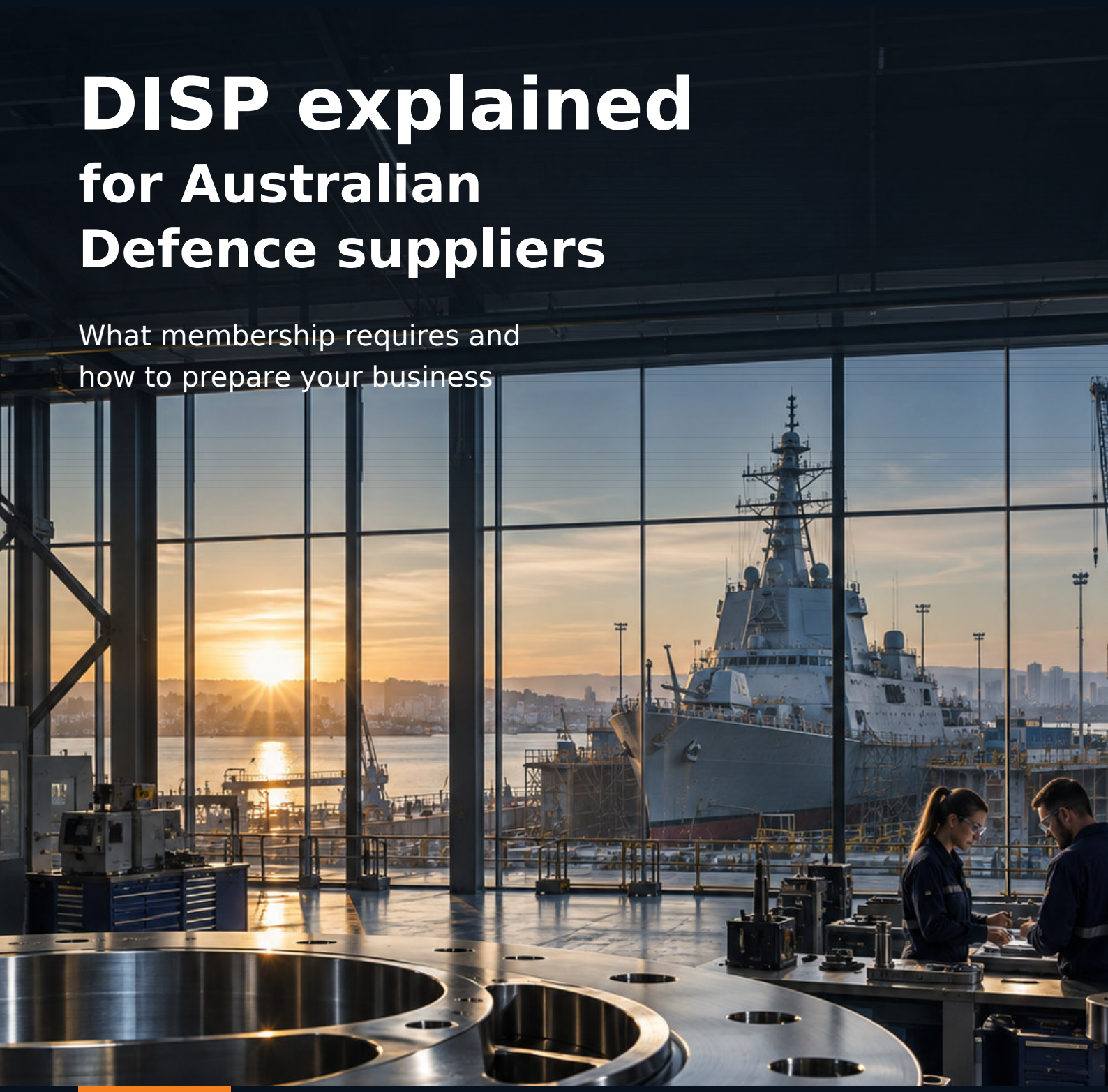
GadSetAccess
Information Security Agency

BUSINESS GUIDE

10 SEPTEMBER 2026

DISP explained for Australian Defence suppliers

What membership requires and how to prepare your business



BUILD DEFENCE READINESS INTO THE BUSINESS PLAN

Australia’s Defence supply chain depends on businesses that can protect the information, people and systems entrusted to them. For a supplier, the Defence Industry Security Program is an important part of demonstrating that capability. Understanding its requirements early can prevent a promising commercial opportunity from becoming an urgent and expensive security remediation project.

Conceptual imagery of Australian Defence industry

01 READ THE GUIDE

Your route to Defence readiness

An engineering company can make an exceptional component and still be unprepared to receive the drawings needed to manufacture it. A technology consultancy can employ experienced specialists yet lack the arrangements to sponsor and manage their clearances. A software supplier can hold ISO 27001 certification while gaps remain in its Defence security obligations.

