





I begin today by acknowledging the Ngunnawal people, Traditional Custodians of the land on which we meet today, and pay my respects to Elders past, present and emerging.



*“It keeps me from looking at my
phone every two seconds.”*

Today's agenda

#	Agenda item	Timing
1	Welcome and purpose	9:45 till 10:00
2	Share the personas	10:00 till 11:00
COFFEE / TEA BREAK		11:00 till 11:10
3	Confirm which skills frameworks to include	11:10 till 11:40
4	Critique the design principles	11:40 till 12:15
LUNCH		12:15 till 1:15
7	Critique the strawman design of the scheme	1:15 till 2:45
8	Share what's next	2:45 till 3:00
SOCIALISING TIME WITH SNACKS		3:00 onwards

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

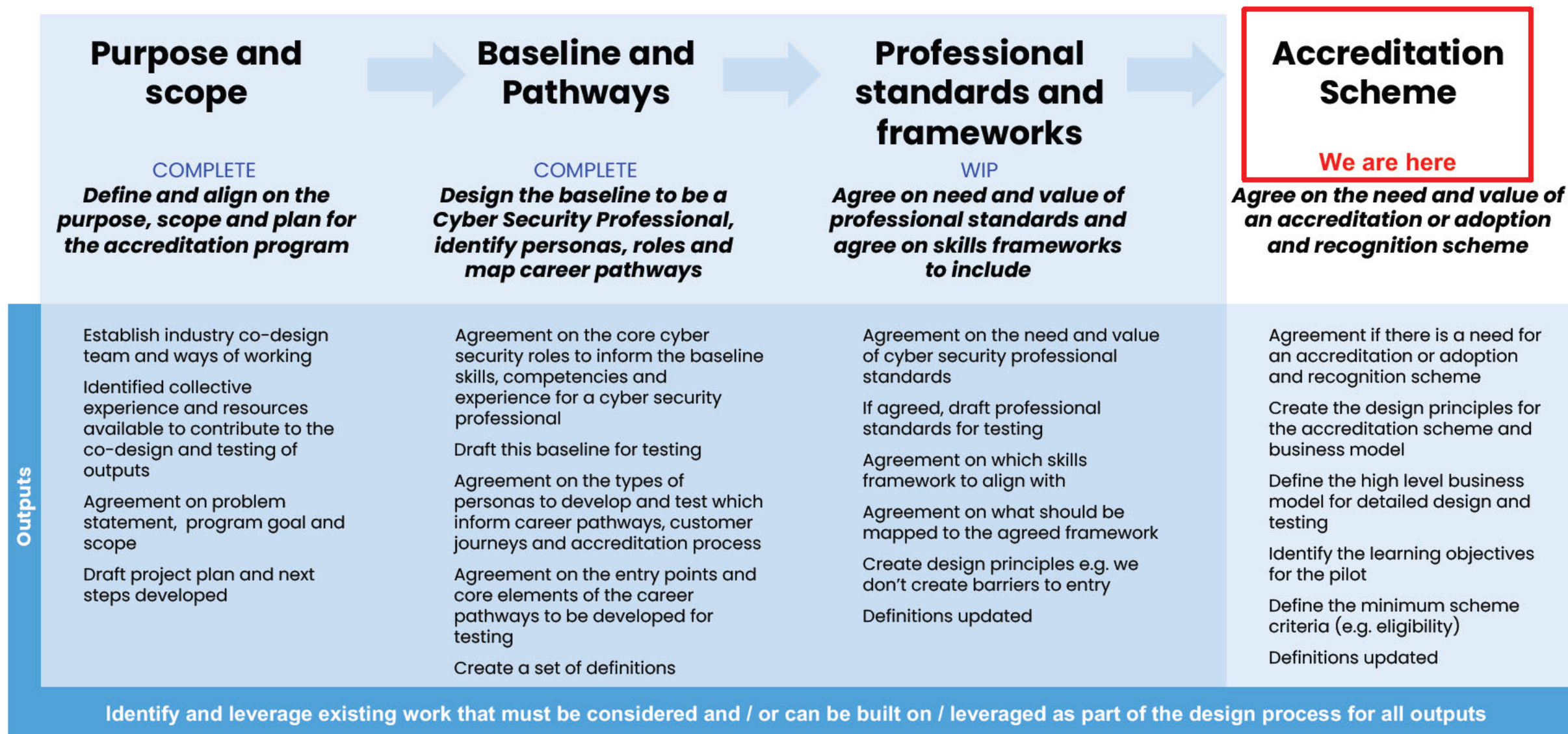
Agreement by the industry if there is a need for an accreditation scheme or an adoption and recognition scheme for cyber security professionals

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



Today's purpose

1. **Confirm** which skills frameworks to include
1. **Design** the high level professional recognition scheme

