



AustCyber
Part of the Stone & Chalk Group

DRAFT

Creating Australia's Cyber Security Accreditation Scheme

DRAFT Program Plan

September 2022

Goal

DRAFT

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

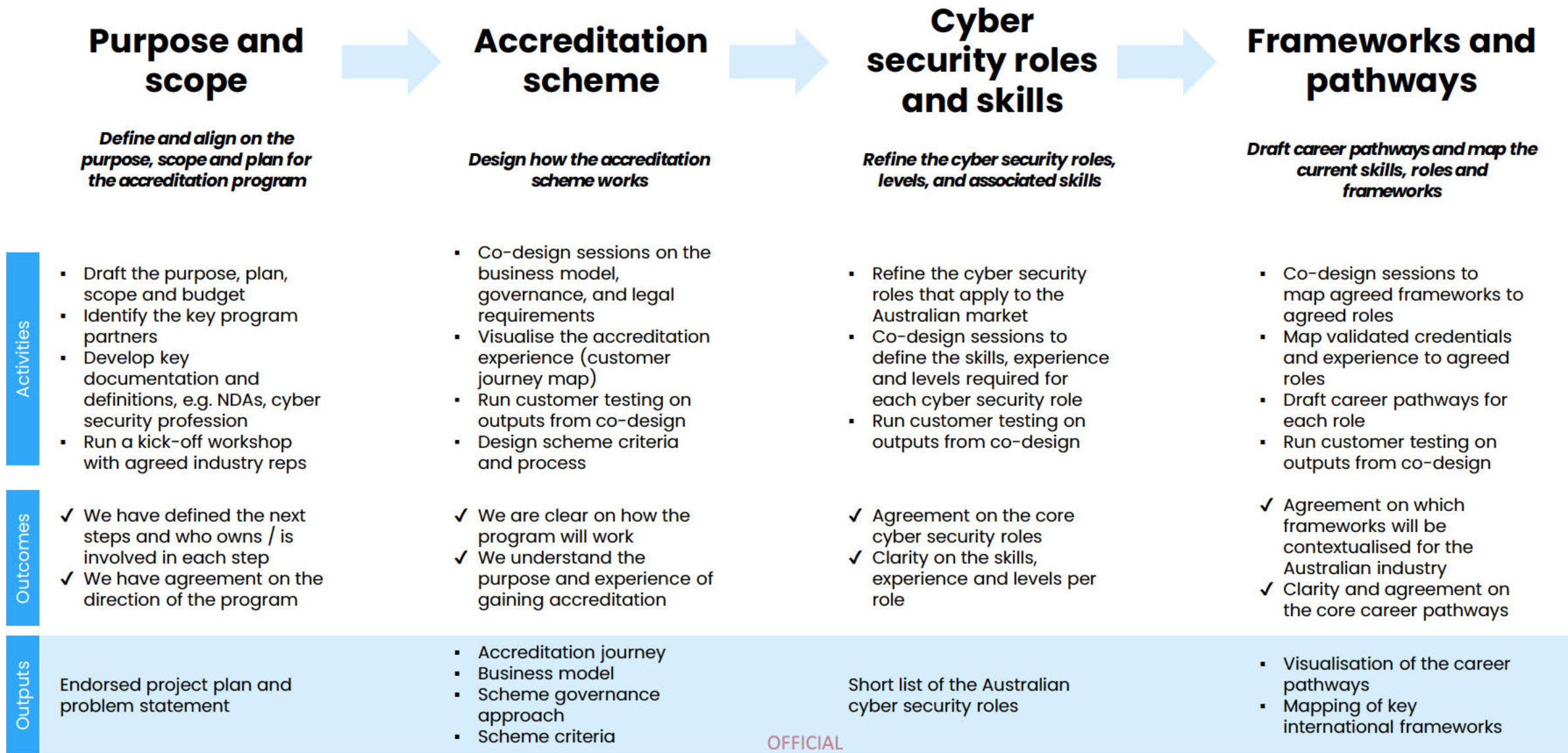


Photo by [Heidi Fin](#) on [Unsplash](#)

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





Focusing questions

Definitions and language

What does cyber security mean?

What is a cyber security professional?

Jobs and career pathways

What are the different cyber security roles?

What skills and knowledge is required for each role?

How do I acquire these skills and knowledge?

Levels and accreditation

Are there different levels of cyber security professionals?

What is the difference between each level?