These are business planning problems as much as security problems. The most useful starting point is to establish what work the organisation intends to perform, what information it will handle, and where that work will happen. Those decisions shape the membership profile, systems, people and evidence required.

This guide explains what DISP is, when it matters, how to prepare an application and how to maintain the resulting security capability. The central recommendation is straightforward: build DISP readiness into the business plan before committing to a contract delivery date.

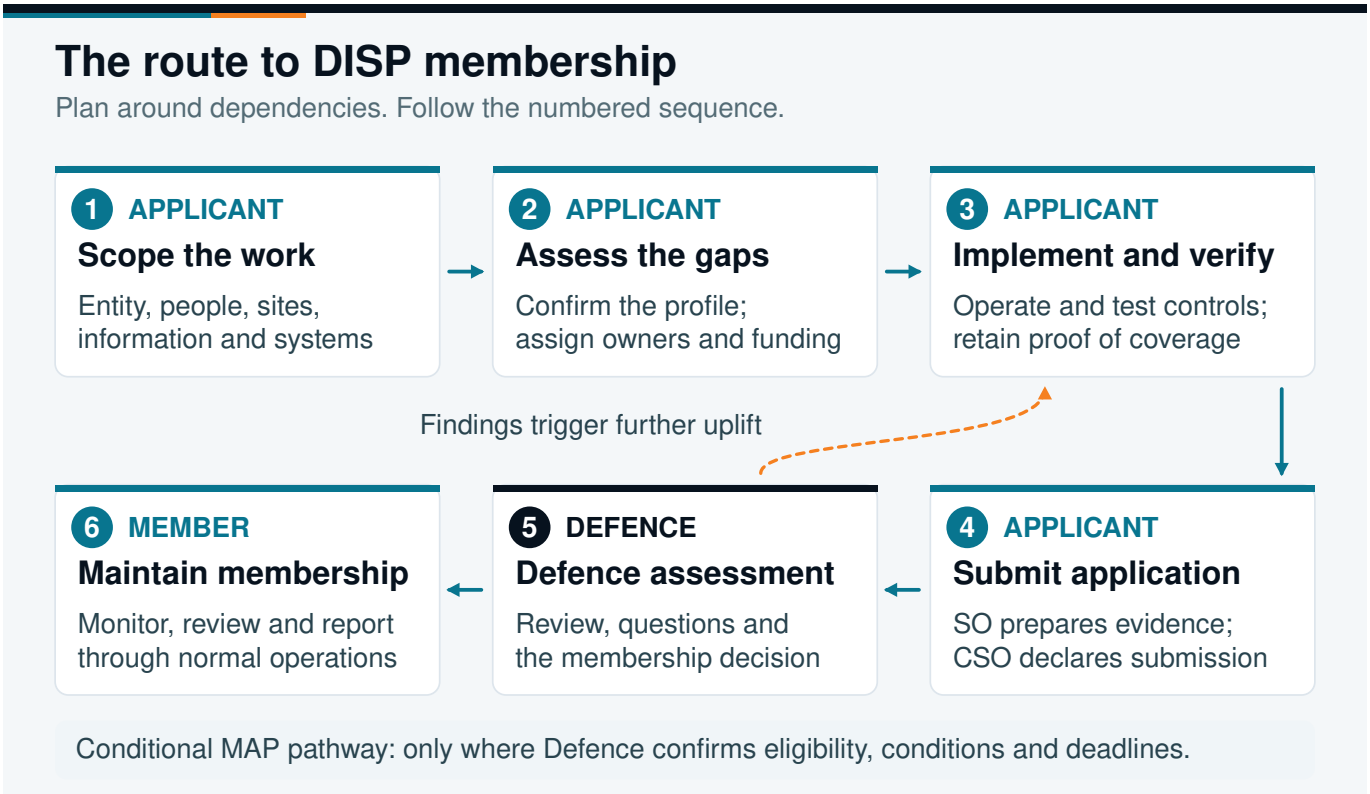


Figure 1. Activities may overlap. SO: Security Officer. CSO: Chief Security Officer. MAP: Maturity Action Plan. Processing time and any conditional membership arrangements remain subject to Defence. [1]

02 PURPOSE AND COMMERCIAL VALUE

Why DISP matters for your business

Secure suppliers protect the capability that Defence depends on. Conceptual illustration.