Introducing s22 (Tech Council)

s22

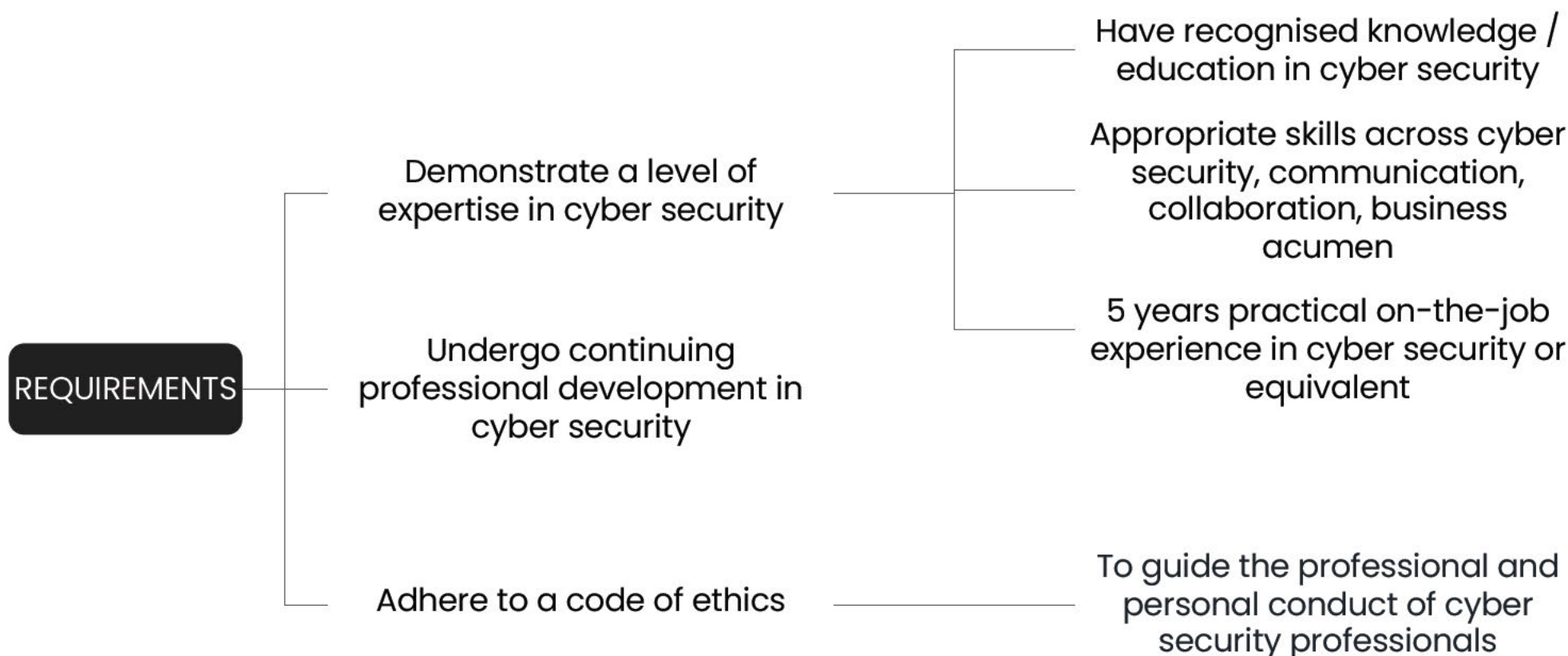
- Focused on enabling our members and the broader tech community to improve knowledge sharing, lift capability across all the Tech Council's focus areas, and building community.
- Facilitates the Digital Employment Forum
- Technology background
- Previously the Chief Technology Officer in an Australian technology business as they scaled globally.
- Expertise: development of technology strategy, building customer-focused software products, and also in cyber security.

I'm passionate about building a robust Australian tech industry, with world leading talent pipelines, a diverse workforce, and a relentless drive for innovation

Tech Council of Australia

Cyber security requirements

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



Walkthrough of the 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.

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.

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 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.

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.

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 16 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

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 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
CISO level: 10 years.*

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.

