

APPENDIX THREE: AU CyberExplorer optimization

Potential additional data field	Utility	Rationale
Gender (m/f/x)	Disaggregation by protected attribute	Provide more timely, and gender-specific, overview of available roles in the labour market (vis-à-vis cyber security)
ANZSIC (Division)	Correct attribution of activity to divisions within the labour market	Alignment between master framework and sub-categorisation of cyber security roles
ANZSCO (Code) (2 digit level)	Sub-category mapping to identify proximate need	Provide granular insights in where new jobs are being advertised/current jobs are
Age	Disaggregation by protected attribute	Provide timely overview of age-related labour market mobility
Remuneration	Indicator of labour market supply/demand	Obtain an indication of the relative value of roles at particular points in time

APPENDIX FOUR: GLOSSARY OF TERMS

ABS	The Australian Bureau of Statistics is an independent statutory agency of the Australian Government which is responsible for statistical collection and analysis of data, and for giving evidence-based advice to federal, state and territory governments.
ANZIC	ANZIC Industry Classifications - Australian and New Zealand Standard Industrial Classification. A system administered jointly by the Australian Bureau of Statistics and Statistics New Zealand which assigns a unique number to each industry in order to identify the firms operating in each class and sub-class and to allow for the collection of data such as location, number of employees, and annual sales.
ANZSCO	An object used for the completion of a business task.
ASSETS	Assets maybe tangible or intangible items and can relate to equipment, software code, data, facilities, personnel, market value and also public opinion.
ANZSCO	Australian and New Zealand Standard Classification of Occupations. The titles used in ANZSCO are intended to convey the clearest possible idea of the nature of the particular occupation.
CyBOK	Cyber Security Body of Knowledge. A comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector.
CyberSecurity	The efforts made to design, implement, and manage and maintain security of business networks, or devices connected to the Internet including the technical aspect to apply these and the training of personnel to manage, implement and maintain them.

APPENDIX FOUR: GLOSSARY OF TERMS

Digital Economy	A digital economy is the results of many technology based connections between individuals or organisations, devices, data, and processes and refers to an economy that is led by digital computing technologies.
NICE Framework	The National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework) is a reference resource that classifies the typical skill requirements and duties of cybersecurity workers.
NIST	The National Institute of Standards and Technology is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. Its mission is to promote American innovation and industrial competitiveness.

F

G

H

I

BIBLIOGRAPHY

AustCyber (2020). *Australia's Cyber Security Sector Competitiveness Plan*. Canberra: AustCyber.

AustCyber (2020). *Digital Trust Report*. Canberra: AustCyber.

Hall, M. & Stanwick, J. (2021). *The stock of qualifications in Australia*. Canberra: NCVER.

IBISWorld (2020). *IT Security Consulting in Australia*. Available online.

National Skills Commission (2021). *Vacancy Report June 2021*. Canberra: National Skills Commission.



CYBER SKILLS FOR A DIGITAL ECONOMY: AN AUSTRALIAN PROFILE

CYBER SECURITY WORKFORCE AND SKILLS
SHORTAGES IN AUSTRALIA

AUTHORS

Suggested citation: AustCyber (2021). *Cyber Skills and Jobs for a Digital Economy: An Australian Profile. A report for the Department of Industry, Science, Energy & Resources.* Canberra: AustCyber.

To the extent permitted by law, all rights are reserved and no part of this publication covered by copyright may be reproduced or copied in any form or by any means except with the written permission of © AustCyber 2021 .

CONTENTS

	Page
ABOUT AUSTCYBER.....	2
REPORT BACKGROUND.....	5
SCOPE OF THE REPORT.....	6
METHODOLOGY.....	7
EMPLOYMENT & SKILLS FOOTPRINT.....	11
CONCLUSION/REPORT SUMMARY.....	
1. Appendix One: Summary Data Sources	
2. Appendix Two: Data Reporting Request Template	
3. Appendix Three: Australian CyberExplorer Optimisation	
4. Appendix Four: Glossary Of Terms	





ABOUT US

AustCyber was established in 2017 as an independent, not-for-profit organisation. We are funded by federal government grants and form a part of two national programs:

- We are part of the federal government's Industry Growth Centres Initiative which was established through the National Innovation and Science Agenda. AustCyber is one of six centres that have been set up in sectors of competitive strength and strategic priority to boost innovation and science in Australia.
- We are an important part of Australia's Cyber Security Strategy as a key enabler for cyber security research and development, as well as innovation.

Our program of activities is underpinned by evidence gained through extensive research and consultation. Our flagship Sector Competitiveness Plan, updated as recently as 2020, outlines the opportunity for Australia's cyber security sector to support growth across the whole economy. We are guided by our Board of esteemed members who have significant industry experience. Our team come from a variety of backgrounds including academia, government and industry.

BACKGROUND

This report is designed to outline the current state of Australia's cyber security workforce and skills and capabilities. The report includes detailed information on data points and sources available for emerging areas of interest in workforce skills and shortages in Australia and internationally.

The report includes a detailed National overview of the current number of Australians employed in the cyber security workforce as well as existing advertised job vacancies.

This report provides a detailed overview and summary of the most common cyber security qualifications in the Australian labour market.

Report information will leverage the NICE framework to frame occupations and job roles and enable international comparison of performance. In conducting this analysis, an inclusion of a comparative overview for the United States, United Kingdom, New Zealand, and Germany; countries where baseline data exists will occur, enabling some comparisons to be made (for example, in areas such as met, oversupply, or shortage).



SCOPE

This report adopts a mixed methods approach to be able to catalogue, describe and analyse available data sources relating to cyber security skills and qualifications in the Australian market. It synthesizes data from a range of sources, to provide an evidence base to inform the optimization of what has been known as CyberSeek AU. This optimization process will be driven by a step-wise approach, underpinned by this report.

These sources include:

- CyberSeek disaggregated data, mapped according to the NICE framework and according to specific roles (sought from a data eco-system partner)
- Public and commissioned reports (including the *Cyber Security Sector Competitiveness Plan 2020*, and the *AustCyber Digital Census 2020*)
- ABS, NSC and NCVER data (where categorization, seasonally, is at a higher, aggregated level)

Data was included if it met one, or a number, of the following criteria:

- pertained to current cyber security job vacancies within Australia
- projected future labour market variation in relation to cyber security within Australia
- outlined methodological challenges to data collection relating to cyber security and the labour market in Australia

Consistent with the data collection and classification protocol adopted by Cyberseek, this report leverages the NICE framework. Developed by the United States National Institute for Standards and Technology (NIST), the NICE Framework has been adopted globally, for the breadth and depth of coverage it provides for the cyber security industry, and it reflects also specific job roles.

In the absence of real-time, and more granular, ABS data, this report uses existing vacancies, as recorded through CyberSeek AU, as a proxy to determine changes (at least in terms of current demand) in the Australian cyber security workforce. This data pertains to live job advertisements, accompanied by detailed role descriptions, for companies domiciled, or with a significant employment footprint, in Australia.

METHODOLOGY

This report adopts a mixed methods approach to be able to catalogue, describe and analyse available data sources relating to cyber security skills and qualifications in the Australian market. The overarching question was: what systems of classification exist in Australia for cyber security roles and the secondary question was: how many cyber security roles exist in Australia and who fills these roles.

Data was scraped from Au CyberSeek, formally sought through a pull request (from all channels that are aggregated to the CyberSeek dashboard, and grey literature was obtained from within the repository of AustCyber.

Cyber security has traditionally been understood in terms of hardware, software and services. The diversity and sophistication of modern cyber security means that this categorisation is no longer appropriate. The way in which we classify skills in Australia, including in relation to cyber security, has long been contested. In some cases, including for migration skills lists, definitions have been inadequate, with only generic ICT categories in operation within ANZSCO, for example. This challenge is not unique, although other countries have more readily adopted frameworks to address this gap in the taxonomy of skills and job roles within cyber security. A range of international definitions and systems of classification have been adopted, for example, emanating from the United Kingdom (i.e. CyBOK) and the United States (NICE Framework). Some of these have been adopted within Government frameworks, and others have been leveraged by industry, to develop tools to map data more effectively and accurately.

Different classification systems for occupations – CyBOK, NICE, ANZIC, ANZSCO

Below we describe the different taxonomies for classifying cyber security skills and qualifications.

The **Cyber Security Body of Knowledge (CyBOK)** is an international collaboration headed by the University of Bristol that structures cyber security according to five main categories:

- **Infrastructure security:** securing computer and digital networks and related physical hardware and systems from intruders and intrusions, whether targeted or opportunistic.
- **Systems security:** operational, network and systems security that includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Software and platform security:** security that focuses on keeping software and an entire computing platform and devices - including mobile, cloud and web applications - resilient to cyber threats. This includes information security that protects the integrity and privacy of data, both in transit and at rest.

- **Attacks and defences:** a proactive and adversarial 'attack' approach to protecting against cyber attacks, which includes penetration and vulnerability testing as well as ethical hacking. Defensive security focuses on reactive measures such as patching software and detection.
- **Human, organisational and regulatory aspects:** tools and services to protect against intentional and unintentional user mistakes; support observance of organisational governance and policies; and enforce compliance with regulatory requirements.

The NICE Framework

The National Initiative for Cybersecurity Education (NICE) have established a [workforce framework](#) that establishes a taxonomy and common lexicon that describes cyber security work and workers irrespective of where or for whom the work is performed.

The NICE Framework is intended to be applied in the public, private, and academic sectors.

It is comprised of the following components:

- Categories (7): A high-level grouping of common cyber security functions.
- Specialty Areas (33): Distinct areas of cyber security work.
- Work Roles (52): The most detailed groupings of cyber security work. This includes specific knowledge, skills, and abilities required to perform tasks in a work role.

The NICE Framework can be harmonised with official Government frameworks, as it provides both a granular (role-centric), as well as an aggregate view of the broad spectrum of cyber related roles. Due to its adoption in the US Market, and benchmarking elsewhere, it also provides a robust framework for comparative analysis between different labour markets.

Framework	Provides broad classification for the cyber security field	Provides specific sub-categorization for cyber roles	Adopted widely outside of originating country(s)
ANZSCO	YES		
CyBOK	YES	YES	YES
NICE	YES	YES	YES

EMPLOYMENT AND SKILLS FOOTPRINT

Snapshot – July 2021

Attachment A

Cyber Security Occupations – For Cyberseek data request

Cyber security functional roles	Identified roles (ASD ¹ Cyber Security Skills Framework*)	Identified roles from stakeholder submissions	Identified roles from Cyberseek	Identified roles from the NICE Framework	# Existing vacancies for Sydney and Melbourne Metro areas (July 2021) – by NICE Category
Cyber Security Analysis	1. Cyber Threat Analyst*	Information Security Governance, Risk & Compliance (Auditor, Analyst, Implementor or Manager roles)	Cyber Security Analyst	Threat/Warning Analyst	Analyze Sydney • 339 Melbourne • 166
	2. Intrusion Analyst*		Cyber Crime Analyst / Investigator	Target Network Analyst	Analyze Sydney • 339 Melbourne • 166
	3. Malware Analyst*			<i>Cyber Forensics Analyst</i>	Protect & Defend Sydney • 923 Melbourne • 570

¹ ASD Cyber Skills Framework – Cyber Security Occupations
<https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf>

Cyber Security Operations	4. Incident Responder*		Incident Analyst /Responder	Cyber Defence Incident Responder	Protect & Defend Sydney • 923 Melbourne • 570
	5. Operations Coordinator*	Security Project/Program Manager	Cyber Security Manager /Administrator	Cyber Operations Planner	Collect & Operate Sydney • 356 Melbourne • 172
Cyber Security Testing	6. Penetration Tester*	Application Security Consultant / Secure Software Developer	Penetration and Vulnerability Tester	Cyber Defence Analyst	Protect & Defend Sydney • 923 Melbourne • 570
	7. Vulnerability Assessor*		IT Auditor	Vulnerability Assessment Analyst	Protect & Defend Sydney • 923 Melbourne • 570
Cyber Security Architecture	8. Cyber Security Advice and Assessment*		Cyber Security Consultant / Cyber Security Specialist	Cyber Defence Analyst	Protect & Defend Sydney • 923 Melbourne • 570

	9. Vulnerability Researcher*	Security Architect	Cyber Security Architect /Cyber Security Engineer	<i>Research and Development Specialist</i>	Securely provision Sydney • 2133 Melbourne • 1302
--	------------------------------	--------------------	---	--	--

Cyber Security non-technical roles					
Cyber Security Functional Roles	Specific roles identified	Specific responsibilities	Related occupation titles		
Training, Education and Awareness.* ²	10. Security Training, Awareness and Communication	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.	- Cyber Instructional Curriculum Developer - Cyber Instructor	Training, Education & Awareness	Oversee & Govern Sydney • 1466 Melbourne • 821
Legal Advice and Advocacy*	11. Cyber Legal Advisor	Provides legal advice and recommendations on relevant topics related to cyber law.	Cyber Legal Advisor	Legal Advice & Advocacy	Oversee & Govern Sydney • 1466 Melbourne • 821
	12. Privacy Officer/Privacy Compliance Manager	Develops and oversees privacy compliance program and privacy	Cyber Privacy Officer/	Legal Advice & Advocacy	Oversee & Govern Sydney

² These are NICE framework cyber security functional domains.

		program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.			• 1466 Melbourne • 821
--	--	--	--	--	--

Australian Labour Market – new standardized roles advertised nationally (June 2020 – June 2021)

ICT Security Specialist	Security Consultant	Security architect or engineer	Auditor	Business or systems analyst	Developer or programmer	Security Officer	Program manager/Manager	Operations & Support	
735	488	891	53	63	66	0	46	0	
442	244	727	0	357	0	0	0	208	
407	212	104	116	60	0	1080	409	0	
418	506	515	0	119	0	0	21	0	
168	374	192	0	259	0	0	0	7	
77	98	33	0	39	0	0	0	11	
18	32	21	0	10	0	45	7	35	
2265	1954	2483	169	907	66	1125	483	261	9713

COMMON QUALIFICATIONS (AUSTRALIAN MARKET)

Overview:

- Australia is a qualified and credentialed country, although not all training in the ICT area is accredited
- In 2018-19 alone, an estimated 10.2 million people reported holding 15.4 million qualifications
- VET qualifications, at a population level, are more common, particularly at CERT III/IV Levels
- Available data for 'ICT Professionals,' which currently subsumes cyber security related roles (at the ANZSCO 2-digit level), shows that **out of a total of 300,000 workers (83% male), they held over 410,000 qualifications.**
 - 52.7% held a single qualification
 - 37.6% held two or more qualifications

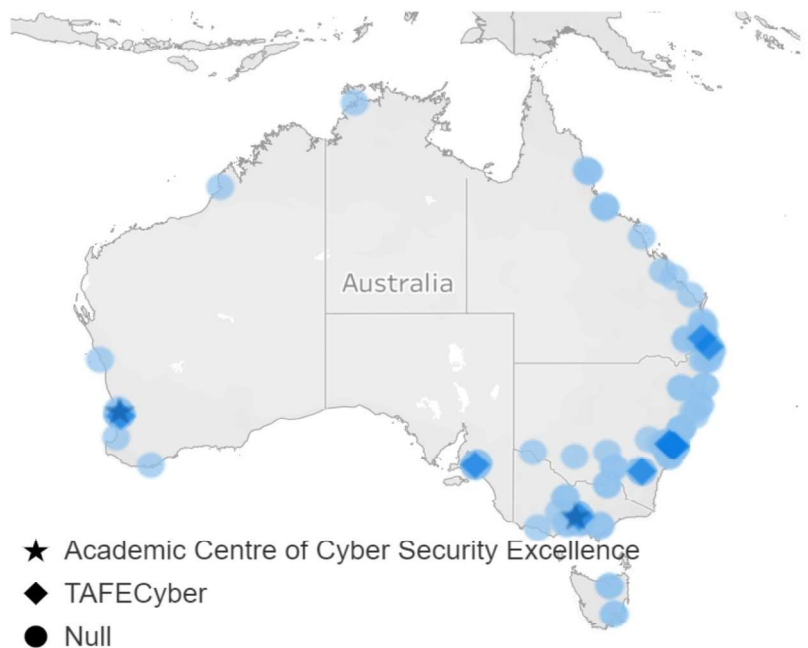
- *Source: Hall & Stanwick (2021).*

AUSTRALIAN CYBER SECURITY : TERTIARY QUALIFICATIONS

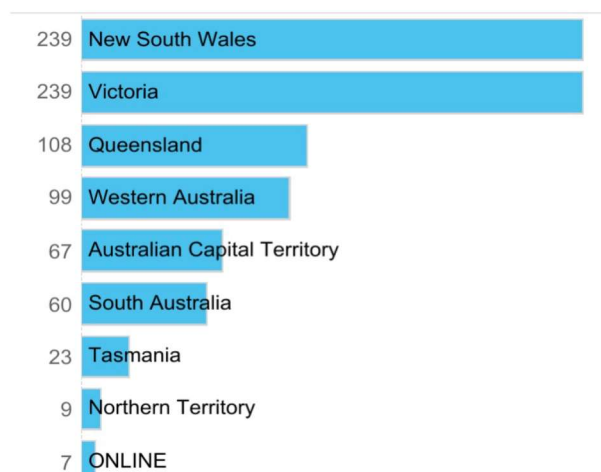
Australian tertiary providers offer a wide range of qualifications, incorporating specific cyber security courses.