What DISP actually is

The Defence Industry Security Program, usually shortened to DISP, is the Department of Defence's membership program for industry security. It helps Australian entities understand and meet security obligations when participating in Defence tenders, contracts and projects. Members gain access to security advice, resources and support, while Defence gains assurance about the organisations in its supply chain. Membership does not guarantee a contract. [2]

DISP is governed by the Defence Security Principles Framework, particularly Principle 16 and Control 16.1. Its four domains are security governance, personnel security, physical security, and information and cyber security. The program examines the organisation's ability to protect Defence work across these domains. [3]

The phrase "DISP accreditation" appears frequently in the market. For most businesses, the outcome being sought is DISP membership. Accreditation of a particular facility or information system is a more specific matter. Keeping that distinction clear helps avoid promises that a membership certificate cannot fulfil.

Why it matters commercially

Defence buyers and prime contractors need confidence that suppliers can protect sensitive work throughout delivery. An exposed engineering file, an unmanaged administrator account or a departed employee with continuing access can create consequences well beyond the supplier's own network. Security weaknesses can affect intellectual property, production schedules and confidence in a wider project.

For a smaller Australian business, preparation creates a practical advantage. It becomes easier to explain the organisation's security arrangements, answer due diligence questions and identify the work it can responsibly accept. A credible security position also helps a prime contractor understand where a subcontractor fits within its delivery model.

The commercial value extends beyond a bid response. Asset inventories improve support decisions. Clear access rules reduce dependence on individual employees. Tested recovery arrangements protect delivery when an incident occurs. An organised evidence base reduces the time spent reconstructing answers for different customers.

We recommend treating DISP as an investment in reliable delivery. The useful question for management is whether security arrangements will still work during a staff departure, a supplier change or an incident immediately before a contractual milestone.

03 CONTRACT AND INFORMATION REQUIREMENTS

When membership is required

Defence identifies mandatory membership triggers that include access to information or assets classified PROTECTED or above; supplying, maintaining, storing or transporting weapons or explosive ordnance; providing security services for Defence bases or facilities; and contracts that explicitly require membership. [4] The governing DSPF also includes Australian Community Members under the Australia-US Defence Trade Cooperation Treaty. [3]

There are defined exceptions. The DSPF describes personnel handling classified information within Defence facilities and using Defence assets and ICT networks, and recognised accreditation under specified international security agreements. Confirm any proposed exception with the Defence contract manager. Working on a Defence site does not, by itself, settle every membership obligation. [3]

Subcontractors must meet applicable membership requirements themselves; the prime contractor's membership does not automatically cover them. [4]

Confirm the requirement in writing

Ask for the required domain levels, information classifications and contract security conditions in writing. Confirm when membership must be held, whether it is a tender condition or a delivery prerequisite, and what restrictions apply before approval. A purchase order with a general security clause deserves the same scrutiny as the main contract.

Businesses can seek membership before winning a Defence contract. [2] For an organisation entering the market, that creates an opportunity to build capability deliberately. It also allows management to discover costly dependencies before a customer expects work to begin.

Membership levels and classifications

DISP has four membership levels aligned to the sensitivity of the information or assets involved. Levels can differ between domains, but security governance must match the highest of the other three. [4]

Membership level	Information classification alignment
Entry Level	OFFICIAL and OFFICIAL: Sensitive
Level 1	PROTECTED
Level 2	SECRET
Level 3	TOP SECRET

Source: Defence membership guidance. These levels are separate from Essential Eight maturity levels. [5]

