2020

SA CYBERSECURITY SKILLS MAPPING AND DEVELOPMENT

South Australia
Innovation Node

Introduction

Cybersecurity workforce is a growing area, both in concern and in recognition globally. Cyber attacks have been increasing in frequency and cost, and questions have been raised around what organisations can and should be doing to address their risk. The solutions to these questions range from products to services and ultimately land on personnel as the key factor.

Drilling specifically into Australia, the AustCyber Sector Competitiveness Plan (SCP) 2019 highlighted that there is a need for 17,600 more cybersecurity professionals by 2026 with a current approximated shortfall of 2,300 cybersecurity professionals today. Much of the local demand has been met by foreign companies, providing both products and services. To address the need and grow Australian cybersecurity capability, AustCyber has acknowledged the shortage of job ready workers in the SCP and advocates for greater skill growth.

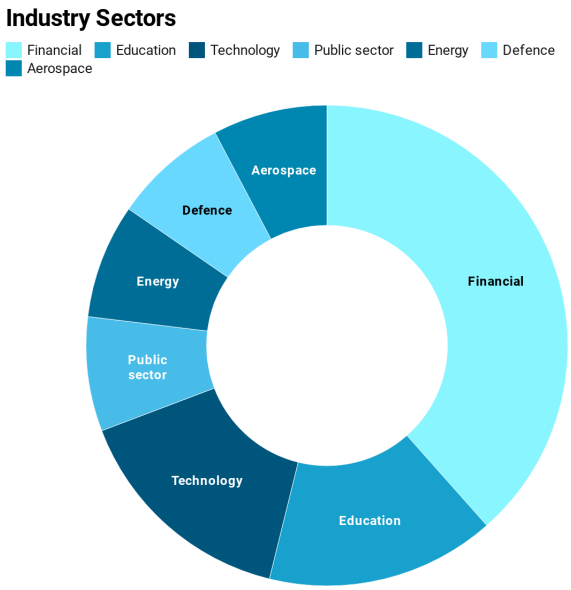
AustCyber SA Innovation Node, part of the network of nodes, has sought to better understand and resolve this issue through a two-stage project to map the requirements of industry to the qualifications available in South Australia under a unifying framework - the NICE Framework.

- Cyber security in Australia employs around **19,500** people
- Total expenditure is **A$4.6 billion** in 2017
- More than three-quarters of the market is **dominated by foreign companies**, mostly with local bases employing Australians
- Many local companies are **not harnessing their full export potential**
- **Australia can compete most effectively in software** (in areas of distinctive research capability) and services (in the protection stack and underlying processes)
- **A$3.6 billion** spent on external cyber security 2017
- **A$960 million** on their internal cyber security functions in 2017
- Small but **fast-growing sector**
- Strong cyber security will **enhance Australia's global reputation** as a trusted and secure place to do business
- **Foundation for future success** of all industries in national economy

Why NICE?

The NICE Framework is a NIST led initiative to partner industry, government and academia to create a resource that categorises and describes cybersecurity work and work roles. The NICE Framework is also endorsed by the US Department of Defence, which is important to note in South Australia as a State that is heavily staffed with the Defence sector.
By leveraging the NICE Framework, this project utilises a widely available and established framework that can be used as a model for cybersecurity employment, education and resourcing in the future.

How and What?



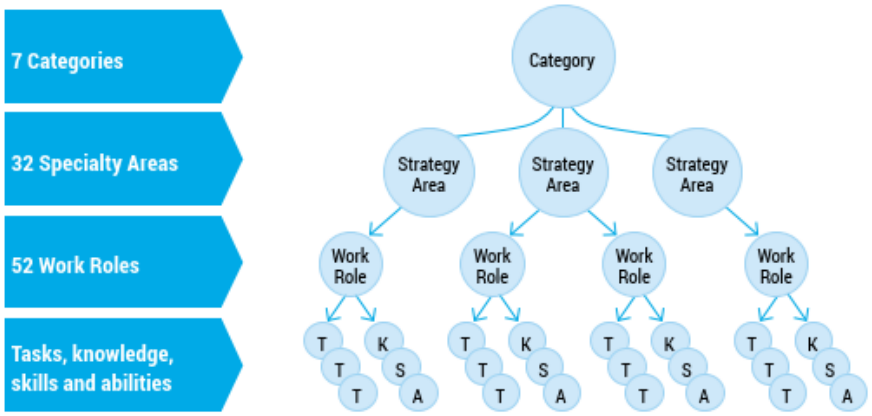
The project was formed in two phases:
1) A survey of a sample set of industry partners was conducted to gather insights into **where industry is now and where it wants to be**. This included what qualifications are expected of future candidates. The respondents were kept anonymous but the sector was provided to allow for a breakdown. Included in this data was information on the number of qualifications and certifications held in SA from various providers in the State.

2) An assessment of certifications and qualifications identified in the survey and identified as present in South Australia was completed to map its alignment to the NICE Framework. Vendor-own alignment and the NICCS Education Map was used for the certifications and assessment activities were taken with the higher education participants.

National Initiative for Cybersecurity Education

The National Initiative for Cybersecurity Education (NICE) is led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. It is a partnership focused on cybersecurity education, training, and workforce development between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. *

Structure of NICE Workforce Framework



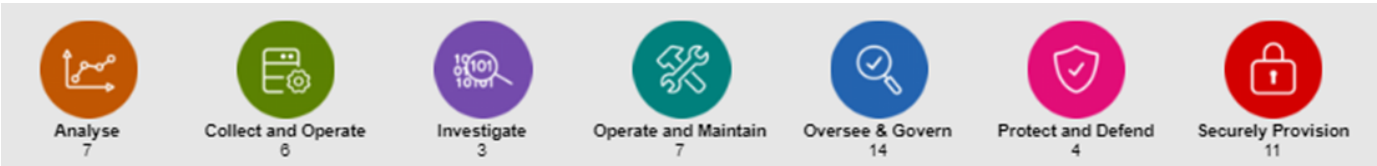
Categories	Description
Securely Provision	Designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development
Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security
Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organisation may effectively conduct cybersecurity work
Protect and Defend	Identifies, analyses, and mitigates threats to internal information technology (IT) systems and/or networks
Analyse	Performs highly-specialised review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Collect and Operate	Provides specialised denial and deception operations and collection of cybersecurity information that may be used to develop intelligence
Investigate	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence

These categories are further divided into 32 specialty areas, 52 work roles and hundreds of tasks, skills, knowledge and abilities.