BREAK



Confirm on which skills frameworks to include

Proposed skills frameworks to include

Include

Fit for our purpose

CIISEC:

Helps us align with the UK to improve pathways

SFIA:

Express in terms of SFIA as a language rather than a set of definitions

NICE workforce framework:

Extremely complex.
Proposal to map to it but not be the up front framework to map to

Reframe

Include in a different way

ANZSCO:

Not relevant for this context.
We can help amplify ANZSCO, we need to share / plug into that work

CyBOK:

Not designed for skills mapping (body of knowledge).
Can use for knowledge + education

Don't include

Not fit for our purpose

ASD cyber skills framework:

Too narrow a focus for our purpose
Designed explicitly for ASD

European Cyber Security Skills Framework (ECSF):

Similar to ASD

ISO / IEC 27001:

Not the right kind of standard for the purpose of this work

ACTIVITY

Please review and provide feedback

15 minute activity

5 minute presentation

Design the professional recognition scheme

What we want to achieve in these activities

1. Confirm the need for a professional recognition scheme (are there other options to consider?)
1. Agree design principles for the scheme
1. Critique the strawman of the professional recognition body and scheme

Design principles

Customer-centered	Flexible	Objective	Transparent	Continual improvement	Collaborative
Should be designed with the needs and perspectives of the intended customers (cyber security workforce and employers) in mind. This includes considering their diverse backgrounds, experience levels, and career goals.	Should allow for different pathways and entry points to professionalisation, recognise a range of qualifications and experience, not create barriers to entry, be relevant to current and emerging cyber security threats and technologies, and needs of the evolving workforce.	The professional recognition process should be unbiased and objective, using valid and reliable assessment methods	The professional standards, and process for professional recognition should be clearly communicated and easily accessible to all stakeholders	The scheme should be regularly reviewed and updated to ensure it remains relevant, effective, and responsive to changes in the cyber security landscape	The co-design team should engage with stakeholders from industry, government, academia, and the wider community to ensure a well-rounded and inclusive design process

ACTIVITY

Critique the principles
Are there any principles missing?

