



CYBERPATH PROFESSIONALISATION PILOT CONSULTATION

Throughout March and April 2026, the CyberPath team held town hall sessions across all states and territories. Practitioners, employers, students, educators and community members raised important questions about how cyber professionalisation should work in Australia.

This document sets out the questions raised and how they are shaping the framework's design. CyberPath is in a design phase, and many of the questions below remain open. Community input will continue to influence the direction of the work.

Question	How we are thinking about this.
<p>Q1 What problem is cyber professionalisation solving, and why now? <i>Raised by: All states and territories</i></p>	<ul style="list-style-type: none">• There is currently no consistent way to assure real-world cyber capability across the sector.• Employers, boards, and government cannot reliably distinguish competence from confidence using existing signals.• Degrees, certifications and titles are imperfect proxies for demonstrated capability.• Cyber risk has escalated into a systemic, public-interest issue that affects the whole community.• CyberPath is intended to improve trust, consistency and capability assurance.• These questions are guiding the design process; the framework itself has not yet been finalised.
<p>Q2 How will CyberPath avoid becoming a gatekeeper or barrier to entry? <i>Raised by: NSW, VIC, QLD, SA, TAS, WA, NT</i></p>	<ul style="list-style-type: none">• CyberPath must expand, not restrict, the cyber workforce.• Multiple entry pathways should be recognised, including non-traditional routes into the profession.• Recognition of Prior Learning (RPL) is intended to be a mainstream pathway, not an exception.• Mandatory participation or licensing was explicitly rejected in community feedback.• Framework design will actively consider how to avoid unintentional exclusion of capable practitioners.

Q3

How will CyberPath avoid credential inflation and certification overload?

Raised by: NSW, QLD, SA, TAS, WA, NT

- CyberPath will not simply introduce another certificate or badge into an already crowded landscape.
- Existing degrees and certifications are intended to be treated as inputs to recognition, not outcomes in themselves.
- Capability demonstrated through evidence of practice is preferred over accumulation of credentials.
- The design process is exploring how to make credential recognition meaningful rather than additive.

Q4

What roles should and should not be within scope for professionalisation?

Raised by: All town halls

- The team is exploring a risk-based approach, not driven by job titles or whether a role includes the word 'cyber'. This is an approach that hasn't been taken elsewhere and will require innovative thinking.
- Initial focus is on areas where failure creates material impact: national security, public safety, critical infrastructure, or significant economic harm.
- Entry-level, routine, or heavily supervised roles are not expected to require professional status.
- Scope must accommodate hybrid, emerging, and multi-role practitioners.
- A narrow and defensible starting scope is preferred, with evidence-based expansion over time.
- Boundaries between cyber, IT and software engineering are acknowledged as complex and will require careful policy judgement.

Q5

How should real-world capability be assessed beyond degrees and certifications?

Raised by: NSW, VIC, QLD, SA, TAS, WA, NT

- Performance-based assessment is preferred over exam-only approaches.
- Portfolios, simulations and supervised practice were strongly supported by community feedback.
- Assessment should reflect the exercise of judgement in real operational contexts.
- The framework is exploring how to make assessment meaningful, accessible and resistant to gaming.

Q6

How will Recognition of Prior Learning (RPL), experience and non-traditional pathways be recognised fairly?

Raised by: All states and territories

- RPL is intended to be a core design principle, not an afterthought or exception pathway.
- Experience and on-the-job learning should be recognised alongside formal education.
- Evidence of capability should be required to support any recognition claim.

	<ul style="list-style-type: none"> • The framework is working to balance consistency (so recognition is trustworthy) with flexibility (so it is genuinely accessible).
<p>Q7 How can intangible skills like judgement and ethics be assessed? <i>Raised by: QLD, SA, TAS, WA, NT</i></p>	<ul style="list-style-type: none"> • Judgement, ethics and problem-solving are considered critical professional attributes. • Observed performance and contextual assessment are preferred over abstract testing. • These skills are acknowledged as harder to assess reliably. • Despite this, the community view was clear: they are essential for high-impact roles and cannot be omitted from the framework.
<p>Q8 What governance model will prevent commercial capture? <i>Raised by: ACT, QLD, SA, WA, NT</i></p>	<ul style="list-style-type: none"> • Governance must be independent and transparent to maintain community trust. • Clear separation is required between standard-setting and training delivery. • Conflicts of interest must be declared and actively managed. • Commercially driven or revenue-focused governance models were identified as a significant credibility risk.
<p>Q9 How will CyberPath provide value to employers and boards? <i>Raised by: ACT, NSW, QLD, SA, TAS, NT</i></p>	<ul style="list-style-type: none"> • Employer uptake is considered decisive — the framework only has value if employers use it. • Value is expected to flow from improved hiring confidence, clearer procurement signals and better workforce planning. • Engagement with employers and boards is ongoing and will inform the pilot design.
<p>Q10 Should CyberPath be voluntary or mandatory? <i>Raised by: ACT, QLD, SA, WA, NT</i></p>	<ul style="list-style-type: none"> • Strong community support exists for starting with a voluntary framework. • Mandatory licensing was widely viewed as premature at this stage. • Any future mandates would need to be narrowly defined, evidence-based, and earned through demonstrated value. • The starting position is voluntary; the question of whether and when mandates might be appropriate is not yet settled.
<p>Q11 How will vendor, academic and overseas certifications be recognised? <i>Raised by: QLD, SA, WA, TAS, NT</i></p>	<ul style="list-style-type: none"> • Certifications should be mapped to defined capability outcomes, not treated as equivalent by brand or prestige. • No vendor or institutional privilege will apply.