NICE Cybersecurity Workforce Framework

The NICE Cybersecurity Workforce Framework (*NICE Framework*) is a US national-focused resource that categorises and describes cybersecurity work. The NICE Framework establishes a taxonomy and common lexicon that describes cybersecurity 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.

The NICE Framework enables organisations to identify what cybersecurity skills their organisation needs and assess their current capabilities. This can help inform hiring practices in line with the direction of the business.*



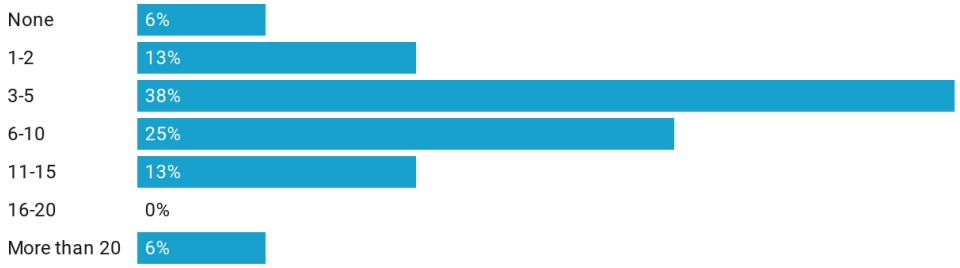
It is important to note that the NICE Framework is not a prescriptive framework requiring all of the roles to be in place regardless of the industry or sector an organisation operates within. It does not state minimum number of roles either. The NICE Framework is a guide to enable the assessment of cybersecurity skills from which well provisioned team formations can be identified also.

*Information and description taken from <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>

Detailed Findings - Where are we now?

The respondents were asked a set of questions to gather information on what level of cybersecurity roles they have, what they see as in demand right now and what qualifications are associated to those roles.

How many cybersecurity roles do you have in your organisation currently?



Average number of current roles

7

Considering the average number of employees calculated of the respondents, who represent some of the largest employers in SA, this number seems low.

A response of "None" required the respondent to answer the question: "***How do you manage cybersecurity in your organisation without dedicated cybersecurity roles?***" The responses entered included:

- "*Roles are defined in job description and KPI. There are separate teams for security Ops and Governance.*"
- "*By relying on a business unit who specialises in cybersecurity and Incident management. While also having employees like myself who understand this jargon to assist exes and other members deal with low-level vulnerabilities.* "

From a cost and operational point of view, there are questions on how these organisations are mitigating their risks in line with their size and possibility as a target.

Why could this be so low?

- A lack of awareness or clarity over cybersecurity role importance/need over operational roles
- Growth in outsourcing cybersecurity roles, tools or specialisations
- A lack of candidates that meet the requirements, or just the size of the candidate pool in SA?

In considering the talent pool, we need to consider what the state of cybersecurity education and qualification in South Australia is currently. Data provided by a number of education providers and certification bodies in the state showed a total of 355 qualifications and certifications existing within the South Australian Cyber Security Professional Community between 2018-2020.

The top qualifications and certifications present are:

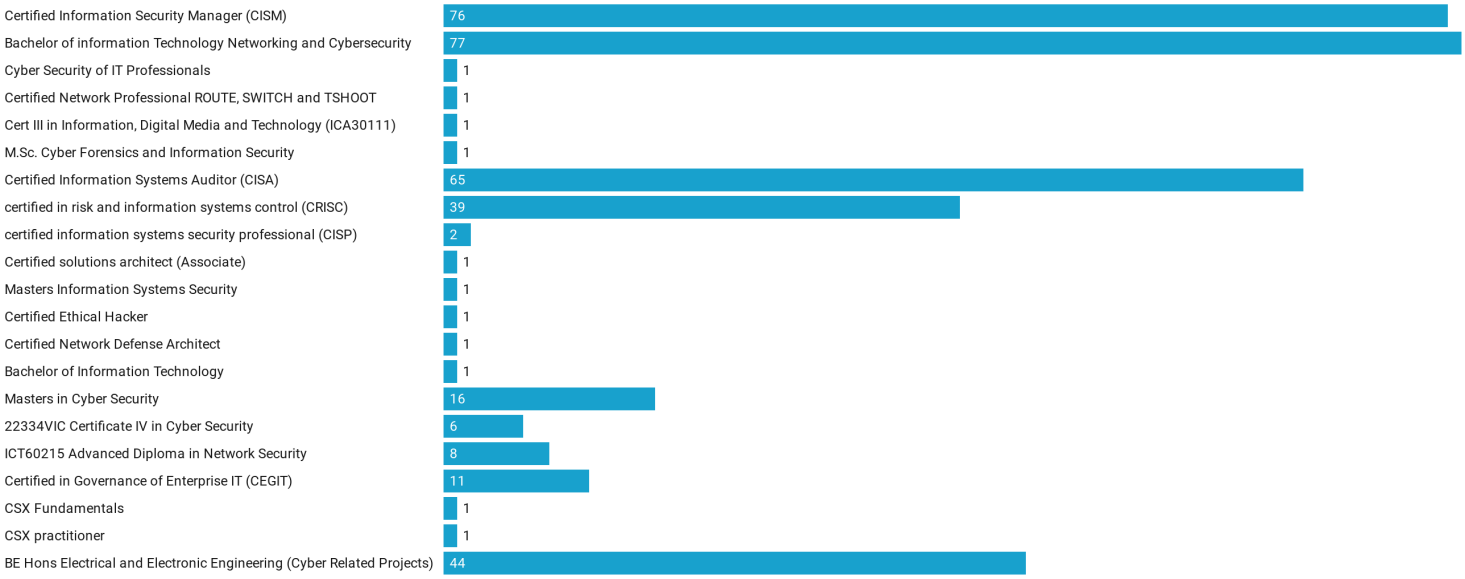
Bachelor of IT (Networking and Cybersecurity)	Certified Information Systems Manager	Certified Information Systems Auditor	BE (Hons) EEE (Cyber-related Project)*	Certified in Risk & Information Systems Control
77	76	65	44	39

The split of the top five is a ratio of **qualifications 2:3 certifications.** The qualifications come from the University of South Australia and the University of Adelaide respectively, and the three certifications are all provided by a single provider, ISACA.

*BE (Hons) EEE (Cyber-related Project) is not a standalone qualification, it is part of the Bachelor of Engineering in Electronic and Electrical Engineer with Honours in which students can research and develop an Honours project in a cybersecurity-related field. Some examples include, research into hacking and securing smart cars, GPS spoofing and digital forensics. The University of Adelaide has since developed cybersecurity specific qualifications - Master of Cyber Security (Management) and Master of Cyber Security (Secure Software Development).

