



Creating Australia's Cyber Security Accreditation Scheme

DRAFT Program Plan

August 2022

Goal

Increase the amount of **appropriately skilled** cyber security professionals in Australia

Purpose

Context:

- Australia's skills and qualification framework is currently characterised by **degrees of fragmentation, information asymmetries, and a misalignment**, in some areas, between career aspirations, qualifications and labour market outcomes
- Guardrails haven't yet been established regarding a standardised approach to the cyber security profession leading to a **lack of clarity for employers and purchasers of cyber security capabilities**
- There is **variety in the quality of the skills** that cyber security workers in Australia have, making it difficult for employers to know what they are hiring
- Australia **hasn't yet defined the core cyber security roles** and their associated levels, skills, and experience



Objective:

Create an industry-designed and supported independent cyber security accreditation scheme



Outputs:

An Australian cyber security accreditation scheme co-designed and supported by industry and government

Approved criteria and process to validate cyber security courses, credentials, and experience

A detailed description of how the Australian accreditation scheme aligns and interacts with other key international accreditation schemes and frameworks

Agreed core cyber security roles defined and mapped to relevant credentials and frameworks as well as clearly described career pathways

Customer journeys of the future state accreditation experience for cyber security professionals, employers and purchasers

Approved criteria and process for cyber security workers to gain professional accreditation

The vision

- Australia has a healthy and growing pipeline of appropriately skilled cyber security professionals
- Employers and purchasers have trust and confidence in the skills and experience of the cyber security professionals they are engaging to fulfil their cyber security needs
- Cyber security roles:
 - are consolidated and simplified into a core set
 - are mapped to relevant credentials and frameworks
 - have defined levels, skills and experience
 - have clearly described career pathways
- It will be straightforward for employers to match workers to their business' cyber security needs
- Global cyber security credentials and skills frameworks are consolidated and aligned to the Australian industry context
- The Australian accreditation scheme is designed and implemented following global best practice



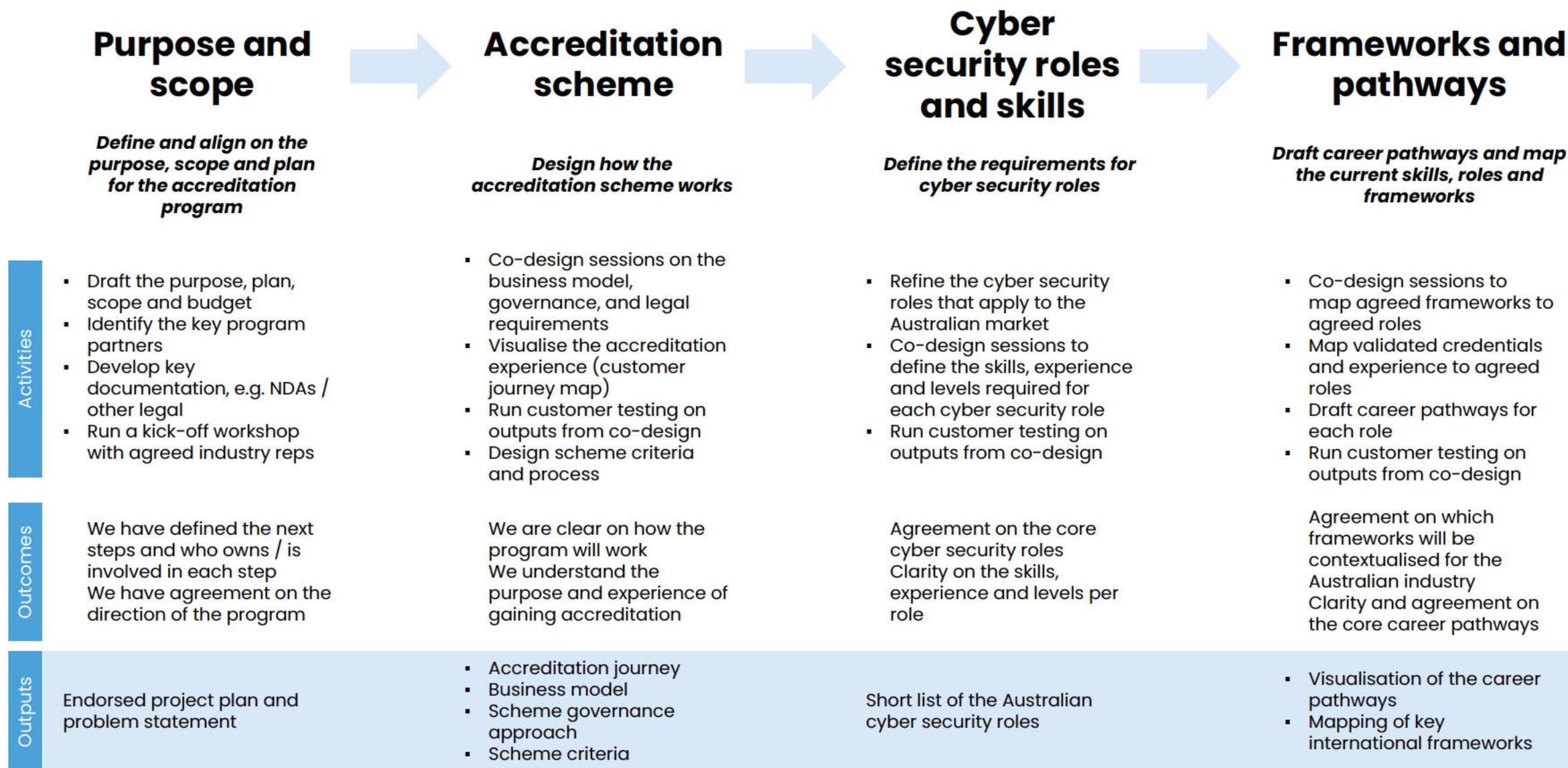
Photo by [Heidi Fin](#) on [Unsplash](#)

Success

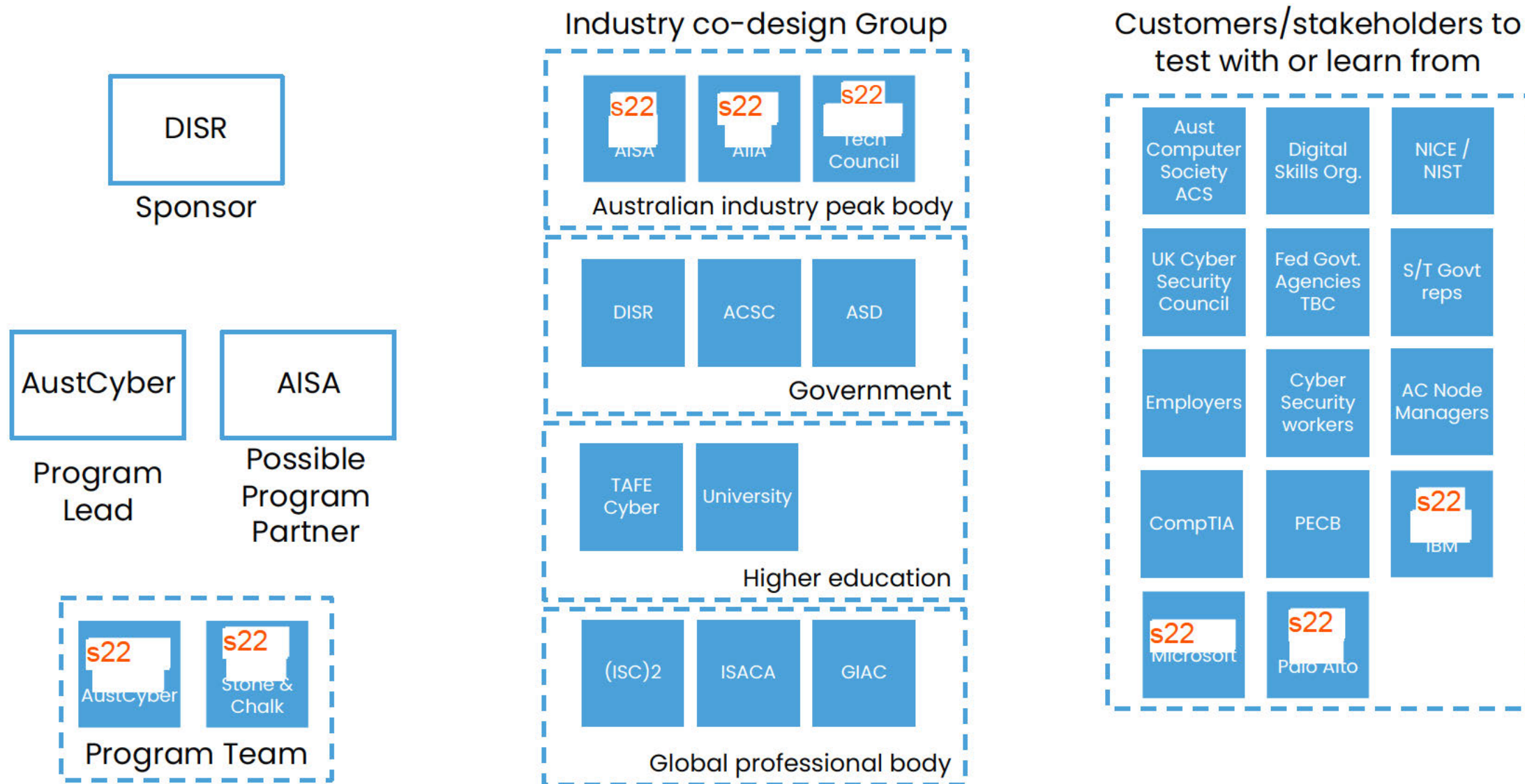
- The scheme and body is **recognised and endorsed** by industry and government
- The scheme and associated collateral **addresses the current and future challenges** in the cyber security skills and workforce in Australia
- Employers and purchasers have **confidence and trust** in the quality of the Australian cyber security workforce
- The scheme **clarifies the pathways** for those entering into the cyber security workforce as well as those seeking career progression
- The scheme is **aligned and builds on** existing assets including international frameworks and collateral



Proposed approach



Proposed structure



S47(1)(b)



Thank you

Australian Cyber Security Professionalisation (ACSP) Program

s22

Director Programs AustCyber

Table of Contents

Executive Summary	2
1.0 Background	4
2.0 Phase one overview	5
2.1 Co-design Team	5
2.2 Phase one plan	7
2.3 Phase one timeline	7
2.4 Customer Research	7
2.4.1 Overview	7
2.4.2 Research approach	8
2.4.3 Key findings	8
2.5 Phase one outputs	9
2.5.1 Baseline requirements and professional standards	9
2.5.2 Employee personas	10
2.5.3 Pathway to professional recognition	12
2.5.4 Skills Frameworks	12
2.5.5 Professional recognition scheme	13
3.0 Next Steps	15
3.1 Phase two overview	15
3.2 Proposed timeline	15
3.3 Phase two outputs	16
3.4 Phase two plan and funding requirements	17
3.4.1 Stage one – detailed development	17
3.4.2 Stage two – test the scheme via in-market pilot	17
Appendix A	19
Qualitative research data	19
Interview templates for employees and employers	20
The co-design team members	22

Executive Summary

From July 2022, the Australian Cyber Security Growth Network (AustCyber), supported by the Department of Industry, Science and Resources (DISR), has been leading the Australian Cyber Security Professionalisation (ACSP) Program to tackle the fragmentation and inconsistencies across the Australian cyber security sector. To ensure industry input, collaboration and support, AustCyber implemented a co-design approach, bringing together Australian and global cyber security leaders and experts to form a co-design team to design the solutions together.

The current members of the AustCyber-led [ACSP co-design team](#) are industry experts and leaders across a range of relevant Australian and global organisations representing industry associations, higher education and professional bodies.

The team has worked together to validate the problem statement, goal and scope of the program's first phase. Designing and testing solutions with stakeholders and end users to ensure a human-centred approach and input from the broader cyber security ecosystem.

Program overview

The goal of the ACSP program is to Improve government, business and community trust and confidence in Australian cyber security professionals in order for the ecosystem to continue to grow.

The first phase of the program resulted in the following [outputs and outcomes](#):

- Agreed and defined goal, purpose, scope and plan
- The baseline requirements to be recognised as a cyber security professional in Australia including skills, competencies and experience*
- Employee personas for a new entrant, career changer, existing practitioner, international worker
- Pathways for the personas to be recognised as a cyber security professional based on baseline requirements*
- Agreement on the need and value in creating professional standards for cyber security and the requirements for these professional standards*
- Agreement on the relevant skills frameworks to include and/or align with*
- Agreement that there is a need for a professional recognition scheme for cyber security professionals in Australia.*
- The high-level design of the:
 - business structure, including a governing body and scheme,*
 - business model for ongoing sustainability.*
- A set of learning themes from qualitative customer research.

* The detailed development and testing of these outputs are planned in phase 2

Next Steps

To capitalise on the outputs and outcomes of phase one and enable Australia to accelerate the professionalisation of its cyber security workforce, funding and support is required for the next phase of the program.

The existing co-design team and stakeholders are committed to continuing their support and input in phase two of the program. They are keen to build on the outputs already created and continue the momentum the program has established in the market. To develop and implement the scheme, phase two is planned to be delivered in two stages as outlined below.

Phase 2 investment

Stage 1: Draft the details of the scheme

Draft professional standards in detail:

- Code of ethics
- CPD model
- Recognised knowledge and education (including certification mapping)
- Qualifying criteria for on-the-job experience
- Assessment process

Establish the governing body, professional recognition scheme and business model

Timeframe: Six months

Investment: \$47(1)(b)

Stage 2: Test the scheme via an in-market pilot

Design and run an in-market pilot in Canberra/Adelaide of the:

- Governing body
- Professional recognition scheme and process
- Business model
- Online tools and resources
- Awareness campaign

Timeframe: Eight months

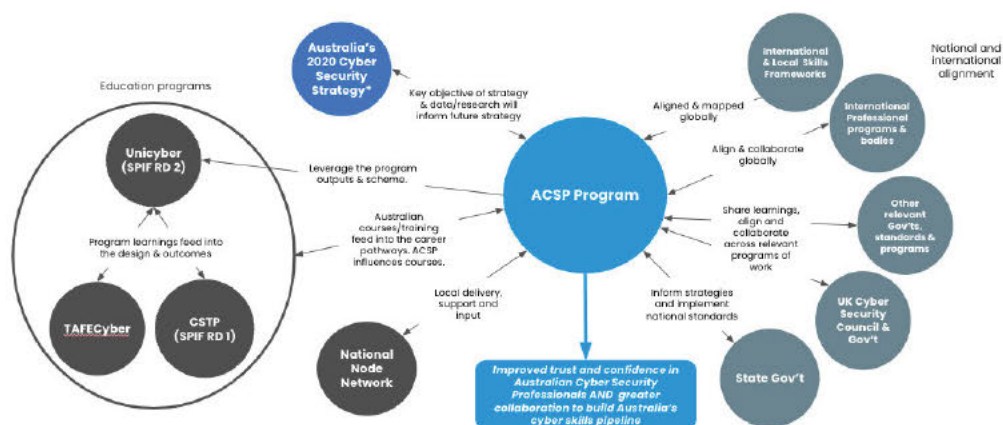
- Six months in-market
- Two months to iterate and create the scaled solution, ready for phased roll-out

Investment: \$47(1)(b)

Investing in the next phase of the ACSP program will enable the acceleration of a sustainable professional recognition scheme that will improve trust and confidence in Australian cyber security professionals globally, ultimately establishing Australia as a world leader in this area. It will strengthen the successful growth and resilience of the sector and contribute to the goal to be the 'most cyber-secure country' in the world by 2030.

ACSP - ecosystem impact & alignment

Key problems: • lack of clear professional standards for cyber security practitioners • the baseline set of skills, competencies, and experience not yet defined • cyber security skills and qualification frameworks not consistent • the industry is currently fragmented



*The 'most cyber-secure country' in the world by 2030
Minister O'Neil, December 2022

1.0 Background

Australia's Cyber Security Strategy 2020 calls attention to the importance of growing a cyber skilled workforce, where quality training, credentialing and accreditation are all central, including through the creation of new frameworks and processes.

It has been identified Australia needs more **trusted** and skilled cyber security professionals¹, and for businesses and the community to have **confidence** in the cyber security industry.²

Because Australia hasn't yet defined the baseline set of skills, competencies, and experience required to be recognised as a cyber security professional, there is a lack of clear professional standards for cyber security practitioners. In addition, skills and qualifications frameworks currently in use are inconsistent and misaligned between career aspirations, qualifications and labour market outcomes.

As part of the Australian Cyber Security Growth Network (AustCyber) growth centre funding, the Department of Industry, Science and Resources (DISR) agreed for AustCyber to lead the Australian Cyber Security Professionalisation (ACSP) Program to establish an industry-led, designed and supported cyber security professional recognition or accreditation scheme. This report details the approach, outputs and outcomes from phase one of the ACSP Program as well as the next steps to develop and test in-market the detailed design and implementation of cyber security professional standards, including the establishment of a sustainable governing body and professional recognition scheme.

ACSP Program Goal

Improve government, business and community trust and confidence in Australian cyber security professionals in order for the ecosystem to continue to grow.