The Eastern Seaboard States, including NSW, Queensland and the ACT, as well as Victoria, offer the highest number in aggregate.

We have provided a breakdown, by State and Territory, of the number of cyber courses offered across Australia, stratified by State and Territory.



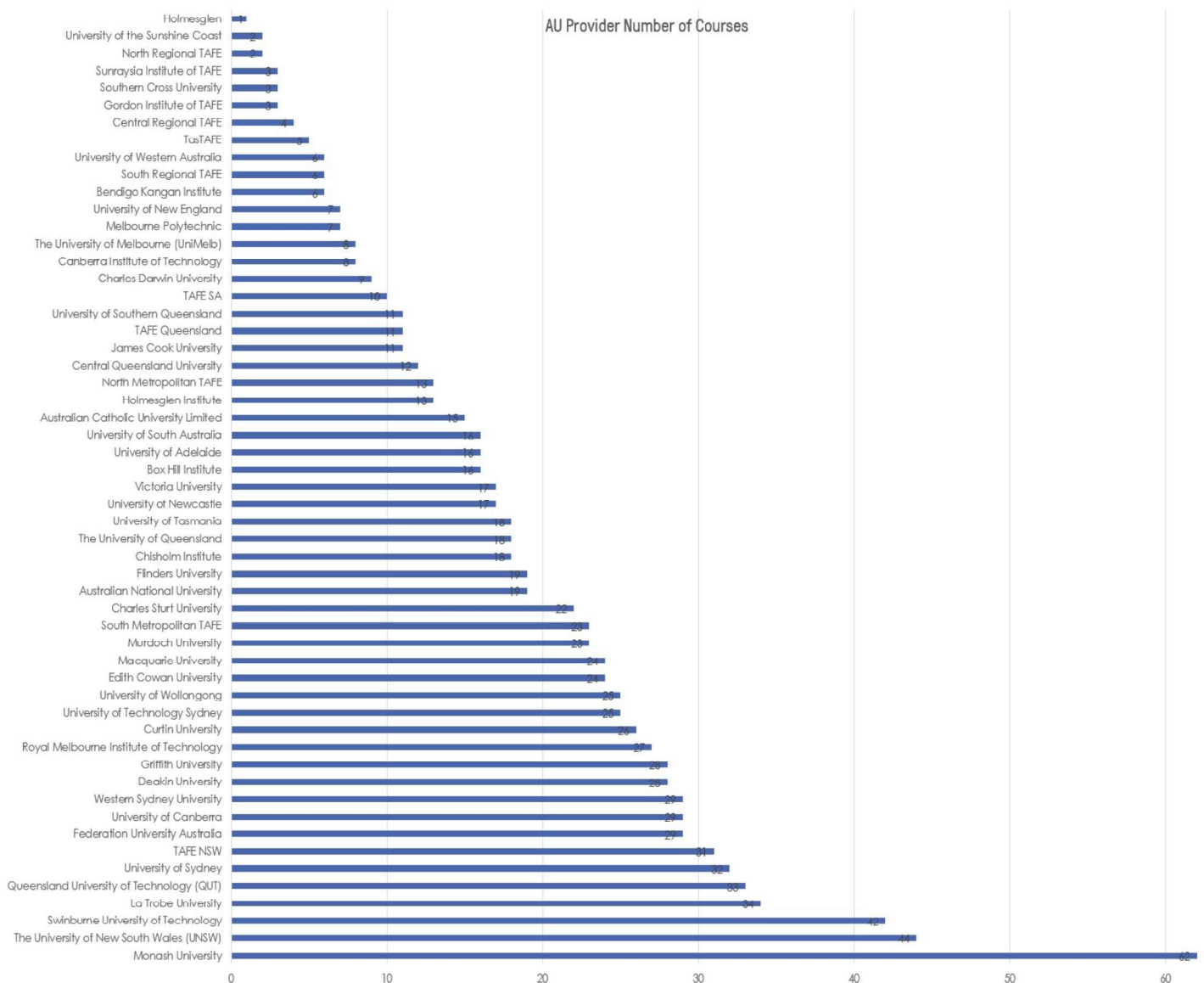
Courses By State



National Courses By Institution

Unsurprisingly, there is a clustering and concentration of cyber security courses, stratified by institution, in both NSW and Victoria.

Each of the top ten highest course providers (by number of qualifications), are from either State. The number of advertised and listed offerings varies greatly, by institution type, with Universities, according to this data, offering a greater variety and number of qualifications, through to Doctoral level study.



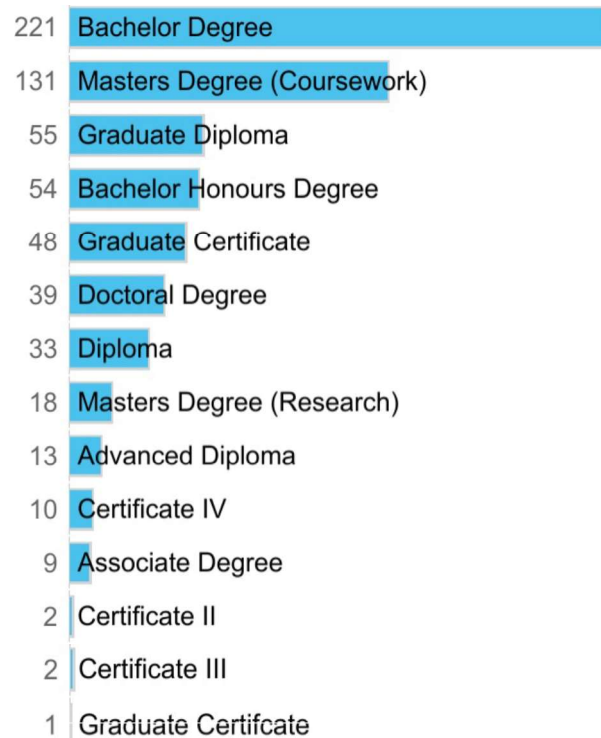
National Courses: By Qualification Level

The Australian cyber security educational landscape is served by a high number of undergraduate qualifications, primarily through bachelor degrees, diplomas and certificates.

There are notable offerings at Masters and Doctoral level too, and an array at graduate level, ranging from Graduate Certificates to Masters (by coursework and research), and Doctoral, degrees.

Course duration

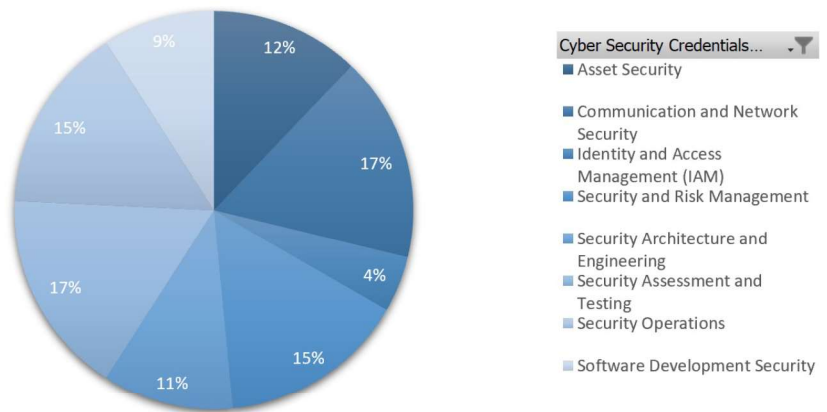
The duration of courses at higher education providers varies greatly, from 19 weeks (in the case of an advanced diploma) to 416 weeks (a combined undergraduate degree), with Masters and Doctoral degrees occupying a middle-point between these.



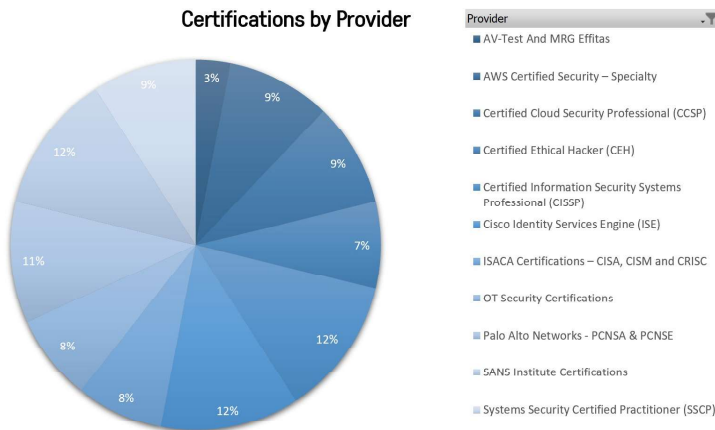
Micro-Credentials

Provider	Cyber Security Credentials By Certification	Certified Information Security Systems Professional (CISSP)	AWS Certified Security – Specialty	Certified Cloud Security Professional (CCSP)	ISACA Certifications – CISA, CISM and CRISC	OT Security Certifications	Palo Alto Networks – PCNSA & PCNSE	Systems Security Certified Practitioner (SSCP)	Certified Ethical Hacker (CEH)	SANS Institute Certifications	Cisco Identity Services Engine (ISE)	AV-Test And MRG Effitas
Certified Information Security Systems Professional (CISSP)	Security and Risk Management	x	x	x	x	x	x	x	x	x	x	
Certified Information Security Systems Professional (CISSP)	Asset Security	x	x	x	x		x	x		x	x	
Certified Information Security Systems Professional (CISSP)	Security Architecture and Engineering	x		x		x	x	x		x	x	
Certified Information Security Systems Professional (CISSP)	Communication and Network Security	x	x	x	x	x	x	x	x	x	x	x
Certified Information Security Systems Professional (CISSP)	Identity and Access Management (IAM)	x								x	x	
Certified Information Security Systems Professional (CISSP)	Security Assessment and Testing	x	x	x	x	x	x	x	x	x	x	x
Certified Information Security Systems Professional (CISSP)	Security Operations	x	x	x	x	x	x	x	x	x	x	
Certified Information Security Systems Professional (CISSP)	Software Development Security	x	x				x		x	x	x	

Certification Type



Certifications by Provider

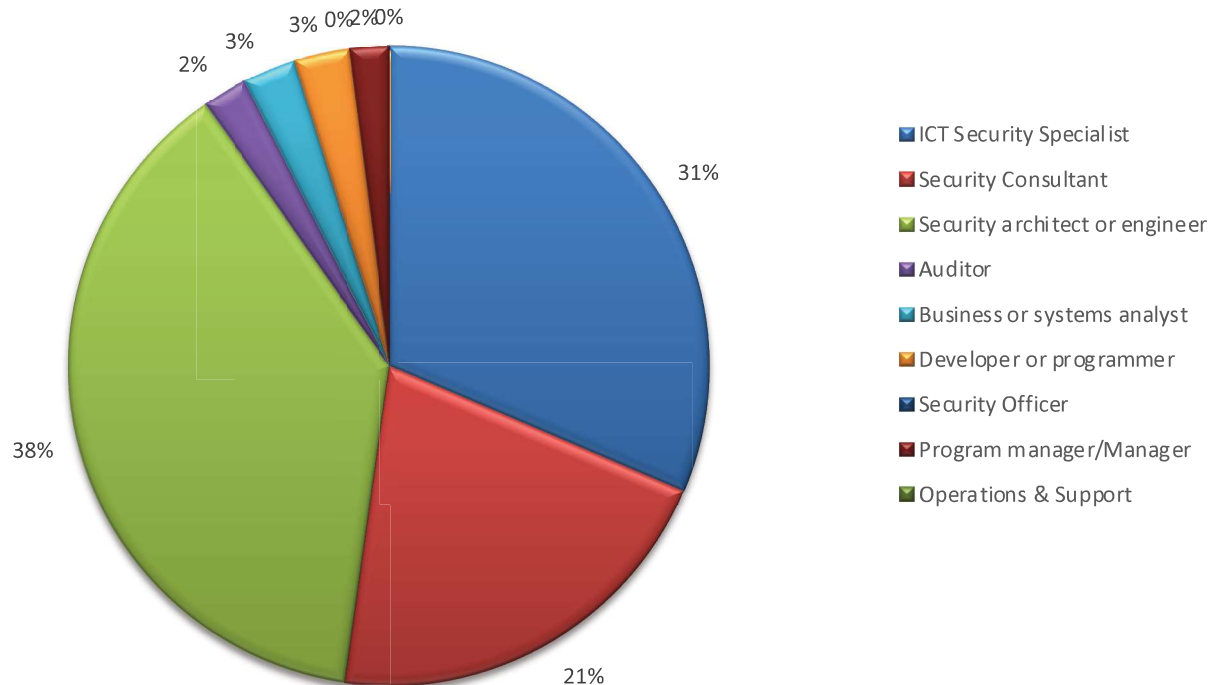


ADVERTISED VACANCIES

In the period June 2020 - June 2021, there were approximately 9713 vacancies advertised across Australia in relation to cyber security (specifically including online job platforms). These were categorized, and standardised, according to the core job roles across the NICE Framework, to enable analysis. They provide insights into the most common *types* of roles across the economy, in relation to cyber security.