Trends in the data show that there is a marked increase year on year for qualifications obtained from the higher education sector. Numbers from TAFE SA show a huge increase for the Certificate IV in Cyber Security for 2020, growing from 4 students successfully completing the qualification in 2019 to approximately 114 students registered into core subjects for the qualification*. In a similar trend both the University of South Australia and University of Adelaide have seen consistent growth in numbers over the last two years.

Qualifications and Certifications held by members of the South Australian Cyber Security Professional Community (2018-2020)



A key factor to the spread and variation of the numbers of qualifications and certifications held is that a professional can, and is likely, to hold more than one. For example, some professionals may have a qualification such as a Bachelors degree as well as a certification like CISA or CISSP, or indeed have multiple certifications alone. In providing data on numbers, ISACA (Adelaide Chapter) totalled 187 certifications held by 184 members.

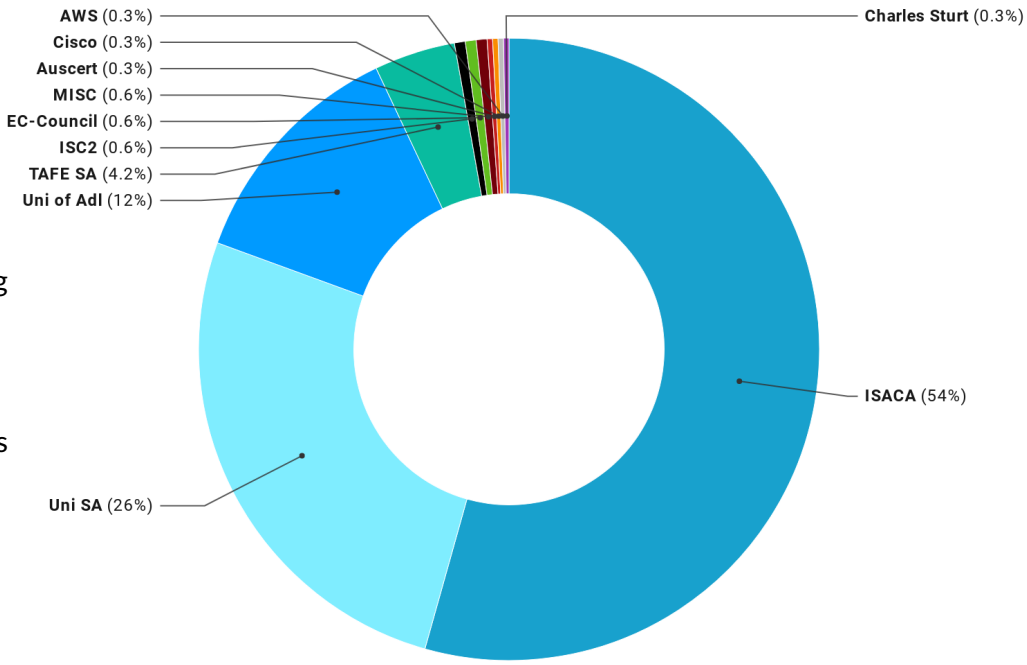
ISACA **54%**

UniSA **26%**

Adelaide Uni **13%**

Top three providers in SA

SA Qualifications and Certifications by Provider



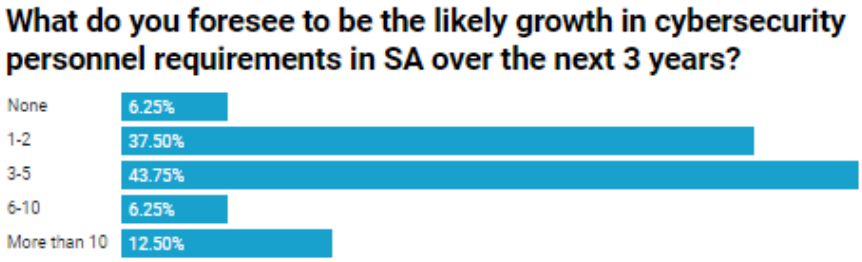
It is unsurprising that ISACA has a high level of coverage due to the large number of professional certifications provided to replace or compliment higher education provisions but the information above on rising students numbers and adoption of new degrees, certificates and diplomas shows growing choice for students and professionals also the importance of cybersecurity skills and education in South Australia. In the past, experience and certifications were the main source of demonstrating capability and learning but the emergence of new qualifications allows for greater consideration of which path is right for the student and/or professional.

*Student enrolments pre-COVID-19

Detailed Findings - Where do we want to be?

Average number of additional roles **4**

When coupled with the current average number of cybersecurity roles, this brings numbers up to 11, a percentage increase of approximately 57 per cent.



What does this mean for organisations?

The average salary for a cybersecurity professional in industry (with 3+ years of experience) was $120,000 in 2018 according to data derived by AustCyber. Taking that into account for a **large organisation**, an increase in personnel is likely to cost an extra $480,000 per year to a total of $1.32 million for cybersecurity professionals.

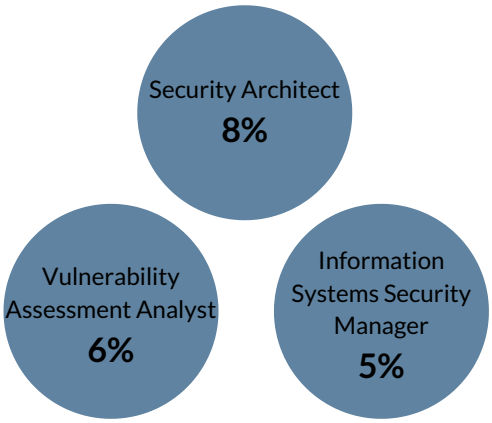
Though this may sound expensive, the 2017 ACSC Threat Report found that the cost of malicious emails alone rose 230 per cent to over $20 million in reported losses. The total salary costs of the foreseen internal cybersecurity roles amounts to just ***6.6 per cent of this loss.***

Regardless of financial cost, the number of foreseen roles is still low. Questions are raised as to what is being done to plug the gaps and enable security in an organisation:

- Cybersecurity product and service outsourcing?
- A lack of necessity or urgency around cybersecurity?
- Cybersecurity as part of other roles

In conjunction with this, respondents were asked the state of recruitment currently, to better understand if the growth is a result of need or difficulty in recruitment.

Which cybersecurity roles does your organisation consider to be in demand?



The 52 work roles in the NICE Framework were provided to respondents to consider what roles are in demand for the organisation.