During the first phase of the program, the co-design team led by AustCyber have:

- Designed and developed solutions building on existing work and learnings
- Tested outputs with customer groups to ensure customer input and feedback have guided the overall solution
- Planned the implementation of the solution at scale in the Australian market (including communication with global organisations as relevant)

¹ *Australia's Cyber Security Strategy 2020 (Clause 20)*

² *Australia's Cyber Security Strategy 2020 (Clause 70)*

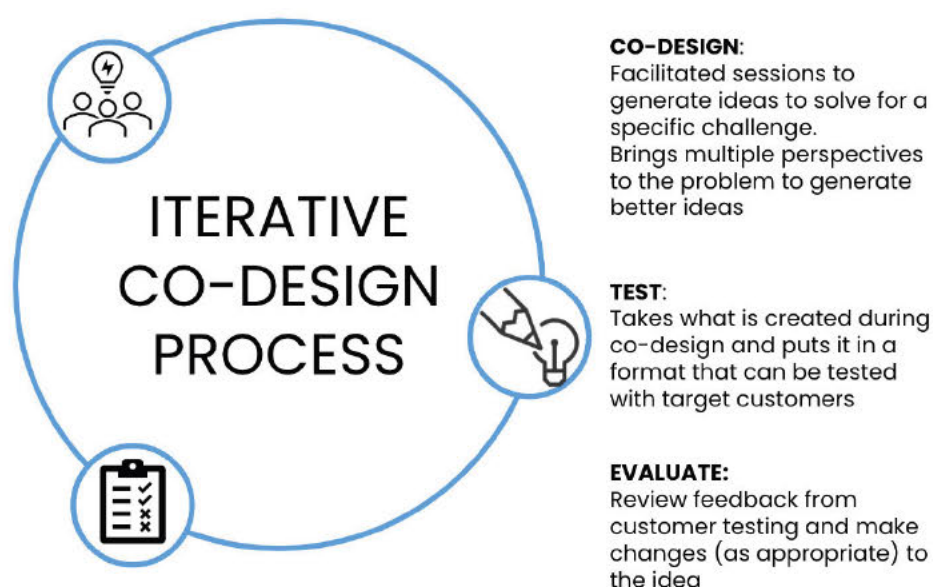
2.0 Phase one overview

A key requirement for this program is the outputs are industry-led, designed, and supported.

To achieve this, AustCyber implemented a co-design process (Figure 1) and brought together Australian and global cyber security leaders and experts to form a co-design team to design the solutions together.

Bringing multiple perspectives to the solution and regularly seeking feedback and input from key stakeholder groups, including the people the program is designing solutions for, increases the likelihood of achieving a successful outcome.

Figure 1: Co-design process



2.1 Co-design Team

To ensure the co-design team was truly 'industry-led', AustCyber scanned the sector to identify the leading Australian experts in cyber security; and the industry peak bodies that represented the most significant number of employees and employers, as well as leading academics and international bodies.

The purpose of the co-design team is to design and develop solutions to improve overall trust and confidence in Australian cyber security professionals for the ecosystem to continue to grow. The team focused on the role of career and education pathways, approaches to professional recognition, consistency of role definitions for cyber security in Australia, and alignment with existing frameworks.

The current members of the AustCyber-led ACSP co-design team comprise industry experts and leaders across a broad range of relevant Australian and global organisations, namely:

s22

To ensure the success of the program, broader stakeholder input and support have been established with both local and global stakeholders.

Cross-government support and collaborators include:

- Department of Industry, Science & Resources (DISR)
- Department of Home Affairs
- Australian Cyber Security Centre (ACSC)
- Australian Public Service Commission (APSC)
- Department of Employment & Workplace Relations (DEWR)

Other collaborators include:

- AustCyber innovation node network
- Digital Skills Organisation
- Engineers Australia

- UK Cyber Security Council and government
- NSW and Victorian Government Cyber Branch

2.2 Phase one plan

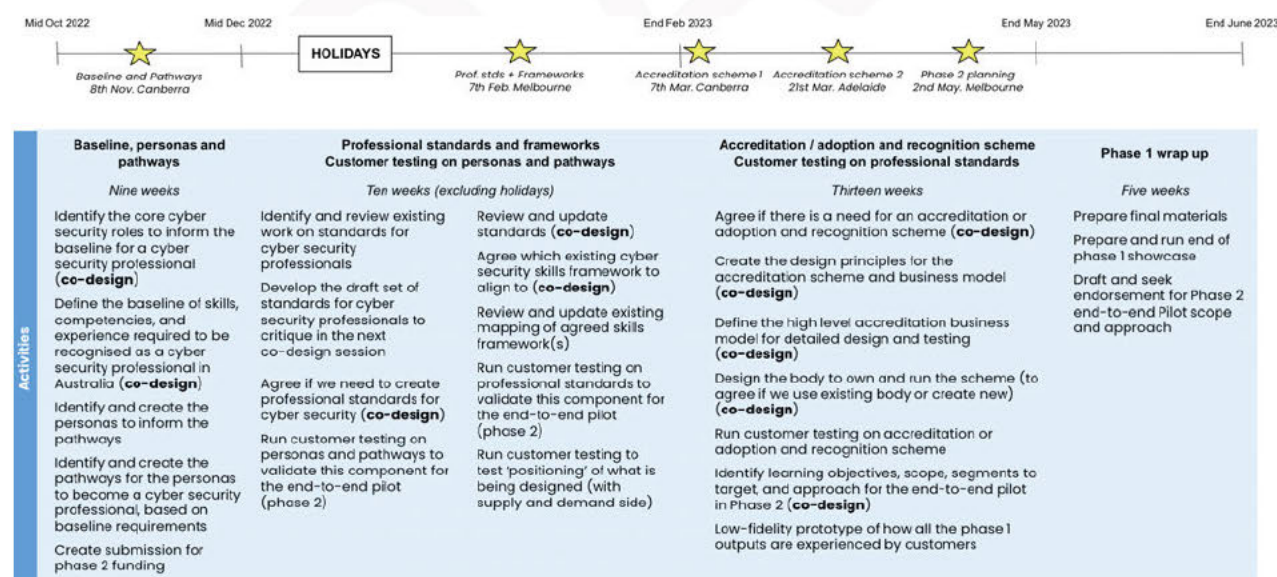
Phase one was split into four areas for the co-design team to focus on as follows:

- Purpose and Scope
 - Define and align on the purpose, scope and plan for the professionalisation program.
- Baseline and Pathways
 - Design the baseline to be recognised as a Cyber Security Professional, identify personas, roles and map career pathways.
- Professional standards and frameworks
 - Agree on the need and value of professional standards and agree on skills frameworks to align with.
- Professional Recognition Scheme
 - Agree on the need and value of an accreditation or recognition scheme.

2.3 Phase one timeline

The co-design team program of work was delivered over October 2022 to end June 2023 (Figure 2).

Figure 2: Phase one program timeline



2.4 Customer Research

2.4.1 Overview

The co-design team identified the need to understand the current experience and needs of both employees and employers to produce a program that was supported and adopted by the industry.

2.4.2 Research approach

Independent qualitative customer research was conducted, which involved 1:1 one-hour interviews with 25 employees and 20 employers. Please refer to Appendix A to review the research data and interview templates.

Employees interviewed:

- Career changers — previously working in a different industry now in cyber security.
- Existing professionals — working in a cyber security role for the past five years or more.
- New entrants — working in a cyber security role for less than one year after graduating (mix of school leavers and university graduates).
- International workers — moved to Australia within the last five years and are working in a cyber security role. They were already working in cyber security in their home country.

Employers interviewed:

- Non-technology focused small to medium enterprises (SMEs)
- Technology focused SMEs
- Corporates

2.4.3 Key findings

- Both employers and employees place a **high degree of value on experience** working in the industry.
- Therefore, when they think of someone operating at the next level, a professional, they want to see a **professional standard that includes relevant experience** working in cyber security.
- Employees are **drowning in the choice** of how they learn about cyber security; this was explicitly called out when talking about certifications.
- Those in the know, people who have been working in the industry for a while, have pieced together their own version of **criteria regarding what certifications they recommend** to their teams or look for when hiring people.
- Feedback suggested that there is **no shortage of certifications, and degrees, that aren't worth the paper they are printed on**, either because they can be gamed by buying 'brain dumps' online or don't teach you what you need to know to work.
- They see **value in a single source of truth on what is valid** and **having these validated ones being called out in a pathway** to becoming a professional.
- Across the employees and employers interviewed, there was a strong theme for the **creation of a new body to administer professional standards**.
- A **government-backed, industry-supported body was preferred**. Employees expressed that this felt like the right balance as **government backing provided validity**, but not being government-run mitigated the risk of red tape, slowness, and bureaucracy.

- When asked which government department made sense, the **ACSC was referred to as the most relevant** due to its focus, and many employees read and listen to the content they put out around cyber security.
- **Industry-led was called out as the speed and voice** needed to ensure the administration kept up to date.
- Employees suggested that having a **diverse group of industry representatives as part of this body** would bring the balance needed to ensure the continued growth of the industry.
- When employers were interviewed, including AIIA and Tech Council members, they understood **this was not about licensing** but about recognition as a professional; they saw the value for themselves and the industry and were supportive.
- **Recruitment** was a key theme: making hiring easier and having better trust in who is being hired and their capabilities.
- However, if there is a professional recognition scheme, it needs to be **flexible and inclusive, not create a barrier to entry**. It must showcase what each individual brings and not lock people into a traditional model where the only pathway is via formal education.
- It is down to the **individual to demonstrate professional qualities**.
- **People outside the cyber security industry would benefit from having some form of professionalisation** to help them know who they are hiring or what to look for.

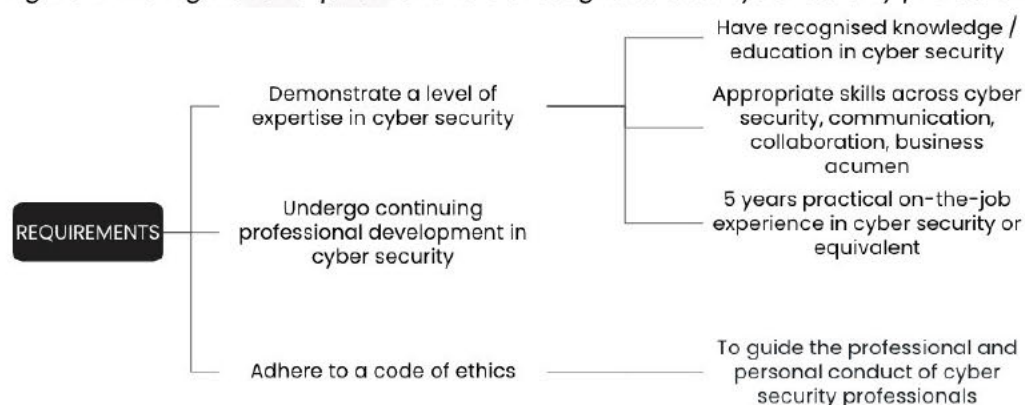
2.5 Phase one outputs

The outputs from phase one inform the next phase of the ACSP program. The co-design team has developed the following outputs.

2.5.1 Baseline requirements and professional standards

The co-design team have agreed on the need and value of professional standards. As a result, the team has designed the high-level requirements to be recognised as a cyber security professional (Figure 3) that will form the basis for the development of the professional standards in phase two. These requirements have been tested with end users via customer research and the broader key stakeholders.

Figure 3: The high level requirements to be recognised as a cyber security professional



2.5.2 Employee personas

The co-design team identified the need to understand the current experience and needs of both employees and employers to design solutions for these two groups of users. It was agreed there were four discrete employee personas to research and develop:

- Existing professional (Figure 4)
- Career changer (Figure 5)
- New entrant (Figure 6)
- International worker (Figure 7)

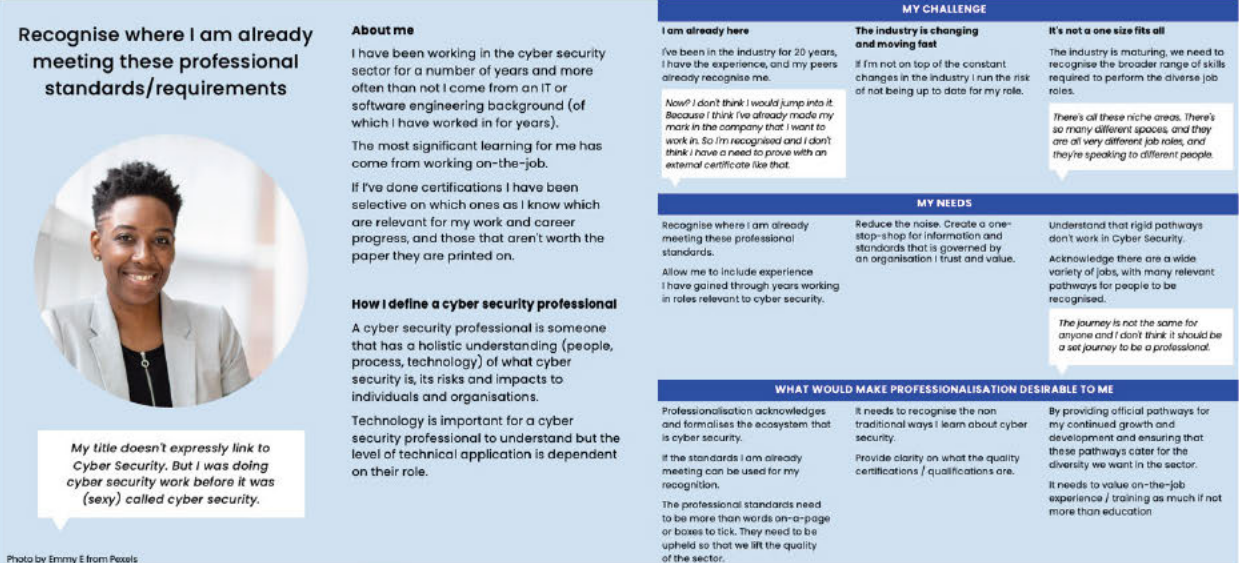
The following employer personas are still under development:

- SME - Non-technical
- SME - Technical
- Corporate

Comprehensive qualitative customer research was conducted to develop the personas.

Figure 4: Existing professional persona

Existing professional



Recognise where I am already meeting these professional standards/requirements

My title doesn't expressly link to Cyber Security. But I was doing cyber security work before it was (sexy) called cyber security.

About me

I have been working in the cyber security sector for a number of years and more often than not I come from an IT or software engineering background (of which I have worked in for years).

The most significant learning for me has come from working on-the-job.

If I've done certifications I have been selective on which ones as I know which are relevant for my work and career progress, and those that aren't worth the paper they are printed on.

How I define a cyber security professional

A cyber security professional is someone that has a holistic understanding (people, process, technology) of what cyber security is, its risks and impacts to individuals and organisations.

Technology is important for a cyber security professional to understand but the level of technical application is dependent on their role.

MY CHALLENGE		
I am already here I've been in the industry for 20 years, I have the experience, and my peers already recognise me. <i>Now? I don't think I would jump into it. Because I think I've already made my mark in the company that I want to work in. So I'm recognised and I don't think I have a need to prove with an external certificate like that.</i>	The industry is changing and moving fast If I'm not on top of the constant changes in the industry I run the risk of not being up to date for my role.	It's not a one size fits all The industry is maturing, we need to recognise the broader range of skills required to perform the diverse job roles. <i>There's all these niche areas. There's so many different spaces, and they are all very different job roles, and they're speaking to different people.</i>
MY NEEDS		
Recognise where I am already meeting these professional standards. Allow me to include experience I have gained through years working in roles relevant to cyber security.	Reduce the noise. Create a one-stop-shop for information and standards that is governed by an organisation I trust and value.	Understand that rigid pathways don't work in Cyber Security. Acknowledge there are a wide variety of jobs, with many relevant pathways for people to be recognised. <i>The journey is not the same for anyone and I don't think it should be a set journey to be a professional.</i>
WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME		
Professionalisation acknowledges and formalises the ecosystem that is cyber security. If the standards I am already meeting can be used for my recognition. The professional standards need to be more than words on-a-page or boxes to tick. They need to be upheld so that we lift the quality of the sector.	It needs to recognise the non traditional ways I learn about cyber security. Provide clarity on what the quality certifications / qualifications are.	By providing official pathways for my continued growth and development and ensuring that these pathways cater for the diversity we want in the sector. It needs to value on-the-job experience / training as much if not more than education

Photo by Emmy E from Pexels

Figure 5: Career Changer persona

Career Changer

Recognise what I bring to the sector and guide me on where to focus my time and effort



As a career changer, I wouldn't consider myself a professional yet – I need to build up my cyber security specific experience.

Photo by Anna Streets from Pixels

About me

I have a background (and hold some qualifications) in another industry, so I have the soft skills and a basic knowledge of cyber that allows me to enter the industry. I moved into cyber security because external (and internal) pressures led me to it. I've always been interested in IT and technology and cyber security is a growing industry with many career opportunities.

