for the work with the relevant contract manager. [1][2]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

02 Record the requested levels and boundary

Record the requested level in each security domain and the business justification. Identify the people, sites, systems and suppliers covered. Keep the scope record under change control. [1]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

03 Assign the CSO and SO

Confirm appointments, required training, clearances and portal access. The SO starts and edits submissions; the CSO reviews, declares and submits. One person may hold both roles. [1][2]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

Prepare governance, people and premises

04 Review security policies and reporting

Assign owners to applicable policies, incident reporting, security training and registers. Record approval and review dates. Establish how the governing body reviews security reporting. [1][4][5]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

05 Check personnel security arrangements

Review screening, induction, clearance responsibilities and any required position registers for the requested level. Current Defence eligibility guidance references AS 4811:2022. [1][4]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

06 Check sites and information handling

Review physical access, storage, handling and destruction arrangements for the information and assets involved. Identify any site assessment or certification needed for the requested level. [1][5]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

Prepare ICT evidence and uplift actions

07 Map the ICT boundary and all eight controls

Inventory corporate ICT systems used to correspond with Defence. Assess all eight mitigation strategies against the current Maturity Level Two baseline. Identify evidence and gaps for each control. [1][3]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

08 Prepare the cyber questionnaire evidence

Assign a knowledgeable, authorised ICT representative. Map answers to dated reports, configuration records, access reviews and restore tests. Check evidence covers the declared systems. [3]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

09 Assign uplift work and unresolved decisions

Record gaps, accountable owners, delivery dates and exception reviews. Confirm any conditional pathway or Maturity Action Plan arrangements with Defence; do not assume a waiver or approval. [2][3]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

Reconcile the application and plan upkeep

10 Check supplier and subcontractor responsibilities

Record provider scope, access and evidence responsibilities. Confirm applicable DISP obligations for subcontractors. Keep applicant accountability separate from contracted ICT implementation work. [1]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

11 Reconcile evidence before CSO review

Compare policies, questionnaire answers and technical evidence. Resolve inconsistent scope or claims. Check the current portal documents and deadlines, then arrange the CSO review and declaration. [1][2][3]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date

12 Schedule ongoing reviews and reporting

Assign owners for the Annual Security Report, incident reporting and changes affecting membership. Schedule evidence refreshes and reviews when systems, people, locations or providers change. [4]

Responsible owner

Working status
Not checked

Current evidence reference and date

Known gap or reason not applicable

Next action and delivery owner

Due date