The most in demand roles are heavily weighted towards technical roles and expertise, spread over all categories of the NICE Framework. The top three roles were *Security Architect*, *Vulnerability Assessment Analyst* and *Information Systems Security Manager*.

All roles gained at least one response with the exception of *IT Investment/Portfolio Manager* and *Product Support Manager*.

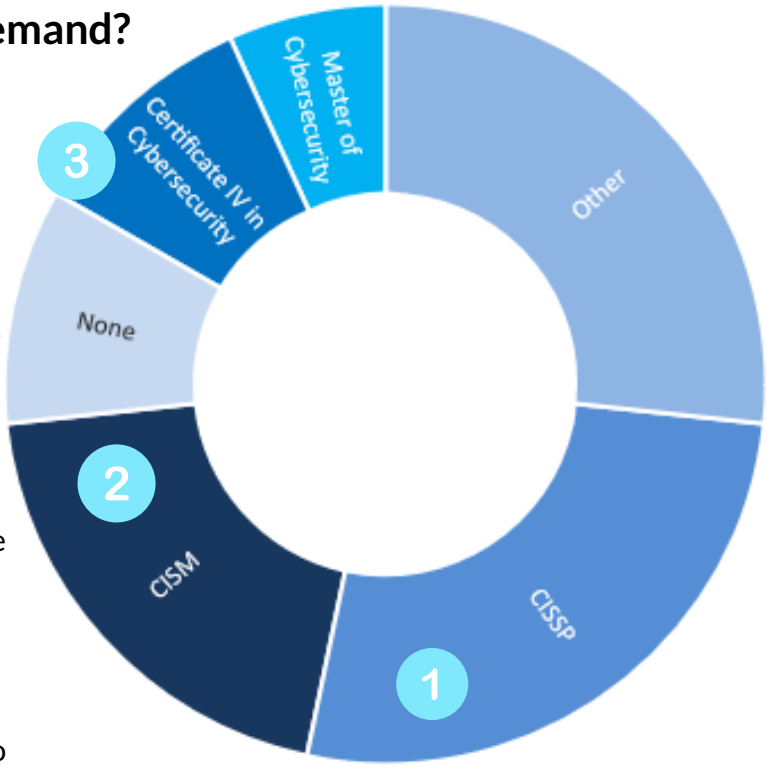
The top three work roles fall under separate NICE Framework categories - *Securely Provision*, *Oversee and Govern*, and *Protect and Defend*, highlighting that industry is not focused on a single area of cybersecurity where recruiting and requirements are concerned.

To understand the issues around recruitment and to meet the needs of *in demand* roles of industry, qualifications and certifications formed part of the consideration in this survey. This was also in response to the growth in cybersecurity-specific qualifications being offered by universities across the country. It is important to consider commentary and discussion on how suitable job application and entry requirements are for the role being advertised, with entry-level roles expected a number of years of experience, and at times with that experience outweighing the existence of the product in question.

What cybersecurity related qualifications/certifications are held by employees in those roles that are in demand?

The survey data appears to show that industry certifications are in higher demand than degree qualifications.
There are a number of possible reasons why this may be the case:

- Qualification mirroring qualifications
  - If these are the qualifications and certifications held in the organisation already, is that influencing the decisions?
- CISSP and CISM have experience requirements built into the certification process as well as knowledge requirements. This would symbolise the idea of industry wanting both education and experience.
- Certificate over Masters/Bachelors degrees
  - Though marginal, does this point to how industry views "traditional" higher education to be non-technical, slow to react or "old world"?



Where "Other" was selected, responses to what qualifications/certifications held included:

- Certified Information Systems Auditor (CISA)
- Offensive Security Certified Professional (OSCP)
- "A mix of graduate, experience and CISSP but all have a degree"
- "Bachelor's degrees and certificates"
- Certified in Risk and Information Systems Control (CRISC)
- GIAC Cyber Defence Certificates
- "Forensic, Data Analytics, Incident Response"
- "PHD relating to satellite, telecommunications and Radio Frequency comms. Critical infrastructure integration."

How do these align to NICE?

Using the Skills Matrix, the Knowledge, Skills and Attributes (KSAs) for **all three** in the in demand top three roles are found in:

- CISSP ✔
- Master of Cybersecurity (UniSA)
- Certificate IV in Cybersecurity (TAFE SA) ✔

On the other hand, CISM aligns to *Information Systems Security Manager* but neither of the other top in demand work roles. CISM is a qualification that is more aligned to Risk Management roles, Cybersecurity management roles, Strategic Planning and Policy roles, Acquisiton and Program/Project Management.

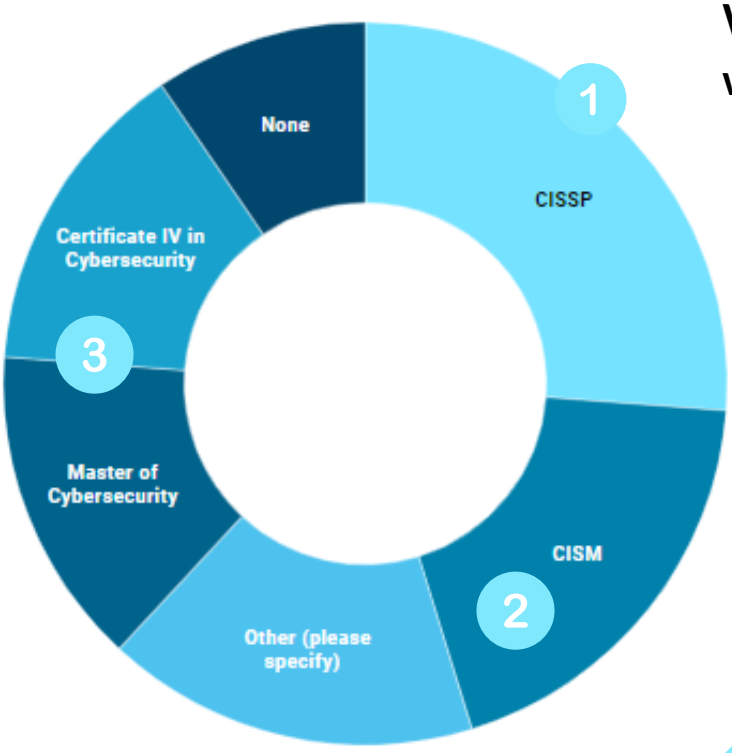
This highlights some disparity in the expectations of industry for qualifications when considering role requirements, and the question becomes "***how do you become work-ready if to get work, you have to have had experience already?***"

75% of industry respondents reported difficulties in recruiting for cybersecurity roles in the last 12 months.