How I define a cyber security professional

A cyber security professional has been in the industry for a while – they know more. They should be able to identify the risks and protect the company or any organisation. They can identify, protect, and detect. They can respond to the incident and develop something to reduce the impacts of the events, and then finally, they can help the company to recover.

MY CHALLENGE

I don't have peer recognition
I'm new in the industry and need to build credibility amongst my peers.

I think just the recognition to be accredited would be enough for me. You know it should be like an industry currency that not just everyone can have access to, so the recognition alone from that would be valuable.

My background isn't in IT
You don't need to spend years learning IT technical skills but I think it's important to understand the basics of IT.

I know people who've moved into SOC from having a technical background have found it a lot easier. Because they already have that foundational knowledge – especially people who come from IT backgrounds or have worked in other technical roles.

It's hard to keep up
It's hard to keep up with the latest skills – once I finish a course or learn a new technique the landscape of the industry has already changed, it's so hard to keep up.

MY NEEDS

I need some sort of currency within the industry.

I need to understand the key principles that underlie how cyber security works, and how organisations can use those principles.

I need to tailor my training and learning to my area of specialisation while still gaining varied experience.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

A tiered model approach would provide incentive for someone like me with less experience, I could achieve it in the next couple of years.

If I can count what I am already paying for that directly relates to achieving this (I can't sign up to all of them).

Clear guidelines and requirements as to what makes a cyber professional.

Be clear on what the requirements are for me if I want to be there, I need to do this, this and this. Just be clear, so I know what I have to do.

There is a pathway that includes hands-on experience and doesn't mandate a university degree.

Make the pathways clear and recognise the various entry points and relevance of different skills.

I don't think it's purely having technical skills because a lot of people have technical skills, but then they lack a lot of soft skills.

Figure 6: New Entrant persona

New Entrant

There isn't a clear pathway for me to get in and be successful in the sector. I need direction on what choices to make



Give me clarity on pathways so I can invest my time and money wisely.

Photo by Pavel Danyuk from Pixels

About me

I have recently entered the industry after moving away from my previous role. I got a certification in IT or Cyber Security to help me break into the industry. I have little to no on-the-job cyber security experience so I have been placed in an entry-level role. The most important thing for me is to get the hands-on experience so I can progress in my career, and be recognised as valuable in my role.

How I define a cyber security professional

A cyber security professional is someone who has had years of experience in the industry, and has the knowledge/theory to back them. They have a foundation in IT and demonstrate 'professional' skills.

MY CHALLENGE

Entry level jobs require experience
How can I gain industry experience, when employers are asking for 1-2 years experience for entry level roles?

There's very limited entry level jobs, and if so they want 1-2 years experience.

I don't know what certifications are valuable
Am I wasting my time and money on something that won't get me employed? There isn't a clear pathway to help me decide on which one to do.

I have studied 10 certifications and maybe two were effective.

The pathways are unclear
I struggle to understand and describe what a professional is because there is a lack of clarity on how to get there.

MY NEEDS

Tell me where the best place to start is and what I need to do to get in there.

Show me what certifications are valuable, so that I spend my time and cash on something that is credible.

Companies out there aren't looking at what degree you have studied, they are only looking at certifications, or ask for previous experience (2 years) in similar industry.

Help me understand what a professional is to give me a goal to work towards

I don't think I have enough experience to understand what the requirements of a professional should be.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

Tell me what employers value and where I can look for a job.

Pathways that recognise all my relevant hands on experience, not just experience after I've finished my graduate program/role.

I would have spent 4 years studying then 5 years in the industry. 9 years is a long time to be recognised. If you do it parallel then it works.

Guidance on potential pathways, and helping me understand how to work my way up in my career.

It doesn't require me to pay for another annual fee/ membership.

A tiered approach to professionalisation so I gain recognition at multiple stages of my career.

If we do a tiered level of experience: Junior: 1-2 years Mid: 5 years CSO level: 10 years.

Figure 7: International worker persona

International worker

Ensure my international certifications and skills are recognised in Australia



To increase migration to Australia, you want to have something that can at least be interoperable with other countries.

About me

I migrated to Sydney last year from <country> for opportunities in cyber security. Before I migrated to Australia, I worked in IT. I was in the cyber security space in <country> for more than five years. I have, at a minimum, a bachelor's degree and multiple certifications, and I often have come in via the Global Talent Program visa.

How I define a cyber security professional

For someone to be considered a professional, they need proven work experience. When I worked in <country>, there were guidelines from a governing body of what a cyber professional is, including a reference framework to show the level of experience a professional has and their progress. It also has interoperability with certifications in other parts of the world.

MY CHALLENGE

Having to do things twice

I've done that [background check] as part of my visa entrance process, so I should not have to do it again.

If it means I have to do extra, extra training, or I have to undergo exams in order to do this, then I'd have to weigh up the value. I probably wouldn't do it.

There is no interoperability with Australia

ISACA, (ISC)2 etc, are recognised internationally but have yet to be applied under a nationally consistent approach in Australia.

If we put a national requirement, it shouldn't be limited only to Australian nationals, I think you need to consider the international workforce and how they may contribute to the Australian sector.

MY NEEDS

Recognise where I've met requirements with my (international) experience.

To make the transition seamless, is there a way where we recognise that your clearance, integrity, qualification, and certifications in your home country... when you come to Australia, you don't necessarily have to start again. You can say, well actually, I've already met all of them. So, therefore, I can then be recognised.

Global recognition.

I guess that is a great way to attract the interoperability of the professional - from both sides.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

A framework that substantiates my integrity as a cyber security professional (when I've already been subject to a police or background check).

Plug into what I already have.

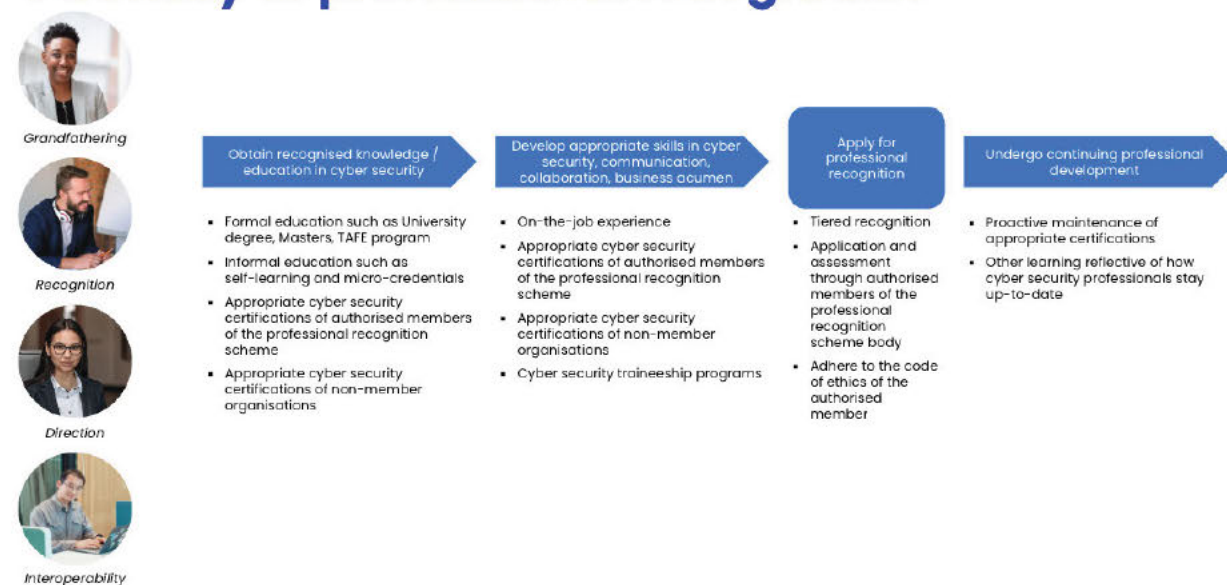
If there was a way to plug in recognised certifications and the work you have to do to get them. Therefore if you could plug what you are already doing there and it is acknowledged by the Australian accreditation program that would make the process easier.

2.5.3 Pathway to professional recognition

A high-level pathway to professional recognition has been designed based on the baseline requirements to be recognised as a cyber security professional and the four employee personas (Figure 8). This high-level pathway will be used to guide the detailed design of the professional recognition processes and experience developed under phase two.

Figure 8: High-level pathway to professional recognition

Pathway to professional recognition



2.5.4 Skills Frameworks

To create consistency and global alignment, the co-design team have reviewed and considered existing cyber security skills frameworks to align with or include. Each skills framework was reviewed in the context of its currency, relevance, purpose and global

usage. The team agreed to include three core skills frameworks (Figure 9), use other current frameworks as resources to reference (Figure 10) and reframed the inclusion of ANZSCO - Australian and New Zealand Standard Classification of Occupations (Figure 11).

Figure 9: Cyber security skills frameworks to include

Skills framework	Why it is included	How it will be included
CIISEC	Helps us align with the UK to improve pathways	Mapped to SFIA + NICE
SFIA	- Expressed using clear language - There is opportunity to feed into new versions	Express in terms of SFIA as a language rather than a set of definitions
NICE	- Allows alignment with the US - Already used by ASD	Refer to but not the primary or sole framework as it is extremely complex

Figure 10: Resources to be used

Resource	Why it is being used as a resource	How it will be used
ASD cyber skills framework	- Considerable government investment and buy-in to this framework - Including it helps this work integrate with government	Use the learning of how they mapped NICE + SFIA
European Cyber Security Skills Framework (ECSSF)	- Strong point of reference regarding governance - Not used as a skills framework due to cultural differences with Europe	Informs detail regarding governance
CyBOK	- So that we have a reference point for relevant cyber security knowledge - Creates another link to the UK to enhance interoperability	As a point of reference for knowledge + education

Figure 11: To be reframed

Resource	Why we are reframing its usage	How it will be used
ANZSCO	- Not relevant for this context. - The classifications are used by government and industry, important they are up-to-date with correct cyber security data	- Help amplify ANZSCO. - Feed into it to improve it as it relates to cyber security occupations

2.5.5 Professional recognition scheme

The co-design team has agreed to the need and value of a professional recognition scheme to implement the professional standards and recognition process.

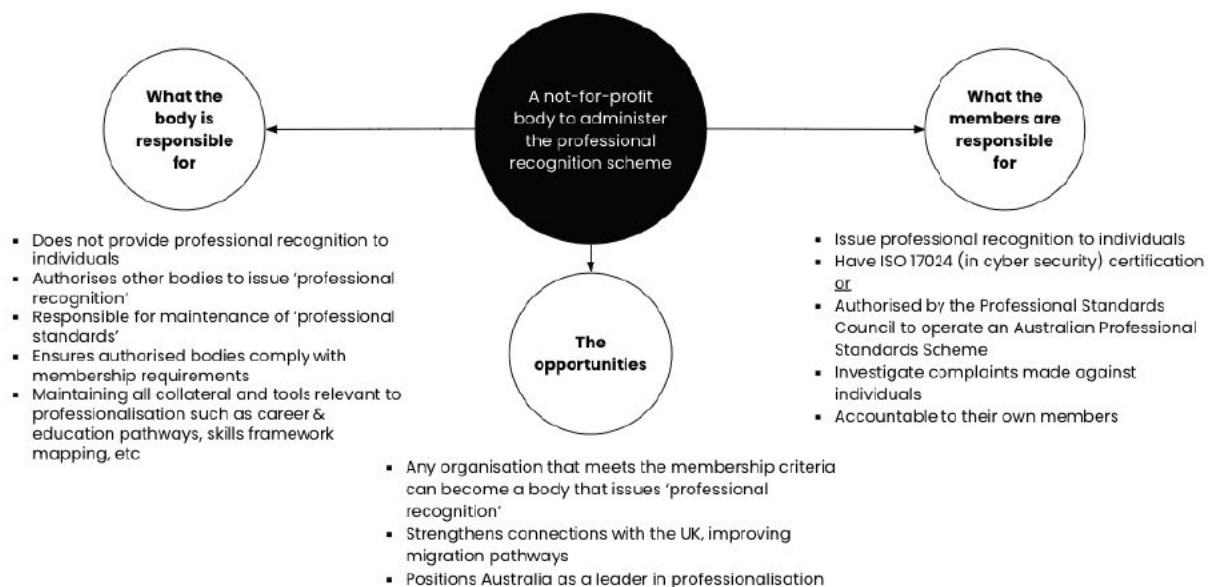
A similar program of work has been designed and is currently being piloted in the United Kingdom (UK) which is supported by the UK Government. The UK Cyber Security Chartered scheme is governed by the recently formed UK Cyber Security Council (Council) and has been in development for approximately two years. The UK Government and Council have openly shared their business model, scheme, and learnings to date.

The co-design team has agreed it would be valuable to consider aligning, where possible, with other similar professionalisation schemes globally to enhance the global relevance and interoperability of Australian professional standards. With this in mind, the team has drawn on the UK experience to design a high-level 'strawman' structure for a similar

governing body in Australia to oversee and implement the professional recognition scheme for further review and discussion (Figure 12).

The team is currently designing a high-level sustainable business model to be further developed and tested in-market in phase two.

Figure 12: Strawman of the governing body



3.0 Next Steps

The ACSP co-design team has established strong local and international relationships and built solid momentum on this program of work. However, to capitalise on this and enable Australia to accelerate the professionalisation of its cyber security workforce, funding and support must be secured for the next development phase, minimising any time delay between phases one and two.

The existing team and stakeholders are committed to continuing their support and input in phase two and are keen to build on the outputs already created to continue the momentum the program has established in the market. The overview of the next phase of development and funding required is detailed below.

3.1 Phase two overview

It is proposed ACSP phase two will be a continuation of phase one and be delivered in two stages (Figure 13) with AustCyber continuing to lead the program of work in collaboration with the already established ACSP co-design team and stakeholders.

Figure 13: Phase two stages

Phase 2

Stage 1:

Draft the details of the scheme

Draft professional standards in detail:

- Code of ethics
- CPD model
- Recognised knowledge and education (including certification mapping)
- Qualifying criteria for on-the-job experience
- Assessment process

Establish the governing body, professional recognition scheme and business model

Timeframe: Six months

Stage 2:

Test the scheme via an in-market pilot

Design and run an in-market pilot in Canberra/Adelaide of the:

- Governing body
- Professional recognition scheme and process
- Business model
- Online tools and resources
- Awareness campaign

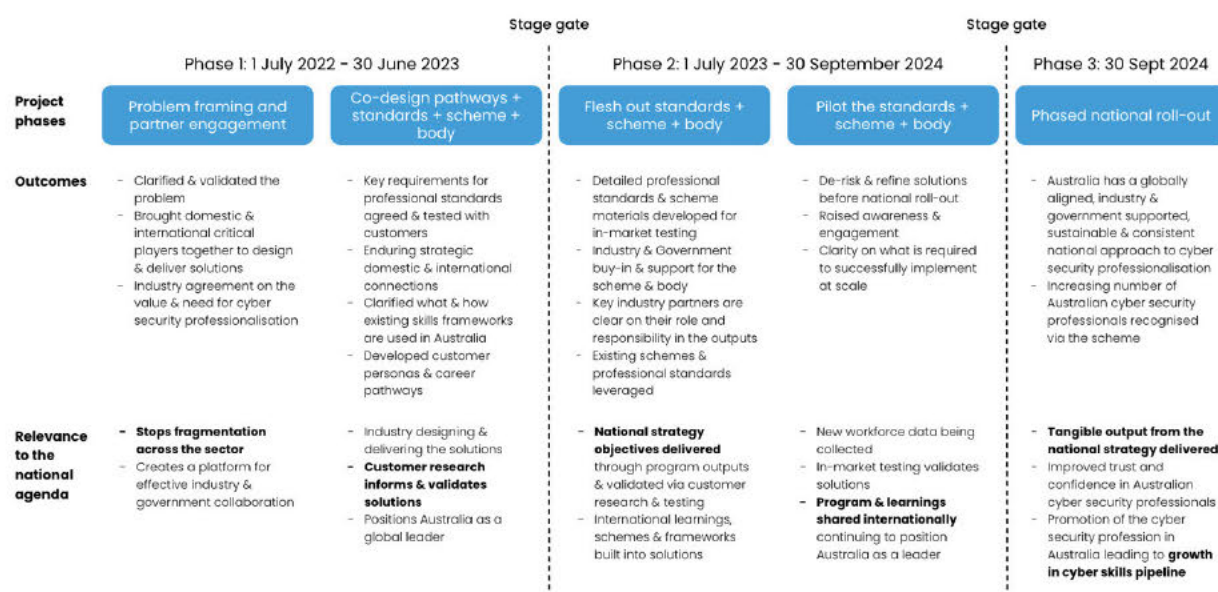
Timeframe: Eight months

- Six months in-market
- Two months to iterate and create the scaled solution, ready for phased roll-out

3.2 Proposed timeline

The table below outlines the proposed timeline of ACSP program deliverables from the design phase through to national roll-out of an Australian cyber security professionalisation scheme (Figure 14).