The data shows that security architects or engineers were the highest proportion of hires (38%), followed by ICT security specialists (31%) and Security Consultants (21%). Formal roles, such as auditors, accounted for only 2% of hires, although it is highly likely that 'security consultants' might absorb some of these functions.

Australian advertised roles in cyber security, by standardised category (June 2020 - June 2021)

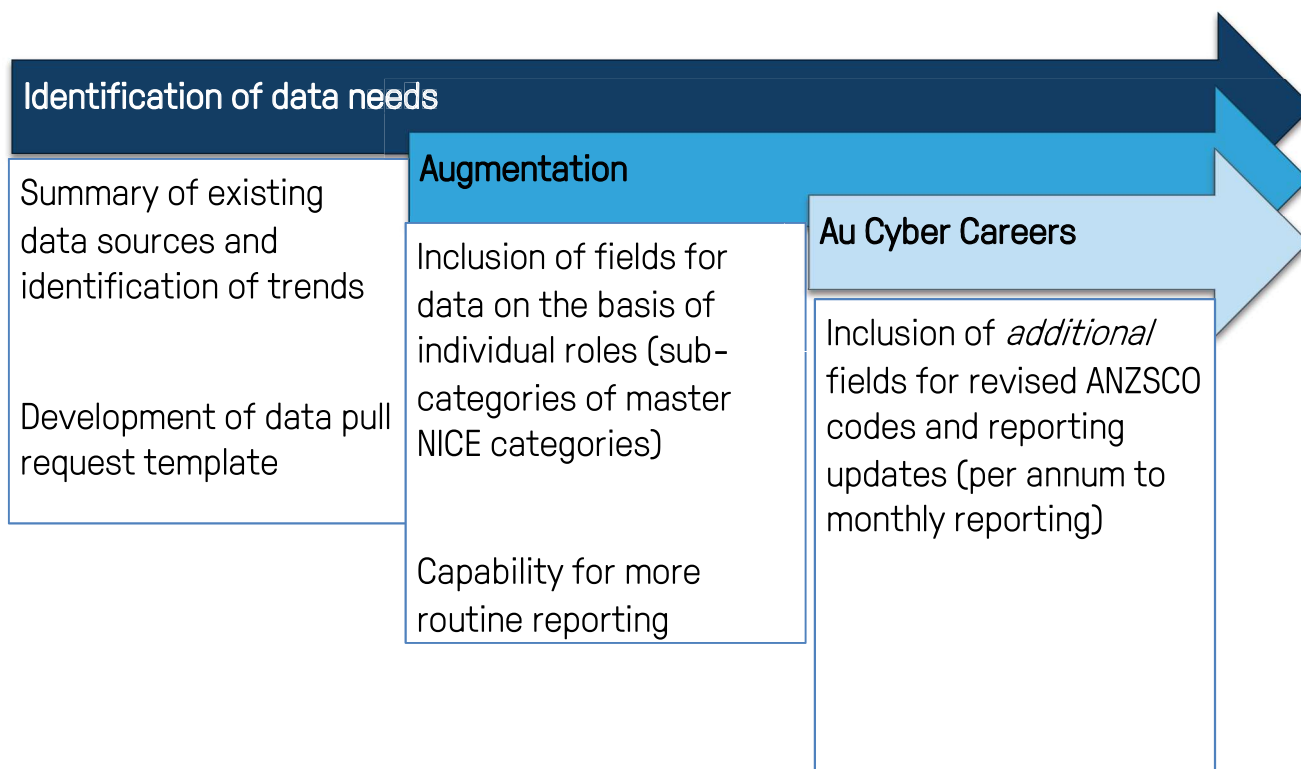


FORWARD GROWTH/FORECASTING: PHASE 2

Forecasting model: Phase two of AuCyberSeek

We envisage the forecasting model, subject to stakeholder input, being developed and enacted in a three stage process, as outlined below. This encompasses the current phase of data analysis, initial augmentation, to improve the quality, breadth and availability of data and, finally, a full optimization, which maps the NICE Categories against the revised ANZSCO codes. It is anticipated that these will be announced in November 2021.

This will enable data to be ingested, digested and modelled over shorter timeframes, including months, which will make comparisons easier, including by location, field of specialization and other relevant criteria.

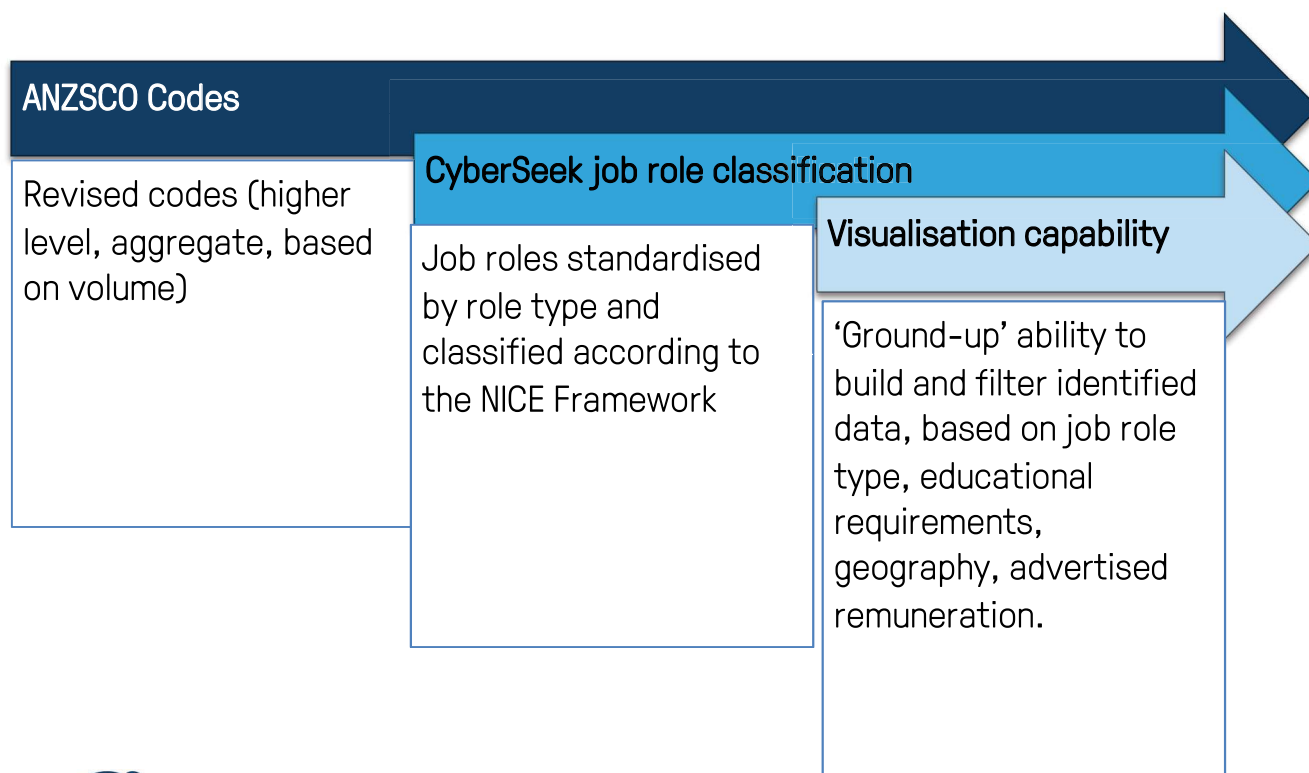


Phase Two: Build model

Principles to inform phase two optimization

Principles

- **Data inputs:**
 - Up to 6-month lag, in terms of algorithmic design
 - Align CyberSeek data with ANZSCO codes (cascading approach – broad categorization to job role alignment)
 - Gender data to be scraped, where possible (from identified job adverts)
- **Visualisation:**
 - Ground-up approach, from a user perspective, is paramount (not just geographically based by State, Territory, or LGA boundaries alone)
 - Configure/build a picture of data by job type, skills profile and LGA/ State and Territory Boundary (and a combination of the three)
 - Gender to be cross-referenced, using ABS Labor Force data (quarterly)



Core augmentation risks

Gender-based data

Based on current labour market data (listed advertisements), gender-based data is lacking (as an input) for an augmented model. ABS quarterly data provides an update, at a high level, on actual labour market trends (new roles, employment rates) but this does not provide adequate granularity to enable an assessment of real-time realities specifically in relation to cyber security, as a field, profession or industry.

As a risk mitigation, it is recommended that the augmented website provide a separate ability to synthesise ABS data, provided quarterly, and contains appropriate disclosures about the ability to report accurately on factors such as gender (i.e. by listing other grounds on which data are captured).

APPENDIX ONE: REFERENCES/DATA SOURCES

Source	Nature of data	Data fields	Frequency
<i>IT Security Consulting in Australia</i> (IBIS World)	Primary and Secondary	- Jobs - Sector growth - Dominant companies	Annual
<i>Digital Census 2020</i> (AustCyber)	Secondary	Aggregate number of cyber security jobs (Australia-wide)	Annual
<i>Vacancy Report June 2021</i> (National Skills Commission)	Primary	ANZSCO code level	Quarterly
<i>Sector Competitiveness Plan</i> (AustCyber)	Primary	Aggregate number of cyber jobs (Australia wide, and State-State)	Annual

APPENDIX TWO: DATA REPORTING TEMPLATE

1. DISER requester details	
Contact name	
Position	
Division/area	
Physical Address	
Telephone number	
Email	
2. Data specification and use	
Data description	Please outline the nature of the data you are seeking. Some factors you might wish to consider include: • Data type (i.e. # of new advertised jobs within x category area) • Level of granularity of data (i.e. aggregated or further defined) • Timeframe of data (i.e. from 2019-2021) • Geospatial parameters (i.e. within the State of NSW, or National)
Frequency of data provision	How frequently will the data need to be provided? ☐ Once off ☐ Quarterly
Uses(s) of the data	<u>Uses</u> Please describe how the data will be used. This might include, for example: preparing detailed briefing notes or supporting evidence for New Policy Proposals. <u>Publication</u> How long will the data be stored for and how, if at all, will it be published?
Will the data be integrated, matched or in any other way compared with existing data sets?	☐ Yes. (if so, which ones, please specify: _____) ☐ No
Data Access	Within your Department, who will have access to the data we generate? For example, will it be IT contractors, policy officers, procurement officers or others?
Relevant conflicts of Interest	Are there any known or potential conflicts of interest in terms of who will obtain the information, or any third parties who may have access to it?
3. Purpose of request	
What is the reason for this data request?	For example, what initiative is this part of, is this sought as part of a response to a Ministerial Briefing request, Question on Notice, Request for Proposals, or to support broader policy development purposes?
Data provision date	When is this data required by?

APPENDIX THREE: AU CyberExplorer optimization

Potential additional data field	Utility	Rationale
Gender (m/f/x)	Disaggregation by protected attribute	Provide more timely, and gender-specific, overview of available roles in the labour market (vis-à-vis cyber security)
ANZSIC (Division)	Correct attribution of activity to divisions within the labour market	Alignment between master framework and sub-categorisation of cyber security roles
ANZSCO (Code) (2 digit level)	Sub-category mapping to identify proximate need	Provide granular insights in where new jobs are being advertised/current jobs are
Age	Disaggregation by protected attribute	Provide timely overview of age-related labour market mobility
Remuneration	Indicator of labour market supply/demand	Obtain an indication of the relative value of roles at particular points in time

APPENDIX FOUR: GLOSSARY OF TERMS

ABS	The Australian Bureau of Statistics is an independent statutory agency of the Australian Government which is responsible for statistical collection and analysis of data, and for giving evidence-based advice to federal, state and territory governments.
ANZIC	ANZIC Industry Classifications - Australian and New Zealand Standard Industrial Classification. A system administered jointly by the Australian Bureau of Statistics and Statistics New Zealand which assigns a unique number to each industry in order to identify the firms operating in each class and sub-class and to allow for the collection of data such as location, number of employees, and annual sales.
ANZSCO	An object used for the completion of a business task.
ASSETS	Assets maybe tangible or intangible items and can relate to equipment, software code, data, facilities, personnel, market value and also public opinion.
ANZSCO	Australian and New Zealand Standard Classification of Occupations. The titles used in ANZSCO are intended to convey the clearest possible idea of the nature of the particular occupation.
CyBOK	Cyber Security Body of Knowledge. A comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector.
CyberSecurity	The efforts made to design, implement, and manage and maintain security of business networks, or devices connected to the Internet including the technical aspect to apply these and the training of personnel to manage, implement and maintain them.

APPENDIX FOUR: GLOSSARY OF TERMS

Digital Economy

A digital economy is the results of many technology based connections between individuals or organisations, devices, data, and processes and refers to an economy that is led by digital computing technologies.

NICE Framework

The National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework) is a **reference resource** that classifies the typical skill requirements and duties of cybersecurity workers.

NIST

The National Institute of Standards and Technology is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. Its mission is to promote American innovation and industrial competitiveness.

F

G

H

I

BIBLIOGRAPHY

AustCyber (2020). *Australia's Cyber Security Sector Competitiveness Plan*. Canberra: AustCyber.

AustCyber (2020). *Digital Trust Report*. Canberra: AustCyber.

Hall, M. & Stanwick, J. (2021). *The stock of qualifications in Australia*. Canberra: NCVER.

IBISWorld (2020). *IT Security Consulting in Australia*. Available online.

National Skills Commission (2021). *Vacancy Report June 2021*. Canberra: National Skills Commission.