17 cybersecurity roles were identified as having been hard to recruit for over the last 12 months, with the top three as *Security Architect*, *Systems Security Analyst* and *Information Systems Security Manager*.

These hard to recruit roles mirror that of the roles considered to be "in demand". It is an unsurprising finding but what is surprising though is that Vulnerability Assessment Analyst was rated higher than Information Systems Security Manager as in demand but is relatively low in difficulty to recruit.

It is important to recognise that these findings were derived from a survey completed pre-COVID-19 which introduced changes to the workplace, day-to-day life and to the number of threats and cybersecurity incidents and attacks as a result of remote working and swift adoption to online service delivery. Working from home opened up some organisations to the reality of gaps in their cybersecurity readiness or capability. The impacts of remote learning and the drop in student enrollment or course provision as a result have also affected the industry and will need to be considered as part of future initiatives by the AustCyber SA Innovation Node. A follow up survey is planned to capture the change in trends as a result of COVID-19 to identify where these findings have been affected.



How do these align to NICE?

Using the Skills Matrix, the KSAs for **all three** hard to recruit roles are found in:

- CISSP ✔
- Master of Cybersecurity (UniSA) ✔
- Certificate IV in Cybersecurity (TAFE SA) ✔

What qualifications and/or certifications will be required by additional personnel?

Responses to "Other" included:

- Certified Information Systems Auditor (**CISA**)
- Offensive Security Certified Professional (**OSCP**)
- Certified in Risk and Information Systems Control (**CRISC**)
- PCI Qualified Security Assessor (**PCI QSA**)
- "*Basic understanding in various fields like network, telecoms, pentesting*"
- "*Hands on experience, business experience, industry application understanding, someone who can understand the regulatory/people/process/technology.*"

Again, as with in demand roles, CISM is the expected qualifications that does not align fully with the roles identified, other than *Information Systems Security Manager*.

Responses to the survey overall seem to indicate a *preference for certifications over qualifications*. This can be seen in both what qualifications would be required of current in demand roles and in the predicted future roles and recruits. There may be an element of hiring based on qualifications/certifications that already exist within the organisation as it is a known marker, which could explain why CISM seems to be expected for more technical roles.

	CISSP	CISM
Provider	(ISC)2	ISACA
Experience	5 years paid (2 domains minimum)	5 years paid (3 domains minimum)
Domains	Security and Risk Management	Information Security Governance
	Asset Security	Information Risk Management
	Security Architecture and Engineering	Information Security Program Development and Management
	Communication and Network Security	Information Security Incident Management
	Identity and Access Management (IAM)	
	Security Assessment and Testing	
	Security Operations	
	Software Development Security	
Validity	3 years	3 years
Maintenance	120 CPEs within 3 years	120 CPEs within 3 years

This ties into the experience requirements of some certifications. CISSP and CISM have experience requirements built into the certification process as well as knowledge requirements. Both certifications require five years of verified experience. Professionals are required to pass a test showcasing the knowledge aspect of learning and skills acquisition, but with the experience requirement, they are likely to have already applied this knowledge in industry or will have to before being able to showcase their certification.

As noted in some of the answers to the surveys, experience is something that organisations are looking at. Is this a reflection of the cyber threat landscape, where organisation require experience candidates to be able to react quickly and respond to threats?

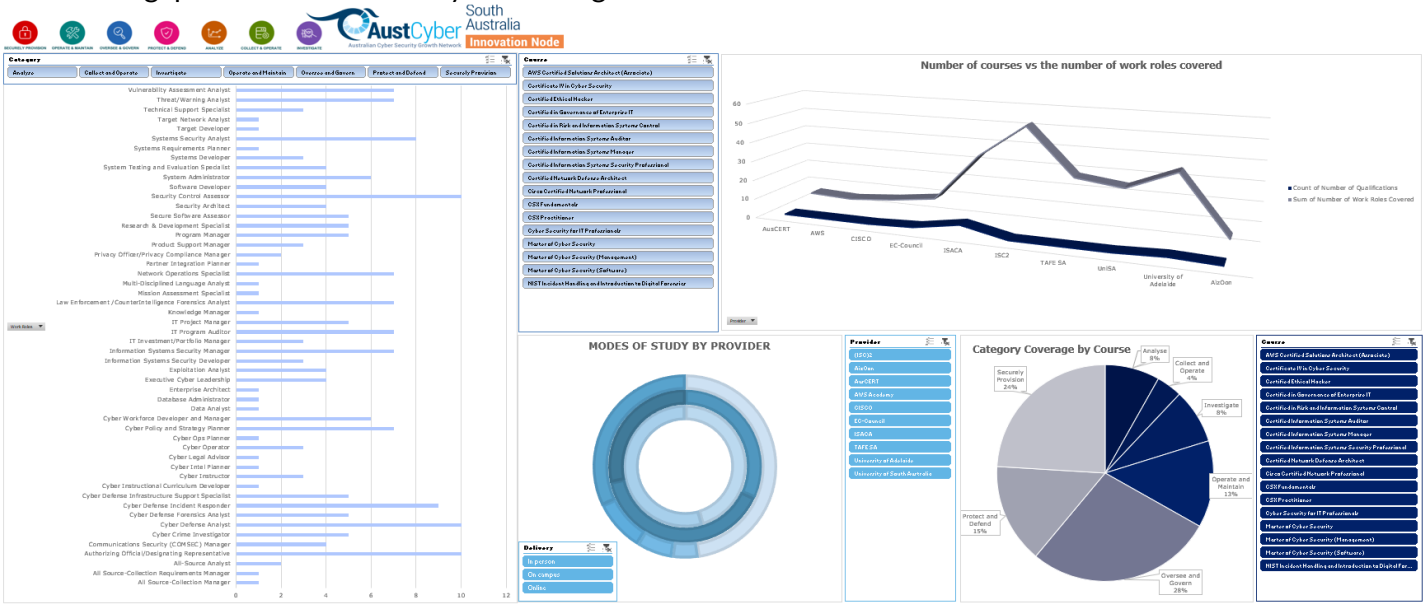
How are graduates to gain this experience if they are excluded from application selection without a certification and how does this link to certificates being considered more in demand or candidates when compared to postgraduate and undergraduate degrees?

There is some recognition of interdisciplinary skills highlighted when looking at additional personnel. For an organisation to be successful here, cybersecurity must be intertwined within an organisation's culture and performance from top to bottom.