Figure 14: Proposed timeline



3.3 Phase two outputs

- Detailed development of:
 - professional standards and associated collateral,
 - professional recognition scheme and process,
 - business structure and model.
- The establishment of the business structure, including terms of reference, membership structure and financial model for ongoing sustainability.
- An end-to-end pilot of the business model and professional recognition scheme and process (conducted in Canberra/Adelaide), including:
 - an interactive digital career pathway tool
 - personas, created in phase one, brought to life as online case studies
 - recognised list of credentials and education that form part of the pathways to be recognised as a cyber security professional
 - interactive skills framework map/matrix that supports the career pathway tool
 - professional standards, code of ethics, guidelines etc
 - innovative CPD requirements
- A phased national implementation roadmap.

3.4 Phase two plan and funding requirements

3.4.1 Stage one – detailed development

- Develop the professional standards and recognition process in detail, including:
 - Code of ethics
 - CPD model and requirements
 - Recognised knowledge and education (including certification mapping)
 - Qualifying criteria for on-the-job experience
 - Assessment process
- Establish the business model, including the governing body, the professional recognition scheme, and the financial model.

s47(1)(b)

3.4.2 Stage two – test the scheme via in-market pilot

Design and run an in-market pilot of the body, scheme and business model in Canberra/ Adelaide including the development of supporting online tools and resources.

Timeframe: Eight months

- Six months in-market
- Two months to iterate and create the scaled solution, ready for phased roll-out

s47(1)(b)

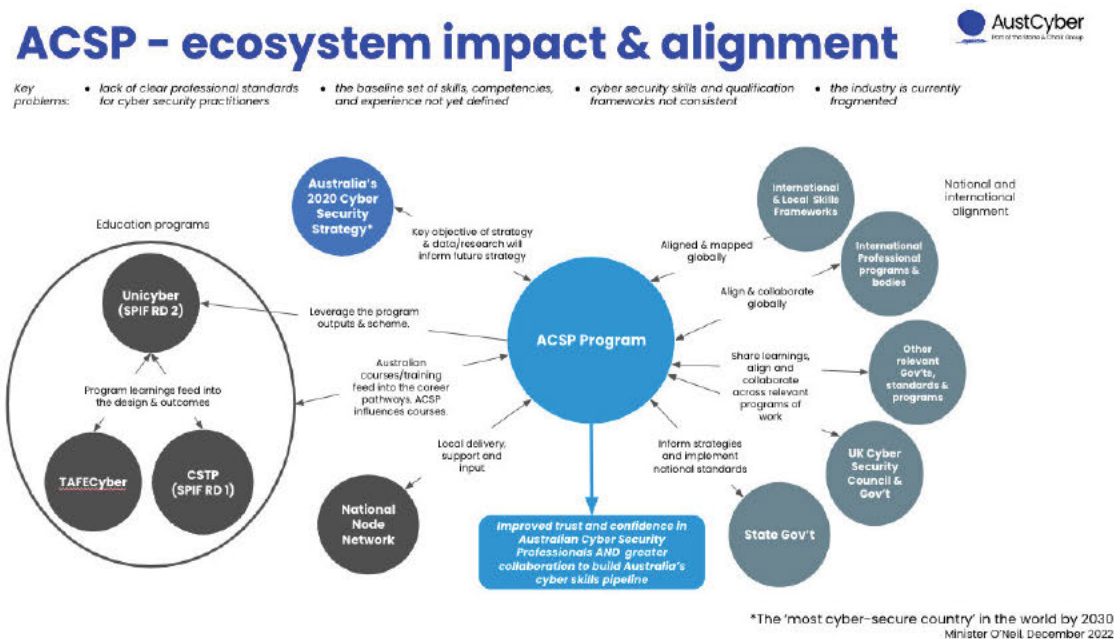
The collaborative co-design team, comprising experts and leaders from various fields, has effectively united to accomplish the program's objectives. By leveraging their collective knowledge, experience, and networks, they have successfully:

- Design the high-level requirements to be recognised as a cyber security professional in Australia that will inform the development of professional standards.

- Conduct customer research to create customer personas and pathways, understand the current employee and employer experiences and needs, and gain feedback and buy-in to the professionalisation of the Australian cyber security sector.
- Agree on the relevant skills frameworks to include and reference.
- Design the high-level business structure and model to implement an Australian professional recognition scheme.

The ACSP program is integral to Australia's broader cyber security agenda, as demonstrated in Figure 15. The introduction of an Australian cyber security professional recognition scheme not only builds trust and confidence in the Australian cyber security workforce but will be central to establishing Australia as a world leader, strengthening the successful growth and resilience of the sector, and the goal to be the 'most cyber-secure country' in the world by 2030.

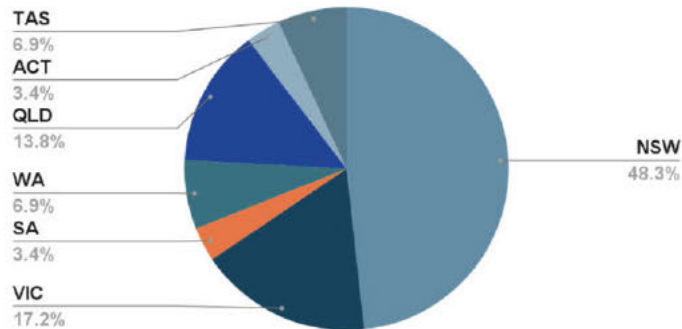
Figure 15: ACSP ecosystem and alignment



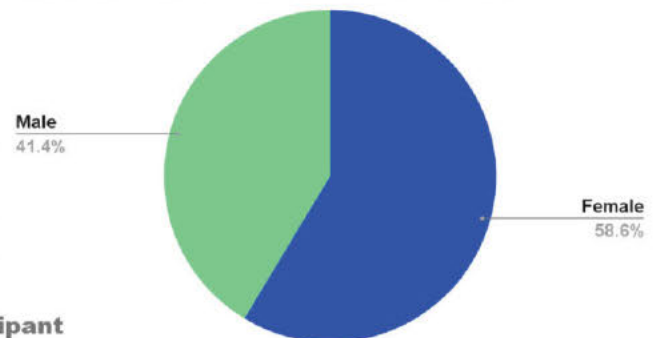
Appendix A

Qualitative research data

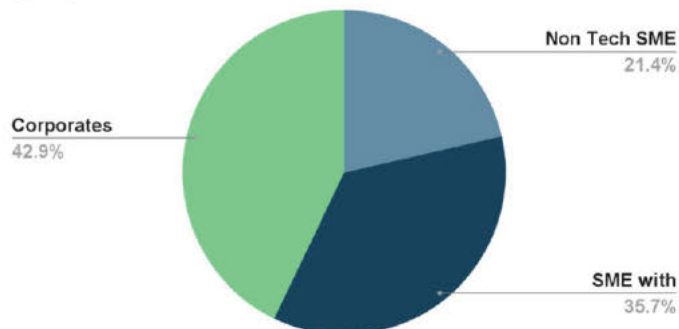
Nearly half of the research participants were from NSW.



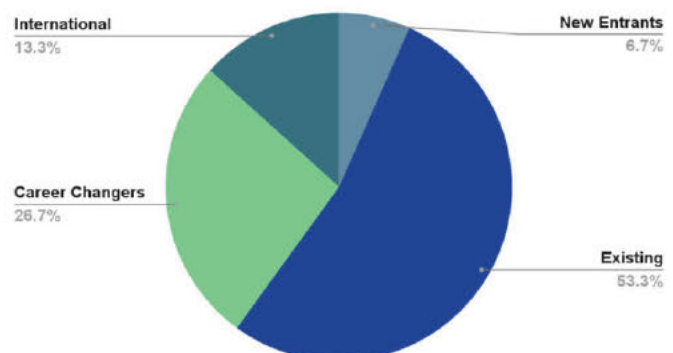
We interviewed more females than males.



Corporate Employers were our biggest participant group.



We found it most difficult to source New Entrants.



Interview templates for employees and employers

<Name> Interview: <DATE>

EXISTING PROFESSIONAL/ NEW ENTRANT/ INTERNATIONAL WORKER/ CAREER CHANGER

Interviewee: <Name>

Timing: 60 minutes

Interviewers: <Name>

Background:

Role:

How employees feel about the idea of formalising what it means to be a cyber security professional

- 1 How do you describe what a cyber security professional is?
- 2 Would you define everyone currently working in the industry as a cyber security professional?
- 3 We are trying to work out how to create nationally consistent requirements for people to be recognised as a cyber security professional.
- 4 From an industry perspective what do you see as the benefits of creating these nationally consistent requirements?

What they think the requirements to be considered a cyber security professional are

- 1 What is your current job title, 'why do you feel this implies you are working in cyber security'?
- 2 For someone to be nationally recognised as a cyber security professional what do you think some of these requirements should be?
- 3 What is your view on the order of priority for these requirements?
- 4 Is there anything you think should absolutely not be a requirement?
- 5 What challenges might exist in meeting these requirements?
- 6 Please provide feedback on the co-design teams requirements
- 7 Who would you expect to get the professional recognition from?

What employees need to become a cyber security professional / what would make it desirable

- 1 What would stop you becoming recognised as a cyber security professional?
- 2 What would make you want to become a cyber security professional?
- 3 To meet the requirements we described before what would make it easier for you to meet them?
- 4 If you became a professional what benefits would you expect to get?
- 5 Describe what you think the pathway to becoming a professional would be

Approaches to continuous Professional development

- 1 Do you currently do any?
- 2 What do you like / don't like about it?
- 3 How would you make CPD better?

Examples of good codes of ethics

- 1 Do you currently adhere to / have signed up to any code of ethics?
- 2 What is the value of having a code of ethics for cyber security professionals to adhere to?
- 3 What do you think should be in the code?

<NAME> Interview: <DATE>

NON TECH SME/ TECH SME/ CORPORATE/ GOVERNMENT

Interviewee: <NAME>**Timing:** 60 minutes**Interviewers:** <NAME>**Background****Role:*****What the current experience is for employers when hiring a cyber security employee or consultant****1 How do you currently get help with cyber security for your company?**2 Why do you get help that way?**3 Have you hired someone to look after your cyber security?**4 Tell me about the experience hiring them**4.1 What was good about this experience?**4.2 What was bad about this experience?**4.3 What would improve your confidence in this experience?**5 Why did you choose that person / provider?**6 Does your business have a need for a cyber security professional vs an entry level worker?**6.1 Why do you need this?****What they think the requirements to be considered a cyber security professional are****1 When hiring someone that calls themselves a cyber security professional what improves your confidence in them?**2 When hiring someone that calls themselves a cyber security professional what decreases your confidence in them?**3 What is the difference between a new entrant to someone calling themselves a cyber security professional?**3.1 Do you feel we need to define the difference between these?**3.2 What are the risks if we don't define the differences?**4 Read these proposed requirements to be considered a cyber security professional**4.1 If someone had met these requirements what does that do to your trust and confidence in them as cyber security professional?**4.2 Why or why not does this change your trust and confidence in them?**4.3 Would you add or remove any of these requirements?****What they would place their trust in****1 If someone classified themselves as a cyber security professional, how would you validate this?**2 Is there an organisation or body you feel that should validate if someone has met these requirements?**3 What would give you confidence or make you trust this organisation or body?*

s22

[REDACTED]

Australian Cyber Security Professionalisation (ACSP) Program

s22

Director Programs AustCyber

Table of Contents

Executive Summary	2
1.0 Background	5
2.0 Phase one overview	6
2.1 Co-design Team	7
2.2 Phase one plan	9
2.3 Phase one timeline	9
2.4 Customer Research	9
2.4.1 Overview	9
2.4.2 Research approach	9
2.4.3 Key findings	10
2.5 Phase one outputs	11
2.5.1 Baseline requirements and professional standards	11
2.5.2 Employee personas	12
2.5.3 Pathway to professional recognition	13
2.5.4 Skills Frameworks	13
2.5.5 Professional recognition scheme	14
2.5.5 Design Principles	15
3.0 Next Steps	17
3.1 Phase two overview	18
3.2 Proposed timeline	19
3.3 Phase two outputs	20
3.4 Phase two plan and funding requirements	20
3.4.1 Detailed development	20
3.4.2 Test the scheme via in-market pilot	21
Appendix A	23
The co-design team members - phase one	23
Appendix B	24
Qualitative research data	24
Interview templates for employees and employers	26
Appendix C	28
Employee Personas	28
Employer Personas	30

Executive Summary

From July 2022, the Australian Cyber Security Growth Network (AustCyber), supported by the Department of Industry, Science and Resources (DISR), has been leading the Australian Cyber Security Professionalisation (ACSP) Program to tackle the fragmentation and inconsistencies across the Australian cyber security sector. To ensure industry input, collaboration and support, AustCyber implemented a co-design approach, bringing together Australian and global cyber security leaders and experts to form a co-design team to design the solutions.

The current AustCyber-led [ACSP co-design team](#) members are industry experts and leaders across various relevant Australian and global organisations representing industry associations, higher education and professional bodies.

The team collaborated to validate the problem statement, goal, and scope of the program's first phase. The team also engaged stakeholders and end users to design and test solutions, ensuring a human-centric approach and input from the broader cyber security community.

Program overview

The goal of the ACSP program is to improve government, business and community trust and confidence in Australian cyber security professionals in order for the ecosystem to continue to grow. The first phase of the program resulted in the following [outputs and outcomes](#):

Co-design team achievements to-date

Collaborated face-to-face

1. Purpose, scope and plan
2. Baseline, personas and pathways
3. Professional standards and frameworks
4. Professional recognition scheme and governing body

Designed and agreed

- Draft baseline requirements to be recognised as a cyber security professional
- The need for and value of professional standards for cyber security
- The cyber security skills frameworks to include
- The need for and value of a professional recognition scheme for cyber security

Produced

- A set of requirements that will inform the professional standards for cyber security
- A set of cyber security employee and employer personas
- A high level pathway to be recognised as a cyber security professional
- The high level design of the structure for the governing body
- A set of design principles to be used in Phase 2
- Draft cyber security specialisms/disciplines for the Australian market

The detailed development and testing of the phase one outputs and outcomes are planned for phase two

Next Steps

To capitalise on the outputs and outcomes of phase one and enable Australia to accelerate the professionalisation of its cyber security workforce for the benefit of the Australian community, funding and support are required for the next phase of the program.

The initial co-design team, collaborators and stakeholders that have helped shape the program from phase one are committed to continuing their support and input in the next phase. They are keen to build on the outcomes and outputs already created and continue the program's momentum in the market along with new co-design team members and stakeholders specifically engaged to support the detailed development and testing in the next phase. Phase two is planned to be delivered as outlined below.

ACSP – Phase two

s47(1)(b)

Detailed development of the scheme

Draft professional standards in detail:

- Code of ethics
- CPD model
- Recognised knowledge and education (including certification mapping)
- Qualifying criteria for on-the-job experience
- Assessment process

Establish the governing body, professional recognition scheme and business model

Timeframe: Six months

Test the scheme via an in-market pilot

Design and run an in-market pilot in Tasmania (and another location) of the:

- Governing body
- Professional recognition scheme and process
- Business model
- Online tools and resources
- Awareness campaign

Timeframe: Eight months

- Six months in-market
- Two months to iterate and create the scaled solution, ready for phased roll-out

The s47(1)(b) phase two investment is seed funding to create a viable national cyber security professional recognition scheme.

This investment funds:

1. design and development of the professional standards
2. design and development of the recognition scheme, process and governing body (including the business model)
3. the execution of the Tasmanian and other state based in-market pilots

Investing in the next phase of the ACSP program will result in the detailed development and testing of Australian cyber security professional standards, a professional recognition scheme and governing body that will ultimately benefit the whole Australian community. Introducing professional standards will guarantee a minimum level of competence among cyber security professionals, which in turn will enhance the security that businesses, government agencies, and individuals rely on.

Professional standards are designed to protect the community by ensuring that cyber security professionals are well-trained, experienced, competent, and adhere to a code of

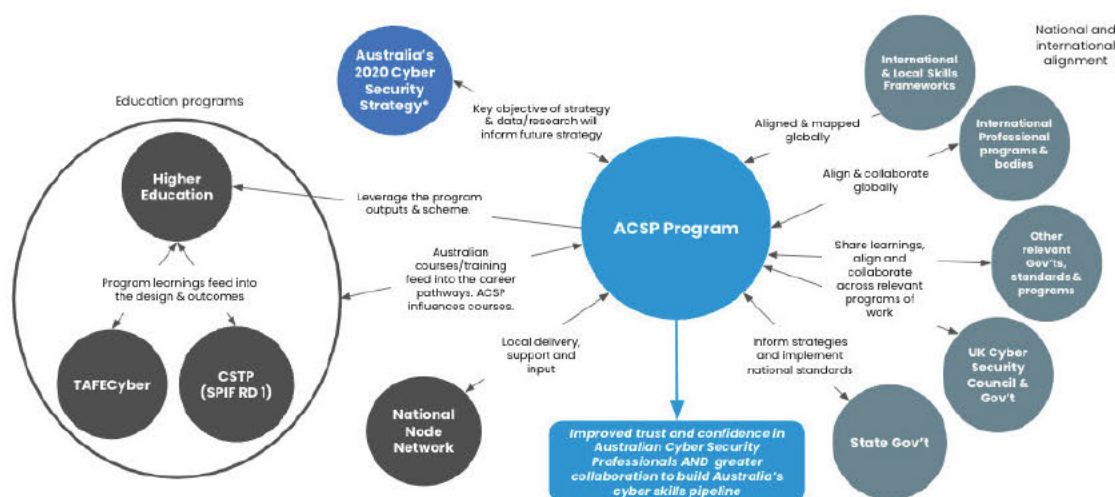
ethics that prioritises safeguarding the public's information and digital assets. This will ultimately foster greater trust in the digital economy, contribute to economic growth, and protect individuals, businesses and institutions from cyber threats.