AUCyberExplorer baseline dataset extension session

Agenda

- Contract requirements review - supply
- Contract requirements review – demand & education
- Next steps

Appendix

- Project development timeline

Session objectives

1. Prioritise contractual requirements, considering feasibility
2. Understand intended uses

Rebranded site

<https://www.aucyberexplorer.com.au/>

Contract requirements review – supply (workforce) baseline dataset extension (15 mins)

	Contractual requirements	Attribution	Feasibility	Intended uses (to be defined)	Must/ Could/ Should
Australian Workforce (supply)	i. Data on the cyber security sector workforce including breakdown by gender, neurodiversity (if known) , age distribution, geography (states/territories)	Gender	EBG has confirmed as feasible, ABS census data will be leveraged		Must
		Neurodiversity	Discussed with EBG, this data is likely unavailable		
		Age distribution	EBG – Feasible, however age is generally not included with other variables in data sources which will restrict ability to visualize with other data points. User stories tbd to support Is there a specific age banding required?		
		Geography	Already discussed under forecasting model as in scope – frameworks to be reviewed to determine appropriate grouping level		Must
	ii. Baseline data of cyber security professionals in each ANZSIC Division by above variables, ANZSCO code and product/service	ANZSIC Division	Already discussed under forecasting model as in scope	Alignment with Aus framework, inform government policy and initiatives	Must
		ANZSCO occupation code <i>Requirement is for the 6 digit code</i>	Already discussed under forecasting model as in scope	As above	Must
		Product/service	Products/services reported in the Industry Capability report are company based, which wont translate to individuals. Product/service can indirectly be derived via skills (skills should be an indicator for the type of product/service an employee will work on)		
	iii. International comparisons of the Australian workforce and skills supply (shortages/met/oversupply)	Threshold measurement to be defined for the following groupings; - Shortages - Met - Oversupply	To be determined with EBG what data is available for comparison across countries (in addition to US which)		

Contract requirements review – Supply (workforce) baseline dataset extension & Education (30 mins)

	Contractual requirements	Attribution	Feasibility	Intended uses (to be defined)	Must/ Could/ Should
Cyber security workforce recruitment	i. Total cyber security job openings, with breakdown by employment type (ie. Full time, part time), geography, ANZSIC Division, ANZSCO code	Employment type	EBG - feasible to be collected from job ads		Must
		Geography	Already discussed under forecasting model as in scope		Must
		ANZSIC Division	Already discussed under forecasting model as in scope		Must
		ANZSCO code <i>Requirement is for 6 digit code</i>	Already discussed under forecasting model as in scope		Must
	ii. Total job openings with breakdown by requested education level, most sought after certifications requested by employers, most sought after skills requested	Education	EBG – Feasible, only for postings which explicitly request a certain education level.		
		Certifications			
		Skills	Skills – was the intent to be mapped to NICE ksat’s? Further detail on validation of skills mapping TBC		
	iii. Breakdown of job openings by job titles including most sought after and salary	Ranking of most sought after (Salary is already met in the baseline dataset)	Is there a specific requirement for how this is defined, is it based on top X advertised and is there a threshold for the number of advertisements?		
	iv. Time to recruit	Time to recruit	EBG – US model would require testing and QA to determine if same model is appropriate for Aus. This would be time intensive and not available until after March 22		
	v. Failure rates	Failure rates	EBG – Difficult to capture, social media profiles could be leveraged but this would be a low confidence measure		
Cyber security related education	i. Enrolments by type of institution		This will be difficult to aggregate as not reported by institutes, what is the intended use for this?		
	ii. Number of graduates		As above		
	iii. Educational institutions and courses		AustCyber’s Education Map provides this information, potentially look at funneling users to the already existing tool?		
	iv. Number and type of certification holders		Delivered by existing dataset/platform, are any changes required to this?		
	v. Linkages between certifications and cyber security jobs via common skills		Data is available in existing dataset, changes required? Is mapping at AQF a requirement?		

Next steps

- AustCyber to document requirements and answer any outstanding questions - ETA Mon 6th Dec
- Requirements documents to be circulated for review
- Requirements to be handed over to vendors – ETA Fri 10th Dec

Clarification points

- ANZSIC Division granularity - are there use cases for having a lower-level granularity within industry?
- ANSZCO code update – Will the data be available at the beginning of March (to be factored into project planning)?
- Relevant framework for geography – LGA, SA4 or other?
- Skills – is there any intent to have these matched to NICE KSAT's? *(to be confirmed with EBG what the skills currently align to (if any) and the validation process. 44 skills total are currently included, refer to the left)*

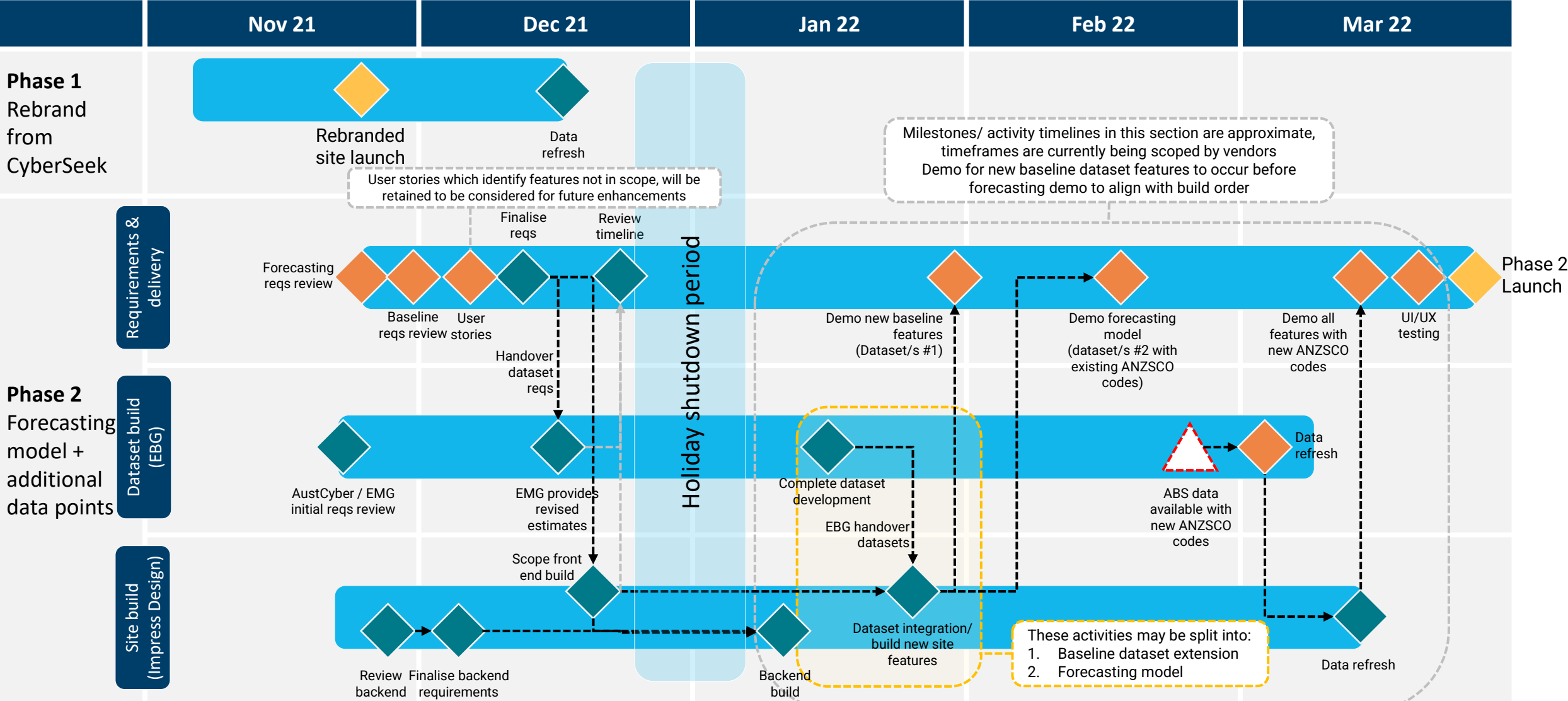
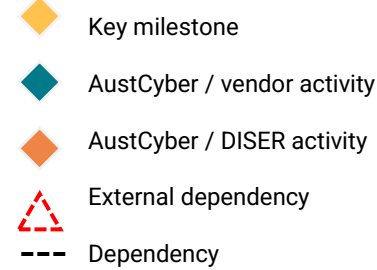
Current skills list

LINUX	Network Security
Java	Audit Planning
Systems Engineering	Cryptography
Accounting	Forensic Toolkit
Intelligence Analysis	Network Engineering
Python	.NET
Information Security	Risk Management
Surveillance	Vulnerability Assessment
Internal Auditing	Information Assurance
Computer Forensics	Asset Protection
Cisco	COBIT
Software Development	Intrusion Detection
SAP Finance	Technical Support
Counter Intelligence	Microsoft C#
Threat Analysis	Virtual Private Networking (VPN)
Information Systems	Security Operations
Penetration Testing	Risk Management Framework
Solution Architecture	Risk Assessment
Project Management	Authentication
System Admin	UNIX
SQL	Intrusion Detection
Financial Analysis	NIST Cybersecurity Framework

Project development timeline

Current activities;

- Rebranded site to be launched this week
- ETA for dataset refresh is mid December, Emsi Burning Glass (EBG) has a dependency on external organisations to provide certifications data
- Backend functionality review is scheduled with Impress Design



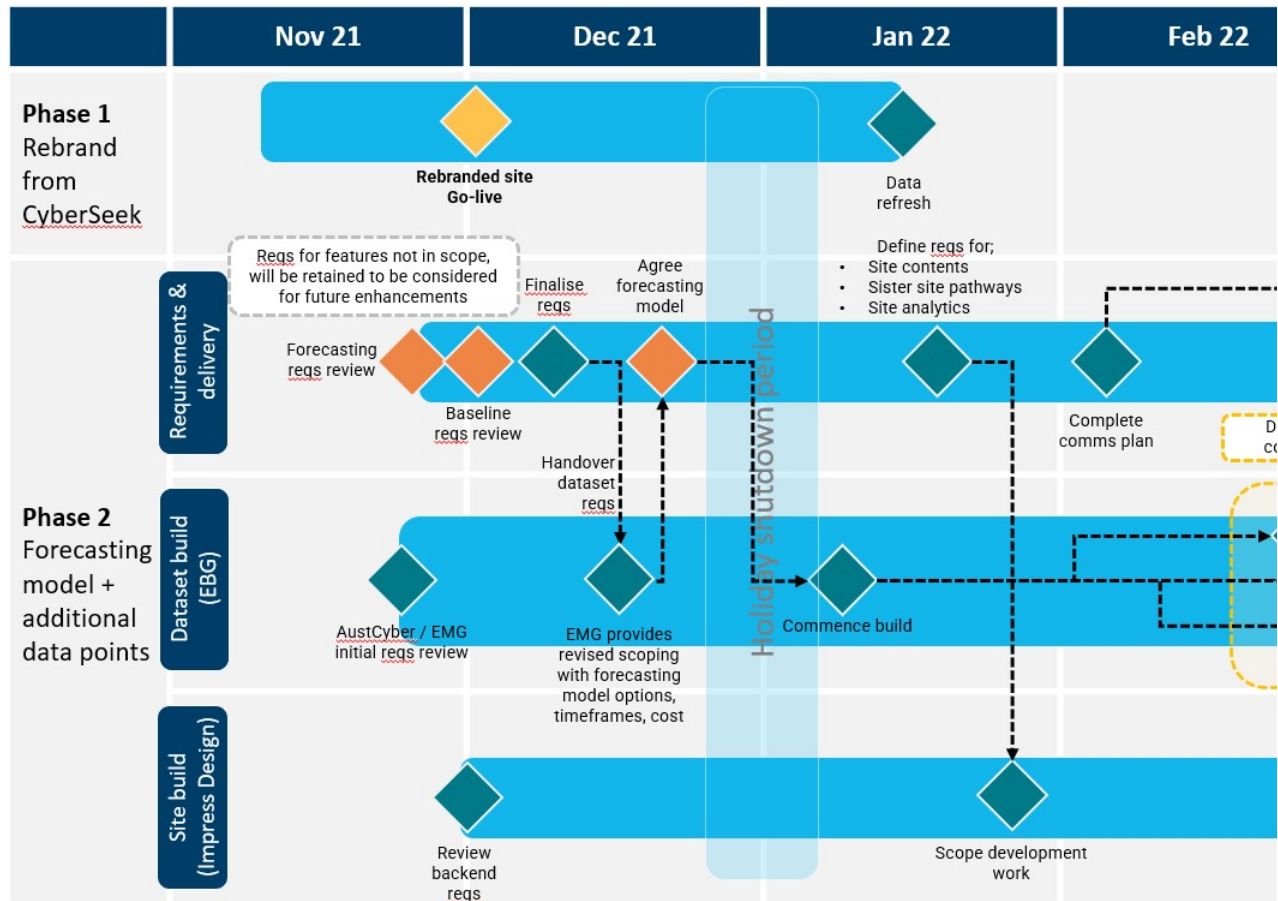
Project development timeline

Current activities;

- Phase 1 data refresh – Impress Design investigating code issues, other data viz options to be assessed
- EBG delivery dates are target dates, may be subject to change

Deliverables

1. Baseline
2. Career p
3. Forecast



Supply and Demand Forecasting Model for AUCyberExplorer

High-Level, Initial Methodology

December 2021

In order to create a supply and demand forecasting model, Emsi Burning Glass (EBG) will lean heavily on the methodologies of proprietary supply and demand forecasting models used within the United States. These methodologies have been rigorously tested within the United States, but additional training and validation will need to be done to ensure that they can properly translate to Australia. EBG reserves the right to alter the below methodology based on learnings during the training and validation process.

Data Sources

- Proprietary EBG Job Posting / Vacancy Data in Australia
 - Time Frame: January 2012 - December 2021
- National Skills Commission 5-Year Employment Projections by:
 - Occupation
 - Industry
 - Region
- ABS Job Mobility Data
- ABS Employment Data

Model Methodology

Demand

Demand projections will leverage proprietary EBG job posting data, which will be pulled by industry, occupation, and geography (SA4, State, National) within Australia from January 2012 through December 2021. This data will be processed to remove seasonality and limit deviations from the rolling mean. It will then be converted into relative counts and transformed into an index for each occupation, industry, and geography combination. If we find insufficient data for a specific geographic level, we will roll up and use the index of the larger geographic level.

We will then pass these indices into a Support Vector Machine (SVM) model to predict job postings over the next five years. We will ensure that negative growth rates are capped to prevent specific occupations from disappearing altogether.

Supply

Supply projections will leverage the demand projections as outlined above with one additional step. These growth projections will be scaled to ensure that they mimic the projected growth rates produced by the National Skills Commission.

Additionally, we will leverage the National Skills Commission employment projections. The National Skills Commission produces 5-year employment projections by occupation, but these are not cut by industry and geography, so some additional processing will need to be done to get to this level of granularity. We will do some additional weighting of the occupation projections, likely utilizing a combination of historical demand and projected supply growth rates for industries and regions. Actual weights will be determined throughout the training and validation process.

We will also use historical ABS employment by industry, occupation, and region to calculate observed year-over-year employment growth rates. We will do some additional processing of this data to ensure that we do not exhibit runaway growth or decline. In the case where there is missingness for an occupation, industry, and geography combination for a certain year, we will take the maximum employment ever reported for that occupation in that industry and geography and then estimate the base year employment using the growth rate. As we will do with the demand projections, we will scale these historical growth rates to ensure that they mimic the projected growth rates produced by the National Skills Commission.

After all the above steps have been taken, we will combine all of the above data points to create a simple weighted average. We will weigh the National Skills Commission supply projections the most, followed by the EBG demand-side projections, and then the ABS historical supply growth rates. Actual weights will be determined throughout the training and validation process.