1. What works why?
2. What doesn't work?
3. How might you make them better?

15 minute activity

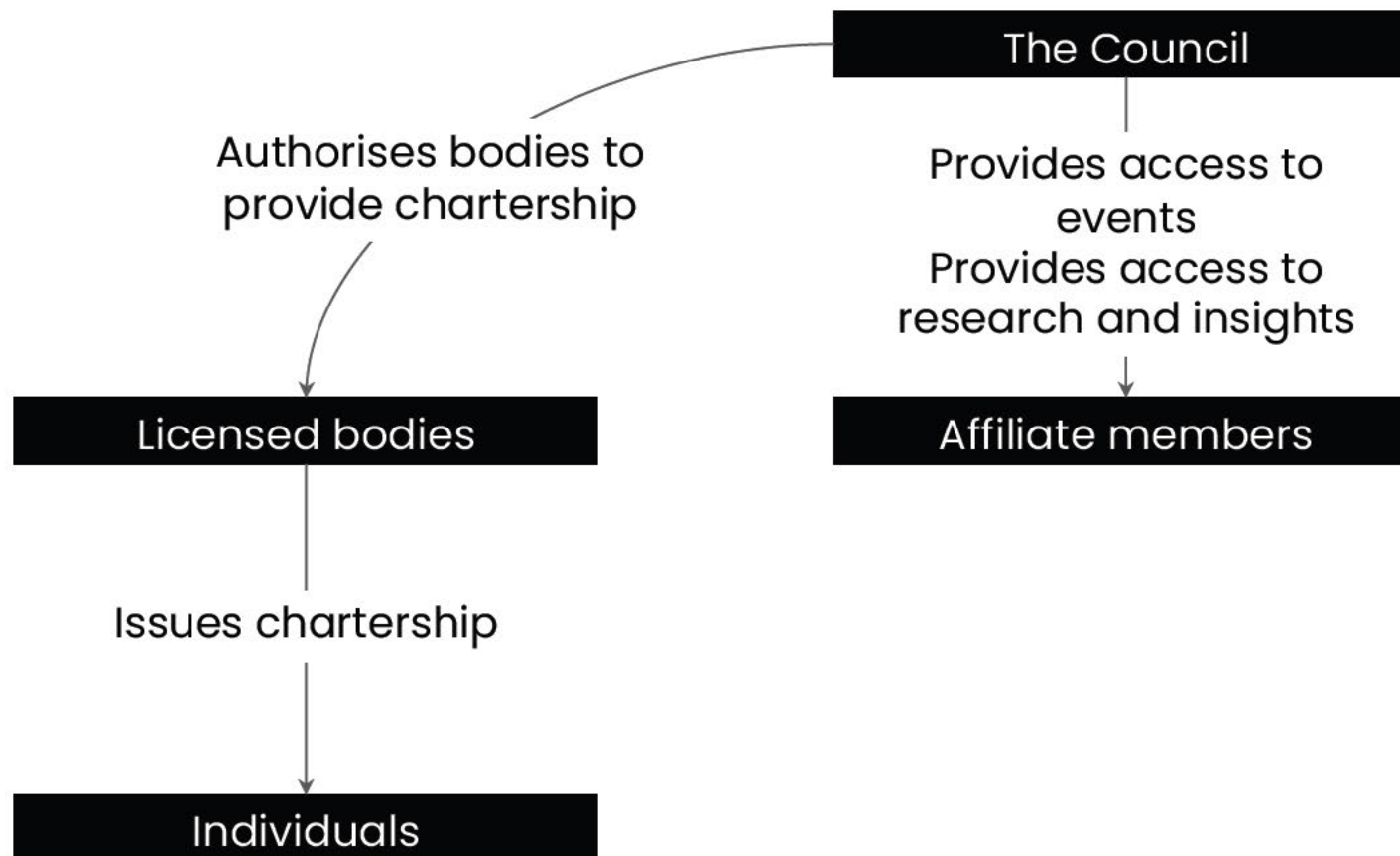
5 minute presentation

LUNCH



Insight into the UK Cyber Security Council

Membership model

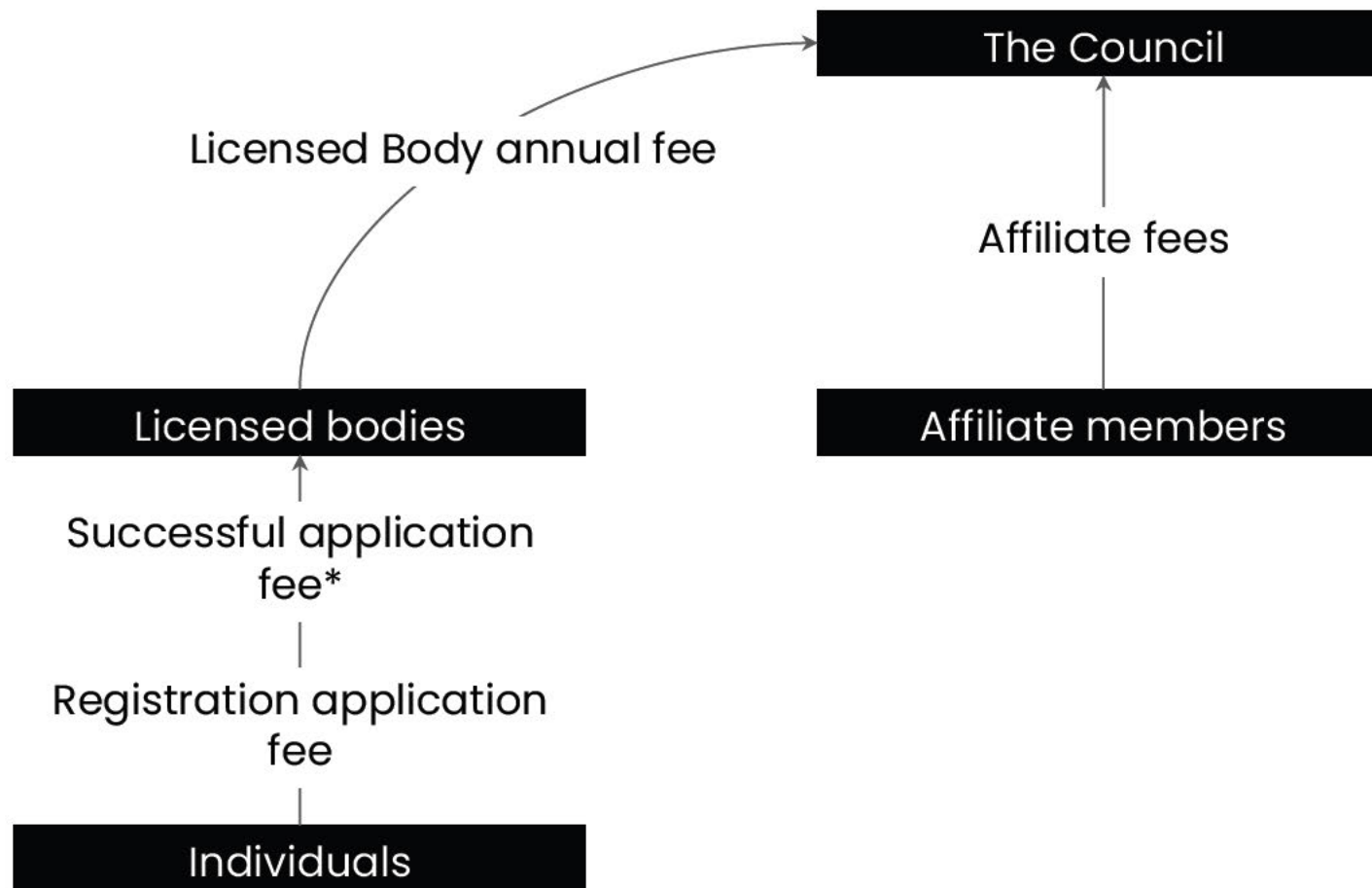


NOTE:

* Fee for successful application to the Council's Professional Registration Register paid to Licensed Body. This fee will be transferred from the Licensed Body to the Council