The establishment of a new sustainable not-for-profit governing body, led by industry and backed by government, will provide the independent oversight needed to ensure the ongoing currency and global alignment of the professional standards and integrity of the professional recognition scheme.

This investment will improve trust and confidence in Australian cyber security professionals globally, ultimately establishing Australia as a world leader in this area. It will strengthen the successful growth and resilience of the sector and contribute to the goal of being the 'most cyber-secure country' in the world by 2030.

ACSP – ecosystem impact & alignment

Key problems: • lack of clear professional standards for cyber security practitioners • the baseline set of skills, competencies, and experience not yet defined • cyber security skills and qualification frameworks not consistent • the industry is currently fragmented



*The 'most cyber-secure country' in the world by 2030
Minister O'Neil, December 2022

1.0 Background

Australia's Cyber Security Strategy 2020 calls attention to the importance of growing a cyber-skilled workforce, where quality training, credentialing and accreditation are all central, including through the creation of new frameworks and processes.

It has been identified that Australia needs more **trusted** and skilled cyber security professionals¹ and for businesses and the community to have **confidence** in the cyber security industry.²

Because Australia still needs to define the baseline set of skills, competencies, and experience required to be recognised as a cyber security professional, there is a need for clear professional standards for cyber security practitioners. In addition, skills and qualifications frameworks currently in use are inconsistent and misaligned between career aspirations, qualifications and labour market outcomes.

As part of the Australian Cyber Security Growth Network (AustCyber) growth centre funding, the Department of Industry, Science and Resources (DISR) agreed that AustCyber should lead a program of work, in collaboration with industry, focused on the development of an accreditation program or scheme for cyber security in Australia. To collaborate effectively and ensure the program was meeting the needs of the sector and broader community, AustCyber implemented a co-design approach to design and deliver the program.

In late 2022 the co-design team and key stakeholders involved in reviewing and validating the program goal, scope and outputs agreed to refine the approach to focus on professional recognition rather than accreditation. This shift was due to a strong concern and view within the sector that 'accreditation' would be mandatory and lead to regulating the cyber security workforce and individuals would require a licence to practice. Regulation would have a significant negative impact on the current workforce and potentially increase the already high skills shortage facing Australia in cyber security.

After extensive consultation, testing and agreement with DISR the Australian Cyber Security Professionalisation (ACSP) Program was established and launched. The ACSP program is focused on the development and implementation of globally aligned professional standards and a professional recognition scheme that will provide existing and future cyber security practitioners with choice and clear career pathways to guide them on their career journey. It will provide clarity and guidance for employers when identifying their cyber security needs and protect the community by ensuring that recognised cyber security professionals are well-trained, experienced, competent, and

¹ *Australia's Cyber Security Strategy 2020 (Clause 20)*

² *Australia's Cyber Security Strategy 2020 (Clause 70)*

adhere to a code of ethics that prioritises safeguarding the public's information and digital assets.

Inline with the original scope of the program existing accreditation systems, schemes and frameworks continue to be part of the scope of this program to ensure, where appropriate, global and local alignment and learnings to support the success of ACSP. .

This report details the approach, outputs and outcomes from phase one of the ACSP Program and the next steps to develop and test in-market the detailed design and implementation of cyber security professional standards, including the establishment of a not-for-profit sustainable governing body and professional recognition scheme.

ACSP Program Goal:

Improve government, business and community trust and confidence in Australian cyber security professionals in order for the ecosystem to continue to grow.

During the first phase of the program, the co-design team led by AustCyber have:

- Designed and developed solutions building on existing work and learnings
- Tested outputs with customer groups to ensure customer input and feedback have guided the overall solution
- Planned the implementation of the solution at scale in the Australian market (including communication with global organisations as relevant)

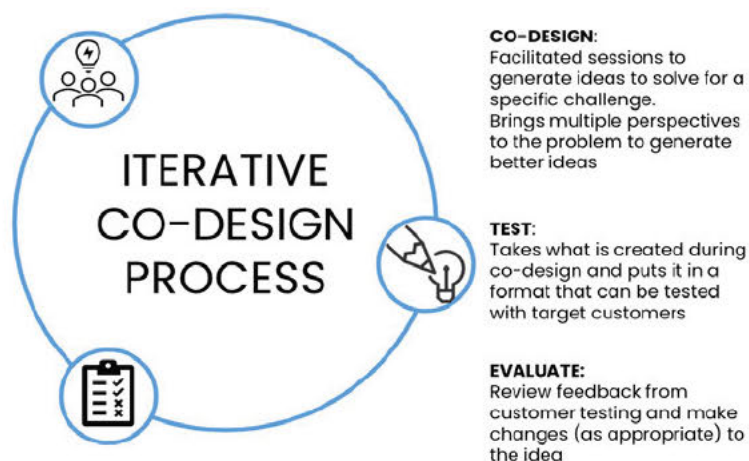
2.0 Phase one overview

A key requirement for this program is that the outputs are industry-led, designed and supported.

To achieve this, AustCyber implemented a co-design process (Figure 1) and brought together Australian and global cyber security leaders and experts to form a co-design team to design the solutions.

Bringing multiple perspectives to the solution and regularly seeking feedback and input from key stakeholder groups, including the people the program is designing solutions for, increases the likelihood of achieving a successful outcome.

Figure 1 - co-design process



2.1 Co-design Team

To ensure the co-design team was truly 'industry-led', AustCyber scanned the sector to identify the leading Australian experts in cyber security; the industry peak bodies that represented the most significant number of employees and employers, and leading academics and international bodies.

The purpose of the co-design team is to design and develop solutions to improve overall trust and confidence in Australian cyber security professionals for the ecosystem to continue to grow. The team focused on the role of career and education pathways, approaches to professional recognition, consistency of role definitions for cyber security in Australia, and alignment with existing frameworks.

The AustCyber-led ACSP phase one co-design team members (Appendix A) comprise industry experts and leaders across a broad range of relevant Australian and global organisations, namely:

- s22

s22

To ensure the success of the program, broader stakeholder input and support have been established with both local and global stakeholders.

Cross-government support and collaborators include:

- Department of Industry, Science & Resources (DISR)
- Department of Home Affairs
- Australian Cyber Security Centre (ACSC)
- Australian Public Service Commission (APSC)
- Department of Employment & Workplace Relations (DEWR)
- Cyber Security Strategy Team
- NSW Government - Investment NSW
- Victorian Government - Cyber Branch
- Tasmanian Government
- Jobs and Skills Australia
- Professional Standards Council

Other collaborators and stakeholders include:

- AustCyber Innovation Network
- Digital Skills Organisation
- Engineers Australia
- UK Cyber Security Council and government
- Australian Women in Security Network (AWSN)
- University sector including: University of Tasmania, Macquarie University, Melbourne University, RMIT, Deakin and ATN
- Lumify Group
- Hudson Group
- Fifth Domain
- Wise Law
- Crest
- Australian Cyber Collaboration Centre
- SFIA

2.2 Phase one plan

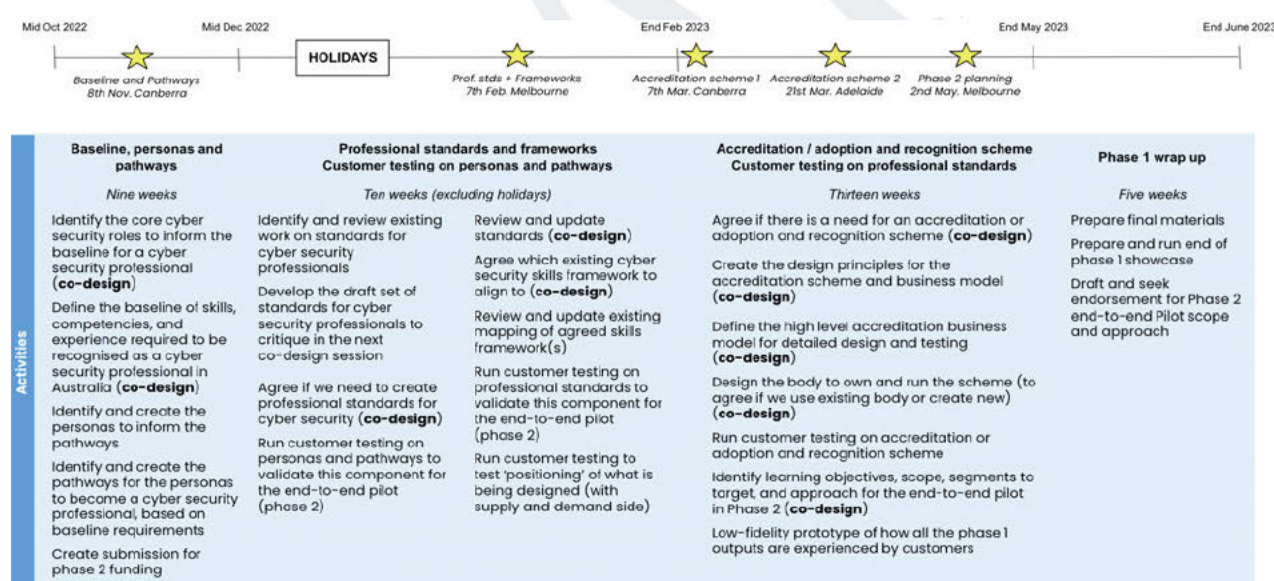
The co-design team was tasked with focusing on the following four key areas during phase one:

- Purpose and Scope
 - Define and align on the purpose, scope and plan for the professionalisation program.
- Baseline and Pathways
 - Design the baseline to be recognised as a Cyber Security Professional, identify personas, roles and map career pathways.
- Professional standards and frameworks
 - Agree on the need and value of professional standards and agree on skills frameworks to align with.
- Professional Recognition Scheme
 - Agree on the need and value of an accreditation or recognition scheme.

2.3 Phase one timeline

The co-design team's program of work was carried out between October 2022 and June 2023. (Figure 2).

Figure 2: Phase one program timeline



2.4 Customer Research

2.4.1 Overview

The co-design team identified the need to understand employees' and employers' current experiences to produce an industry-supported program.

2.4.2 Research approach

Independent qualitative customer research was conducted, which involved 1:1 one-hour interviews with 25 employees and 20 employers. Please refer to Appendix B to review the research data and interview templates.

Employees interviewed:

- Career changers — previously working in a different industry, now in cyber security.
- Existing professionals — working in a cyber security role for the past five years or more.
- New entrants — working in a cyber security role for less than one year after graduating (mix of school leavers and university graduates).
- International workers — moved to Australia within the last five years and are working in a cyber security role. They were already working in cyber security in their home country.

Employers interviewed:

- Non-technology-focused small to medium enterprises (SMEs)
- Technology focused SMEs
- Corporates

2.4.3 Key findings

- Both employers and employees place a **high degree of value on experience** working in the industry.
- Therefore, when they think of someone operating at the next level, a professional, they want to see a **professional standard that includes relevant experience** working in cyber security.
- Employees are **drowning in the choice** of how they learn about cyber security; this was explicitly called out when talking about certifications.
- Those in the know, people who have been working in the industry for a while, have pieced together their version of **criteria regarding what certifications they recommend** to their teams or look for when hiring people.
- Feedback suggested that there is **no shortage of certifications, and degrees, that aren't worth the paper they are printed on**, either because they can be gamed by buying 'brain dumps' online or don't teach you what you need to know to work.
- They see **value in a single source of truth on what is valid** and **having these validated ones called out in a pathway** to becoming a professional.
- Across the employees and employers interviewed, there was a strong theme for **creating a new body to administer professional standards**.
- A **government-backed, industry-supported body was preferred**. Employees expressed that this felt like the right balance as **government backing provided validity**, but not being government-run mitigated the risk of red tape, slowness, and bureaucracy.
- When asked which government department made sense, the **ACSC was referred to as the most relevant** due to its focus, and many employees read and listen to the content they put out around cyber security.

- **Industry-led was called out as the speed and voice** needed to keep the administration current.
- Employees suggested that having a **diverse group of industry representatives as part of this body** would bring the balance needed to ensure the industry's continued growth.
- When employers were interviewed, including AIIA and Tech Council members, they understood **this was not about licensing** but about recognition as a professional; they saw the value for themselves and the industry and were supportive.
- **Recruitment** was a key theme: making hiring easier and having better trust in who is hired and their capabilities.
- However, if there is a professional recognition scheme, it needs to be **flexible and inclusive, not create a barrier to entry**. It must showcase what each individual brings and not lock people into a traditional model where the only pathway is via formal education.
- It is down to the **individual to demonstrate professional qualities**.
- **People outside the cyber security industry would benefit from having some form of professionalisation** to help them know whom they are hiring or what to look for.

Summarising:

What was learnt from speaking to employees and employers that a professionalisation scheme is not only desirable but essential to the sector. This research validated that professionalisation at its core solves for the trust and confidence challenge we currently face in the sector.

The faster we act on testing and implementing the scheme the sooner we can increase trust and confidence in professionals working in the sector.

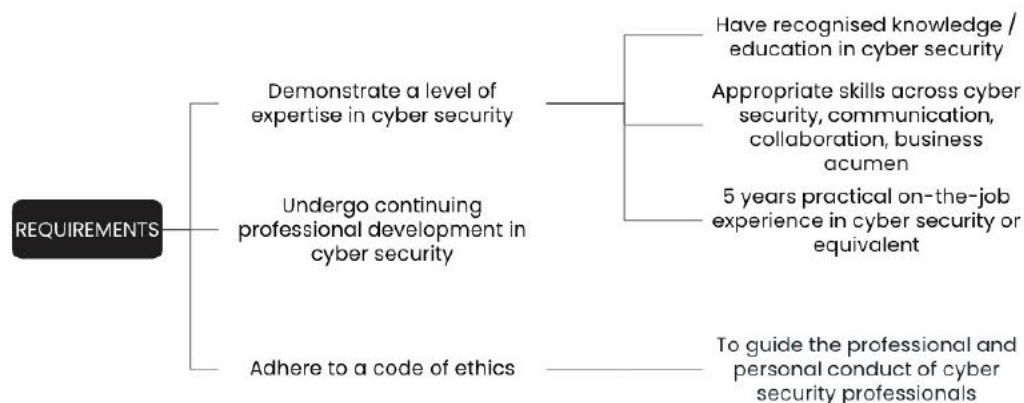
2.5 Phase one outputs

The outcomes from phase one inform the next phase of the ACSP program. Therefore, the co-design team has developed the following outputs.

2.5.1 Baseline requirements and professional standards

The co-design team have agreed on the need and value of professional standards. As a result, the team has designed the high-level requirements to be recognised as a cyber security professional (Figure 3) that will form the basis for developing the professional standards in phase two. These requirements have been tested with end users via customer research and the broader key stakeholders.

Figure 3: The high level requirements to be recognised as a cyber security professional



2.5.2 Employee personas

The co-design team identified the need to understand the current experience and needs of employees and employers to design solutions for these two groups of users. It was agreed that there were four discrete employee personas (Figure 4) and three employer personas to research and develop (Figure 5).

Figure 4: The four employee personas

Four employee personas

Existing professional



My title doesn't expressly link to Cyber Security. But I was doing cyber security work before it was (sexy) called cyber security.

Career changer



As a career changer, I wouldn't consider myself a professional yet – I need to build up my cyber security specific experience.

New entrant



Give me clarity on pathways so I can invest my time and money wisely.

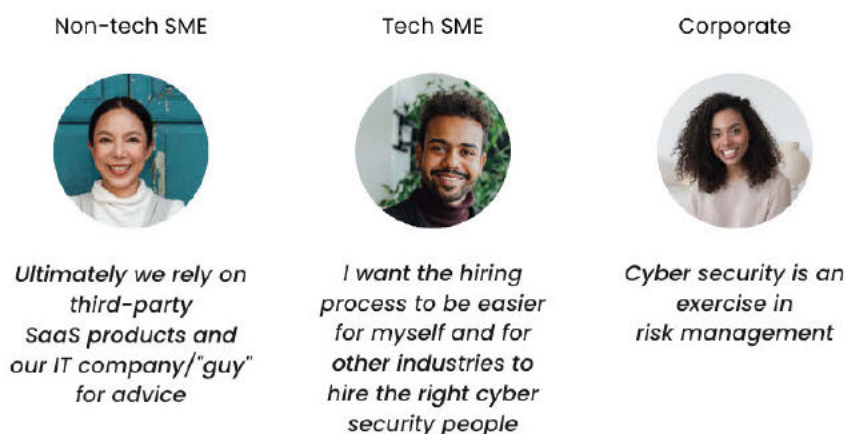
International worker



To increase migration to Australia, you want to have something that can at least be interoperable with other countries.