04 SCOPE THE MEMBERSHIP

Match membership to the work

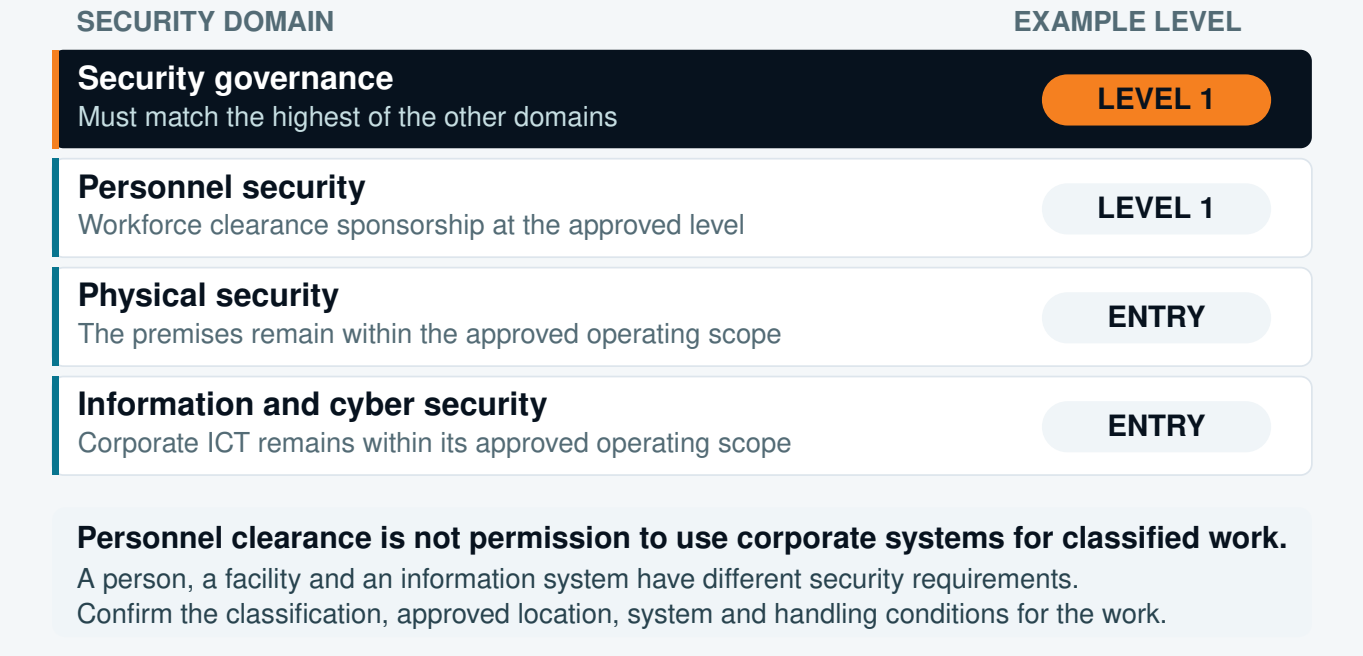


Figure 2. Membership is a profile across four domains. This example illustrates the scoping principle, subject to justified business need and Defence approval. [4]

Defence advises organisations without a Defence contract to apply for Entry Level across all domains. Higher levels require a justified business need. [3,4] Request the profile supported by the proposed work, rather than treating a higher level as a general commercial credential.

Choose the profile needed for the intended operating model. For example, a consultancy whose personnel work on customer systems may have different requirements from a manufacturer storing classified drawings and producing sensitive components at its own premises. A business description such as “Defence technology company” is too broad to make that decision.

The initial information and cyber security application is generally limited to Entry Level, with specified exceptions for existing Defence certification and accreditation or an explicit current contract requirement. Higher ICT levels require the relevant assessment and authorisation pathway. [3]

This is why scoping matters before purchasing technology or redesigning a facility. Do not assume that choosing Level 1 on a form permits PROTECTED information to be stored in an ordinary corporate environment. Confirm the approved systems, locations and operating conditions for the actual work.

05 RESPONSIBILITIES AND EVIDENCE

The four domains in everyday business terms

The following examples translate the four domains into practical management questions. They are a preparation aid, rather than a replacement for Defence's requirements.

Domain	Management question	Examples of useful evidence
Security governance	Who owns security decisions and checks that they are implemented?	Approved plans, risk decisions, assigned responsibilities, training records and incident exercises
Personnel security	Who can access the work, and how is their suitability maintained?	Screening records, clearance management where relevant, access approvals and departure checks
Physical security	How are workplaces, equipment and information protected?	Site risk assessments, visitor records, access reviews and applicable facility approvals
Information and cyber security	Which systems handle the work and how are their controls verified?	System inventories, configurations, technical assessments, recovery tests and remediation records

Security responsibilities connect management, personnel and operations. Conceptual illustration.

In practice, the domains overlap. A contractor leaving the business may require personnel records to be updated, digital access removed, a pass returned and the customer notified. A good security process connects those actions and records their completion. Four separate policy documents will not achieve that on their own.

06 CYBER REQUIREMENTS

Essential Eight at Maturity Level 2

Technical controls need operational ownership and current evidence. Conceptual illustration.

Defence's current cyber guidance states that assessments against only the "Top 4" concluded on 15 November 2025. DISP members are now required to achieve and maintain the full Essential Eight at Maturity Level 2. The relevant corporate ICT systems are those used to correspond with Defence. Advice based solely on the older Top 4 approach is insufficient for current planning. [6]

The eight strategies cover application control, application patching, Microsoft Office macro settings, user application hardening, restricting administrative privileges, operating system patching, multi-factor authentication and regular backups. ASD recommends reaching the same target maturity across all eight. The model is designed for internet-connected IT; operational technology may need different or additional mitigations. [7]

For implementation, start with visibility. Identify devices, applications, identities, administrative pathways, cloud services and the information moving between them. Then test what actually happens. Can an ordinary user run an unapproved application? Can an old administrator account still sign in? Can the team restore a critical service from protected backups? A policy statement alone will not answer these questions.