Cybersecurity, as shown in the NICE Framework, is not just about technical roles and these roles will have to communicate to multiple levels within the organisation. Hence, the NICE Framework as a prime choice to provide students and professionals, industry and education providers a benchmark to standardise recruitment and skill objectives in the Skills Dashboard.

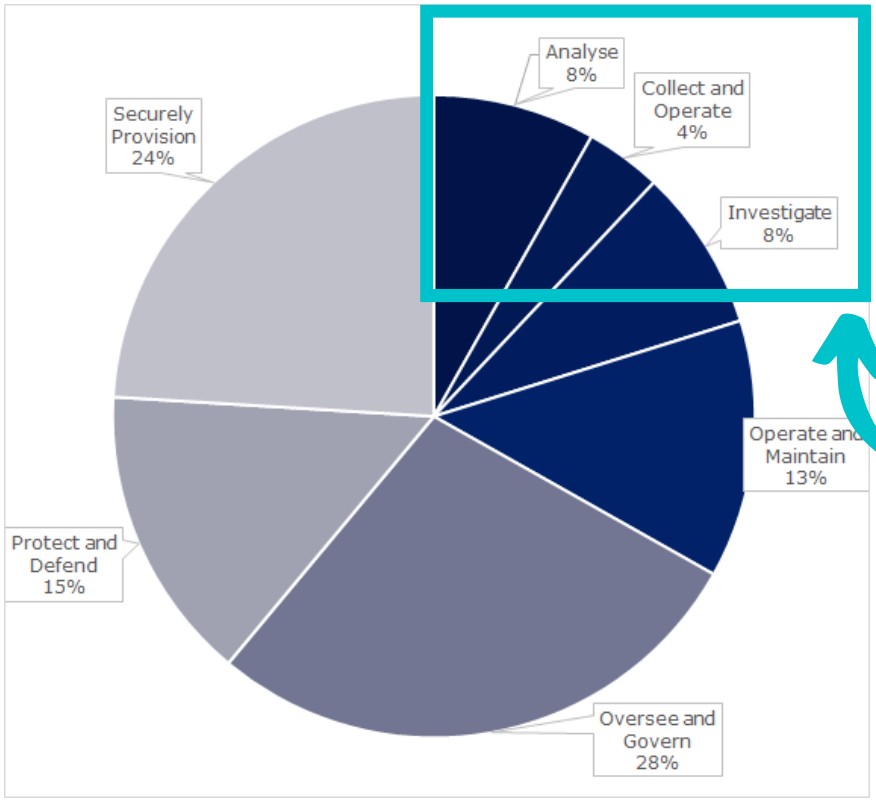
Skills Dashboard

The AustCyber SA Innovation Node has designed an easy to use dashboard to compliment the AustCyber Education Map. It is aimed at students, professionals, industry and education to enable greater understanding what qualifications and certifications are available in South Australia at this time and how they align to work roles, and where gaps in skills and delivery of learning exist.



The Dashboard is broken down into three areas:

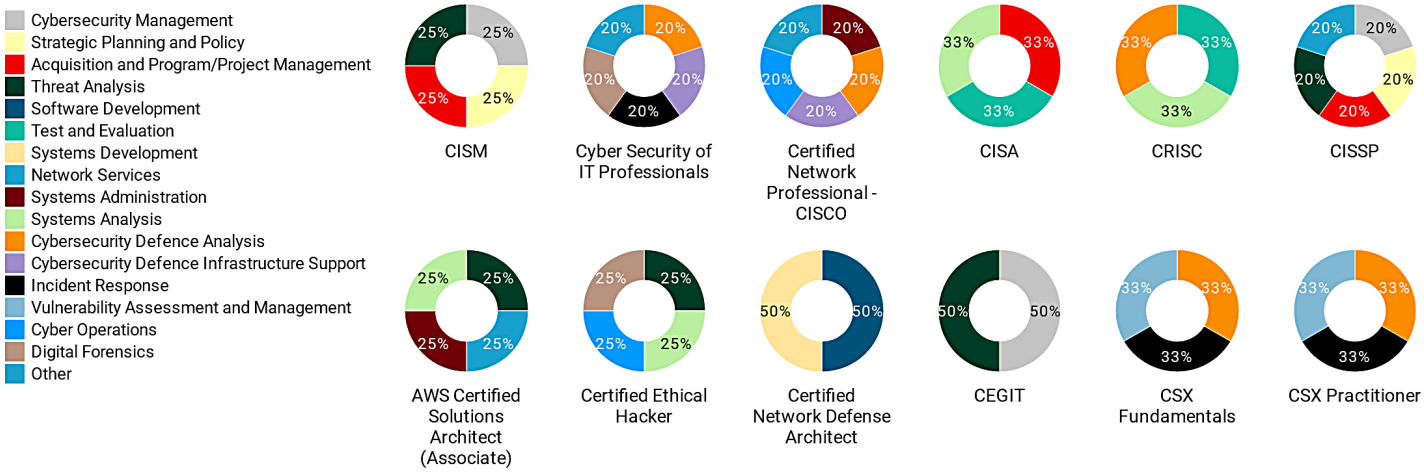
- NICE Framework **Work Role filter** that identifies which courses, qualifications and certifications align to that role
- **Modes of study** from on campus, online and specially run courses
- The **levels of coverage** provided by the courses, qualifications and certifications that enable the education sector to identify strengths and areas of weakness in current provisions.



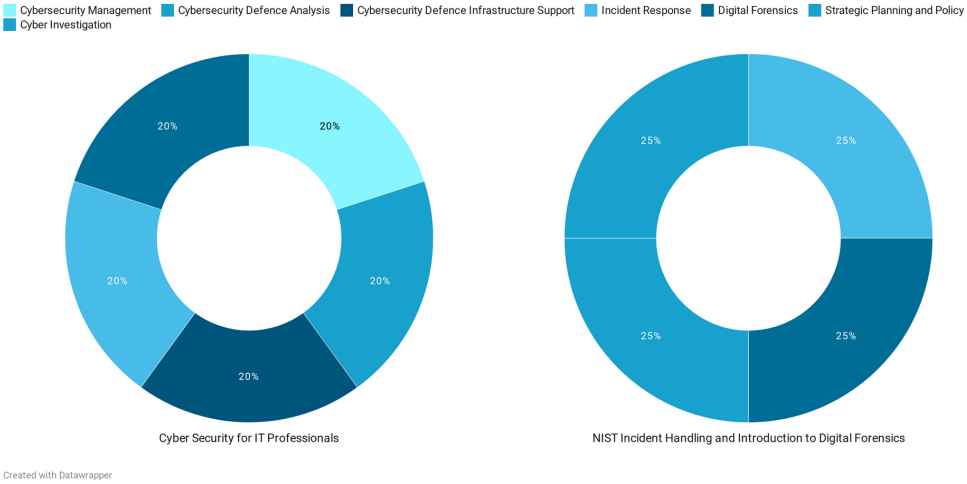
The design of the matrix is such that it can be updated as qualifications emerge and change, and, most importantly, can be filtered to highlight qualifications providing the skills for specific work roles. This is important for two main reasons:

- Cybersecurity competitiveness hinges on being able to train and recruit the right candidates. Using the matrix and increased participation from education and training providers, gaps can be identified and highlighted for opportunities to develop training or course provisions. For example, the weakness of coverage in ***Collect and Operate***, ***Analyse*** and ***Investigate***.
- Survey data shows that work role titles and required skills are not mapping to a single source industry-wide. Adoption of the NICE work roles descriptions add for clarity of all involved parties and the dashboard provides a quick reference supported by the details in the background.

The Skills Dashboard provides the data set that can be used to display skill coverage information in a quick and visually accessible way. Using the data, below are displays of the divide between, industry and vendor certifications, specialised certifications and broader higher education qualifications.



Certifications are addressing niche areas of the NICE Framework. Excluding CISSP, most certifications cover less than 10 of the 42 Specialty Areas.

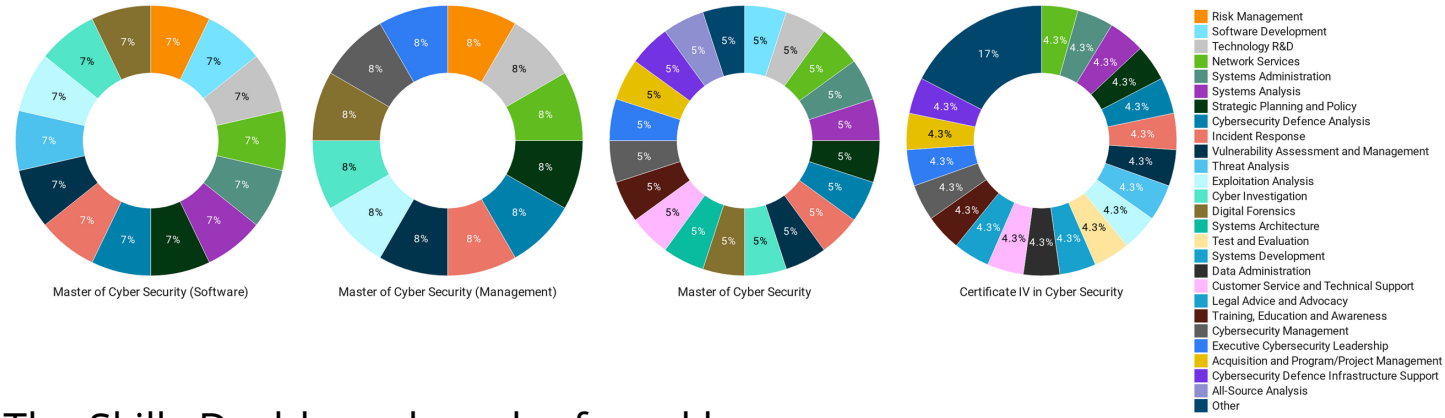


AusCERT provide specialist courses that can be delivered for an organisation or group of interested parties specifically to address incident response and ***Investigate*** work roles.

More recently, the Australian Cyber Collaboration Centre (A3C) was launched in Lot Fourteen to provide specialist training to interested parties and for organisations to request and run. NIST Incident Handling and Introduction to Digital Forensics ran in July 2020 addressing some areas of alignment missing from some better-known certifications and higher education provisions.

As displayed below, higher education qualifications are more broad with a larger number of the NICE Framework KSAs addressed during the course of completion. Shortfalls have been found in areas of ***Analyse*** and ***Collect and Operate***, as well as Knowledge Management and Systems Requirements Planning as having little to no coverage in core courses.

There is scope that these may be addressed with elective courses, but as these can include non-cybersecurity related courses, there are questions over alignment. These electives are useful to address inter-disciplinary skills and learning, but may not align exactly to the NICE Framework.



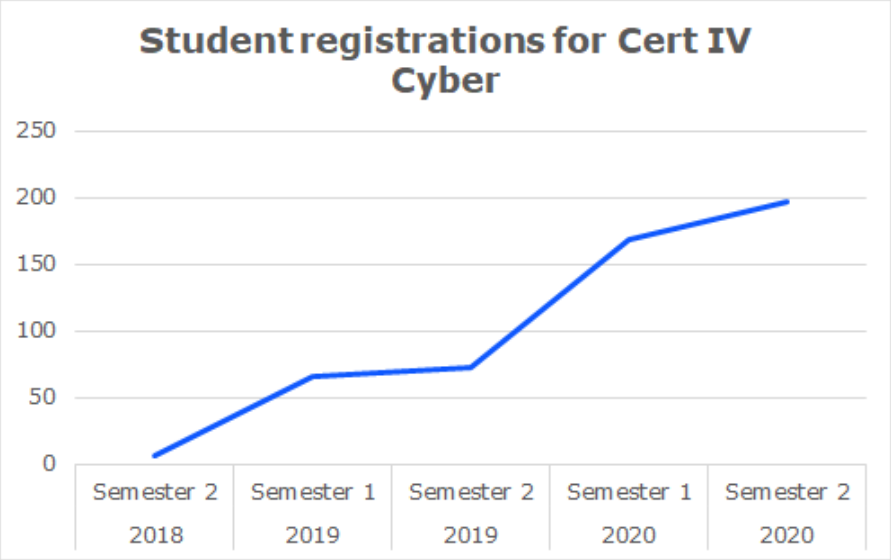
The Skills Dashboard can be found here:

https://www.austcyber.com/educate/career-paths-and-opportunities

Conclusion - What next?

The forecasted growth in SA cybersecurity education provisions is aligning to predicted demand with the introduction of new courses and the increase in enrolment numbers year on year. Continued growth will enable South Australia to plug the gaps in skills and provide a more work-ready workforce.

South Australia's growth of educational offerings is targeting all age groups, including school age students, with the potential inclusion of cyber in the curriculum in state in the near future. As well as course offerings such as the advanced diploma in cyber via TAFE SA and a suite of micro credential options.