ANZSCO Occupation code to NICE work role mapping

In the AUCyberExplorer demand dataset (which is derived from internet job postings) advertised job titles will be mapped to ANZSCO Occupat

- There are significantly more NICE work roles than ANZSCO occupation codes
- The ANZSCO Occupation codes are based on the latest codes released in December 21
- Mappings have been done based on definitions from each framework, there are some NICE work roles where there is no ANZSCO code with :
- For roles which do not map, general roles/groupings have been created, or an alternative non cyber security ANZSCO code has been suggest

NIST NICE work role definitions: [NIST' tab in this document](#)

ABS ANZSCO occupation definitions: <https://consult.abs.gov.au/standards-and-classifications/anzsco-targeted-update-2021-proposed-chg>

ANZSCO Occupation	Specialisations	# mapped work roles	% of total
135111 – Chief Information Officer	Chief Information Security Officer	1	2%
135112 – ICT Project Manager	ICT Security Project Manager	3	6%
261312 – Developer Programmer	Cyber Security Developer	6	12%
261315 – Cyber Security Engineer		3	6%
261317 – Penetration Tester		1	2%
262114 – Cyber Security Analyst	Cyber Threat Analyst, Malware Analyst, Cyber Security Vulnerability Assessor, Cyber Security Vulnerability Researcher	17	33%
262115 – Cyber Security Operations Coordinator	Cyber Security Incident Responder	2	4%
262116 – Cyber Security Advice and Assessment Specialist		4	8%
262117 – Cyber Security Architect		1	2%
262118 – Cyber Governance Risk and Compliance Specialist		3	6%
261111 - ICT Business Analyst		1	2%
Manager - Cyber Security		3	6%

Training & Education - Cyber Security		2	4%
Legal - Cyber Security		1	2%
Workforce Development - Cyber Security		1	2%
Product Manager - Cyber Security		1	2%
None		2	4%
		52	100%

These roles do not map between ANZSCO and NICE.
AUCyberExplorer can be used as an assessment tool to measure whether roles are advertised that fit into these categories.

ion codes via NICE work roles. Notes for this mapping exercise;

a definition that aligns
ed

[https://www.mcafee.com/au/resources/supporting_documents/CYBER%20SECURITY_Occupation%20Groups_Proposed%20Cl](#)

Work roles	ANZSCO Occupation
Authorizing Official/Designating Representative	262118 – Cyber Governance Risk and Compliance Specialist
Security Control Assessor	262116 – Cyber Security Advice and Assessment Specialist
Software Developer	261312 – Developer Programmer
Secure Software Assessor	262114 – Cyber Security Analyst
Enterprise Architect	None
Security Architect	262117 – Cyber Security Architect
Research & Development Specialist	262114 – Cyber Security Analyst
Systems Requirements Planner	261111 - ICT Business Analyst
System Testing and Evaluation Specialist	261317 – Penetration Tester
Information Systems Security Developer	261312 – Developer Programmer
Systems Developer	261312 – Developer Programmer
Database Administrator	261312 – Developer Programmer

Data Analyst	262114 – Cyber Security Analyst
Knowledge Manager	Manager - Cyber Security
Technical Support Specialist	261315 – Cyber Security Engineer
Network Operations Specialist	261315 – Cyber Security Engineer
System Administrator	261315 – Cyber Security Engineer
Systems Security Analyst	262114 – Cyber Security Analyst
Cyber Legal Advisor	Legal - Cyber Security
Privacy Officer/Privacy Compliance Manager	262118 – Cyber Governance Risk and Compliance Specialist
Cyber Instructional Curriculum Developer	Training & Education - Cyber Security
Cyber Instructor	Training & Education - Cyber Security
Information Systems Security Manager	262116 – Cyber Security Advice and Assessment Specialist
Communications Security (COMSEC) Manager	Manager - Cyber Security
Cyber Workforce Developer and Manager	Workforce Development - Cyber Security
Cyber Policy and Strategy Planner	262116 – Cyber Security Advice and Assessment Specialist
Executive Cyber Leadership	135111 – Chief Information Officer
Program Manager	135112 – ICT Project Manager
IT Project Manager	135112 – ICT Project Manager

Product Support Manager	Product Manager - Cyber Security
IT Investment/Portfolio Manager	135112 – ICT Project Manager
IT Program Auditor	262118 – Cyber Governance Risk and Compliance Specialist
Cyber Defense Analyst	262114 – Cyber Security Analyst
Cyber Defense Infrastructure Support Specialist	262114 – Cyber Security Analyst
Cyber Defense Incident Responder	262114 – Cyber Security Analyst
Vulnerability Assessment Analyst	262114 – Cyber Security Analyst
Threat/Warning Analyst	262114 – Cyber Security Analyst
Exploitation Analyst	262114 – Cyber Security Analyst
All-Source Analyst	262114 – Cyber Security Analyst
Mission Assessment Specialist	262116 – Cyber Security Advice and Assessment Specialist
Target Developer	261312 – Developer Programmer
Target Network Analyst	262114 – Cyber Security Analyst
Multi-Disciplined Language Analyst	261312 – Developer Programmer
All Source-Collection Manager	262114 – Cyber Security Analyst
All Source-Collection Requirements Manager	Manager - Cyber Security
Cyber Intel Planner	262115 – Cyber Security Operations Coordinator
Cyber Ops Planner	262115 – Cyber Security Operations Coordinator
Partner Integration Planner	None
Cyber Operator	262114 – Cyber Security Analyst

Cyber Crime Investigator	262114 – Cyber Security Analyst
Law Enforcement /CounterIntelligence Forensics Analyst	262114 – Cyber Security Analyst
Cyber Defense Forensics Analyst	262114 – Cyber Security Analyst

[anges%20v1.3%20updated%208102021.pdf](#)

Mapping notes	Specialisation (if relevant)
NICE work roles include a 'Enterprise Security Architect', meaning the Enterprise Architect role will not be specifically related to cyber and does not require to be mapped	
	Cyber Security Researcher or Vulnerability Researcher
There is no cyber related ANZSCO code that correlates with this role, it has been mapped to the equivalent ICT role. Consider a specialisation for future ANZSCO reviews	
	Cyber Security Developer
	Cyber Security Developer
	Cyber Security Developer

There is no cyber related ANZSCO code that correlates with this role, management related roles have been grouped into a general category. Note: 224213 - Health Information Manager may be considered for future ANZSCO reviews (if associated roles are found to be advertised through AUCyberExplorer)	
	Network Programmer
No cyber related roles, could potentially be mapped to 271299 - Judicial and Other Legal Professionals nec	
ANZSCO definition does not refer to privacy specifically, refers to compliance and policy broadly	
There is no cyber related ANZSCO code that correlates with this role, training & education related roles have been grouped into a general category	
There is no cyber related ANZSCO code that correlates with this role, training & education related roles have been grouped into a general category	
	Cyber Security Advisor
There is no cyber related ANZSCO code that correlates with this role, management related roles have been grouped into a general category Note: 342312 - Communications Operator may be considered for future ANZSCO review (if associated roles are found to be advertised through AUCyberExplorer)	
There is no cyber related ANZSCO code that correlates with this role, management related roles have been grouped into a general category, introducing a grouping for workforce related roles.	
	Cyber Security Advisor
These roles are mapped based on a broad association of Executive leadership roles	
This role would be more senior than a project manager	

There is no cyber related ANZSCO code that correlates with this role, introducing a grouping for product related roles.	
This role would be more senior than a project manager	
Role requires more specific skills than a cyber security analyst, cyber security analyst would be a predecessor in a pathway	Cyber Security Incident Responder
Role requires more specific skills than a cyber security analyst, cyber security analyst would be a predecessor in a pathway	Cyber Security Vulnerability Assessor
Role requires more specific skills than a cyber security analyst, cyber security analyst would be a predecessor in a pathway	Cyber Threat Analyst
	Cyber Threat Analyst
	Malware Analyst
	Cyber Security Developer
	Cyber Security Vulnerability Assessor
	Software Developer
	Malware Analyst
There is no cyber related ANZSCO code that correlates with this role, management related roles have been grouped into a general category. For alignment with other roles which have associated pathways this role could be grouped under 262114 - Cyber Security Analyst (Malware related) or ICT Business Analyst (associated with requirements management)	
There is no cyber related ANZSCO code that correlates with this role, unable to identify what other ANZSCO codes correlate with the role	
	Cyber Threat Analyst

	Cyber Security Vulnerability Assessor

NICE Framework Specialty Areas and Work Role Table of Contents

As of 7/7/2020

NICE Specialty Area

NICE Specialty Area Description

Oversee and Govern

Investigate

Cyber Investigation (INV)

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

[Click to view the Master KSA List](#)

[Click to view the Master Task List](#)

Work Role	Work Role Description	Work Role ID	KSAs	Tasks
IT Investment/Portfolio Manager	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.	OV-PMA-004	Click to view KSAs	Click to view Tasks
Cyber Crime Investigator	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.	IN-INV-001	Click to view KSAs	Click to view Tasks

OPM Code (Fed Use)
804
221

AUCyberExplorer Project Status Report

Overall status this week

G

Overall status last week

G

	RAG status	Commentary
Schedule	A	Issue raised relating to delays for dataset build, which may impact commencement of site build and go-live.
Scope changes	G	DISER have determined to proceed with fast tracking updates to 6-digit code taxonomy
Risks	G	None to report
Issues	G	As per comments against schedule. The issue has a low rating due to low impact, minor schedule delay which does not impact project outcomes or exceed contract timeframe

Green = Project is on track
Amber = Issues have occurred and are being managed
Red = Severe issues have occurred which will impact delivery

Scope changes

This section provides an overview of required changes to the project scope.

Change description	Action required	Outcome
Limitation on feasibility of including 6-digit ANZSCO codes in phase 2 delivery	Draft options paper submitted to DISER	DISER have determined to proceed with fast tracking

Risks & Issues

This section provides an overview of key risks & issues which are impacting project delivery and require resolution or escalation

Risk name	Risk description	Mitigation strategy	Outcome	Inherent risk rating	Status
None to report					

Issue name	Issue description	Impact	Action plan	Issue rating	Status
Delay to dataset build due to contract delay	Due to the extended time required to negotiate the contract scope, there is an approximate 2 week delay to datasets being handed over for site build	Impress Design has a dependency on datasets being handed over to commence site build	Track progress to handing over sample datasets with EBG. EBG have flagged first sample datasets are targeted to be handed over mid-March, if Impress Design can complete majority of the build with the sample datasets (and if they are not further delayed) then the delay to go-live may be reduced	D	Open

Document 11 - LEX 300027

Week ending
25th February 2022

Schedule

This section provides an overview of key activities occurring this and next week.

Activity	Status	Due date	Completed date
Survey user group on site content	In progress	4/03/22	
Agreement of BAU handover plan	In progress	4/03/22	
Legal review of contract	In progress	4/03/22	
Finalise site content	In progress	4/03/22	
Site mockups complete		11/03/21	

Actions

This section provides an overview of actions discussed this week.

See next slide

#	Date raised	Stakeholder group	Action required	Assigned to	Outcome	Status	Closed date
ACT-23	27/01/2022	DISER	Determine availability of uni enrolment data (uCube)	s22(1)(a)(ii)	27/01: Emailed s22(1)(a)(ii) generic inbox with request 4/02: Discussed with s22(1)(a)(ii) at DESE, additional data is available but introducing variables will limit ability to tabulate dataset. To determine granularity requirements with DISER, recommendations from DESE is to separate disability and indigenous into whole numbers (rather than splitting by state etc.) 9/02: s22(1)(a)(ii) to determine the useable combinations of attributes 23/02: s22(1)(a)(ii) following up with Ben for advice on grouping. Other dependencies for inclusion of 'Education Insights' feature in this phase (post delivery of baseline enhancements, international data & forecasting model) include: 1. Ongoing management of data updates ref ACT-26. 2. Budget dependencies - Current budget includes contingency for site build, estimate to be refined once Impress Design has completed mock ups and can estimate hours required for build. Closed - DISER agreed this is not a priority for this phase. s22(1)(a)(ii) to explore whether there is an opportunity to	Closed	23/02/2021
ACT-24	1/02/2022	DISER	Paper outlining options relating to scope changes and the inclusion of 6-digit ANZSCO Occupation codes to be submitted to DISER	s22(1)(a)(ii)	2/02: Draft submitted to DISER, excluding timeframe for taxonomy work to be completed early. Dependency on EBG to provide this information 23/02: Updated paper with costs & timeframes submitted to DISER, DISER to review 24/02: DISER has decided to not fast track the taxonomy updates	Closed	24/02/2022
ACT-25	4/02/2022	DISER	Determine need for geographic concentration measure	s22(1)(a)(ii)	8/02: DISER has provided further response via email, to be discussed in weekly meeting 9/02. 9/02: s22(1)(a)(ii) to organise user testing with small cohort	Open	
ACT-26	4/02/2022	DISER	Determine with ABS viability of age group/gender combinations; - Employed persons by age, sex, state - Employed persons by sex, age group, 4-digit ANZSCO Occupation code	s22(1)(a)(ii)	8/02: ABS has run tabulations on a number of sets of variables, majority of which return an RSE of >25% across the variable in the dataset (this is due to a small volume of data points). The combination of sex, age group and state (excluding ANZSCO codes) are within the acceptable RSE limit (<25%). s22(1)(a)(ii) to confirm how DISER would like to proceed before advising EBG. 14/02: ABS have provided a quote, AustCyber are currently reviewing the terms which state data can only be used for internal use. Plan for ongoing site maintenance to be developed as the custom dataset will be an ongoing cost 23/02: Ongoing management plan to be resolved internally by AustCyber by 25/02	Open	
ACT-27	21/02/2022	DISER	Review average salary for feeder roles, when the career pathways dataset is provided. Previously AustCyber had expressed concern about the average salary for the feeder roles being too low, so the salaries were excluded from the dataset. AustCyber / DISER to review outputs from new dataset to determine inclusion.	s22(1)(a)(ii)	To be reviewed when new datasets are handed over	Open	
ACT-28	23/02/2021	DISER	Determine potential for certifications to be included in AustCyber Education Map. Also to be determined if enrolments & completions VET/Uni tab can be complementary sources for Education Map	s22(1)(a)(ii)		Open	

AUCyberExplorer Project Status Report

Overall status this week		G	Overall status last week		G
	RAG status	Commentary			
Schedule	A	Overall the go-live dates will be delayed 2-4 weeks, due to time taken for the contract negotiation and review. AustCyber will be able to rebaseline and provide new dates once the contract has been finalized.			
Scope changes	G				
Risks	G				
Issues	G	As per comments against schedule. The issue has a low rating due to low impact, minor schedule delay which does not impact project outcomes or exceed contract timeframe			

Green = Project is on track
Amber = Issues have occurred and are being managed
Red = Severe issues have occurred which will impact delivery

Schedule

This section provides an overview of key activities occurring this and next week.

Activity	Status	Due date	Completed date
Legal review of contract	In progress	18/03/22	
Site mockups complete (to be re baselined)		11/03/22	
ABS data request approved and submitted	Complete	11/03/22	11/03/22
Rebaselined go-live dates to be provided		18/03/22	

Scope changes

This section provides an overview of required changes to the project scope.

Change description	Action required	Outcome

Risks & Issues

This section provides an overview of key risks & issues which are impacting project delivery and require resolution or escalation

Risk name	Risk description		Mitigation strategy	Outcome	Inherent risk rating	Status
Legal review of Emsi Burning Glass contract	If the legal review of contract with Emsi Burning Glass takes an extended period of time then there is a risk that the handover of datasets could be delayed		Prioritise legal review	Legal review is complete, risk to be closed out once contract is finalised next week.	C	Open
Issue name	Issue description	Impact	Action plan		Issue rating	Status
Delay to dataset build due to contract delay	Due to the extended time required to negotiate the contract scope, there is an approximate 2-week delay to datasets being handed over for site build	Impress Design has a dependency on datasets being handed over to commence site build	Track progress to handing over sample datasets with EBG. EBG have flagged first sample datasets are targeted to be handed over mid-March, if Impress Design can complete majority of the build with the sample datasets (and if they are not further delayed) then the delay to go-live may be reduced		D	Open

Actions

This section provides an overview of actions discussed this week.