Avoid purchasing a product on the assumption that it delivers an entire maturity level. Technology needs configuration, coverage, operational ownership and verification. A control that works on most laptops but misses a critical engineering workstation can leave a material gap in the environment being assessed.

Defence's Cyber Security Questionnaire supports its assessment of the organisation. Current guidance identifies 107 controls in Part B and recommends completion by someone with sufficient knowledge of the ICT infrastructure. Incomplete or weakly supported answers can delay an application. [6]

Prepare a control evidence register that records the requirement, responsible person, systems covered, supporting evidence and unresolved issues. Give evidence a date and scope. A screenshot showing that a setting exists is less useful than evidence showing which systems receive it and whether exceptions have been investigated.

07 CONNECT GOVERNANCE AND TECHNICAL ASSURANCE

Where ISO 27001 and IRAP fit

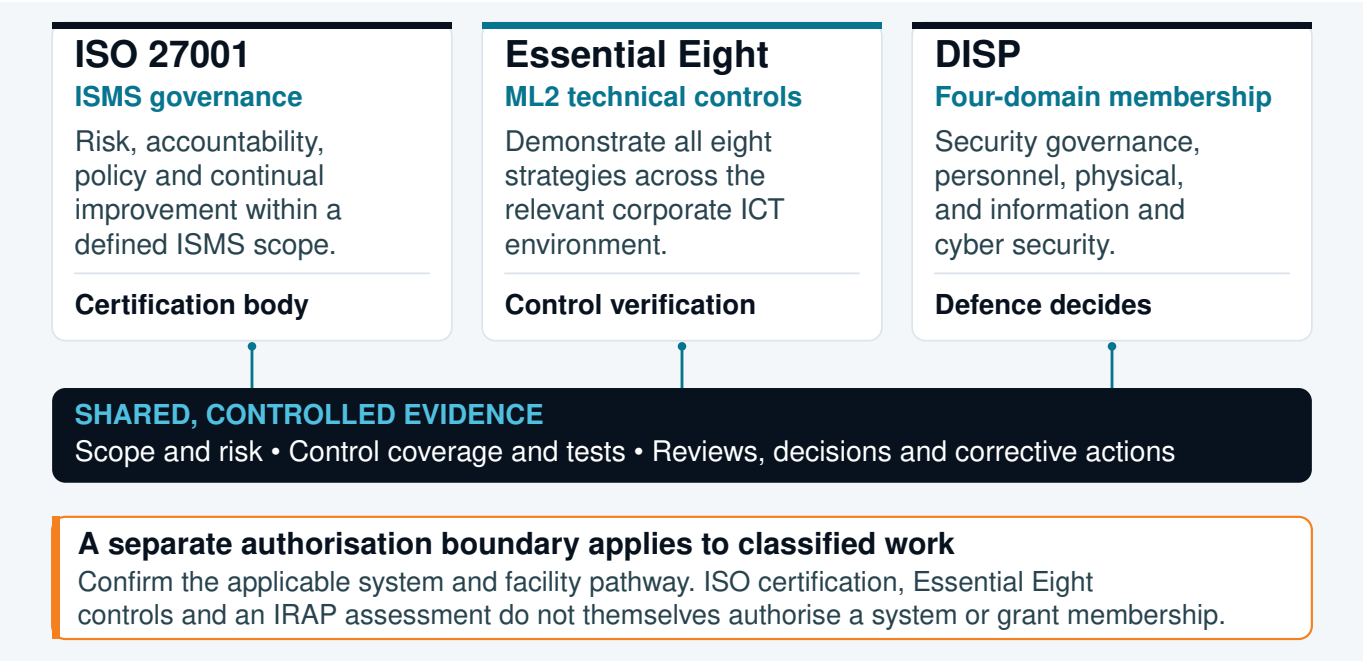


Figure 3. Coordinate the evidence while preserving each requirement and approval boundary. ISO 27001 and Essential Eight implementation do not automatically confer DISP membership or authorise classified handling. [3,4,8,9]

ISO/IEC 27001:2022 provides requirements for an information security management system, or ISMS. It gives an organisation a structured way to manage information security risk and improve its arrangements over time. Certification involves an independent certification body assessing the management system within a defined scope. [8]

That structure can support a DISP program. We recommend using one coordinated set of risk records, responsibilities, policies, corrective actions and management reviews wherever requirements overlap. The organisation should still be able to trace each DISP obligation to the evidence that satisfies it. Shared documentation is useful only when its scope and content match the work.

Defence accepts ISO 27001 documentation as partial supporting evidence, while still requiring demonstration of all Essential Eight strategies. [4] An ISO certificate covering one service or business unit should not be assumed to cover every system used for Defence work.