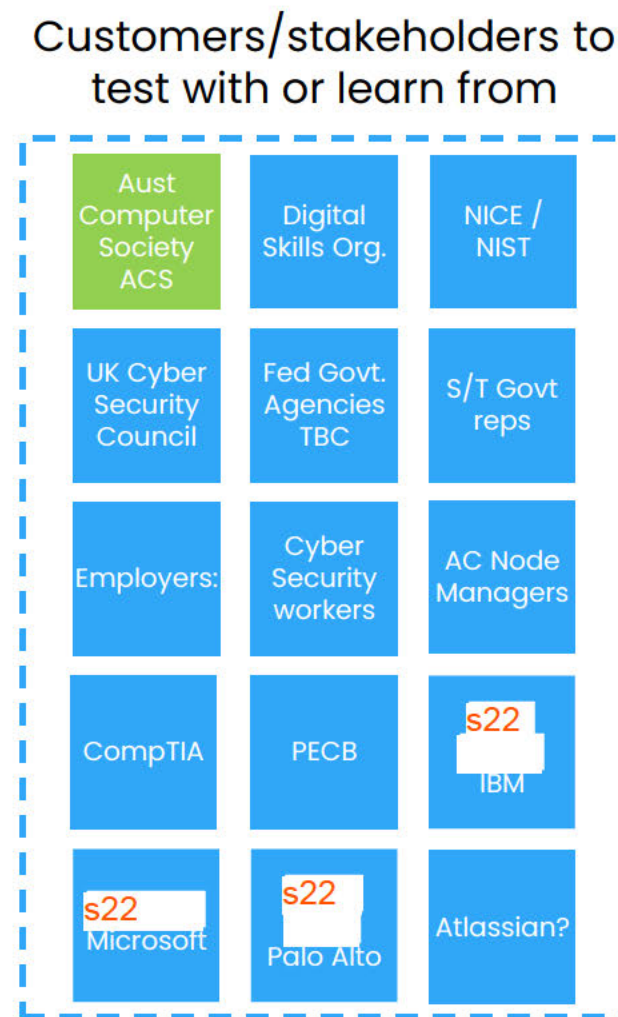
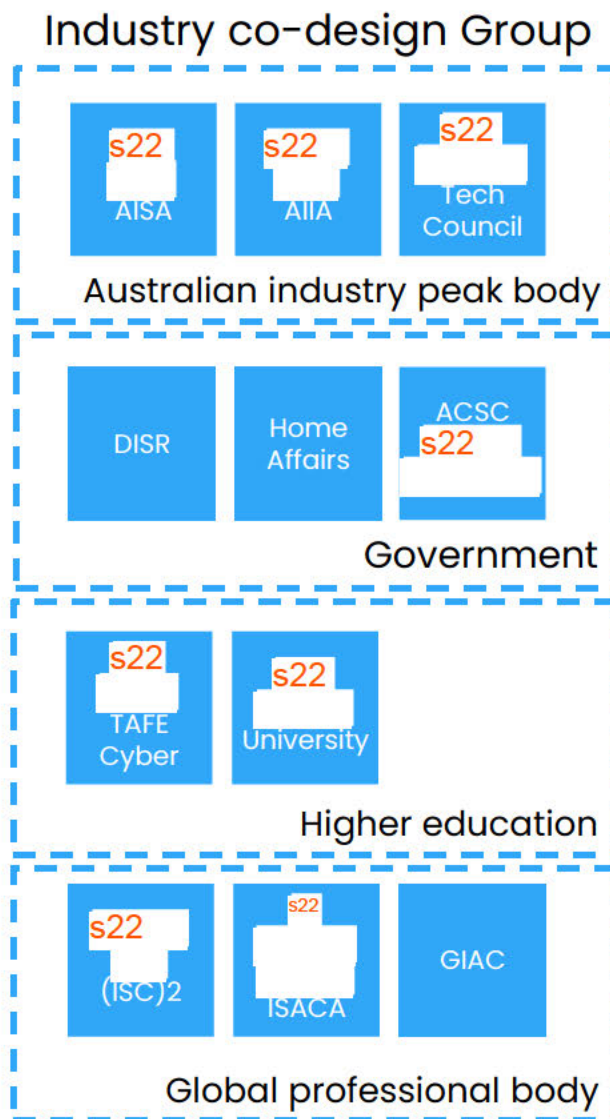
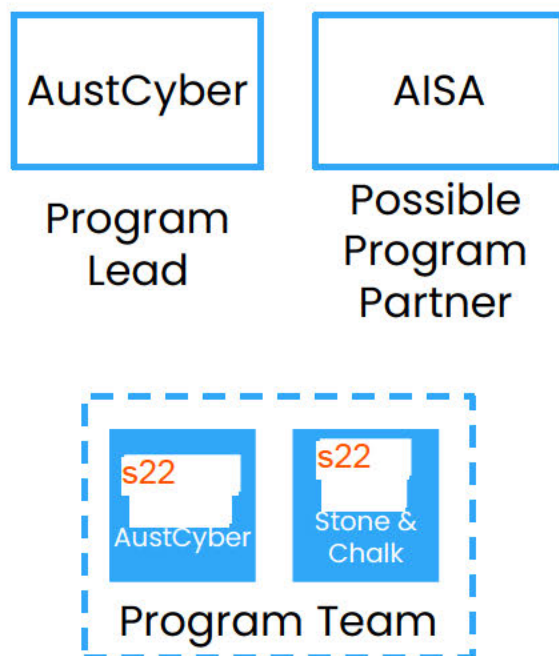
Who determines what level I am at?

Governance

Where does all this information live?

Who keeps this information up-to-date?

Proposed structure



- Lock in all co-design participants. Does Home Affairs want a participant in this group? – yes please
- Confirm where the central voice for this work best comes from at a government level
- Run the kick-off workshop, 28th September



AustCyber
Part of the Stone & Chalk Group

DRAFT

Thank you



AustCyber
Part of the Stone & Chalk Group

ACSP Program: Improving trust and confidence in Australia's Cyber Security professionals

Government stakeholder briefing

16th February 2023

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

Who we are working with

Industry co-design team

s22

Government Partners

- DISR
- Home Affairs
- ACSC
- APSC
- DEWR

Other collaborators

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

Australian Cyber Security Professionalisation program goal

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

Scope

Challenge statement

How might we improve government, business and community **trust and confidence** in Australian cyber security professionals

Approach

AustCyber to lead an industry co-design team to:

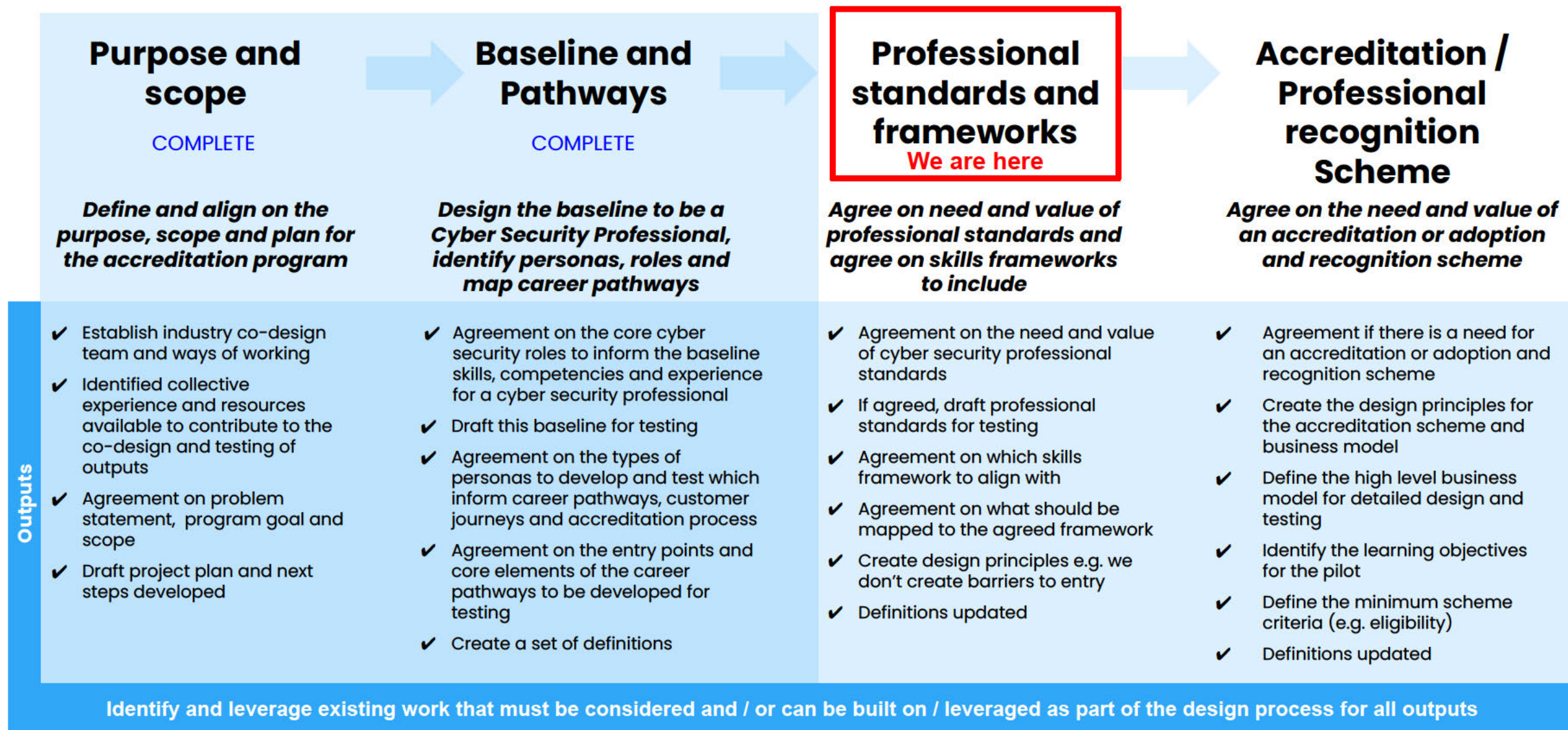
- Design and develop solutions building on existing work and learnings
- Test outputs with customer groups to ensure customer input and feedback is guiding the overall solution
- Implement the solution at scale in the Australian market (include communication with global organisations as relevant)