	<ul style="list-style-type: none"> • Overseas qualifications should be recognised where supported by evidence of comparable outcomes. • Transparency in recognition decisions is a stated design requirement.
<p>Q12 How will pilot success be measured? <i>Raised by: All town halls</i></p>	<ul style="list-style-type: none"> • Success measures should include employer adoption and meaningful use of the framework. • RPL uptake and utilisation of multiple entry pathways are key indicators. • Diversity, workforce retention and practitioner mobility outcomes should be tracked. • Independent evaluation is supported by the community. • Community feedback was clear that practitioner sign-ups alone are not a measure of success. Evidence of changed hiring practices is required. • Adoption will take years, not months; unrealistic expectations about speed should be actively managed.
<p>Q13 How will CyberPath support early-career practitioners? <i>Raised by: QLD, SA, VIC, TAS , VIC</i></p>	<ul style="list-style-type: none"> • Supervised practice and mentoring are strongly supported as early-career pathways. • Work-integrated learning models were viewed as particularly valuable. • Clearer articulation of what is expected at entry level was identified as essential. • The framework will need to avoid inadvertently raising barriers for people entering the profession.
<p>Q14 How will CyberPath align with existing frameworks (SFIA, NIST, IRAP, NICE)? <i>Raised by: ACT, QLD, SA, NT</i></p>	<ul style="list-style-type: none"> • Strong community preference exists for interoperability with established frameworks, including SFIA, NIST, IRAP and NICE. • Duplication of existing frameworks should be avoided. • Alignment should simplify workforce planning for employers, not add another layer to manage. • The exact nature of alignment is still being worked through.
<p>Q15 How will regional, remote and small-team contexts be supported? <i>Raised by: TAS, WA, NT, QLD</i></p>	<ul style="list-style-type: none"> • Flexible, place-based implementation was strongly supported by communities in regional and remote areas. • Recognition of multi-role practitioners is considered essential — many practitioners in these contexts do not have specialist-only roles.

	<ul style="list-style-type: none"> • Remote and distributed assessment options will need to be available. • One-size-fits-all approaches were rejected; the framework must accommodate different operating environments.
<p>Q16 How will CyberPath remain agile as technology evolves? <i>Raised by: QLD, SA, WA, NT</i></p>	<ul style="list-style-type: none"> • Modular capability updates will be required to keep the framework relevant over time. • Continuing professional development should be integral to the framework, not an add-on. • Regular review cycles are necessary to prevent the framework from becoming obsolete. • The risk of a static framework that falls behind the pace of technology change was raised as a genuine concern.
<p>Q17 How will ethics and AI governance be embedded and enforced? <i>Raised by: ACT, QLD, SA, NT</i></p>	<ul style="list-style-type: none"> • Clear accountability and enforcement mechanisms will be needed. • The community acknowledged that further policy design work is required before the mechanisms can be specified. • AI governance is an area of particular focus given the pace of change.
<p>Q18 What are the cost and wage impacts of professionalisation? <i>Raised by: TAS, QLD, SA, NT, VIC</i></p>	<ul style="list-style-type: none"> • Potential cost burden on individuals and small-to-medium enterprises is acknowledged as a real concern. • Affordability and access concerns were raised, particularly for practitioners who may need to self-fund participation. • Employer incentives and innovative funding models are being explored as potential mitigations. • These questions have not yet been resolved and will be part of the pilot design process.
<p>Q19 How will senior practitioner knowledge be retained and recognised? <i>Raised by: QLD, SA, TAS, NT</i></p>	<ul style="list-style-type: none"> • Recognition of mentoring and supervision activities was strongly supported by senior practitioners. • Structured pathways that value knowledge transfer, not just technical currency, are encouraged. • Knowledge transfer from experienced practitioners to the next generation was identified as essential to workforce sustainability.