#	Date raised	Stakeholder group	Action required	Assigned to	Outcome	Status
ACT-26	4/02/2022	DISER	Determine with ABS viability of age group/gender combinations; - Employed persons by age, sex, state - Employed persons by sex, age group, 4-digit ANZSCO Occupation code	s22(1)(a)(ii)	8/02: ABS has run tabulations on a number of sets of variables, majority of which return an RSE of >25% across the variable in the dataset (this is due to a small volume of data points). The combination of sex, age group and state (excluding ANZSCO codes) are within the acceptable RSE limit (<25%). s22(1)(a)(ii) to confirm how DISER would like to proceed before advising EBG. 14/02: ABS have provided a quote, AustCyber are currently reviewing the terms which state data can only be used for internal use. Plan for ongoing site maintenance to be developed as the custom dataset will be an ongoing cost 23/02: Ongoing management plan to be resolved internally by AustCyber by 25/02 2/03: AustCyber to confirm copyright clause will not be breached 9/03: Data request approved and submitted, approx. 10 day turn around 11/03: Closed, dataset received	Closed
ACT-27	21/02/2022	DISER	Review average salary for feeder roles, when the career pathways dataset is provided. Previously AustCyber had expressed concern about the average salary for the feeder roles being too low, so the salaries were excluded from the dataset. AustCyber / DISER to review outputs from new dataset to determine inclusion.	s22(1)(a)(ii)	To be reviewed when new datasets are handed over	Open
ACT-28	23/02/2022	DISER	Determine potential for certifications to be included in AustCyber Education Map. Also to be determined if enrolments & completions VET/Uni tab can be complementary sources for Education Map	s22(1)(a)(ii)	Open as an ongoing investigation into how the certification providers fit into existing product	Open
ACT-29	25/02/2022	DISER	New requirement to confirm with DISER: main visualisations to be displayed in one view without scrolling	s22(1)(a)(ii)	11/03: s22(1)(a)(ii) to include as part of design brief.	Closed
ACT-30	2/03/2022	DISER	New requirement to be reviewed and confirmed: Expanding on measure descriptions	s22(1)(a)(ii)	11/03: s22(1)(a)(ii) to review definitions as part of tool tip/data dictionary review.	Open
ACT-31	9/03/2022	DISER	Confirm when 6 monthly data refreshes should occur ie. What month		11/03: DISER team to discuss	Open

AUCyberExplorer Project Status Report

Overall status this week	G	Overall status last week	G
--------------------------	---	--------------------------	---

	RAG status	Commentary
Schedule	A	Overall the go-live dates will be delayed 2-4 weeks, due to time taken for the contract negotiation and review. AustCyber will be able to rebaseline and provide new dates once the contract has been finalized.
Scope changes	G	
Risks	G	
Issues	G	As per comments against schedule. The issue has a low rating due to low impact, minor schedule delay which does not impact project outcomes or exceed contract timeframe

Green = Project is on track
Amber = Issues have occurred and are being managed
Red = Severe issues have occurred which will impact delivery

Schedule

This section provides an overview of key activities occurring this and next week.

Activity	Status	Due date	Completed date
Legal review of contract	In progress	18/03/22	
Site mockups complete (to be re baselined)	In progress	11/03/22	
Rebaselined go-live dates to be provided		25/03/22	

Scope changes

This section provides an overview of required changes to the project scope.

Change description	Action required	Outcome

Risks & Issues

This section provides an overview of key risks & issues which are impacting project delivery and require resolution or escalation

Risk name	Risk description	Mitigation strategy	Outcome	Inherent risk rating	Status
Legal review of Emsi Burning Glass contract	If the legal review of contract with Emsi Burning Glass takes an extended period of time then there is a risk that the handover of datasets could be delayed	Prioritise legal review	Legal review is complete, risk to be closed out once contract is finalised next week.	C	Open

Issue name	Issue description	Impact	Action plan	Issue rating	Status
Delay to dataset build due to contract delay	Due to the extended time required to negotiate the contract scope, there is an approximate 2-week delay to datasets being handed over for site build	Impress Design has a dependency on datasets being handed over to commence site build	Track progress to handing over sample datasets with EBG. EBG have flagged first sample datasets are targeted to be handed over mid-March, if Impress Design can complete majority of the build with the sample datasets (and if they are not further delayed) then the delay to go-live may be reduced	D	Open

Actions

This section provides an overview of actions discussed this week.

#	Date raised	Stakeholder group	Action required	Assigned to	Outcome	Status
ACT-20	25/01/2022	DISER	Determine with NSC if they have plans to introduce 6-digit code to dataset	s22(1)(a)(ii)	9/02: DISER confirmed the 6-digit ANZSCO codes are expected to be included in the NSC dataset 2/03: Reopened for review, further advice from DISER is that it is unlikely the 6-digit ANZSCO codes will be included in this data, currently it is only at 4-digit code level 16/03: s22(1)(a)(ii) is sourcing contacts within NSC to meet and work through the assumptions from each party (will also be meeting with ABS to confirm plans for 6-digit code modelling)	Open
ACT-27	21/02/2022	DISER	Review average salary for feeder roles, when the career pathways dataset is provided. Previously AustCyber had expressed concern about the average salary for the feeder roles being too low, so the salaries were excluded from the dataset. AustCyber / DISER to review outputs from new dataset to determine inclusion.	s22(1)(a)(ii)	To be reviewed when new datasets are handed over	Open
ACT-28	23/02/2022	DISER	Determine potential for certifications to be included in AustCyber Education Map. Also to be determined if enrolments & completions VET/Uni tab can be complementary sources for Education Map	s22(1)(a)(ii)	Open as an ongoing investigation into how the certification providers fit into existing product 16/03: s22(1)(a)(ii) has a meeting next week to discuss internally. Closed for AustCyber to manage internally, DISER to have visibility of outcome once progressed	Closed
ACT-30	2/03/2022	DISER	New requirement to be reviewed and confirmed: Expanding on measure descriptions	s22(1)(a)(ii)	11/03: s22(1)(a)(ii) to review definitions as part of tool tip/data dictionary review. 16/03: Closed out to be delivered as part of the project.	Closed
ACT-31	9/03/2022	DISER	Confirm when 6 monthly data refreshes should occur ie. What month	s22(1)(a)(ii)	11/03: DISER team to discuss 16/03: Align to Labour Force refresh period, taking into consideration 4-6 weeks. Current data refresh ends in Jan 22 in line with most recent Labour Market dataset, potentially moving forward data period will end in Jan/Jul each year (refresh takes approx. 4-6 weeks so will be complete by April/October)	Open
ACT-32	16/03/2022	DISER	Determine if digital/tech providers have reached out with interest in AUCyberExplorer's data	s22(1)(a)(ii)		Open

AUCyberExplorer Project Status Report

Overall status this week		G	Overall status last week		G
	RAG status	Commentary			
Schedule	A	Overall the go-live dates will be delayed 2-4 weeks, due to time taken for the contract negotiation and review. AustCyber will be able to rebaseline and provide new dates once the contract has been finalized, ETA for this is by 11/03.			
Scope changes	G	Changes to inclusion of 6-digit codes has been resolved.			
Risks	G	There is a risk of further delay due to legal review of the contract which is currently in progress.			
Issues	G	As per comments against schedule. The issue has a low rating due to low impact, minor schedule delay which does not impact project outcomes or exceed contract timeframe			

Green = Project is on track
Amber = Issues have occurred and are being managed
Red = Severe issues have occurred which will impact delivery

Scope changes
This section provides an overview of required changes to the project scope.

Change description	Action required	Outcome

Risks & Issues
This section provides an overview of key risks & issues which are impacting project delivery and require resolution or escalation

Risk name	Risk description	Mitigation strategy	Outcome	Inherent risk rating	Status
Legal review of Emsi Burning Glass contract	If the legal review of contract with Emsi Burning Glass takes an extended period of time then there is a risk that the handover of datasets could be delayed	Prioritise legal review		C	Open

Issue name	Issue description	Impact	Action plan	Issue rating	Status
Delay to dataset build due to contract delay	Due to the extended time required to negotiate the contract scope, there is an approximate 2-week delay to datasets being handed over for site build	Impress Design has a dependency on datasets being handed over to commence site build	Track progress to handing over sample datasets with EBG. EBG have flagged first sample datasets are targeted to be handed over mid-March, if Impress Design can complete majority of the build with the sample datasets (and if they are not further delayed) then the delay to go-live may be reduced	D	Open

Schedule
This section provides an overview of key activities occurring this and next week.

Activity	Status	Due date	Completed date
Agreement of BAU handover plan	Complete	4/03/22	2/03/22
Legal review of contract	In progress	11/03/22	
Finalise site content	Complete	4/03/22	
Site mockups complete (to be re baselined)		11/03/22	
ABS data request approved and submitted		11/03/22	

Actions
This section provides an overview of actions discussed this week.

See next slide

#	Date raised	Stakeholder group	Action required	Assigned to	Outcome	Status
ACT-20	25/01/2022	DISER	Determine with NSC if they have plans to introduce 6-digit code to dataset	s22(1)(a)(ii)	9/02: DISER confirmed the 6-digit ANZSCO codes are expected to be included in the NSC dataset 2/03: Reopened for review, further advice from DISER is that it is unlikely the 6-digit ANZSCO codes will be included in this data, currently it is only at 4-digit code level	Open
ACT-25	4/02/2022	DISER	Determine need for geographic concentration measure	s22(1)(a)(ii)	8/02: DISER has provided further response via email, to be discussed in weekly meeting 9/02. 9/02: s22(1)(a)(ii) to organise user testing with small cohort 1/03: Survey designed, pending AustCyber approval to push to 10x cyber companies (target = approx. 20 users) 2/03: Closed, to be completed under post project activities as broader user testing	Closed
ACT-26	4/02/2022	DISER	Determine with ABS viability of age group/gender combinations; - Employed persons by age, sex, state - Employed persons by sex, age group, 4-digit ANZSCO Occupation code	s22(1)(a)(ii)	8/02: ABS has run tabulations on a number of sets of variables, majority of which return an RSE of >25% across the variable in the dataset (this is due to a small volume of data points). The combination of sex, age group and state (excluding ANZSCO codes) are within the acceptable RSE limit (<25%). s22(1)(a)(ii) to confirm how DISER would like to proceed before advising EBG. 14/02: ABS have provided a quote, AustCyber are currently reviewing the terms which state data can only be used for internal use. Plan for ongoing site maintenance to be developed as the custom dataset will be an ongoing cost 23/02: Ongoing management plan to be resolved internally by AustCyber by 25/02 2/03: AustCyber to confirm copyright clause will not be breached	Open
ACT-27	21/02/2022	DISER	Review average salary for feeder roles, when the career pathways dataset is provided. Previously AustCyber had expressed concern about the average salary for the feeder roles being too low, so the salaries were excluded from the dataset. AustCyber / DISER to review outputs from new dataset to determine inclusion.	s22(1)(a)(ii)	To be reviewed when new datasets are handed over	Open
ACT-28	23/02/2022	DISER	Determine potential for certifications to be included in AustCyber Education Map. Also to be determined if enrolments & completions VET/Uni tab can be complementary sources for Education Map	s22(1)(a)(ii)	Open as an ongoing investigation into how the certification providers fit into existing product	Open
ACT-29	25/02/2022	DISER	New requirement to confirm with DISER: main visualisations to be displayed in one view without scrolling	s22(1)(a)(ii)		Open
ACT-30	2/03/2022	DISER	New requirement to be reviewed and confirmed: Expanding on measure descriptions	s22(1)(a)(ii)		Open

Project options: AUCyberExplorer digital platform optimisation, incorporating forecasting model

Background

AUCyberExplorer is a digital platform which visualises data on the cyber security worker supply and job demand market in Australia, as well as providing information on career pathways and how to upskill and transition between roles. AustCyber has a contract with DISER to deliver a suite of enhancements to the platform, including additional data points, which are outlined under the project scope below.

Emsi Burning Glass (EBG) are a US based company that were part of the original consortium to deliver Cyber Seek AU (previous iteration of AUCyberExplorer before it was rebranded) and are the data providers for AUCyberExplorer and Cyber Seek US, which the Australian model was originally based on. The data modelling for the AUCyberExplorer datasets is based on the models which have been developed and tested in the US.

A key requirement in the contract between DISER and AustCyber to develop AUCyberExplorer is to incorporate the new 6-digit ANZSCO Occupation codes relating to cyber security, which were published in December 2021. During the scope development phase of the project a number of issues in being able to incorporate the 6-digit ANZSCO codes into the dataset in the short term (Q2 2022) have been determined, these are outlined below.

Current project scope

The current scope of work is to deliver;

1. Enhancements to baseline datasets;
 - New data points;
 - Worker age, worker gender, urban vs regional location, ANZSCO 4-digit Unit Group code
 - Historical data back to 2019 (for all the data points on the existing platform and those listed above)
 - Comparisons between Australia, UK and US data for the following data points
 - Total supply of workers, total demand for roles, average advertised salary, role (standardized role based on EBG's taxonomy)
2. Deliver a 5-year forecast of job supply and demand with data points for;
 - ANZSCO 4-digit Unit Group codes, ANZSIC industry division, state, SA4, urban vs regional
 - 5 year forecast of projected capabilities required at a national level (not available at state level)

Current Issues

1. *Availability of worker supply data which has been reclassified with the new 6-digit ANZSCO Occupation codes, relating to cyber security.*

The worker supply data is sourced from the Australian Bureau of Statistics (ABS) Census and Labour data. Although the updates to cyber security 6-digit ANZSCO Occupation codes were published in December 2021, the reclassification exercise of the historical data will not be complete until later this year, the current target date is November 2022. There is a hard dependency on ABS to complete the reclassification exercise to be able to deliver supply data with the new 6-digit ANZSCO Occupation codes.

For the same reasons, the 6-digit ANZSCO Occupation Codes cannot be incorporated into the forecasting model until the historical data is available. The forecasting model will need to leverage historical ABS data, so the forecasting model will be delivered at the 4-digit ANZSCO Unit Group code level (*Note: The forecasting model also sources the National Skills Commission's projections data, which is currently at a 4-digit level. Further investigation will be required to determine the feasibility of weighting the forecasting model to the 6-digit ANZSCO Occupation code level*).

2. Feasibility of classifying job demand data against the new 6-digit ANZSCO Occupation codes

The job demand data is scraped from online job postings by EBG, applying the same modelling used in the US to the Australian market. In the current iteration of AUCyberExplorer the taxonomy for roles is based on EBG's own standard classification of roles. The options to incorporate the 6-digit ANZSCO Occupation codes are outlined in this document.

3. Delivery of worker 'gender' and 'age group' data points in consolidated datasets and views

DISER have identified a requirement to see all new data points in a consolidated visualisation, however due to the availability and associated confidence of consolidating the age group and gender data points, the attributes will need to be split into multiple views.

Originally it was thought that AustCyber would be able to request a custom dataset from ABS, which would provide all of the required data points in one consolidated dataset. AustCyber has liaised with ABS on the required data, and the advice from ABS is that combining all of the required data points would produce a dataset with a Relative Standard Error Rate (RSE) of 25% or higher, which ABS defines as too high for practical purposes.

Options

1. Availability of worker supply data which has been reclassified with the new 6-digit ANZSCO Occupation codes, relating to cyber security.