Outputs from phase 1 of this program:

- ✓ A baseline for an Australian cyber security professional:
 - skills
 - competencies
 - experience
- ✓ Personas for a new entrant, career changer, existing practitioner, international worker
- ✓ Pathways for the personas to become a cyber security professional based on baseline requirements
- ✓ Agreement on the need and value in creating professional standards for cyber security
- ✓ Agreement by the industry if there is a need for an accreditation scheme or an adoption and recognition scheme for cyber security professionals
- ✓ If required: the high level design of the accreditation scheme*
 - business model
 - accreditation process
 - customer journeys of the future state accreditation experience

* The need for and type of accreditation scheme will be determined by the co-design team

Co-design topics and outputs



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

Designed and agreed

- The draft baseline requirements to be recognised as a cyber security professional
- That there is a need for a code of ethics that cyber security professionals should adhere to
- The need and value of professional standards for cyber security

Started customer
research

Who:

- Employees - new entrant, career changer, existing worker, international worker
- Employers - corporate, SME non-tech, SME tech but no cyber security expertise

Learning objectives:

- Understand their needs and current experiences working in cyber security and employing cyber security skills
- How they feel about the idea of professionalisation

Co-design session three: Purpose

1. **Agree** on the value of professional standards
2. **Agree** which skills frameworks to include

Co-design session three: Achievements

1. **Agreed** as a team in principle for the need and value of professional standards for cyber security
2. **Expanded** direct engagement with members of the co-design representatives

Program collaboration to-date

Digital Skills Organisation

Clarified and visualised how our programs cross-over

Engineers Australia

Shared our focus and provided input into the cyber engineering design work

UK Cyber Security Council & UK Gov't

Learnt in detail about what they have designed and locked in more collaboration time

Tech Council and AIIA Members

Clarified what this program is, and isn't, solving for which lead to strong support for this programs objectives

Government stakeholders: DISR, ACSC, DEWR, APSC, Home Affairs

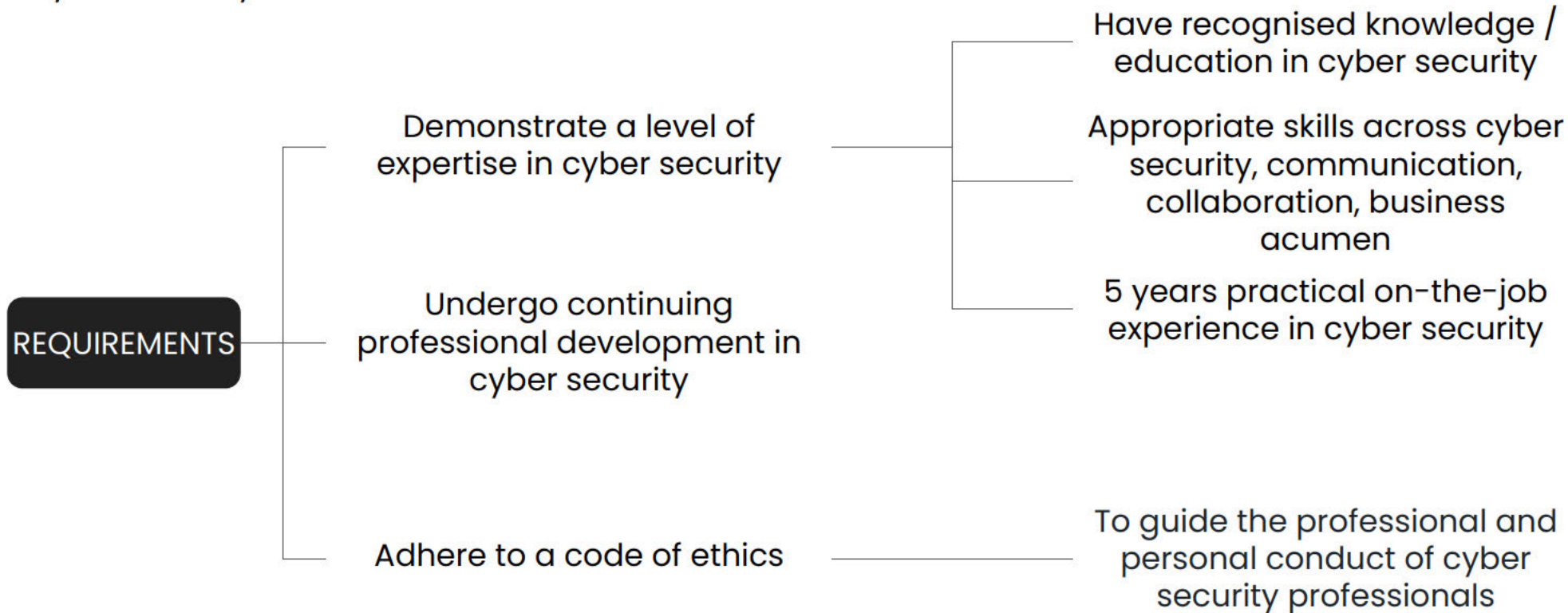
Updated on this teams progress and received positive feedback on how we are working together and work delivered so far