Insight into the UK Cyber Security Council

Fees Structure

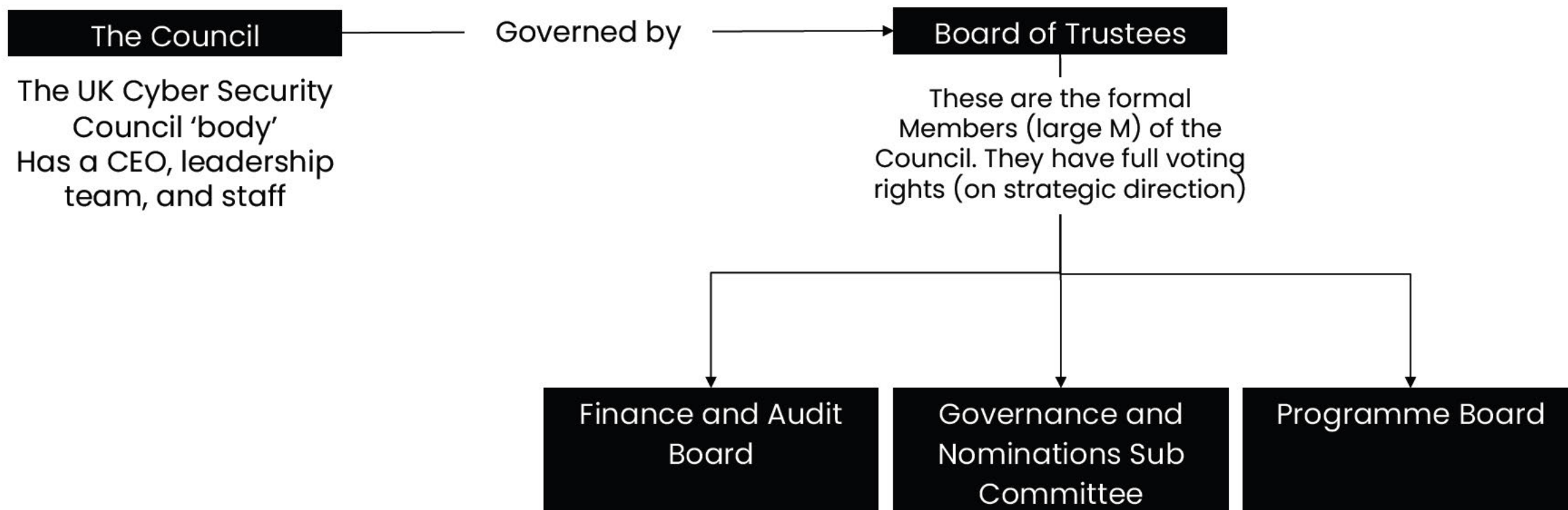


NOTE:

* Fee for successful application to the Council's Professional Registration Register paid to Licensed Body. This fee will be transferred from the Licensed Body to the Council

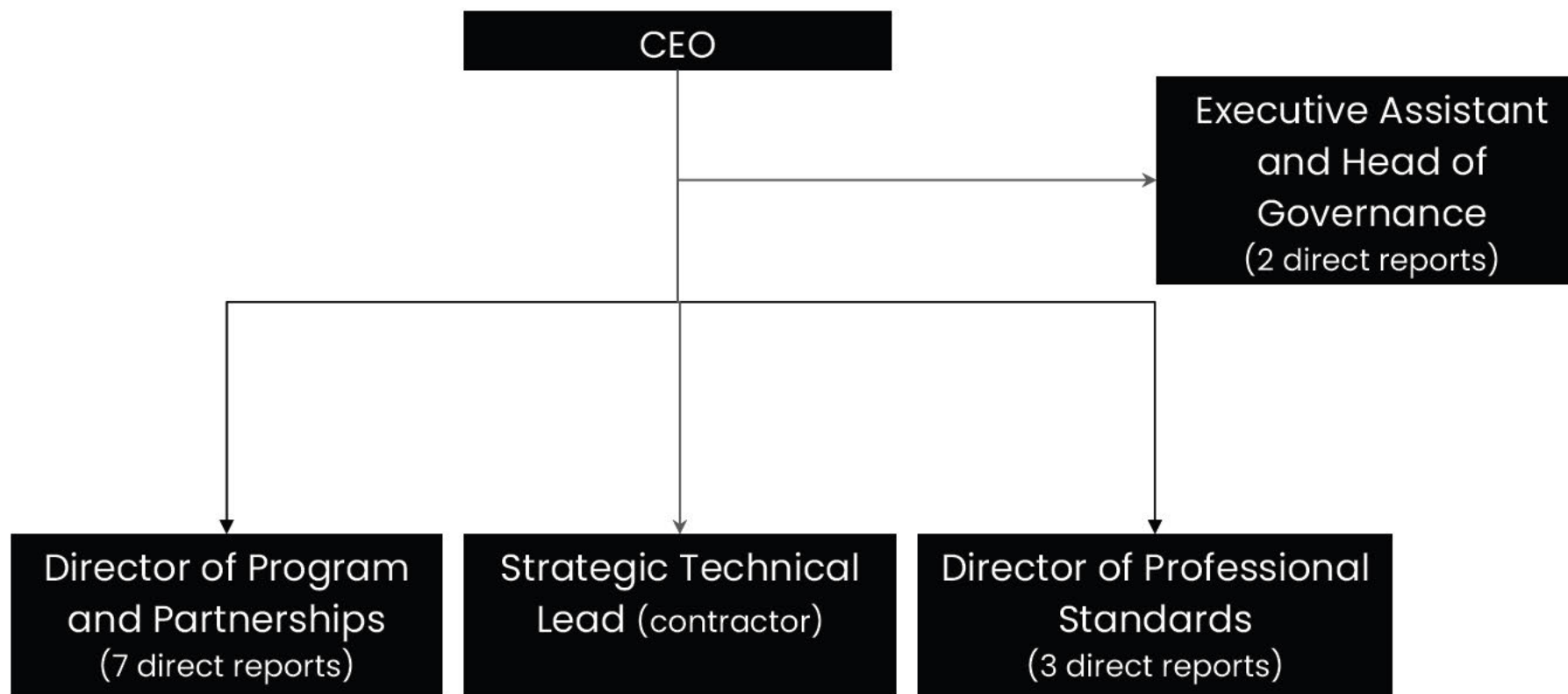
Insight into the UK Cyber Security Council