- a. Due to the hard dependency on ABS to reclassify data, data with the new 6-digit ANZSCO Occupation codes can be incorporated when the data is available (ETA November 2022).*

2. Feasibility of classifying job demand data against the new 6-digit ANZSCO Occupation codes

There are 2 methods which could be used to classify job demand data, either via developing a taxonomy which maps 6-digit ANZSCO codes to job ads or creating an association via the National

Institute for Cyber security Education (NICE) work roles (the US framework for cyber security labour and education classification), both are outlined below.

As a further deliverable to the options outlined below, the 6-digit ANZSCO Occupation codes will be able to be associated with the 4-digit ANZSCO Unit Groups on the 'Career Pathways' section of the platform. This provides a method to introduce the new 6-digit ANZSCO Occupation codes to the public, until they can be incorporated into the data.

a. EBG will create a taxonomy for the new 6-digit ANZSCO occupation codes, considerations are outlined below.

- i. Taxonomy will be defined by mapping the titles, skills and certifications in online job advertisements to the 6-digit ANZSCO Occupation definitions. This direct mapping will provide a more robust output which creates an accurate relationship between the advertised roles and 6-digit ANZSCO Occupation codes. Once this exercise is complete, the 6-digit ANZSCO Occupation codes can be incorporated into the AUCyberExplorer dataset.
- ii. Timeline considerations include;
 1. EBG have planned to update their existing taxonomy between December 2022 – February 2023, as part of their internal development roadmap. Due to internal dependencies the vendor is unable to provide a smaller window but has provided 90% confidence that the work will happen during this period.
 2. If the work is commissioned ahead of internal development roadmap the time required by Emsi Burning Glass to deliver updated taxonomy will be 6 weeks. The start date is subject to availability of resourcing (the earliest start would be May 2022) and contract amendment being signed.
 3. Cost to deliver updated taxonomy for online job postings is s47(1)(b) ex GST. Factoring in the costs for datasets already in scope and the AUCyberExplorer site build, this would exceed the original value of DISER and AustCyber's contract to deliver phase 2 (digital platform optimization, incorporating forecasting model) of AUCyberExplorer.

b. The new ANZSCO 6-digit Occupation codes can be incorporated into the dataset via a mapping to NICE work roles. The following considerations and risks exist with this method;

- i. Based on review of the definitions for the 6-digit ANZSCO Occupations and NICE work roles the two frameworks do not have clear alignment for a large portion of roles and definitions, there are significant gaps between the frameworks.
- ii. If the 6-digit ANZSCO Occupation codes are mapped via NICE work roles, they will not be mapped directly to job advertisements, based on the requirements of the job advertisement. This reduces the accuracy of correctly aligning the advertised job and 6-digit ANZSCO Occupation definitions.
- iii. From an end user perspective, it may be a better user experience to deliver 6-digit ANZSCO Occupation codes in both the supply and demand data at

the same time (in comparison to delivering 6-digit ANZSCO Occupation codes in only the job demand data).

3. *Delivery of 'worker gender' and 'age group' data points in consolidated datasets and views*
 - a. 'Age group' and 'gender' can be split in the following groupings, as per the ABS Labour Market data;
 - i. Gender and Age Group by Occupation Sub-Major Group (but no Geography)
 - ii. Gender by State and 4-Digit ANZSCO (but no Age)
 - iii. Potential to investigate a custom dataset including Age, Gender and State (ANZSCO codes cannot be included in this combination)

Recommendations / decisions required

1. *Availability of worker supply data which has been reclassified with the new 6-digit ANZSCO Occupation codes, relating to cyber security.*

Due to the hard dependency on ABS reclassifying the data, DISER has agreed the 6-digit ANZSCO codes will be descoped from the worker supply data. No further decisions are required.

1. *Feasibility of classifying job demand data against the new 6-digit ANZSCO Occupation codes*

Consideration and agreement on approach is required from DISER, based on the options outlined in the 'Options' section of this paper. Based on the dependencies and constraints which exist, AustCyber's recommendation from a project management perspective is to continue with delivery of the scope outlined in this paper, which includes the 4-digit ANZSCO Occupation Unit Group codes, and target delivery of the 6-digit ANZSCO Occupation codes for Q4 2022. This phased delivery will also create the positive opportunity to continue to evolve the platform in a valuable way.

2. *Delivery of worker gender and age group data points in consolidated datasets and views*

AustCyber and DISER to review options to include Age Group and Gender attributes against original requirements and determine new requirements (meeting scheduled for 4/02/22).

To provide additional visibility of the ongoing delivery of the project, moving forwards AustCyber will provide a weekly project status report to the DISER team, each Friday until delivery.

Development timeline

...a refresh – Impress Design investigating code issues, other data viz options to be

...dates are target dates, may be subject to change

Document 16 - LEX 300027

Deliverables

1. Baseline dataset + new features
2. Career pathways dataset + new features
3. Forecasting dataset + new features

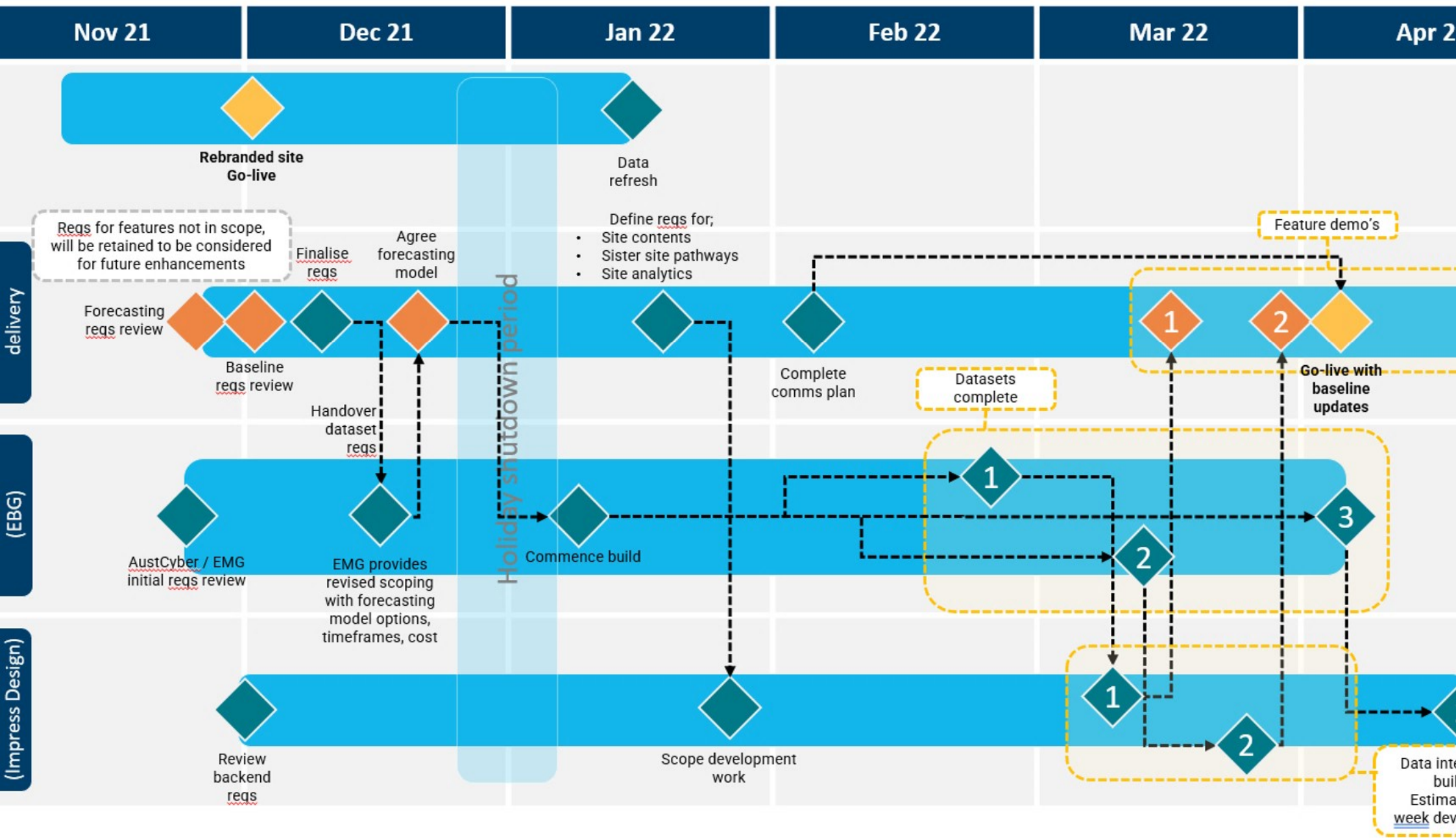
Key milestone

AustCyber / ve

AustCyber / DI

External depen

--- Dependency



Project options: AUCyberExplorer digital platform optimisation, incorporating forecasting model

Background

AUCyberExplorer is a digital platform which visualises data on the cyber security worker supply and job demand market in Australia, as well as providing information on career pathways and how to upskill and transition between roles. AustCyber has a contract with DISER to deliver a suite of enhancements to the platform, including additional data points, which are outlined under the project scope below.

Emsi Burning Glass (EBG) are a US based company that were part of the original consortium to deliver Cyber Seek AU (previous iteration of AUCyberExplorer before it was rebranded) and are the data providers for AUCyberExplorer and Cyber Seek US, which the Australian model was originally based on. The data modelling for the AUCyberExplorer datasets is based on the models which have been developed and tested in the US.

A key requirement in the contract between DISER and AustCyber to develop AUCyberExplorer is to incorporate the new 6-digit ANZSCO Occupation codes relating to cyber security, which were published in December 2021. During the scope development phase of the project a number of issues in being able to incorporate the 6-digit ANZSCO codes into the dataset in the short term (Q2 2022) have been determined, these are outlined below.

Current project scope

The current scope of work is to deliver;

1. Enhancements to baseline datasets;
 - New data points;
 - Worker age, worker gender, urban vs regional location, ANZSCO 4-digit Unit Group code
 - Historical data back to 2019 (for all the data points on the existing platform and those listed above)
 - Comparisons between Australia, UK and US data for the following data points
 - Total supply of workers, total demand for roles, average advertised salary, role (standardized role based on EBG's taxonomy)
2. Deliver a 5-year forecast of job supply and demand with data points for;
 - ANZSCO 4-digit Unit Group codes, ANZSIC industry division, state, SA4, urban vs regional
 - 5 year forecast of projected capabilities required at a national level (not available at state level)

Current Issues

1. *Availability of worker supply data which has been reclassified with the new 6-digit ANZSCO Occupation codes, relating to cyber security.*

The worker supply data is sourced from the Australian Bureau of Statistics (ABS) Census and Labour data. Although the updates to cyber security 6-digit ANZSCO Occupation codes were published in December 2021, the reclassification exercise of the historical data will not be complete until later this year, the current target date is November 2022. There is a hard dependency on ABS to complete the reclassification exercise to be able to deliver supply data with the new 6-digit ANZSCO Occupation codes.

For the same reasons, the 6-digit ANZSCO Occupation Codes cannot be incorporated into the forecasting model until the historical data is available. The forecasting model will need to leverage historical ABS data, so the forecasting model will be delivered at the 4-digit ANZSCO Unit Group code level (*Note: The forecasting model also sources the National Skills Commission's projections data, which is currently at a 4-digit level. Further investigation will be required to determine the feasibility of weighting the forecasting model to the 6-digit ANZSCO Occupation code level*).

2. Feasibility of classifying job demand data against the new 6-digit ANZSCO Occupation codes

The job demand data is scraped from online job postings by EBG, applying the same modelling used in the US to the Australian market. In the current iteration of AUCyberExplorer the taxonomy for roles is based on EBG's own standard classification of roles. The options to incorporate the 6-digit ANZSCO Occupation codes are outlined in this document.

3. Delivery of worker 'gender' and 'age group' data points in consolidated datasets and views

DISER have identified a requirement to see all new data points in a consolidated visualisation, however due to the availability and associated confidence of consolidating the age group and gender data points, the attributes will need to be split into multiple views.

Originally it was thought that AustCyber would be able to request a custom dataset from ABS, which would provide all of the required data points in one consolidated dataset. AustCyber has liaised with ABS on the required data, and the advice from ABS is that combining all of the required data points would produce a dataset with a Relative Standard Error Rate (RSE) of 25% or higher, which ABS defines as too high for practical purposes.

Options

1. Availability of worker supply data which has been reclassified with the new 6-digit ANZSCO Occupation codes, relating to cyber security.

- a. Due to the hard dependency on ABS to reclassify data, data with the new 6-digit ANZSCO Occupation codes can be incorporated when the data is available (ETA November 2022).*

2. Feasibility of classifying job demand data against the new 6-digit ANZSCO Occupation codes

There are 2 methods which could be used to classify job demand data, either via developing a taxonomy which maps 6-digit ANZSCO codes to job ads or creating an association via the National

Institute for Cyber security Education (NICE) work roles (the US framework for cyber security labour and education classification), both are outlined below.

As a further deliverable to the options outlined below, the 6-digit ANZSCO Occupation codes will be able to be associated with the 4-digit ANZSCO Unit Groups on the 'Career Pathways' section of the platform. This provides a method to introduce the new 6-digit ANZSCO Occupation codes to the public, until they can be incorporated into the data.

a. EBG will create a taxonomy for the new 6-digit ANZSCO occupation codes, considerations are outlined below.

- i. Taxonomy will be defined by mapping the titles, skills and certifications in online job advertisements to the 6-digit ANZSCO Occupation definitions. This direct mapping will provide a more robust output which creates an accurate relationship between the advertised roles and 6-digit ANZSCO Occupation codes.
- ii. Timeline considerations include;
 1. EBG have planned to update their existing taxonomy in Q3/Q4 2022. Once this exercise is complete, the 6-digit ANZSCO Occupation codes can be incorporated into the AUCyberExplorer dataset.
 2. EBG have been asked to provide an indicative timeline for the taxonomy update to the 6-digit ANZSCO Occupation codes, if it was to be completed ahead of the planned update by the taxonomy team.

b. The new ANZSCO 6-digit Occupation codes can be incorporated into the dataset via a mapping to NICE work roles. The following considerations and risks exist with this method;

- i. Based on review of the definitions for the 6-digit ANZSCO Occupations and NICE work roles the two frameworks do not have clear alignment for a large portion of roles and definitions, there are significant gaps between the frameworks.
- ii. If the 6-digit ANZSCO Occupation codes are mapped via NICE work roles, they will not be mapped directly to job advertisements, based on the requirements of the job advertisement. This reduces the accuracy of correctly aligning the advertised job and 6-digit ANZSCO Occupation definitions.
- iii. From an end user perspective, it may be a better user experience to deliver 6-digit ANZSCO Occupation codes in both the supply and demand data at the same time (in comparison to delivering 6-digit ANZSCO Occupation codes in only the job demand data).