NSW Government: Investment NSW, Cyber Security Branch

Learnt about the focus for NSW Govt. and are responding to their request for further briefings and collaboration on our work

Agreed cyber security requirements

The elements we have defined of what constitutes a Cyber Security Professional



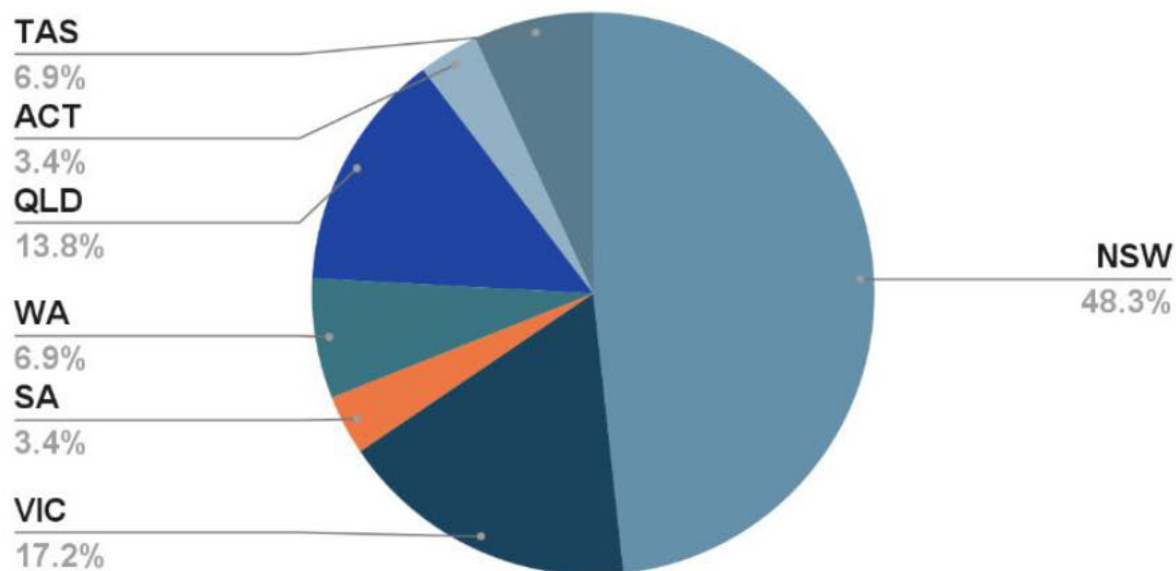
Emerging learning from the interviews*

*We will continue interviewing participants after this co-design session

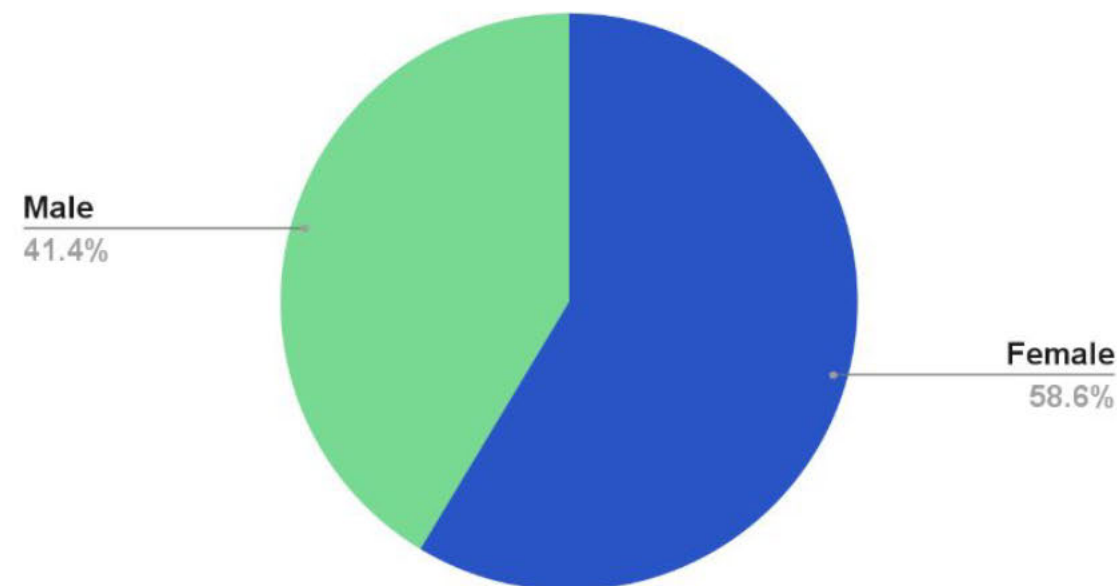
Participant makeup of our interviews

Interviews completed as at 3 February

Nearly half of the research participants were from NSW.

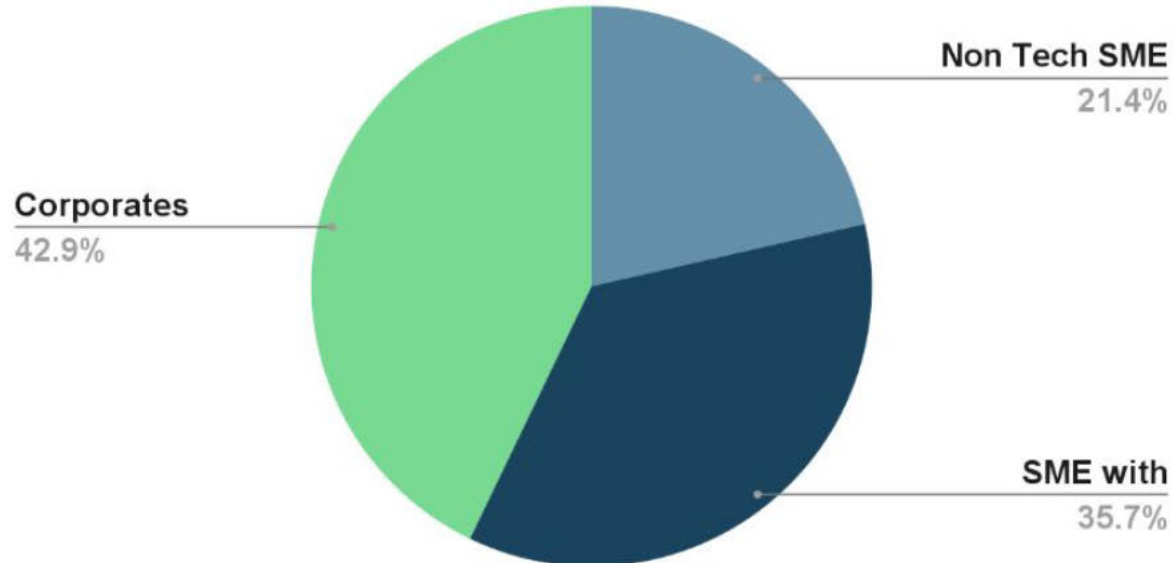


We interviewed more females than males.