Governance Structure



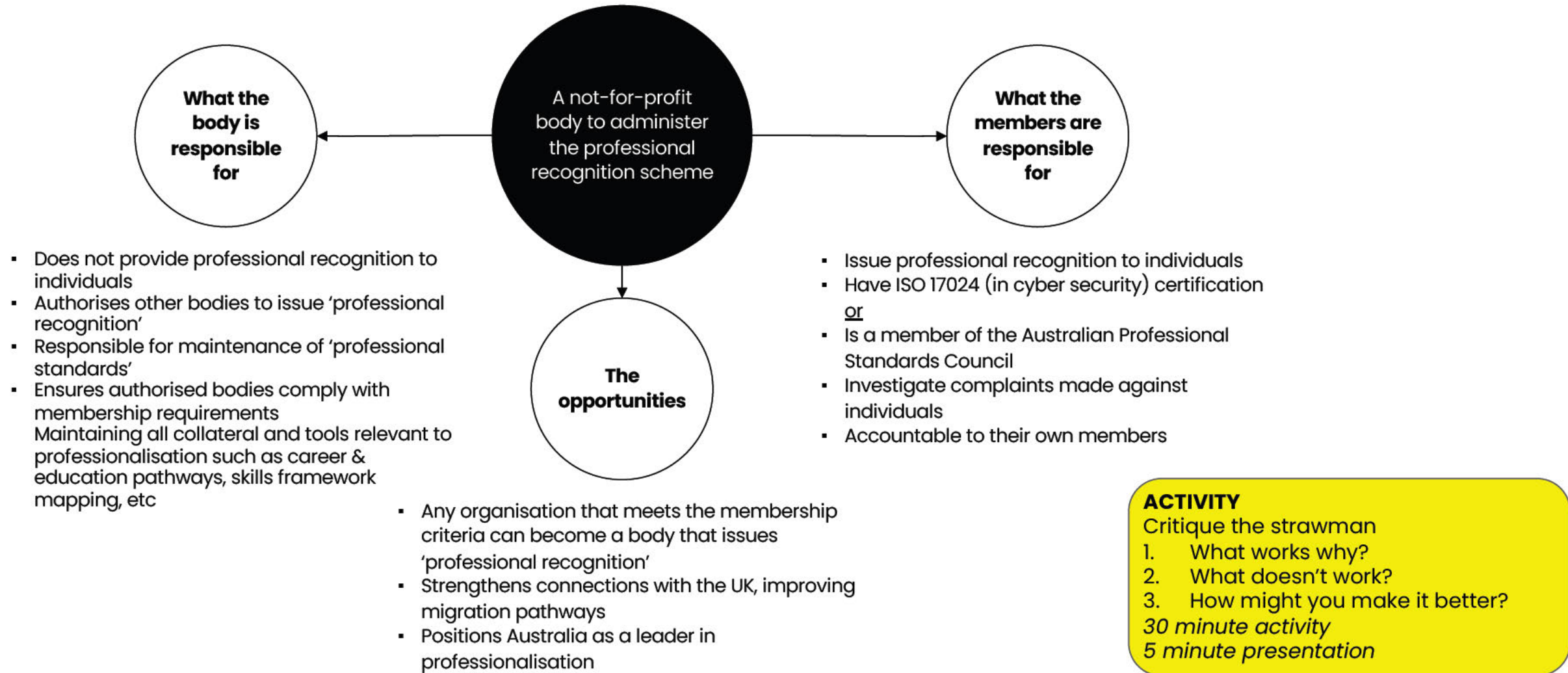
Insight into the UK Cyber Security Council