3. Delivery of 'worker gender' and 'age group' data points in consolidated datasets and views

a. 'Age group' and 'gender' can be split in the following groupings, as per the ABS Labour Market data;

- i. Gender and Age Group by Occupation Sub-Major Group (but no Geography)
- ii. Gender by State and 4-Digit ANZSCO (but no Age)

- iii. Potential to investigate a custom dataset including Age, Gender and State (ANZSCO codes cannot be included in this combination)

Recommendations / decisions required

1. *Availability of worker supply data which has been reclassified with the new 6-digit ANZSCO Occupation codes, relating to cyber security.*

Due to the hard dependency on ABS reclassifying the data, DISER has agreed the 6-digit ANZSCO codes will be descope from the worker supply data. No further decisions are required.

1. *Feasibility of classifying job demand data against the new 6-digit ANZSCO Occupation codes*

Consideration and agreement on approach is required from DISER, based on the options outlined in the 'Options' section of this paper. Based on the dependencies and constraints which exist, AustCyber's recommendation from a project management perspective is to continue with delivery of the scope outlined in this paper, which includes the 4-digit ANZSCO Occupation Unit Group codes, and target delivery of the 6-digit ANZSCO Occupation codes for Q4 2022. This phased delivery will also create the positive opportunity to continue to evolve the platform in a valuable way.

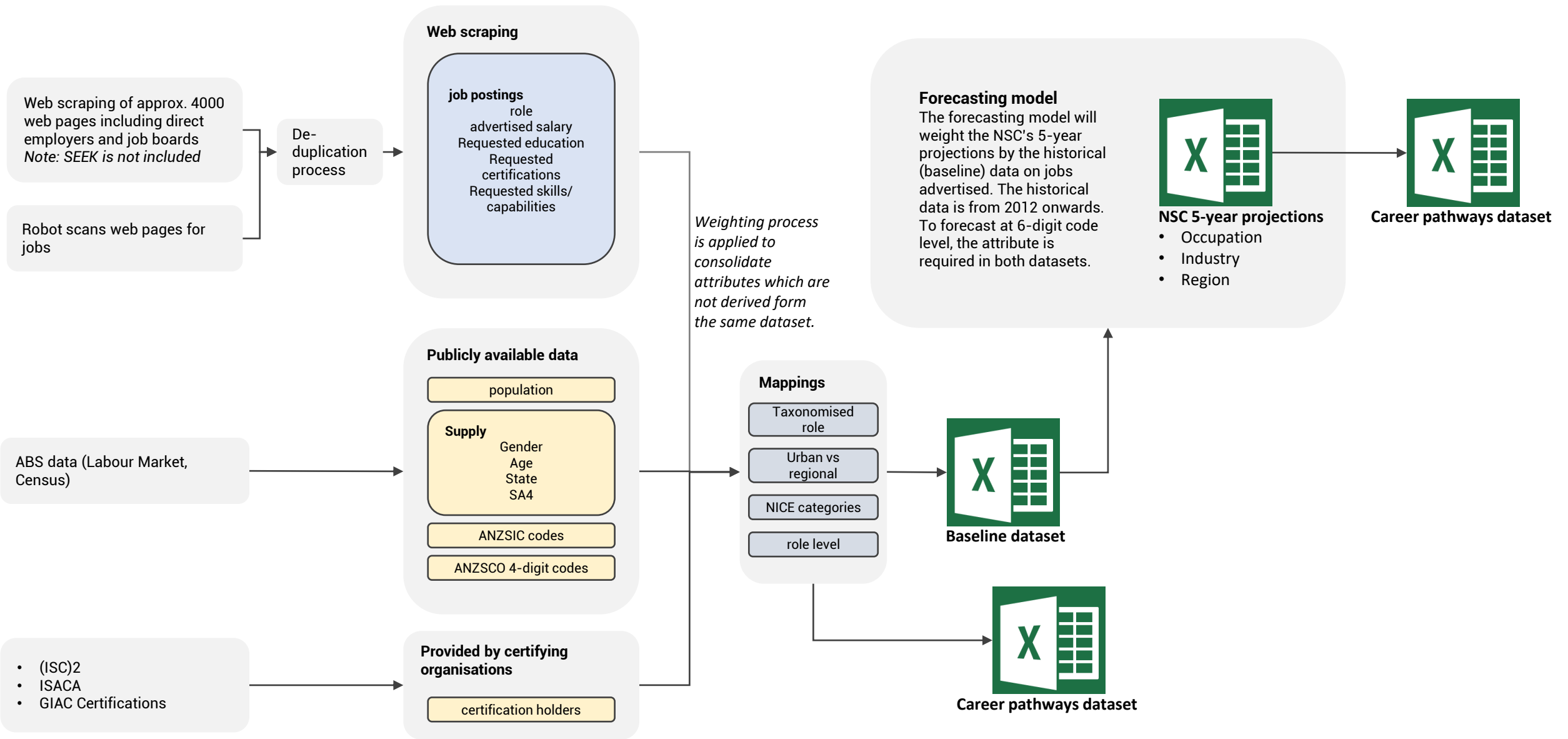
2. *Delivery of worker gender and age group data points in consolidated datasets and views*

AustCyber and DISER to review options to include Age Group and Gender attributes against original requirements and determine new requirements (meeting scheduled for 4/02/22).

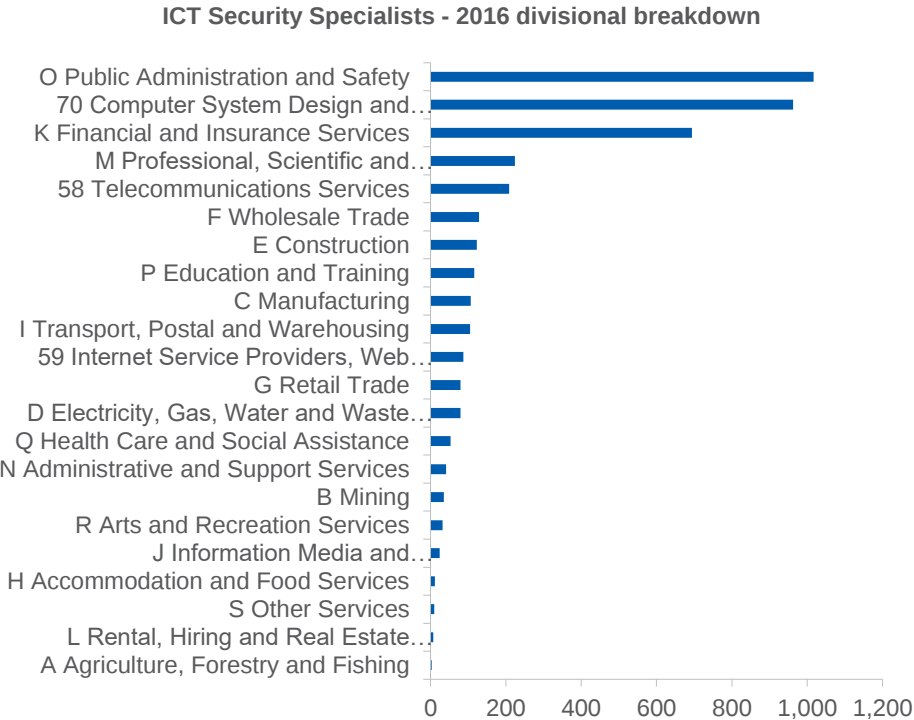
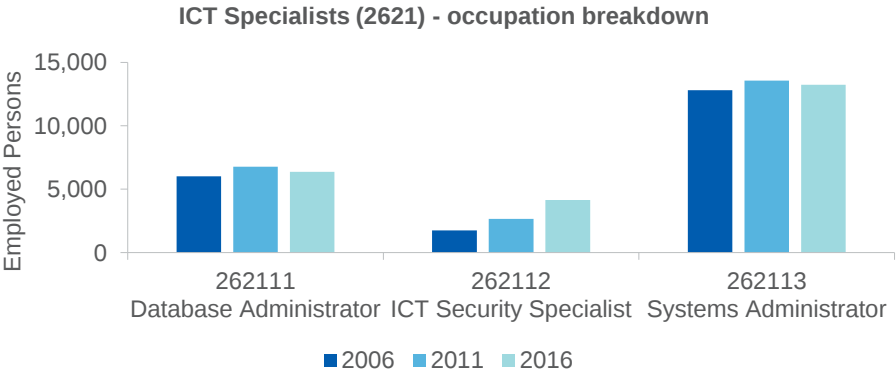
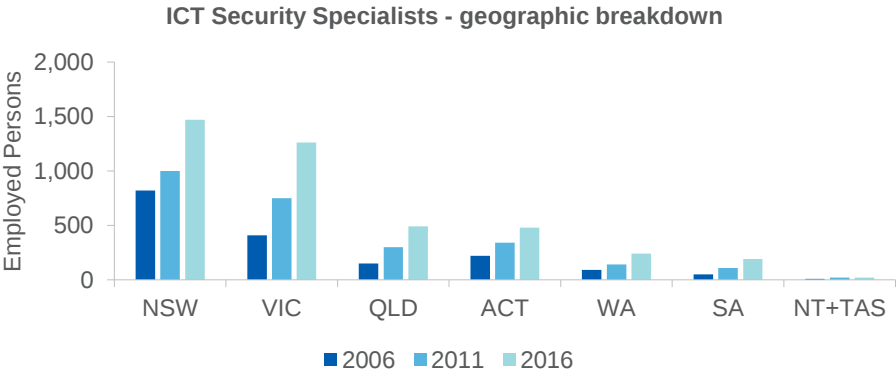
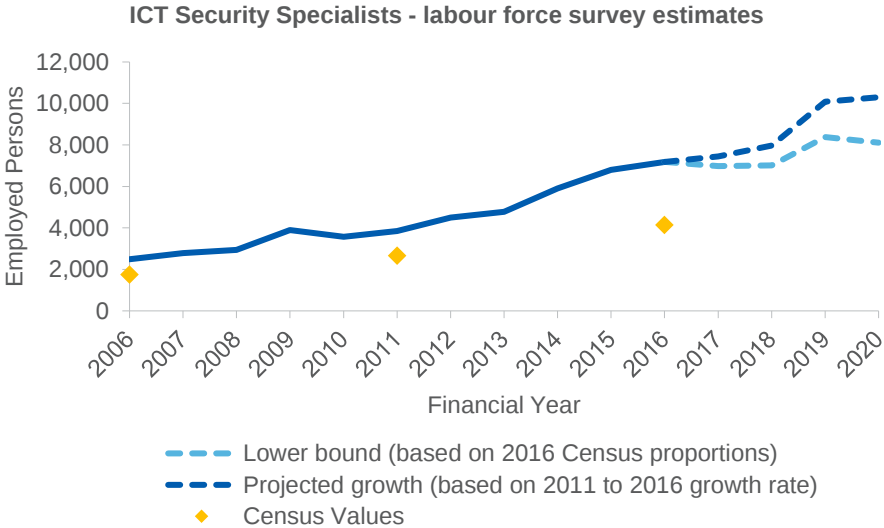
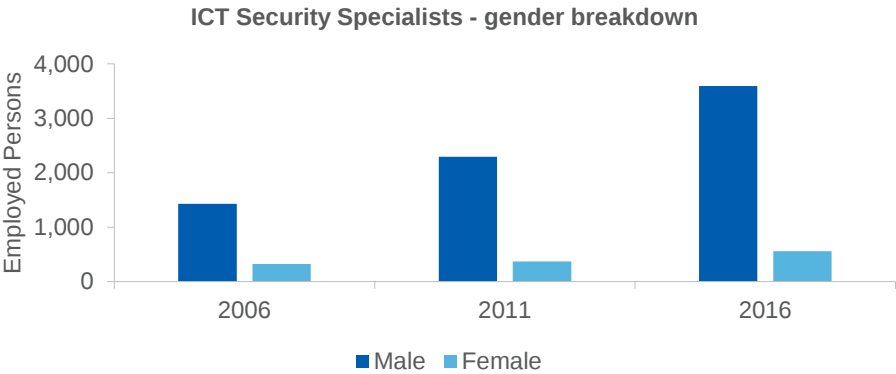
To provide additional visibility of the ongoing delivery of the project, moving forwards AustCyber will provide a weekly project status report to the DISER team, each Friday until delivery.

AUCyberExplorer Data inputs – Phase 2

Note: Not all derived measures and dimensions are shown in this diagram



Employment in the occupation 'ICT Security Specialist'



Data Caveats
Data is based on a custom census request from the ABS with some calculations done by AID. Data captures direct employment in the occupation 'ICT Security Specialists' only and does not include employment in related roles where a part of the job may be cyber security related. In Census data there are small random adjustments made to all values to protect the confidentiality of data. As such small values are subject to some inaccuracy and should not be taken literally, There are differences between Census and Labour Force Survey data due to the data collection times and methods, with the Census generally considered most accurate.

Data Tables

Divisional breakdown

Industry	2006	2011	2016
A Agriculture, Forestry and Fishing	0	0	3
B Mining	10	18	35
C Manufacturing	62	79	107
D Electricity, Gas, Water and Waste Services	26	43	80
E Construction	21	89	123
F Wholesale Trade	49	70	129
G Retail Trade	34	53	80
H Accommodation and Food Services	7	3	12
I Transport, Postal and Warehousing	45	42	105
J Information Media and Telecommunications (other than sub-div 58,59)	22	27	24
58 Telecommunications Services	66	102	209
59 Internet Service Providers, Web Search Portals and Data Processing Services	10	24	87
K Financial and Insurance Services	317	400	694
L Rental, Hiring and Real Estate Services	10	0	7
M Professional, Scientific and Technical Services (other than sub-div 70)	105	143	224
70 Computer System Design and Related Services	483	749	963
N Administrative and Support Services	11	31	41
O Public Administration and Safety	383	676	1017
P Education and Training	44	60	116
Q Health Care and Social Assistance	22	31	53
R Arts and Recreation Services	14	9	32
S Other Services	8	11	10
Total	1750	2660	4150

Occupation breakdown

Year	262111 Database Administrator	262112 ICT Security Specialist	262113 Systems Administrator	Total
2006	6020	1750	12820	20590
2011	6780	2660	13560	23000
2016	6370	4150	13240	23760

Geographic breakdown

Year	NSW	VIC	QLD	ACT	WA	SA	NT+TAS	Total
2006	820	410	150	220	90	50	10	1750
2011	1000	750	300	340	140	110	20	2660
2016	1470	1260	490	480	240	190	20	4150

Labour force survey – constructed time series

Financial Year	Employment (based on avg annual change)	Lower bound (based on 2016 proportions)	Projected growth (based on 2011 to 2016 growth rate)
2006	2490		
2007	2790		
2008	2940		
2009	3890		
2010	3580		
2011	3850		
2012	4500		
2013	4770		
2014	5910		
2015	6800		
2016	7180	7180	7180
2017		6980	7450
2018		7020	7970
2019		8380	10080
2020		8110	10300

Gender breakdown

Year	Male	Female	Total
2006	1430	320	1750
2011	2290	370	2660
2016	3590	560	4150

Data Caveats

Data is based on a custom census request from the ABS with some calculations done by AID. Data captures direct employment in the occupation 'ICT Security Specialists' only and does not include employment in related roles where a part of the job may be cyber security related. In Census data there are small random adjustments made to all values to protect the confidentiality of data. As such small values are subject to some inaccuracy and should not be taken literally. There are differences between Census and Labour Force Survey data due to the data collection times and methods, with the Census generally considered most accurate.