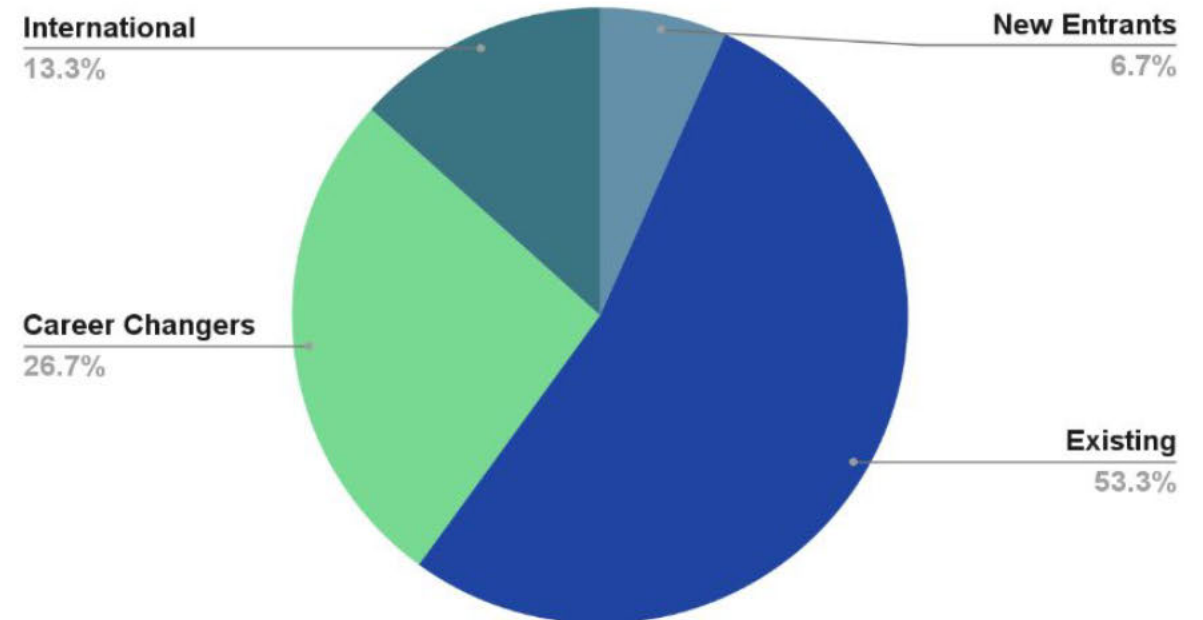


Participant makeup of our interviews cont.

Corporate Employers were our biggest participant group.



We found it most difficult to source New Entrants.



Emerging learning from our interviews

***You've read the textbook but
have you flown the plane?***

***Help me sort the wheat
from the chaff***

***Government-backed,
industry-supported***

***Professionalisation, why hasn't
this already been done?***

You've read the textbook but have you flown the plane?

- We learnt that 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.**

*I think when you're looking at the recognised knowledge, education and practical on the job experience, I think they almost need to be combined because, to me, **on the job experience far outweighs any industry certification that someone can get.***

*A degree means nothing, but a CV where you've worked, what have you done – it really just comes back to **if you can't do the work, you can't get a job.** You need to be able to do the work.*

*For new people coming in, for students, and I actually do speak to high school students who are coming in, I recommend TAFE because **it's about hands on skilling. And it's what will get you in the door into employment quicker because they want those hands on skills rather than just book learning.***

Help me sort the wheat from the chaff

- 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 **personal 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.

The certification puzzle – there's 1,000 different cyber security certifications – and I don't know the value of each of those and how legitimate each one is and the requirements for passing the certification. I don't understand (all) certifications (except for the big ones) well enough to say, okay, you've got a certification then you must be actually really good at this.

When I was at uni, it was a waste of \$30,000 and three years in my life – everything that I was taught was out of date the second I graduated, and I could have been instead in the field for three extra years. It was not worthwhile whatsoever. I've done multiple interviews recently, to try and find other people to join my team. And to be honest, if I look and see that they've gone to uni, that means less than nothing

*Too much weight is put on certifications, when certifications can easily be fudged. As I said, brain dumps are a thing and they are out there for every type of certification so people can fake that they know that information in order to get that certification. **You can't fake experience.***

Government-backed, industry-supported

- Across employees and employers we interviewed, there was a strong theme for the **creation of a new body to administer the professional standards.**
- We consistently heard that a **government-backed, industry-supported body was preferred.** Employees told us 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.

If you were to certify something, like a quality assessment it gives more kudos but you have to regulate the certification.

If it's purely business and not recognised by government it means nothing. You will view it as a money making exercise. Government certified is much better. Industry certified is weaker but second best.

I think it needs to have some government involvement, even if it is around recognition of the body. I don't think they would need to, you know, actually set what the requirements are because, in my experience, government is actually lagging behind a lot of businesses.

Does having that federal backing behind it, provide greater assurance in the UK, America, that I'm a certified Australian cybersecurity professional, therefore, you know, do other countries have similar bodies

Professionalisation, why hasn't this already been done?

- When we spoke to AIIA, Tech Council members, and interviewed employers, and they understood **this was not about licensing but about recognition as a professional**; they saw the value for them and the industry and were supportive.
- **Recruitment** was a key theme: making hiring easier and having better trust in who I am hiring 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**.
- They also felt that **people outside of 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.

Honestly, it would make it easy to be able to hire. I think that might be a benefit at the same time when it comes to looking at cybersecurity internally within an organisation and for our industry.

*This is the target and how you get there, there's different paths to get there. There's different skills that you need to collect along the way and no there's not one mould, a one size fits all for everybody. **You must have some skills, you must have something that can be certified against or you know, some sort of experience but how you do it is much more flexible.***

*I started to think, what are his credentials? He got recommended by another small business owner. And he seemed to know what he was doing. And so that's how we went down the the path.
But going through these [insurance] forms, I started to think it's like plumbers and electricians and builders, they have to have licences.*

A hand holding a pen is writing on a checklist on a piece of paper. The checklist has several items with checkboxes, some of which are already marked. The background is a blurred image of a desk with a calculator and other papers.