TAFE SA S2 2019 - S2 2020 *increase enrolments* of **63%**

This is in line with AustCyber's 2019 SCP prediction that the number of graduates could quadruple by 2026. The establishment of centres such as the A3C will provide a greater opportunity for the delivery of skills across the state and to various audience levels from specialist training courses to executive level training and events.

There is also the opportunity for this project not only to continue to assess all of the higher education providers of cybersecurity-specific courses within the state to include in the Skills Dashboard, but to extend nationwide. As highlighted in this report, cybersecurity is an inter-disciplinary industry, a further stage could be to include data-related qualifications or other areas of related education, law or languages for example.

Acknowledgements

AustCyber SA Innovation Node gratefully acknowledges the following participants for their contributions to industry insights, education provision, and extensive and existing NICE Framework material and knowledge:

AustCyber SA Innovation Node Industry Partners
Department of the Premier and Cabinet, South Australian Government
National Initiative for Cybersecurity Education (NICE)
National Institute of Standards and Technology (NIST)
TAFESA
University of Adelaide
University of South Australia

NICE Framework resources, references and mapping publications from:
(ISC)2
ISACA
EC-Council
National Initiative for Cybersecurity Careers and Studies (NICCS)

MORE INFORMATION

info@austcyber.com

www.austcyber.com/news-events/node-south-australia

https://www.linkedin.com/company/south-australia-cyber-security-innovation-node/

South Australia
Innovation Node

SA Cybersecurity Skills Matrix and the NICE Workforce Framework

The AustCyber SA Innovation Node undertook a survey of industry partners to understand the current position of the cybersecurity roles and skills, and take a view over the future state our partners are forecasting. This focused on work roles, current and forecast, what certifications and qualifications are expected for those roles, and how these align to the NICE Framework as a benchmark.

The aim of this is to support the creation a Skills Matrix and promote further use and understanding of the NICE Framework by students, professionals, industry and the education sector.

Why NICE?

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.

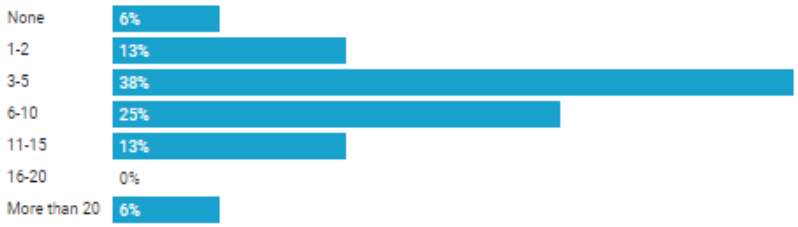
Estimated 18,000 additional cybersecurity workers in Australia by 2026

Where are we now?

7

Average number of cybersecurity roles in respondents' organisations

How many cybersecurity role do you have in your organisation currently?



Within the SA Cyber Security Professional Community, the current qualifications held are wide ranging across higher education qualifications and industry-leading certifications. The current held top qualifications and certifications currently include:

- Bachelor of IT (Networking and Cybersecurity) **77**
- Certified Information Systems Manager **76**
- Certified Information Systems Auditor **65**

When mapped to the NICE Framework, our strengths are in the ***Protect and Defend*** category with all work roles covered by at least one qualification or certification held within SA, however there are large weaknesses in the ***Analyse*** category with **four out of the five** work roles not appearing as matched to the current qualification and certification skills held.

Top three providers in SA

- ISACA 54%
- UniSA 26%
- Adelaide Uni 13%

AustCyber
Australian Cyber Security Growth Network

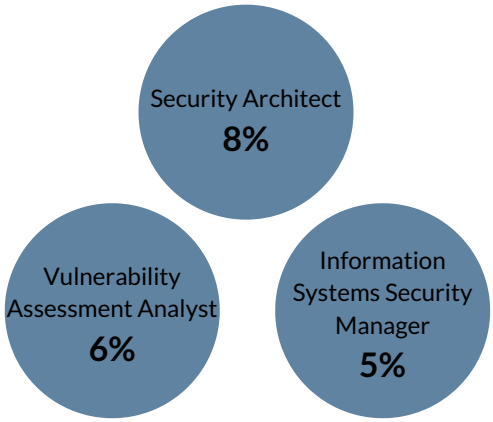
South Australia
Innovation Node

Where do we want to be?

4

Average increase in the number of cybersecurity roles required

The most in demand roles are:



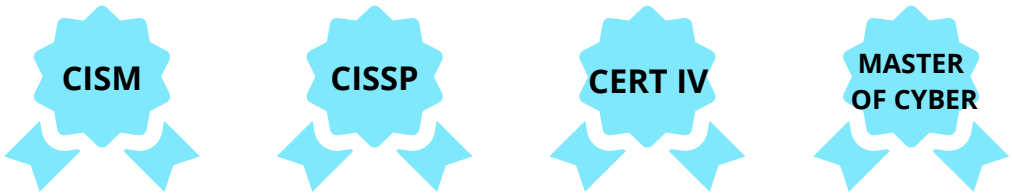
The 52 work roles in the NICE Framework were provided to respondents to consider what roles are in demand for the organisation.

The most in demand roles are heavily weighted towards technical roles and expertise, spread over all categories of the NICE Framework. The top three roles were *Security Architect*, *Vulnerability Assessment Analyst* and *Information Systems Security Manager*.

All roles gained at least one response with the exception of *IT Investment/Portfolio Manager* and *Product Support Manager*.

75% of industry respondents reported difficulties in recruiting for cybersecurity roles in the last 12 months*

For both in demand and hard to recruit work roles, the qualifications and certification expected of those roles overlap with the following 4 as desired:



Using the Skills Matrix, the KSAs for **all four** of the in demand and hard to recruit roles are found in:

- CISSP
- Master of Cybersecurity (UniSA)
- Certificate IV in Cybersecurity (TAFE SA)

On the other hand, CISM aligns to *Information Systems Security Manager* but neither of the other top in demand work roles. It is a qualification that is more aligned to risk management roles, cybersecurity management roles, strategic planning and policy roles, acquisition and program/project management.

We can see that there is a "*over-expectation*" for work roles that are not consistently applied when hiring or looking to hire. A process to match qualifications and certifications against a single list of work roles would enable industry and professionals to speak the same language.

To this end, we invited you to see how the Cybersecurity Skills Dashboard could help you at:

https://www.austcyber.com/educate/career-paths-and-opportunities

AustCyber
Australian Cyber Security Growth Network

South Australia
Innovation Node