IRAP is different again. An assessment by an ASD-endorsed IRAP assessor examines security controls and identifies findings for a particular scope. The assessor does not accredit or certify systems on behalf of ASD, and an assessment does not itself authorise a system's use. [9]

These distinctions matter when evaluating a cloud provider or managed service. Ask for the relevant scope, findings, customer responsibilities and authorisation requirements. A marketing claim about "government-grade" infrastructure tells a prospective supplier very little about whether its own proposed use is acceptable.

08 PREPARE FOR MEMBERSHIP

Scope the work and appoint owners

Define the operating boundary

Begin with the target contracts and the work to be performed. Map the legal entity, sites, people, subcontractors, information flows and supporting systems. Include remote work, shared corporate services and third parties that can administer the environment. Record the intended information classification and who has confirmed it.

This produces the scope against which readiness can be assessed. It also exposes dependencies early. An outsourced IT provider might control an essential setting. A landlord might control physical access. A customer might require a system approval that has a longer lead time than the rest of the project.

Confirm eligibility

An applicant must be an Australian legal business entity with an ABN or ACN, be financially solvent and have suitable people to fulfil the Chief Security Officer and Security Officer roles. [4] Foreign Ownership, Control or Influence must be assessed and declared. Foreign interests require transparent disclosure and assessment; an Australian registration alone does not resolve that assessment. [10]

Give security officials authority and time

The Chief Security Officer provides senior accountability, while the Security Officer manages the security arrangements in practice. The same person can hold both roles. Defence's role guidance requires Australian citizenship and appropriate clearances for the nominated security officials; clearance requirements depend on the role and membership profile. [11]

Company membership and individual clearances are different. In the personnel domain, Entry Level does not permit workforce clearance sponsorship; Levels 1, 2 and 3 allow sponsorship up to Baseline, NV1 and NV2 respectively, subject to genuine need and sponsorship obligations. [12] The Security Officer's own requirements can be higher: a Level 1 Security Officer must hold NV1. [3]

Arrange the mandatory DISP Security Officer course for both nominated officials early. The course requires at least Baseline clearance for access, and refresher training is required every three years. Confirm the applicable completion arrangements with DISP. [13]

Select people with authority, availability and enough organisational knowledge to do the work. Give the Security Officer time to maintain records, coordinate incidents, oversee training and follow through on remediation. Appoint a deputy or define continuity arrangements so that leave and staff turnover do not interrupt essential reporting.

09 CLOSE GAPS AND PREPARE THE PORTAL

Build the evidence before you apply

Assess the gaps and fund the work

Compare the current position with the relevant DSPF requirements, contract conditions and Essential Eight controls. Separate missing documentation from missing implementation. Both matter, but they require different resources and cannot be repaired through the same work package.

For each gap, assign an owner, a completion date and the evidence that will demonstrate closure. Identify dependencies and budget for recurring operations as well as initial changes. The board or executive should know which gaps prevent the business from accepting particular work.

Prioritise high-impact practical weaknesses: uncontrolled administrative access, unsupported systems, untested recovery, incomplete workforce screening or unmanaged access to premises. Build policies around the resulting operating arrangements. Documents should describe what the organisation can demonstrate, rather than an ideal state it has not implemented.

Establish credible evidence

Run the processes long enough to produce credible records. Complete access reviews, test recovery, exercise the incident plan and verify departure procedures. Sample evidence across different sites, devices and worker types. The purpose is to find inconsistent implementation before an assessor or a real incident exposes it. Workforce screening should be aligned with AS 4811:2022. [4]

Keep an evidence index with access controls appropriate to its contents. Security records can reveal sensitive architecture, vulnerabilities and personal information. Share them through the authorised application and assessment channels, and check what information is actually being requested.

Prepare the portal and application

The current application route is the DISP Member Portal, using Digital ID and Relationship Authorisation Manager. The submission includes entity and officer details, the requested profile, Foreign Ownership, Control or Influence information, the cyber questionnaire and supporting documents. [1] The Security Officer prepares the submission and the Chief Security Officer reviews and declares it. [11]

Establish a monitored DISP@company-domain mailbox that meets Defence’s naming and hosting rules. The guide excludes shared, web-based and cPanel hosting and requires Australian data storage unless the DISP Cyber Team expressly authorises encrypted offshore hosting. [14]

Make administrative preparation part of the project plan. Confirm that the principal authority and delegated users can access the service, that the required mailbox is monitored, and that company details are consistent across the application and supporting records. Small administrative mismatches can consume time even when the underlying security work is sound.

Once an application is commenced in the portal, it must be submitted within 60 business days or it will be removed and a new application will be required. [1]

10 DEFENCE ASSESSMENT AND EXPENDITURE

Plan assessment and delivery

Respond to assessment findings

Defence's assessment includes review of the organisation's security documentation, engagement with security staff and assessment of its cyber position. Identified gaps require attention. [6] Be ready to explain how controls operate, who checks them and what happens when something fails.