Council Leadership Structure



For critique: The professional recognition body

We have created this strawman for critique



Next steps

1. Update and share the strawman of the scheme/body
1. Update the personas
1. Share Phase 1 report including draft scope and approach for phase 2
1. Secure funding for phase 2

Food for thought

Branding ideas

Option 1



Option 3



Option 2



Option 4



AFTERNOON TEA AND SOCIALISING TIME







AustCyber
Part of the Stone & Chalk Group

Improve trust and confidence in Australia's Cyber Security professionals

Program Overview and Plan

17th October 2022

Commercial in Confidence

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

This programs goal

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

Commercial in Confidence

Photo by [Annie Spratt](#) on [Unsplash](#)

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

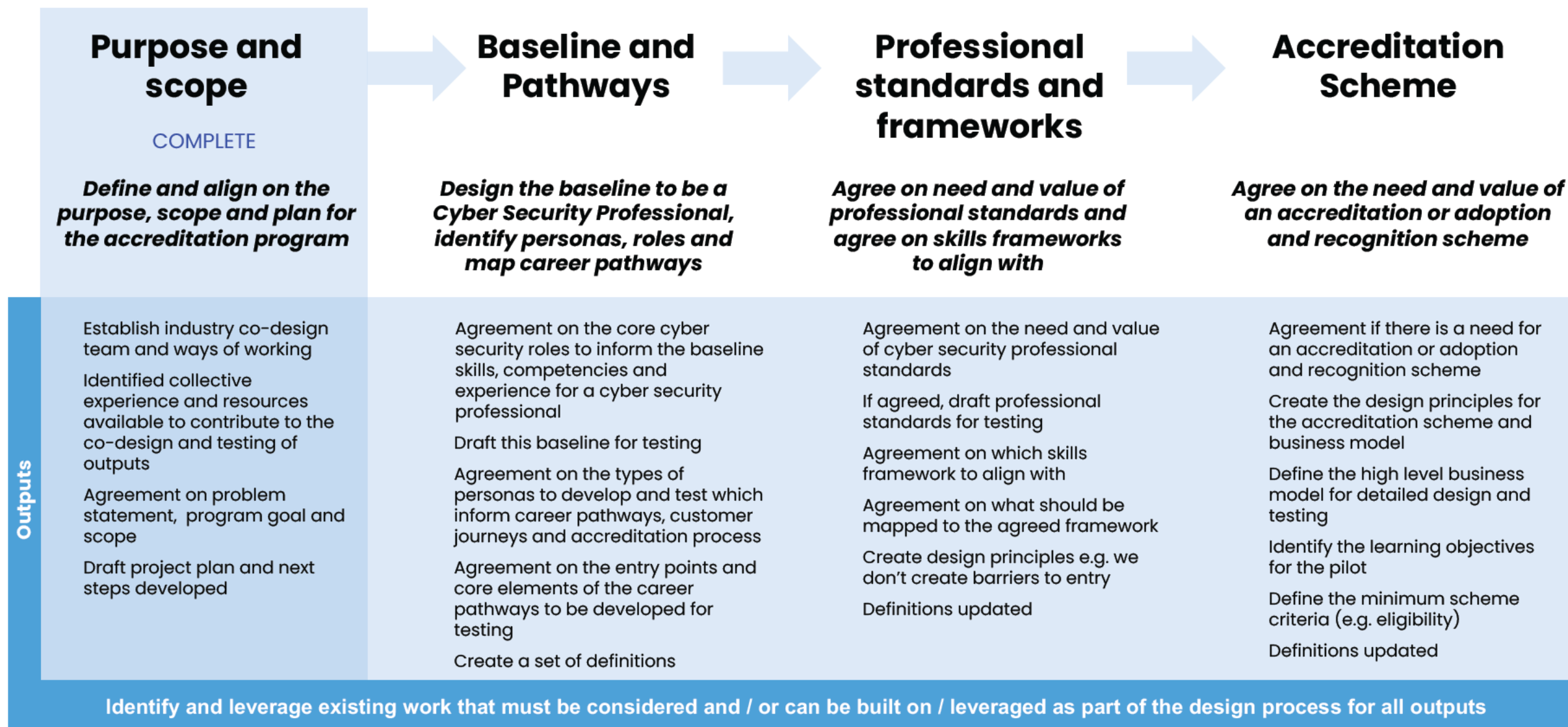
Agreement by the industry if there is a need for an accreditation scheme or an adoption and recognition scheme for cyber security professionals