Figure 5: The three employer personas

Three employer personas



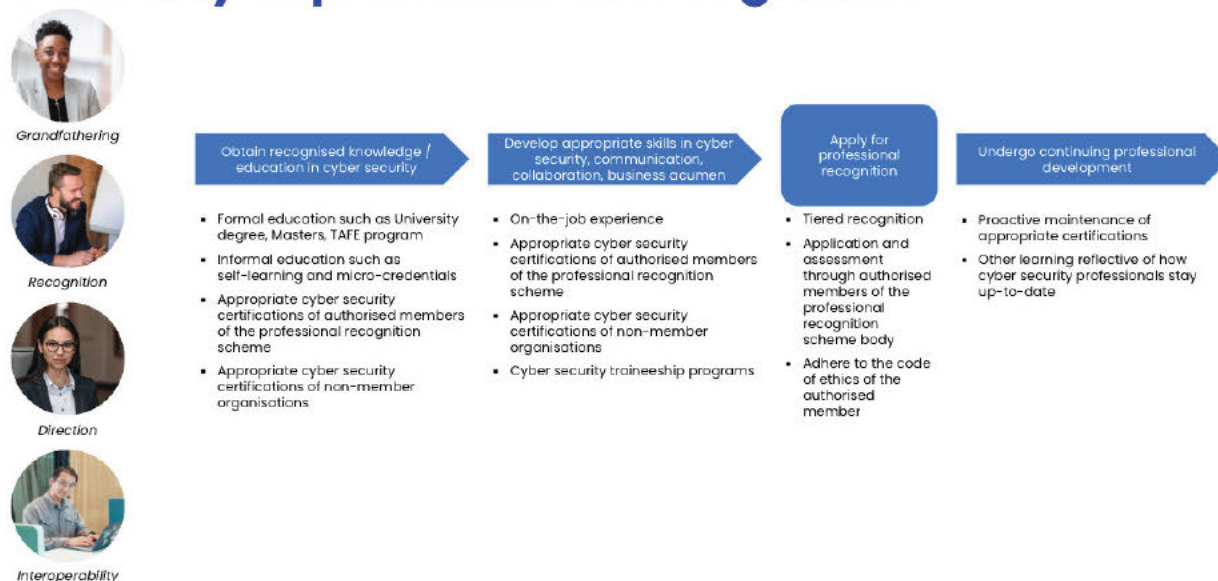
We conducted comprehensive qualitative customer research to develop the personas. Please refer to Appendix C to review the detailed personas.

2.5.3 Pathway to professional recognition

A high-level pathway to professional recognition has been designed based on the baseline requirements to be recognised as a cyber security professional and the four employee personas (Figure 6). This high-level pathway will guide the detailed design of the professional recognition processes and experience developed under phase two.

Figure 6: High-level pathway to professional recognition

Pathway to professional recognition



2.5.4 Skills Frameworks

To create consistency and global alignment, the co-design team have reviewed and considered existing cyber security skills frameworks to align with or include. Each skills

framework was reviewed in the context of its currency, relevance, purpose and global usage. As a result, the team agreed to include three core skills frameworks (Figure 7), use other current frameworks as resources to reference (Figure 8) and reframe the inclusion of ANZSCO–Australian and New Zealand Standard Classification of Occupations (Figure 9).

Figure 7: Cyber security skills frameworks to include

Skills framework	Why it is included	How it will be included
CIISEC	Helps us align with the UK to improve pathways	Mapped to SFIA + NICE
SFIA	- Expressed using clear language - There is opportunity to feed into new versions	Express in terms of SFIA as a language rather than a set of definitions
NICE	- Allows alignment with the US - Already used by ASD	Refer to but not the primary or sole framework as it is extremely complex

Figure 8: Resources to be used

Resource	Why it is being used as a resource	How it will be used
ASD cyber skills framework	- Considerable government investment and buy-in to this framework - Including it helps this work integrate with government	Use the learning of how they mapped NICE + SFIA
European Cyber Security Skills Framework (ECSSF)	- Strong point of reference regarding governance - Not used as a skills framework due to cultural differences with Europe	Informs detail regarding governance
CyBOK	- So that we have a reference point for relevant cyber security knowledge - Creates another link to the UK to enhance interoperability	As a point of reference for knowledge + education

Figure 9: To be reframed

Resource	Why we are reframing its usage	How it will be used
ANZSCO	- Not relevant for this context. - The classifications are used by government and industry, important they are up-to-date with correct cyber security data	- Help amplify ANZSCO. - Feed into it to improve it as it relates to cyber security occupations

2.5.5 Professional recognition scheme

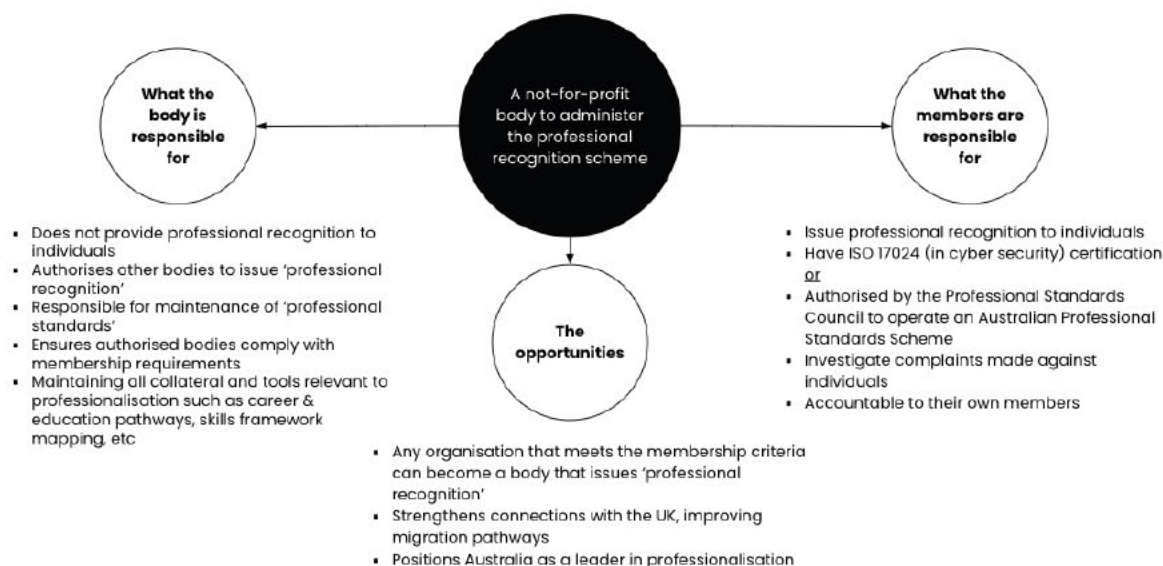
The co-design team has agreed to the need and value of a professional recognition scheme to implement the professional standards and recognition process.

A similar program of work has been designed and is currently being piloted in the United Kingdom (UK), which the UK Government supports. The UK Cyber Security Chartered scheme is governed by the recently formed UK Cyber Security Council (Council) and has been in development for approximately two years. The UK Government and Council have openly shared their business model, scheme and learnings.

The co-design team has agreed it would be valuable to consider aligning, where possible, with other similar professionalisation and accreditation schemes globally to enhance the global relevance and interoperability of Australian professional standards. With this in

mind, the team has initially drawn on the UK experience to design a high-level 'strawman' structure for a similar governing body in Australia to oversee and implement the professional recognition scheme for further review and discussion (Figure 10).

Figure 10: Strawman of the governing body



The governing body would be a new independent not-for-profit entity ideally managed by industry and supported by the government. The team has agreed that the body and scheme must be sustainable for its ongoing viability beyond initial establishment and have identified some possible revenue and business opportunities to develop further and test in phase two.

2.5.5 Design Principles

The team has developed and agreed on the following seven design principles (Figure 11) that will guide the overall detailed design of the professional standards and scheme in the next phase.

Figure 11: Design principles

Design principles

Customer-centered

Designed with the needs and perspectives of mid / experienced practitioners, employers, government, industry, academia in mind. This includes consideration for their diverse backgrounds, experience levels, and career goals.

Continuously improving

The scheme should be regularly reviewed and updated (based on clear measures of success) to ensure it remains relevant, effective, and responsive to changes in the cyber security context. Key stakeholders should have input and influence.

Simple

The scheme should be straightforward to understand and should simplify stakeholders understanding of why you want to become a professional.

Objective

The professional recognition process should be unbiased and objective (vendor agnostic), using valid and reliable assessment methods that are measurable and tangible. It should recognise different types of professionals.

Flexible

Allow for different pathways and entry points to professionalisation by recognising a range of qualifications and experiences, not create barriers to entry, be relevant to current and emerging cyber security threats and technologies, and the needs of the workforce.

Transparent

The professional standards, and the process for professional recognition should be clearly communicated and easily understood by all stakeholders.

Collaborative

The co-design team should engage with stakeholders from industry, government, academia, and the wider community to ensure an appropriate and inclusive design process. Aligned to international partners schemes.

3.0 Next Steps

The ACSP co-design team has established strong local and international relationships and built solid momentum on this program of work. However, to capitalise on this and enable Australia to accelerate the professionalisation of its cyber security workforce, funding and support must be secured for the next development phase, minimising any time delay between phases one and two.

The co-team and stakeholders from phase one are committed to continuing their support and input in phase two, however as the program moves into the next phase of detailed design and testing there are some strategic changes to the co-design team and new key stakeholders becoming more involved.

The co-design team established to drive the next phase of the program include:

- s22

Additional key stakeholders engaged to date to assist with specific aspects of the next phase include:

- Australian Cyber Security Centre (ACSC)
- Australian Women in Security Network (AWSN)
- Tasmanian Government
- Investment NSW
- Victorian Government - Cyber branch
- Key Australian universities
- Global skills/competency frameworks including: SFIA, NICE, CIISEC
- International professional bodies including: (ISC)², ISACA, Crest, CompTIA

The overview of the next phase of development and funding required is detailed below.

3.1 Phase two overview

It is proposed that ACSP phase two will be a continuation of phase one (Figure 12), with AustCyber continuing to lead the program of work in collaboration with the already established ACSP co-design team, collaborators and stakeholders.

Figure 12: Phase two overview

ACSP – Phase two

s47(1)(b)

Detailed development of the scheme

Draft professional standards in detail:

- Code of ethics
- CPD model
- Recognised knowledge and education (including certification mapping)
- Qualifying criteria for on-the-job experience
- Assessment process

Establish the governing body, professional recognition scheme and business model

Timeframe: Six months

Test the scheme via an in-market pilot

Design and run an in-market pilot in Tasmania (and another location) of the:

- Governing body
- Professional recognition scheme and process
- Business model
- Online tools and resources
- Awareness campaign

Timeframe: Eight months

- Six months in-market
- Two months to iterate and create the scaled solution, ready for phased roll-out

As highlighted in figure 12, phase two will focus on the detailed design, development and in-market testing of all the components of the professional standards, the professional recognition scheme and assessment process, the governing body and the business model for ongoing sustainability.

To support the successful detailed design and development work the following stakeholders have committed to contributing their expertise and resourcing to date:

- Australian Computer Society (ACS)
- Engineers Australia
- Professional Standards Council of Australia
- (ISC)²
- ISACA
- Crest
- SFIA
- Australian Public Service Commission (APSC)
- Jobs and Skills Australia
- Digital Skills Organisation
- UK Cyber Security Council and UK government
- Lumify Group
- Fifth Domain
- Select Australian universities

To support an in-market pilot, Tasmania has indicated their strong desire to be one of the locations selected to run a pilot. On 26th May 2023 the Australian Computer Society (ACS) ran a *Building Tasmania's Cyber Security Professionalism* event in Hobart. This event, supported by the Tasmanian Government, attracted over 50 leaders in Tasmania across cyber security, banking, TAFE, and higher education (University of Tasmania). The event included a keynote speech from s22 AustCyber, to provide an overview of the ACSP Program, an ACSP co-design team panel discussion facilitated by s22, Department Premier and Cabinet (TAS) including s22 (ACS), and s22 (ISC)², and a facilitated workshop over lunch where participants generated ideas on how they might contribute to the success of a Tasmanian pilot of the ACSP program. This event generated over 50 ideas as well as strong engagement and buy-in to both the ACSP program and AustCyber's role as the nodal player bringing the sector together to solve national challenges.

The following stakeholders have committed to supporting an in-market pilot in Tasmania:

- Tasmanian Government
- University of Tasmania
- Australian Computer Society (ACS)
- Australian Women in Security Network (AWSN)
- TasTAFE
- Leading Tasmanian businesses

The s47(1)(b) phase two investment is seed funding to create a viable national cyber security professional recognition scheme.

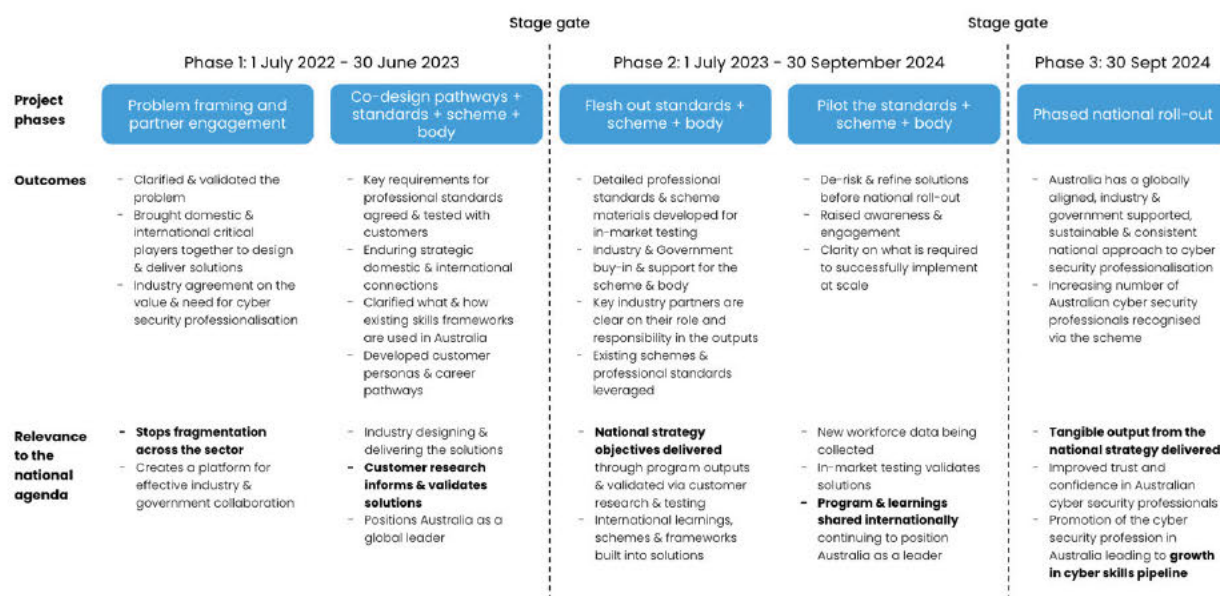
This investment funds:

4. design and development of the professional standards
5. design and development of the recognition scheme, process and governing body (including the business model)
6. the execution of the Tasmanian and other state based in-market pilots

3.2 Proposed timeline

The table below outlines the proposed timeline of ACSP program deliverables from the design phase through to the national roll-out of an Australian cyber security professionalisation scheme, assuming phase two receives financial support to begin 1 July 2023. (Figure 13).

Figure 13: Proposed timeline



3.3 Phase two outputs

- Detailed design and development of:
 - professional standards and associated collateral,
 - professional recognition scheme and process,
 - governing body business structure and model.
- Establish the business structure, including terms of reference, membership structure and financial model for ongoing sustainability.
- An end-to-end pilot of the business model and professional recognition scheme and process (conducted in Tasmania and other locations to be determined), including:
 - an interactive digital career pathway tool
 - personas, created in phase one, brought to life as online case studies
 - recognised list of credentials and education that form part of the pathways to be recognised as a cyber security professional
 - interactive skills framework map/matrix that supports the career pathway tool
 - professional standards, code of ethics, guidelines etc
 - innovative CPD requirements
- A phased national implementation roadmap.

3.4 Phase two plan and funding requirements

3.4.1 Detailed development

- Develop the professional standards and recognition process in detail, including:
 - Code of ethics
 - CPD model and requirements
 - Recognised knowledge and education (including certification mapping)

- Qualifying criteria for on-the-job experience
- Assessment process
- Establish the business model, including the governing body, the professional recognition scheme and the financial model

s47(1)(b)

3.4.2 Test the scheme via in-market pilot

Design and execute an in-market pilot of the body, scheme and business model in Tasmania (and other locations to be determined).