Treat requests for clarification as evidence work. Provide a clear answer linked to the relevant system, process or record. Avoid submitting a large undifferentiated folder and expecting the assessor to infer compliance.

Defence currently offers a conditional membership pathway that can permit membership before an Essential Eight ML2 Maturity Action Plan is fully completed. [1] This is a Defence-managed arrangement with conditions, not a general exemption from the required standard. Obtain explicit confirmation of eligibility, deadlines and permitted activities. Submitting an application does not itself confer membership or permission to handle information outside the approved scope.

Budget for the complete capability

There is no DISP membership fee, but the applicant pays for meeting and maintaining the required security standards. [2] The meaningful budget therefore includes staff time, technical changes, training, assurance, relevant personnel vetting and any required facility or system work.

There is also no universal end-to-end completion date. Defence's application guidance acknowledges processing constraints, and readiness differs substantially between businesses. [1] Avoid building a bid schedule around a consultant's best-case estimate without examining the assumptions behind it.

Use three separate planning tracks: internal readiness, external dependencies and Defence assessment. Internal readiness includes uplift and evidence. External dependencies may include clearance processing, building changes and third-party technical work. Defence assessment includes review, questions and any required follow-up. Progress in one track does not automatically complete the others.

Before approving expenditure, ask what the business needs at each contractual milestone. A well-scoped Entry Level program may be proportionate for one opportunity; another may require a materially different operating environment. The most expensive mistake is to discover that distinction after committing to delivery.

Make membership part of normal operations

After approval, transfer responsibilities into business operations. Assign the reporting calendar, review access and security risks, monitor technical controls and track changes to the organisation. Keep the membership scope visible to commercial teams so that new contracts do not silently exceed the organisation's approved capability.

11 CONTINUOUS SECURITY ASSURANCE

Maintain DISP membership

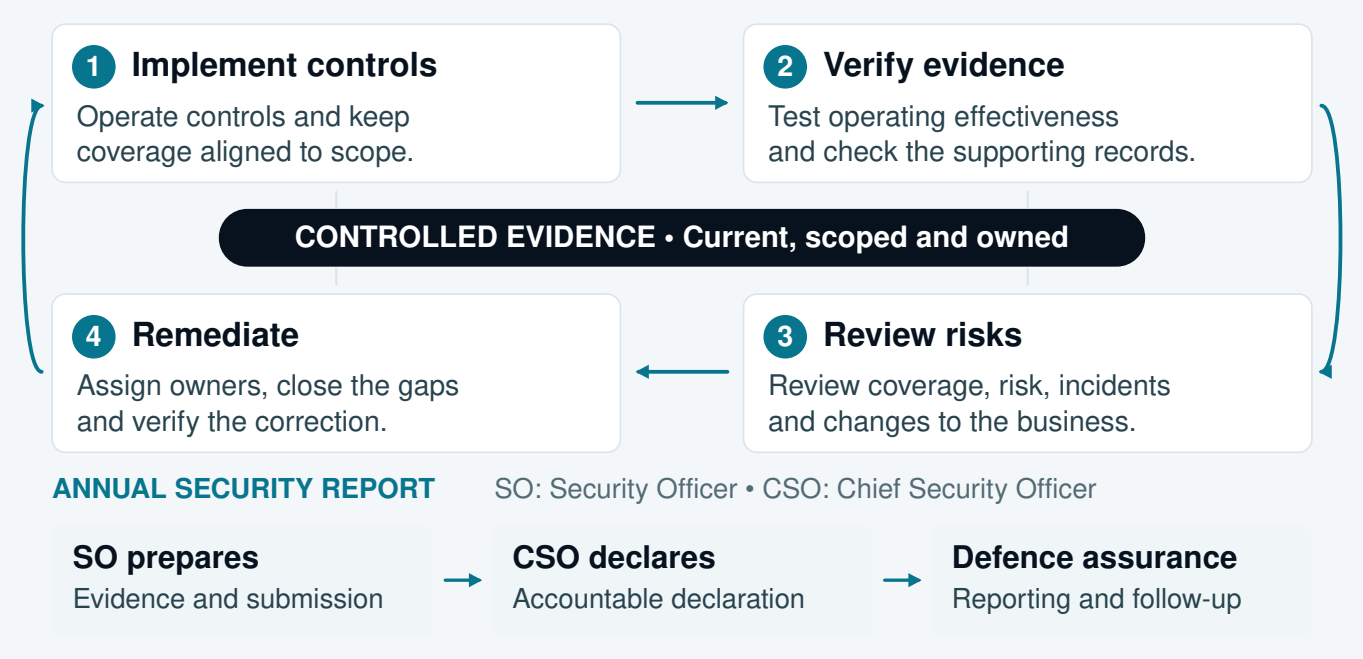


Figure 4. An operating rhythm for continuous assurance. Current control evidence supports management decisions and annual declarations. Incident and change reporting also occur when required during the year. [15,16]