Agree on the value of professional standards

Context setting: professional standards

What are professional standards

Establish the minimum standard of competence / excellence to be considered as a professional

Professional standards
are vendor neutral and
independent

Built around a complete
requirement for full
professional formation

Dependent on the
maintenance of
competence through
continuing professional
development and
education

Supported by a
disciplinary code with a
process for public
complaint and
sanctions

Without Professional Standards of excellence / competence we cannot ensure good quality, governance, duty of care, validation and verification of results

How we are proposing to apply them

- ✓ As the professional requirements individuals would need to meet to be recognised as a cyber security professional
- ✓ As the set of criteria that an individual would agree to as part of ongoing professional recognition

How we are not proposing to apply them

- ✗ The standards will not be applied as an entry level requirement
- ✗ We will not be imposing the standards as a license to operate in the industry
- ✗ We will not be imposing a registration or licensing system to work in cyber security (at entry level)

The UK Cyber Security Council

Introduction & Updates

████████████████████
████████████████████
████████████████████
Chief Executive Officer

January 2023





VISION

To create a world where the whole of society is safe and secure in cyber space

MISSION

To enhance and expand the nation's cyber skills, knowledge and profession at every level

THE STRATEGY

- Pillar One

The UK Cyber Ecosystem

- Objective 2

Enhance and expand the nations cyber skills at every level, including through a world class and diverse cyber security profession that inspires and equips future talent