Timeframe: Eight months

- Six months in-market
- Two months to iterate and create the scaled solution, ready for phased national roll-out

s47(1)(b)

The collaborative co-design team, comprising experts and leaders from various fields, has effectively united to accomplish the program's phase one objectives. By leveraging their collective knowledge, experience, and networks, they have successfully:

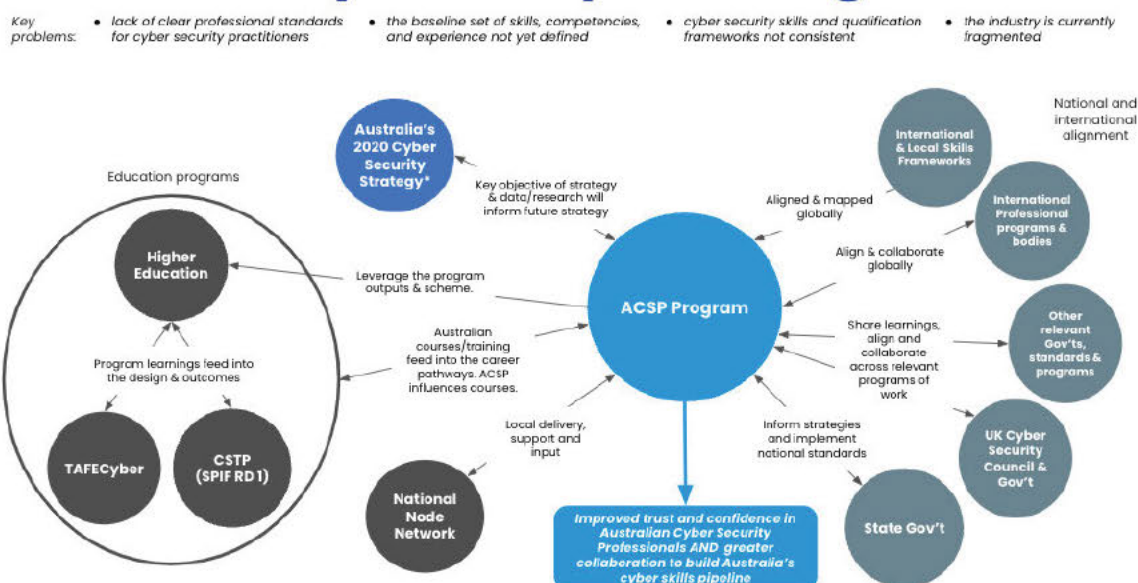
- Designed the high-level requirements to be recognised as a cyber security professional in Australia that will inform the development of professional standards,
- Conducted customer research to create customer personas and pathways understand the current employee and employer experiences and needs, and gain feedback and buy-in to the professionalisation of the Australian cyber security sector,
- Agreed on the relevant skills frameworks to include and reference,

- Designed the high-level business structure and model to implement an Australian professional recognition scheme,
- Agreed on the design principles to guide the development of the scheme, and
- Secured support and commitment from a broad range of key stakeholders and collaborators to develop and execute the next phase of the program.

The ACSP program is integral to Australia's broader cyber security agenda, as demonstrated in Figure 14. The introduction of an Australian cyber security professional recognition scheme not only builds trust and confidence in the Australian cyber security workforce but will be central to establishing Australia as a world leader, strengthening the successful growth and resilience of the sector, and the goal to be the 'most cyber-secure country' in the world by 2030.

Figure 14: ACSP ecosystem and alignment

ACSP – ecosystem impact & alignment



*The 'most cyber-secure country' in the world by 2030
 Minister O'Neill, December 2022

Appendix A

The co-design team members - phase one

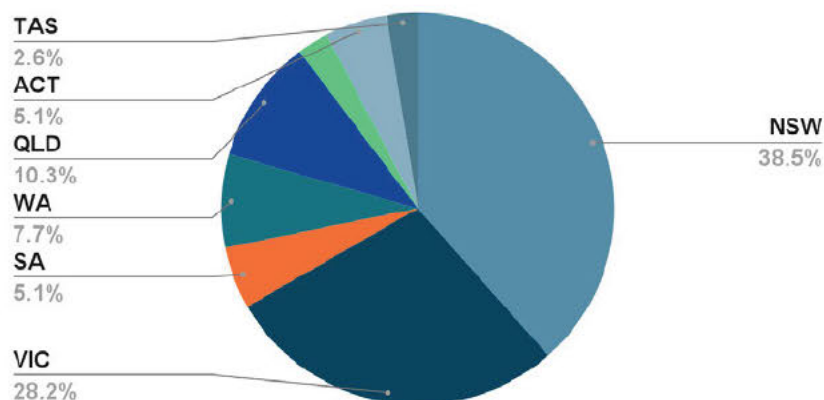
s22



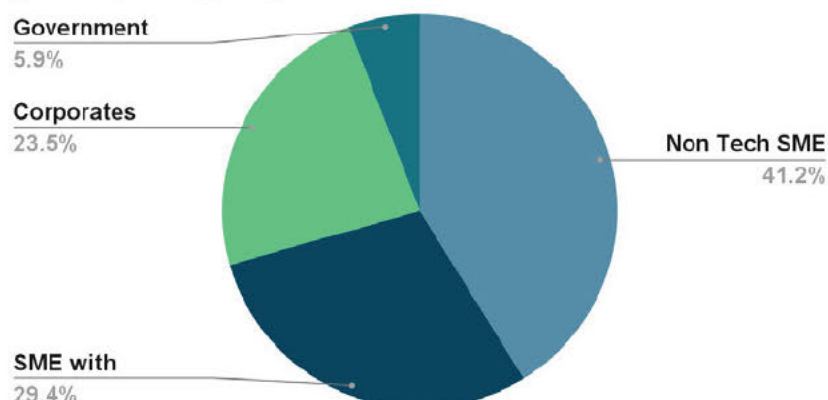
Appendix B

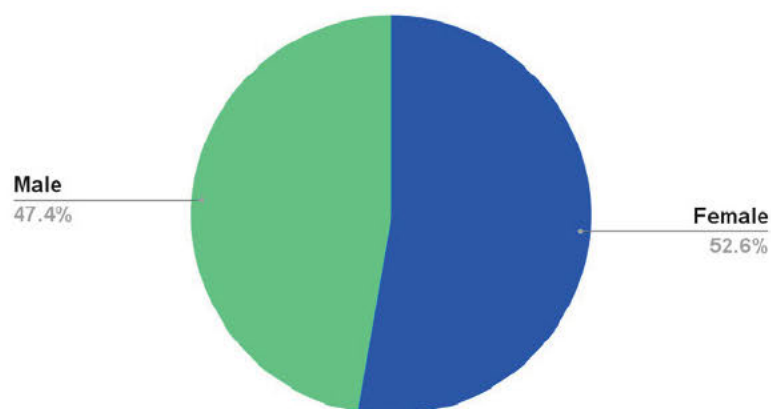
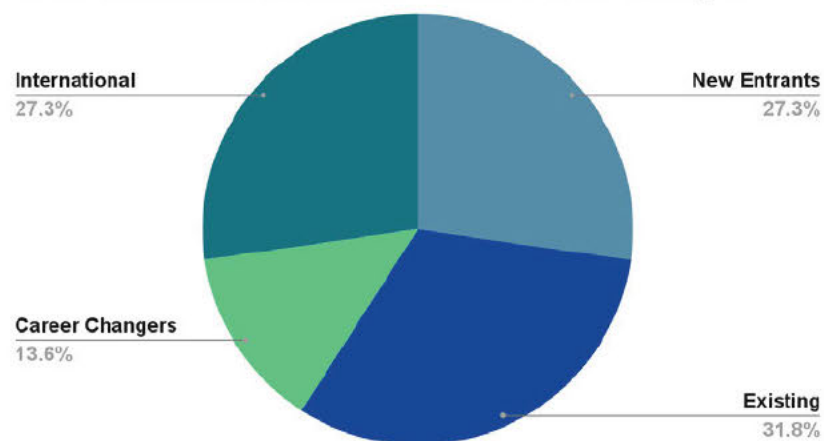
Qualitative research data

Nearly half of the research participants were from NSW.



Non Tech SMEs Employers were our biggest participant group.



We interviewed more females than males.**We found it most difficult to source Career Changers**

Interview templates for employees and employers

<Name> interview: <DATE>

EXISTING PROFESSIONAL/ NEW ENTRANT/ INTERNATIONAL WORKER/ CAREER CHANGER

Interviewee: <Name>

Timing: 60 minutes

Interviewers: <Name>

Background:

Role:

How employees feel about the idea of formalising what it means to be a cyber security professional

- 1 How do you describe what a cyber security professional is?
- 2 Would you define everyone currently working in the industry as a cyber security professional?
- 3 We are trying to work out how to create nationally consistent requirements for people to be recognised as a cyber security professional.
- 4 From an industry perspective what do you see as the benefits of creating these nationally consistent requirements?

What they think the requirements to be considered a cyber security professional are

- 1 What is your current job title, 'why do you feel this implies you are working in cyber security'?
- 2 For someone to be nationally recognised as a cyber security professional what do you think some of these requirements should be?
- 3 What is your view on the order of priority for these requirements?
- 4 Is there anything you think should absolutely not be a requirement?
- 5 What challenges might exist in meeting these requirements?
- 6 Please provide feedback on the co-design teams requirements
- 7 Who would you expect to get the professional recognition from?

What employees need to become a cyber security professional / what would make it desirable

- 1 What would stop you becoming recognised as a cyber security professional?
- 2 What would make you want to become a cyber security professional?
- 3 To meet the requirements we described before what would make it easier for you to meet them?
- 4 If you became a professional what benefits would you expect to get?
- 5 Describe what you think the pathway to becoming a professional would be

Approaches to continuous Professional development

- 1 Do you currently do any?
- 2 What do you like / don't like about it?
- 3 How would you make CPD better?

Examples of good codes of ethics

- 1 Do you currently adhere to / have signed up to any code of ethics?
- 2 What is the value of having a code of ethics for cyber security professionals to adhere to?
- 3 What do you think should be in the code?

<NAME> interview: <DATE>

NON TECH SME/ TECH SME/ CORPORATE/ GOVERNMENT

Interviewee: <NAME>**Timing:** 60 minutes**Interviewers:** <NAME>**Background****Role:****What the current experience is for employers when hiring a cyber security employee or consultant**

1 How do you currently get help with cyber security for your company?

2 Why do you get help that way?

3 Have you hired someone to look after your cyber security?

4 Tell me about the experience hiring them

4.1 What was good about this experience?

4.2 What was bad about this experience?

4.3 What would improve your confidence in this experience?

5 Why did you choose that person / provider?

6 Does your business have a need for a cyber security professional vs an entry level worker?

6.1 Why do you need this?

What they think the requirements to be considered a cyber security professional are

1 When hiring someone that calls themselves a cyber security professional what improves your confidence in them?

2 When hiring someone that calls themselves a cyber security professional what decreases your confidence in them?

3 What is the difference between a new entrant to someone calling themselves a cyber security professional?

3.1 Do you feel we need to define the difference between these?

3.2 What are the risks if we don't define the differences?

4 Read these proposed requirements to be considered a cyber security professional

4.1 If someone had met these requirements what does that do to your trust and confidence in them as cyber security professional?

4.2 Why or why not does this change your trust and confidence in them?

4.3 Would you add or remove any of these requirements?

What they would place their trust in

1 If someone classified themselves as a cyber security professional, how would you validate this?

2 Is there an organisation or body you feel that should validate if someone has met these requirements?

3 What would give you confidence or make you trust this organisation or body?

Appendix C

Employee Personas

Existing professional

Recognise where I am already meeting these professional standards/requirements



My title doesn't expressly link to Cyber Security. But I was doing cyber security work before it was (sexy) called cyber security.

Photo by Emmy E from Pixels

About me

I have been working in the cyber security sector for a number of years and more often than not I come from an IT or software engineering background (of which I have worked in for years).

The most significant learning for me has come from working on-the-job.

If I've done certifications I have been selective on which ones as I know which are relevant for my work and career progress, and those that aren't worth the paper they are printed on.

How I define a cyber security professional

A cyber security professional is someone that has a holistic understanding (people, process, technology) of what cyber security is, its risks and impacts to individuals and organisations.

Technology is important for a cyber security professional to understand but the level of technical application is dependent on their role.

MY CHALLENGE

I am already here

I've been in the industry for 20 years, I have the experience, and my peers already recognise me.

Now I don't think I would jump into it. Because I think I've already made my mark in the company that I want to work in. So I'm recognised and I don't think I have a need to prove with an external certificate like that.

The industry is changing and moving fast

If I'm not on top of the constant changes in the industry I run the risk of not being up to date for my role.

It's not a one size fits all

The industry is maturing, we need to recognise the broader range of skills required to perform the diverse job roles.

There's all these niche areas. There's so many different spaces, and they are all very different job roles, and they're speaking to different people.

MY NEEDS

Recognise where I am already meeting these professional standards.

Allow me to include experience I have gained through years working in roles relevant to cyber security.

Reduce the noise. Create a one-stop-shop for information and standards that is governed by an organisation I trust and value.

Understand that rigid pathways don't work in Cyber Security.

Acknowledge there are a wide variety of jobs, with many relevant pathways for people to be recognised.

The journey is not the same for anyone and I don't think it should be a set journey to be a professional.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

Professionalisation acknowledges and formalises the ecosystem that is cyber security.

If the standards I am already meeting can be used for my recognition.

The professional standards need to be more than words on-a-page or boxes to tick. They need to be upheld so that we lift the quality of the sector.

It needs to recognise the non-traditional ways I learn about cyber security.

Provide clarity on what the quality certifications / qualifications are.

By providing official pathways for my continued growth and development and ensuring that these pathways cater for the diversity we want in the sector. It needs to value on-the-job experience / training as much if not more than education.

Career Changer

Recognise what I bring to the sector and guide me on where to focus my time and effort



As a career changer, I wouldn't consider myself a professional yet - I need to build up my cyber security specific experience.

Photo by Anna Shweta from Pixels

About me

I have a background (and hold some qualifications) in another industry, so I have the soft skills and a basic knowledge of cyber that allows me to enter the industry. I moved into cyber security because external (and internal) pressures led me to it. I've always been interested in IT and technology and cyber security is a growing industry with many career opportunities.

How I define a cyber security professional

A cyber security professional has been in the industry for a while - they know more. They should be able to identify the risks and protect the company or any organisation. They can identify, protect, and detect. They can respond to the incident and develop something to reduce the impacts of the events, and then finally, they can help the company to recover.

MY CHALLENGE

I don't have peer recognition

I'm new in the industry and need to build credibility amongst my peers.

I think just the recognition to be accredited would be enough for me. You know it should be like an industry currency that not just everyone can have access to, so the recognition alone from that would be valuable.

My background isn't in IT

You don't need to spend years learning IT technical skills but I think it's important to understand the basics of it.

I know people who've moved into GRC from having a technical background have found it a lot easier. Because they already have that foundational knowledge - especially people who come from IT backgrounds or have worked in other technical roles.

It's hard to keep up

It's hard to keep up with the latest skills - once I finish a course or learn a new technique the landscape of the industry has already changed, it's so hard to keep up.

MY NEEDS

I need some sort of currency within the industry.

I need to understand the key principles that underlie how cyber security works, and how organisations can use those principles.

I need to tailor my training and learning to my area of specialisation while still gaining varied experience.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

A tiered model approach would provide incentive for someone like me with less experience, I could achieve it in the next couple of years.

If I can count what I am already paying for that directly relates to achieving this (I can't sign up to it of them).

Clear guidelines and requirements as to what makes a cyber professional.

Be clear on what the requirements are for me. If I want to be there, I need to do this, this and this. Just be clear, so I know what I have to do.

There is a pathway that includes hands-on experience and doesn't mandate a university degree.

Make the pathways clear and recognise the various entry points and relevance of different skills.

I don't think it's purely having technical skills because a lot of people have technical skills, but then they lack a lot of soft skills.

New Entrant

There isn't a clear pathway for me to get in and be successful in the sector. I need direction on what choices to make



Give me clarity on pathways so I can invest my time and money wisely.

Photo by Pavel Daniyuk from Pixels

About me

I have recently entered the industry after moving away from my previous role. I got a certification in IT or Cyber Security to help me break into the industry. I have little to no on-the-job cyber security experience so I have been placed in an entry-level role. The most important thing for me is to get the hands-on experience so I can progress in my career, and be recognised as valuable in my role.

How I define a cyber security professional

A cyber security professional is someone who has had years of experience in the industry, and has the knowledge/theory to back them. They have a foundation in IT and demonstrate 'professional' skills.

MY CHALLENGE		
Entry level jobs require experience How can I gain industry experience, when employers are asking for 1-2 years experience for entry level roles? <i>There's very limited entry level jobs, and if so they want 1-2 years experience.</i>	I don't know what certifications are valuable Am I wasting my time and money on something that won't get me employed? There isn't a clear pathway to help me decide on which one to do. <i>I have studied 16 certifications and maybe two were effective.</i>	The pathways are unclear I struggle to understand and describe what a professional is, because there is a lack of clarity on how to get there.
MY NEEDS		
Tell me where the best place to start is and what I need to do to get in there.	Show me what certifications are valuable, so that I spend my time and cash on something that is credible. <i>Companies out there aren't looking at what degree you have studied, they are only looking at certifications, or ask for previous experience (2 years) in similar industry.</i>	Help me understand what a professional is to give me a goal to work towards. <i>I don't think I have enough experience to understand what the requirements of a professional should be.</i>
WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME		
Tells me what employers value and where I can look for a job. Pathways that recognise all my relevant hands on experience, not just experience after I've finished my graduate program/role. <i>I would have spent 4 years studying then 5 years in the industry. 9 years is a long time to be recognised. If you do it parallel then it works.</i>	Guidance on potential pathways, and helping me understand how to work my way up in my career. It doesn't require me to pay for another annual fee/ membership.	A tiered approach to professionalisation so I gain recognition at multiple stages of my career. <i>If we do a tiered level of experience: Junior 1-2 years, Mid 3 years, CSO level 10 years.</i>

International worker

Ensure my international certifications and skills are recognised in Australia



To increase migration to Australia, you want to have something that can at least be interoperable with other countries.