DISP requires ongoing reporting and assurance. Members submit an Annual Security Report, report relevant changes in circumstances and participate in assurance activities. Plan to submit the ASR by the original membership anniversary; Defence's maintaining-membership guidance specifies submission within 10 business days of that date. The Security Officer prepares it and the Chief Security Officer makes the final declaration. Changes to the nominated CSO or SO must be notified within 14 days. [16]

Defence's August 2026 member factsheet also addresses insider threat arrangements, annual security awareness training for security-cleared and Defence-engaged personnel, subcontractor security and incident reporting. It specifies reporting security incidents through XP188 within 24 hours of their occurrence or becoming known. [15]

Operationally, we recommend reviewing evidence throughout the year. A new cloud service, overseas support arrangement, acquisition or change of premises should trigger a security assessment before implementation. Procurement and HR processes should alert the Security Officer to changes that could affect membership or contract obligations.

A useful management view shows control coverage, unresolved risks, overdue remediation, incidents and upcoming obligations. It should make weaknesses visible early enough for someone to act. Reporting every control as green until the annual declaration is due defeats the purpose of oversight.

For suppliers using AI tools, include those services in the same information handling decisions. Determine what data enters them, who can access it and what actions they may perform. An assistant helping prepare evidence should not be given unrestricted access to sensitive records merely because the output is a compliance report.

12 PRACTICAL SUPPORT FOR ISO 27001 AND DISP

Gadget Access and CiBRAI

Security operations, investigation and evidence should support the security program. Conceptual illustration.

Gadget Access and CiBRAI are aligned to helping our clients achieve ISO/IEC 27001 certification and DISP membership, with practical security uplift that remains effective after the initial assessment.

Gadget Access helps organisations translate security requirements into an executable program: establishing the scope, assessing gaps, developing the ISMS and governance arrangements, coordinating Essential Eight uplift and preparing evidence for assessment. Our focus is on making responsibilities and remediation clear enough that the business can act on them.

CiBRAI complements that work through a cybersecurity operating platform that brings together signals from endpoint, identity, cloud and network tools. Its agentic AI capabilities, guided response workflows and audit trails can support investigation, oversight and evidence development when appropriately configured for the client's environment. [17]

The organisation remains accountable for its controls and declarations. Defence determines DISP membership, and an independent certification body determines ISO 27001 certification. The value of the combined approach is a better connection between the written security program, technical operations and the evidence management needs to make informed decisions.

If your business is preparing to enter the Defence supply chain, speak with Gadget Access about the work you intend to win and the security capability required to deliver it. Establishing that picture early gives you a practical basis for investment, application readiness and ongoing compliance.

Discuss your DISP and ISO 27001 readiness

gadgetaccess.com | cibrai.com

13 EVIDENCE AND PUBLICATION NOTES

Sources and further reading

Requirements checked against current public Defence and ASD guidance on 10 September 2026. Confirm applicable requirements and contractual scope when planning an application.

Primary references

01 Department of Defence
How to apply

02 Department of Defence
Defence Industry Security Program

03 Department of Defence
DSPF Principle 16 and Control 16.1 public version

04 Department of Defence
Eligibility and suitability

05 Department of Defence
Applying for DISP membership factsheet February 2025

06 Department of Defence
Cyber and assurance

07 Australian Signals Directorate
Essential Eight maturity model

08 International Organization for Standardization
ISO IEC 27001 2022 information security management systems

09 Australian Signals Directorate
Infosec Registered Assessors Program

10 Department of Defence
Foreign ownership control and influence factsheet

11 Department of Defence
Chief Security Officer and Security Officer roles and responsibilities

12 Department of Defence
Sponsoring Defence clearances securely

13 Department of Defence
Security training

14 Department of Defence
How to create a DISP email address

15 Department of Defence
Requirements of a DISP Member August 2026

16 Department of Defence
Maintaining membership

17 CiBRAI
Platform overview

Publication notes

Earlier factsheets are cited for the specific eligibility, role and classification details discussed. Current Defence guidance governs cyber requirements and application processing. The practical management examples are preparation guidance. Conceptual images do not depict actual Gadget Access or Defence facilities.

Published by Gadget Access Pty Ltd. Gadget Access and CiBRAI are aligned to helping clients achieve ISO/IEC 27001 certification and DISP membership. Defence determines membership; an independent certification body determines ISO certification.