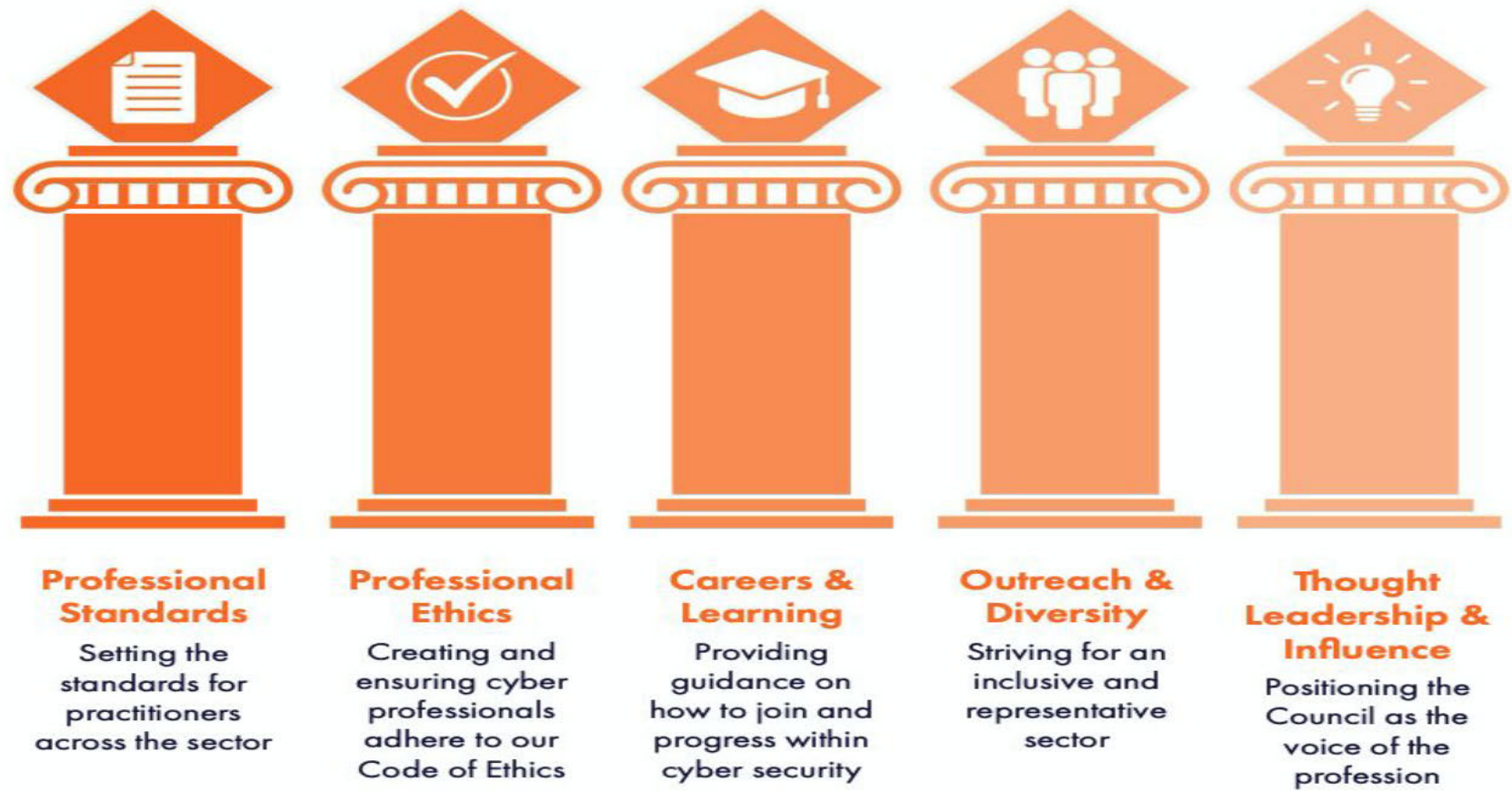


National Cyber Strategy 2022

Pioneering a cyber future with
the whole of the UK



► THE UK CYBER SECURITY COUNCILS FIVE PILLARS



THE ROYAL CHARTER PROFESSIONAL TITLES

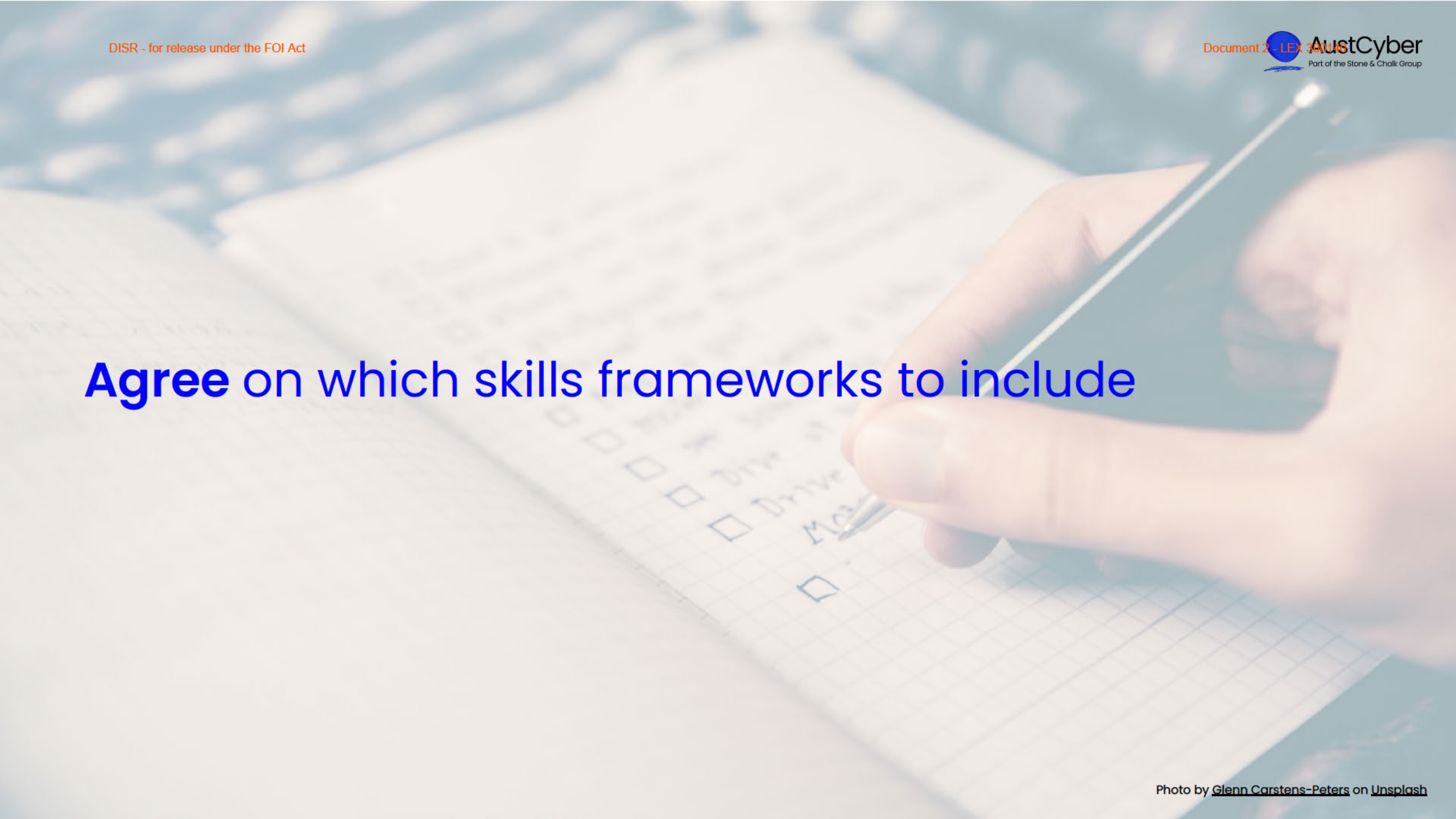
- ❖ Charter - ChCSP
- ❖ Principal – PCSP
- ❖ Associate – ACSP

Apprenticeships

GCSE/BTECS/
A'Level

Technical Levels

Certificates &
Qualifications

A hand holding a pen is writing on a checklist on a piece of paper. The checklist has several items with checkboxes, some of which are already marked. The background is a blurred image of a desk with a calculator and other papers.

Agree on which skills frameworks to include

Skills frameworks under reviewed for inclusion

SFIA

ASD cyber skills
framework

CyBOK

NICE workforce
framework

ANZSCO

European Cyber
Security Skills
Framework (ECSF)

CIISEC

ISO / IEC 27001

Existing frameworks

Framework Name	Purpose/description	Disciplines/Profiles/Specialisms/Categories	Who is it for	Use	Company/ Body	Country of Origin	Last Updated
SFIA - Skills Framework for the Information Age	SFIA is a practical resource for people who manage or work in or with business and technology professionals who design, develop, implement, manage and protect the data and technology that power the digital world. SFIA brings together professional skills, behaviours / behavioural factors and knowledge. The behavioural factors are distributed throughout the generic attributes specified for each level of responsibility. - It provides a framework consisting of professional skills on one axis and seven levels of responsibility on the other. - It describes the professional skills at various levels of responsibility. - It describes the levels of responsibility, in terms of generic attributes of Autonomy, Influence, Complexity, Business Skills and Knowledge SFIA is an experience-based framework based on levels of responsibility and skills. An individual has a particular competency because they have demonstrated that they have a level of responsibility and have demonstrated a number of skills at the levels required in real-world situations. Certifications and qualifications can be aligned to SFIA, but if they only test knowledge they do not indicate experience nor a level of responsibility.	Industry's most common role families. 4 Information and cyber security role family <i>(Each role family covers numerous related job titles and maps to security specific and non-security SFIA Skills)</i> - Security Operations - Incident management practitioners - Security risk management, audit and compliance - Security leadership, strategy and management	- Individuals - Line managers - Organisational leaders - Human resource professionals - Learning and development professionals - Operating model and organisation design consultants - Procurement, supplier management and service providers - Recruiters - Professional bodies and their Bodies of Knowledge - Education providers, training providers, curriculum designers - Reward and recognition consultants	- APSC - Cyber security roles, Career Finder tool - DSO - skills clusters - ASD Framework - as a tool to assess technical ICT proficiencies - ACS - ISC(2) - map to SFIA - ISACA - map to SFIA	SFIA	UK	November 2021 - SFIA 8
NICE - National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework)	The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) NIST Special Publication 800-181, revision 1) provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills. <i>NICE Framework defines entry level knowledge, skills and abilities for 52 work roles in US cyber security eco-system</i> US Gov't supported	Comprises of: 7 Categories (high level groupings of common cyber security functions) 33 Speciality areas (distinct areas of cyber security work) 52 Work roles Categories include: - Analyse - 7 specialty areas - Collect and Operate - 6 specialty areas - Investigate - 3 specialty areas - Operate and Maintain - 7 specialty areas - Oversee and Govern - 14 specialty areas - Protect and Defend - 4 specialty areas - Securely Provision - 11 specialty areas	- Employers - Educators - Learners	- AustCyber - AUCyberExplorer workforce maps and roles - AUCyberscape - education taxonomy - AustCyber NICE Workforce Framework Dashboard - Possible future use - SPIF R2 UniCyber project - TAFECyber - CertIV in Cyber Security - ISC(2) - map to NICE - ISACA - map to NICE - ASD Framework - roles mapped to NICE	National Institute of Standards and Technology (NIST)	US	November 2020 - NIST Special Publication 800-181 Revision 1