Photo by Kindel Media from Pixels

About me

I migrated to Sydney last year from <country> for opportunities in cyber security. Before I migrated to Australia, I worked in <country> for more than five years. I have, at a minimum, a bachelor's degree and multiple certifications, and I often have come in via the Global Talent Program visa.

How I define a cyber security professional

For someone to be considered a professional, they need proven work experience. When I worked in <country>, there were guidelines from a governing body of what a cyber professional is, including a reference framework to show the level of experience a professional has and their progress. It also has interoperability with certifications in other parts of the world.

MY CHALLENGE	
Having to do things twice I've done that [background check] as part of my visa entrance process, so I should not have to do it again. <i>If it means I have to do extra, extra training, or I have to undergo exams in order to do this, then I'd have to weigh up the value. I probably wouldn't do it.</i>	There is no interoperability with Australia ISACA, (ISC)2 etc, are recognised internationally but have yet to be applied under a nationally consistent approach in Australia. <i>If we put a national requirement, it shouldn't be limited only to Australian nationals. I think you need to consider the international workforce and how they may contribute to the Australian sector.</i>
MY NEEDS	
Recognise where I've met requirements with my (international) experience. <i>To make the transition seamless, is there a way where we recognise that your clearance, integrity, qualification, and certifications in your home country... when you come to Australia, you don't necessarily have to start again. You can say, well actually, I've already met all of them. So, therefore, I can then be recognised.</i>	Global recognition. <i>I guess that is a great way to attract the interoperability of the professional - from both sides.</i>
WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME	
A framework that substantiates my integrity as a cyber security professional (when I've already been subject to a police or background check).	Plug into what I already have. <i>If there was a way to plug in recognised certifications and the work you have to do to get them. Therefore if you could plug what you are already doing there and it is acknowledged by the Australian accreditation program that would make the process easier.</i>

Employer Personas

Non-technical SMEs

I've just taken the IT "guy" on through word-of-mouth



Ultimately we rely on third-party SaaS products and our IT company/"guy" for advice

Photo by Katar Kubicki from Pexels

About me

As a small business owner with up to 10-20 employees, cyber security is not a priority for my non-technology-focused business.

We mainly use third-party SaaS products to hold customer data and don't have much data at risk. So while I'm concerned about hacking, system corruption, and scams, we can manage these risks without hiring a dedicated cyber security person.

We rely on our IT company, who I found via word of mouth, for advice. In addition, we have a cyber security insurance to cover any potential risks.

MY CHALLENGE

I don't understand IT so I put my trust in my IT company/"guy"

We hired our IT company/"guy" through word-of-mouth - he was recommended by another small business owner. And he seemed to know what he was doing.

The less you know about the topic, the more the recommendations mean

MY NEEDS

To trust the IT professional I have hired to perform the required tasks based on objective criteria so that I am not reliant only on word-of-mouth recommendations.

I'm not even sure what to look for in an IT professional - it's usually from a word-of-mouth recommendation. There is nowhere to validate that what has been done is correct - except potentially word of mouth case studies.

Finding and selecting the right professional for my needs

It's hard to know what to look for when selecting an IT and cyber security professional. I'm not clear on the specific skills and qualifications required.

Guidance on what to look for in an IT and cyber security professional for my specific needs - the qualifications and credentials I should be looking for.

Knowing where to look for trustworthy IT professionals in a specific field such as cybersecurity.

It's hard to keep up when it's not my focus

It's hard to stay on top of the constantly evolving requirements for IT and now with the addition of cyber security, especially when I am a small organisation with limited resources.

I think with IT in smaller businesses, there's a lot of trust you're putting in that individual because you're time poor. And it's not always necessary or clever to me personally, I don't set up a business to focus on IT but it is part of the

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

Having a reliable and objective method for evaluating the quality of work done by the IT professional, particularly for when companies have no expertise in the area.

Assurance that the IT professional is current and complies with protocols and processes applied to my IT - particularly for my insurance.

Access to a diverse range of resources and networks, with more experience and knowledge, for seeking advice and recommendations on hiring IT/cyber security professionals, in addition to word-of-mouth referrals.

Easy access to up-to-date and trusted information and guidance on the constantly evolving requirements for cyber security for SMEs.

Knowing what areas of my business require cyber security and what I need to do about it.

...the accounts person had a spreadsheet of every single password of the organisation. And then you start thinking about what who has access to that or not, and suddenly you're not considering cyber security or not.

Tech SMEs

Make it easy for me to hire



I want the hiring process to be easier for myself and for other industries to hire the right cyber security people

Photo by Jovita Robinson from Pexels

About me

I own/work for a cyber security startup, and lead a small team.

My hiring practices come from industry connections and recommended applicants with a strong skill set and who are eager to learn.

There's a skill shortage so I need to make sure the people I hire are able to do what I need them for.

MY CHALLENGE

There is a skills shortage

There is a skills shortage in the industry, which has made the hiring process harder. We rely on recommendations and/or we identify qualities and traits that are suitable to bring this person on and skill them up.

Our hiring practices have commonly been through trusted relationships, you come recommended. It's necessary for a small business, they are critical to your business success.

There is a lack of clarity on what each role entails

This makes it difficult to determine levels of expertise, recognise previous education and experience, and validate skill sets.

MY NEEDS

Easy recognisable roles and skill sets across the industry.

Different organisations require different roles/skill sets. In order to make it easier on employers, roles/skill sets need to be easily recognisable across industry - the job description needs to outline exactly what the business is looking for, so if its risk management then it needs to be in the title.

Guidance on which qualifications and courses are most valuable and applicable to specific roles, perhaps through the development of a career path framework or hiring matrix.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

Validating and accrediting someone's base level skills in the industry if they have experience in another discipline.

Clear and flexible pathways that recognise education and experience levels.

What you want to build into this model is flexibility and the pathways people can take to get to that professional level.

Provide support for employers to help them understand cyber security and validate employee's skills.

Educate employers outside of the industry on cybersecurity roles and the required skill sets to ensure that they hire the right cybersecurity professionals.

Corporate employers

I find hiring really tricky



Cyber security is an exercise in risk management

About me

I am working in a senior role overseeing the cyber security for the entire organisation. This involves international teams as well.

My role requires me to think strategically about the cyber security of the organisation and how to engage effectively with my peers in senior management.

I have a number of employees working for me all who have accountability to keep the organisation cyber secure. They have a mixture of technical and non-technical backgrounds.

MY CHALLENGE

Hiring the right candidate is a challenge

It can be hard to find suitable candidates with the necessary skills and cultural fit. It is difficult to accurately identify the skills required for a role and determine a candidate's experience based on their qualifications alone.

The prime candidates do look different across the spectrum of disciplines

There is no clear end framework for defining consistent standards, qualifications and pathways

One that is inclusive of diverse backgrounds and experiences and provides confidence and structure to employers and employees alike.

The risk is that it is too far off out there, and it means asking people to come into the industry and have more diversity in the industry is important to provide structure and an idea of how people can ramp up their skills

There isn't currently a body that I see as effective, trustworthy, and credible

A model that builds and establishes trust with the right organisational structure

MY NEEDS

Consistency regarding the level and types of (technical) skills required for different roles and disciplines and how to assess candidates accordingly.

Up-to-date and practical cybersecurity education that reflects the fast-changing industry.

The ability to attract and retain diverse talent in the industry by recognising and valuing diversity and non-traditional pathways to success.

The creation of a recognised body that is valuable to cyber security professionals and employers.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

Standardisation of cyber security titles and clarity in the job titles to accurately identify and fill roles, especially in a constantly evolving industry where new roles are constantly emerging.

Ongoing assessment and development of training programs to keep up with the constantly evolving industry.

A trusted body to provide a framework and pathways to success for individuals based on experience, skills, and qualifications where relevant from all backgrounds.

To address shortages and prevent salary increases caused by competition for candidates, an inclusive framework that enables more people to enter the industry.

Photo by Emma's Sharaka from Pexels



AustCyber
Part of the Stone & Chalk Group

Improve trust and confidence in Australia's Cyber Security professionals

PHASE 2: Scope, approach and funding scenarios

15th February 2023

Industry led

Industry co-design team

s22

Government Partners

- DISR
- Home Affairs
- ACSC
- APSC
- DEWR

Other collaborators

- National node network
- Digital skills organisation
- Engineers Australia
- UK Cyber Security Council
- NSW Govt. Cyber Branch

Context

Situation:

Australia's Cyber Security Strategy 2020 calls attention to the importance of growing a cyber skilled workforce, where quality training, credentialing and accreditation are all central, including through the creation of new frameworks and processes:

- Australia needs more **trusted** and skilled cyber security professionals (clause 20)
- Businesses and the community need to have **confidence** in the cyber security industry (clause 70)

The Sector Competitiveness Plan 2020 states: Continuing to regulate cyber security will help to maintain **trust** and **confidence** in Australia's digital infrastructure and businesses (section 3.2)

Complication:

- There is a **lack of clear professional standards for cyber security practitioners** leading to diminished trust and confidence for employers and purchasers when sourcing cyber security capability
- Australia hasn't yet defined **the baseline set of skills, competencies, and experience** required to become a cyber security professional
- There is a lack of agreement around the **cyber security skills and qualification framework** to be used in the Australian context
- **The industry is currently fragmented** with numerous organisations delivering programs of work related to cyber security standards, skills and qualification frameworks

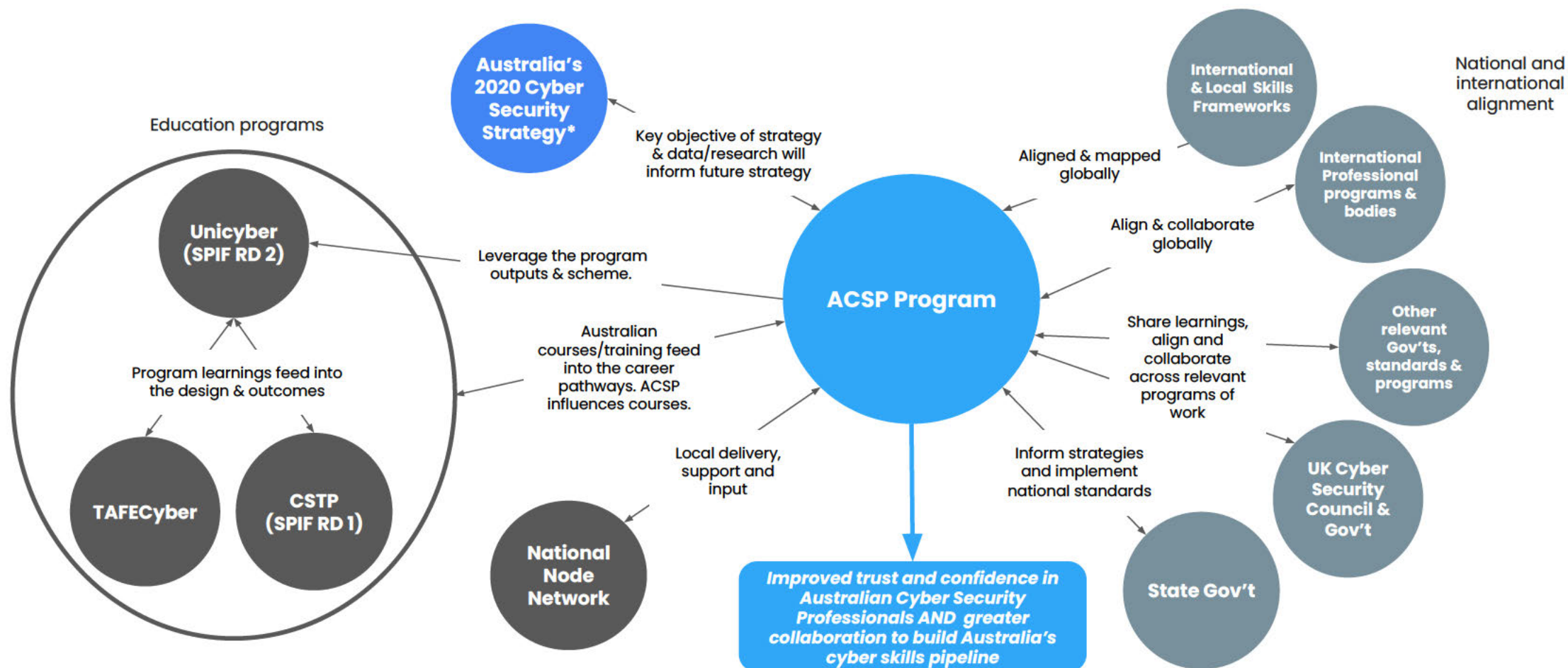
Australian Cyber Security Professionalisation (ACSP) program goal

Improve government, business and community **trust and confidence** in Australian cyber security professionals in order for the ecosystem to continue to grow

ACSP – ecosystem impact & alignment

Key problems:

- lack of clear professional standards for cyber security practitioners
- the baseline set of skills, competencies, and experience not yet defined
- cyber security skills and qualification frameworks not consistent
- the industry is currently fragmented



*The 'most cyber-secure country' in the world by 2030
Minister O'Neil, December 2022

ACSP Program milestones

	Stage gate		Stage gate		
	Phase 1: 1 July 2022 – 30 June 2023		Phase 2: 1 July 2023 – 30 September 2024		Phase 3: 30 Sept 2024
Project phases	Problem framing and partner engagement	Co-design pathways + standards + scheme + body	Flesh out standards + scheme + body	Pilot the standards + scheme + body	Phased national roll-out
Outcomes	- Clarified & validated the problem - Brought domestic & international critical players together to design & deliver solutions - Industry agreement on the value & need for cyber security professionalisation	- Key requirements for professional standards agreed & tested with customers - Enduring strategic domestic & international connections - Clarified what & how existing skills frameworks are used in Australia - Developed customer personas & career pathways	- Detailed professional standards & scheme materials developed for in-market testing - Industry & Government buy-in & support for the scheme & body - Key industry partners are clear on their role and responsibility in the outputs - Existing schemes & professional standards leveraged	- De-risk & refine solutions before national roll-out - Raised awareness & engagement - Clarity on what is required to successfully implement at scale	- Australia has a globally aligned, industry & government supported, sustainable & consistent national approach to cyber security professionalisation - Increasing number of Australian cyber security professionals recognised via the scheme
Relevance to the national agenda	- Stops fragmentation across the sector - Creates a platform for effective industry & government collaboration	- Industry designing & delivering the solutions - Customer research informs & validates solutions - Positions Australia as a global leader	- National strategy objectives delivered through program outputs & validated via customer research & testing - International learnings, schemes & frameworks built into solutions	- New workforce data being collected - In-market testing validates solutions - Program & learnings shared internationally continuing to position Australia as a leader	- Tangible output from the national strategy delivered - Improved trust and confidence in Australian cyber security professionals - Promotion of the cyber security profession in Australia leading to growth in cyber skills pipeline

Phase 2 scope

Challenge statement

How might we test and iterate a national professional recognition scheme so that we improve government, business and community **trust and confidence** in Australian cyber security professionals

Approach

AustCyber to lead an industry co-design team to:

- Design and run an in-market pilot of the solutions developed as part of phase 1
- Raise awareness of the program including the broader Australian market via roadshows and marketing campaigns

Outputs from phase 2 of this program:

1. An end-to-end pilot, in Canberra/Adelaide containing
 - ✓ A cyber security professional recognition scheme platform:
 - An interactive digital career pathway tool (tested as part of the pilot)
 - Personas, created in phase 1, brought to life as case studies
 - Recognised list of credentials and education that form part of the pathways to be recognised as a cyber security professional
 - Interactive skills framework map/matrix that supports the career pathway tool
 - Professional standards, code of ethics, guidelines etc
 - Innovative CPD requirements developed for pilot
 - ✓ The establishment of professional scheme governing body, including terms of reference, who the body members are, and the financial model
2. A phased national implementation roadmap

Phase 2 investment

Step 1: Draft the details of the scheme

Draft professional standards in detail:

- Code of ethics
- CPD model
- Recognised knowledge and education (including certification mapping)
- Qualifying criteria for on-the-job experience
- Assessment process

Establish the governing body and the accreditation/professional recognition scheme and business model

Timeframe: Six months

s47(1)(b)

Step 2: Test the scheme via an in-market pilot

Design and run an in-market pilot of the body, scheme and business model in Canberra / Adelaide

Timeframe: Eight months

- Six months in-market
- Two months to iterate and create the scaled solution, ready for phased roll-out (Phase 3)

s47(1)(b)