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



Proposed Phase 1 timeline



Activities	Baseline, personas and pathways	Professional standards and frameworks Customer testing on personas and pathways		Accreditation / adoption and recognition scheme Customer testing on professional standards	Phase 1 wrap up
	Nine weeks	Ten weeks (excluding holidays)		Thirteen weeks	Five weeks
	Identify the core cyber security roles to inform the baseline for a cyber security professional (co-design) Define the baseline of skills, competencies, and experience required to be recognised as a cyber security professional in Australia (co-design) Identify and create the personas to inform the pathways Identify and create the pathways for the personas to become a cyber security professional, based on baseline requirements Create submission for phase 2 funding	Identify and review existing work on standards for cyber security professionals Develop the draft set of standards for cyber security professionals to critique in the next co-design session Agree if we need to create professional standards for cyber security (co-design) Run customer testing on personas and pathways to validate this component for the end-to-end pilot (phase 2)	Review and update standards (co-design) Agree which existing cyber security skills framework to align to (co-design) Review and update existing mapping of agreed skills framework(s) Run customer testing on professional standards to validate this component for the end-to-end pilot (phase 2) Run customer testing to test 'positioning' of what is being designed (with supply and demand side)	Agree if there is a need for an accreditation or adoption and recognition scheme (co-design) Create the design principles for the accreditation scheme and business model (co-design) Define the high level accreditation business model for detailed design and testing (co-design) Design the body to own and run the scheme (to agree if we use existing body or create new) (co-design) Run customer testing on accreditation or adoption and recognition scheme Identify learning objectives, scope, segments to target, and approach for the end-to-end pilot in Phase 2 (co-design) Low-fidelity prototype of how all the phase 1 outputs are experienced by customers	Prepare final materials Prepare and run end of phase 1 showcase Draft and seek endorsement for Phase 2 end-to-end Pilot scope and approach

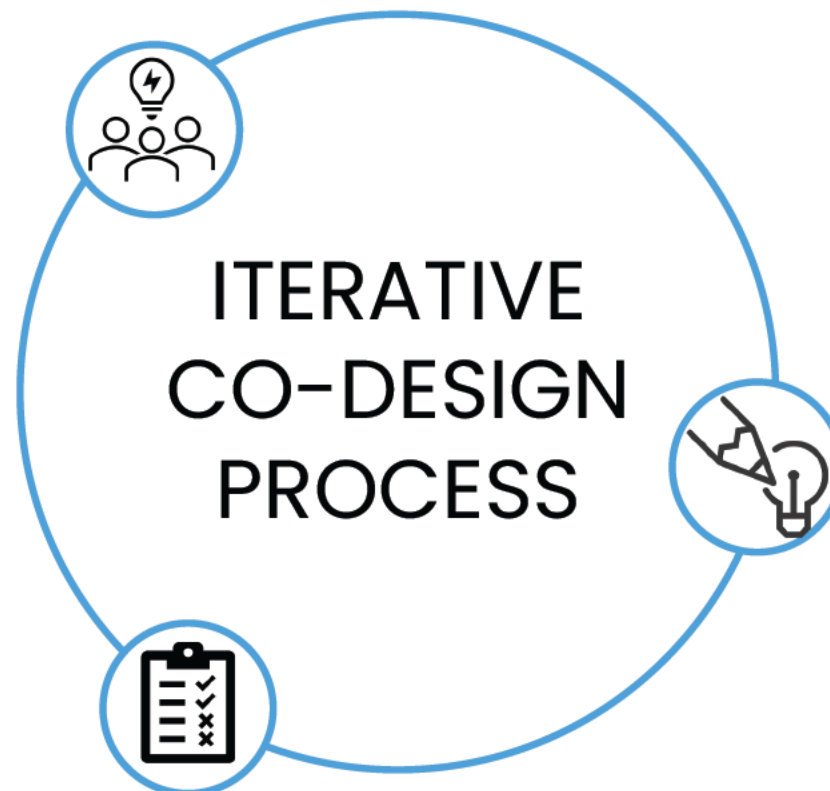
Co-design and customer testing process

The approach:

Throughout this program whatever we create in our co-design sessions we will test with customers. This visual represents the basics of the cycle we will go through

The value:

By bringing multiple perspectives to the solution and constantly getting feedback from the people we are designing for, what you create has a higher likelihood of achieving its objective



CO-DESIGN:

Facilitated sessions to generate ideas to solve for a specific challenge. Brings multiple perspectives to the problem to generate better ideas

TEST:

Takes what is created during co-design and puts it in a format that can be tested with target customers

EVALUATE:

Review feedback from customer testing and make changes (as appropriate) to the idea