Existing frameworks

Framework Name	Purpose/description	Disciplines/Profiles/Specialisms/Categories	Who is it for	Use	Company/Body	Country of Origin	Last Updated
ASD Cyber Skills Framework v2.0	The ASD Cyber Skills Framework defines the roles, capabilities and skills proficiencies that are essential to cyber missions, and that can be used in both the security and offensive contexts. The ASD Cyber Skills Framework enables targeted recruitment of cyber specialists, provides a development pathway for current and future cyber staff and aligns skills, knowledge and attributes with national and international industry standards. The ASD Cyber Skills Framework is relevant to wider government, industry and academia which can be implemented and used as a tool for understanding and profiling cyber skills in any organisation.	9 Roles in 4 groups (developed from 3 core frameworks - SFIA, CII Sec and ILS) 6 levels of proficiency - Cyber Security Analysis - Cyber Threat Analysis - Intrusion Analyst - Malware Analyst - Cyber Security Operations - Incident Response - Operations Coordinator - Cyber Security Architecture - Cyber Security Advice and Assessment - Vulnerability Researcher - Cyber Security Testing - Penetration Tester - Vulnerability Assessor 9 Core Capabilities - Information Security Governance and Strategy - Threat Assessment and Information Risk Management - Systems Development and Implementation - Assurance: Audit, Compliance and Testing - Operational Security Management - Incident Management, Investigation and Forensics - Information Security Research - Management, Leadership, Business and Communications	Defence - Recruiters - Practitioners Wider government, industry and academia to understand and profile cyber skills in any organisation	Defence sector??	Australian Department of Defence	Australia	September 2020
CyBOK Version 1.1- Cyber Security Body of Knowledge	A comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector.	21 knowledge areas under 5 Categories - Attacks and Defences - Human, Organisational & Regulatory Aspects - Infrastructure Security - Systems Security - Software & Platform Security	- Education - Professional training - Broader global community	- AustCyber - AUCyberscape - basis of the cyber security product/services taxonomy	University of Bristol	UK	July 2021

Existing frameworks

Framework Name	Purpose/description	Disciplines/Profiles/Specialisms/Categories	Who is it for	Use	Company/Body	Country of Origin	Last Updated
CII Sec Skills Framework	The CII Sec Skills Framework describes the range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles. It was developed through collaboration between both private and public sector organisations and world-renowned academics and security leaders. It defines the skills and capability expected of security professionals in practical application and not just an assessment of their knowledge.	CII Sec Capability Methodology The CII Sec Capability Development Methodology (CDM) has been designed to help organisations to develop, recruit and retain talent. It can be adapted and tailored for your organisation and will align comfortably with your internal standards and any external standards that may use.	For organisations to develop, recruit and retain talent	ASD Framework - to define the majority of cyber capability and skills within the ASD framework	CII Sec - Chartered Institute of Information Technology	UK	I am unable to download a copy of these frameworks
CII Sec Knowledge Framework	The CII Sec Knowledge Framework expands upon the widely used CII Sec Skills Framework allowing Information Security professionals to have a consistent view of Cyber Security and Information Security.						
CII Sec Roles Framework	The CII Sec Roles Framework sets out a typical set of skills expected of Information Security and Information Assurance Professionals in the effective performance of their roles. It was developed through collaboration between both private and public sector organisations and world-renowned academics and security leaders.						
CII Sec Accreditation Framework	The CII Sec Accreditation Framework has been developed to define the competency requirements for Security Professionals to gain Associate, Full and Fellow levels of accreditation. Our approach has been used to underpin external schemes run by the NCSC and law enforcement. Unable to access these frameworks without payment.						
European Cybersecurity Skills Framework (ECSF)	The European Cybersecurity Skills Framework (ECSF) is a practical tool to support the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals. The ECSF summarises all cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies. It provides a common understanding of the relevant roles, competencies, skills and knowledge required, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programmes. The framework is complemented by a user manual, which constitutes a practical guide to its utilisation, based on examples and use cases. The manual includes three examples for private organisations that need to hire, upskill and/or reskill their personnel in cybersecurity, along with use cases, which reflect the experience of seven organisations using the ECSF in different contexts.	12 Cybersecurity Profiles <i>(Each profile covers numerous related alternate job/role titles)</i> • Chief Information Security Officer (CISO) • Cyber Incident Responder • Cyber Legal, Policy & Compliance Officer • Cyber Threat Intelligence Specialist • Cybersecurity Architect • Cybersecurity Auditor • Cybersecurity Educator • Cybersecurity Implementer • Cybersecurity Researcher • Cybersecurity Risk Manager • Digital Forensics Investigator • Penetration Tester	The target audience for the ECSF is: • organisations' leadership teams, human resources (HR) and cybersecurity functions, • cybersecurity professionals, newcomers and cyber enthusiasts, • providers of learning programmes of all types in the public and private context, • sector associations, • market researchers, and • policy makers.		ENISA - European Union Agency For Cybersecurity	Europe (head office Greece)	September 2022

Existing frameworks

Framework Name	Purpose/description	Disciplines/Profiles/Specialisms/Categories	Who is it for	Use	Company/Body	Country of Origin	Last Updated
ANZSCO - Australian and New Zealand Standard Classification of Occupations	ANZSCO is the skill-based classification used to categorise all occupations and jobs undertaken for profit in the Australian and New Zealand labour markets . It is used in the collection and dissemination of all official statistics on occupation and is a key tenet of Australia's statistical infrastructure.	135111 – Chief Information Officer (Specialisation: Chief Information Security Officer) 135112 – ICT Project Manager (Specialisation: ICT Security Project Manager) 261312 – Developer Programmer (Specialisation: Cyber Security Developer) 261315 – Cyber Security Engineer 261317 – Penetration Tester 262116 – Cyber Security Analyst 262118 – Cyber Security Operations Coordinator 262115 – Cyber Security Advice and Assessment Specialist 262117 – Cyber Security Architect 262114 – Cyber Governance Risk and Compliance Specialist	- Government - Education providers	ANZSCO is applied to a range of data sets, including the Census of Population and Housing, that inform and support government policy settings and programs – from vocational education and training to skilled migration programs. AUCyberExplorer	ABS	Australia	2022
ISO/IEC 27001 Information Security Management System (ISMS) Framework	ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS) and their requirements. Additional best practice in data protection and cyber resilience are covered by more than a dozen standards in the ISO/IEC 27000 family . Together, they enable organizations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties.		Organisations	- ISO certified professional organisations e.g. - ISC2 - ISACA	ISO Standards	Globally recognised Geneva, Switzerland	

Next steps

1. Finish customer research and create personas
2. Create detailed pathways to professional recognition for each persona
3. Share which skills frameworks to include in our mapping and why
4. Lock-in dates for AISA member roadshows
5. Prepare for co-design session 4 - accreditation / professional recognition scheme