A SCHEME FOR THE PROFESSIONAL RECOGNITION OF AUSTRALIAN CYBER SECURITY PROFESSIONALS

AUTHOR: TONY VIZZA
CONTACT: www.tonyvizza.com

INTRODUCTION

HOW GOVERNMENT, INDUSTRY AND ACADEMIA CAN PROFESSIONALISE THE CYBER SECURITY PROFESSION IN AUSTRALIA

This paper offers evidence-based and internationally proven guidance to Australian Government, Industry and Academia stakeholders in relation to setting up a professional accreditation scheme for the cyber security workforce in Australia.

This guidance is based on the adoption of mechanisms that are well understood and valued by the market and industry, coupled with flexibility that caters to individuals who may follow non-traditional pathways to entry into the cyber security profession.

The mechanisms described in this scheme are aligned with internationally recognised standards, congruent with similar schemes that have been adopted by some of Australia's international partners, which incorporate respected indicators of competency and success. Most importantly, the guidance will rely on collaboration and partnerships within the existing value chain to ensure scalability and maximum penetration of the scheme across the Australian cyber security ecosystem.

ANALYSIS OF THE ISSUES WITHIN THE AUSTRALIAN CYBER SECURITY PROFESSION TODAY

There is broad consensus across many sectors of the Australian economy, including government, industry, and academia, that the cyber security sector requires some levels of professionalisation to bring it in line with standards of competence that are commonly in existence in in more established industries. By introducing standards of competency for individuals working within the sector which utilises and aligns to many of the credentials and qualifications that already exist for cyber security professionals, professional work experience and background checks, such a scheme would help in answering long-standing questions which have often plagued and compounded efforts to address the cyber skills shortage. These include:

- **Who, or what, is a 'cyber security professional'?** Robust discussions often centre on whether experienced information technology professionals can, or should, be considered a cyber security professional; or what percentage of a technology professionals day-to-day work needs to take place in cyber security for that person to be considered a cyber professional; or how much 'industry experience' a cyber security professional should have; or what does 'industry experience' entail.
- **The lack of a formal education and career pathway for budding cyber security professionals to follow.** Different stakeholders within the cyber security ecosystem such as universities, TAFE's, private colleges, certification bodies and other training providers such as technology vendors extoll the perceived value of their own offerings, often understating the importance of other, competing offerings. It is true of course that each stakeholder brings value to the ecosystem. However, there is often confusion, mischaracterisation, or a misunderstanding as to what the value of a specific offering may represent, both to the individual as well as to the market. A view that is commonly raised by industry, whether rightly or wrongly, is that recently graduated individuals are not 'job ready', as an example, or that tertiary education courses do not reflect the needs of industry.
- **The rapid pace of change that inherently exists in cyber security, and more broadly in the IT sector.** As so often happens in the cyber security space, education programs can be out of date by the time they can be operationalised. Delivering an up-to-date education program that incorporates a relevant and up to date curriculum is daunting and the rapid change that happens in the sector further hinders the crystallisation of an accepted education and career journey for cyber security professionals.
- **A lack of enough people and skills in the sector, coupled with long-standing issues related to the relatively homogenous nature of the existing workforce and inclusivity of minority and neurodiverse individuals.** The cyber skills gap and workforce shortage both Australia and more broadly, around the world, is well documented. However, it goes beyond just the insatiable demand for cyber (and IT) professionals. Despite initiatives to diversify the IT profession and promote the sector to women, women still only make up 28% of the ICT workforce in Australia[1] and only 18.3% of the cyber security workforce[2]. Similarly, only 128 individuals from ATSI backgrounds work within information security today.[3] This reflects the general trend within STEM (science, technology, engineering and mathematics), with female participation in STEM education remaining at not too similar levels over the last 20 years, despite the focus on increasing female participation in STEM[4].

[1] ACS, *Australia's Digital Pulse – Driving Australia's International ICT Competitiveness and Growth, 2018,* https://www.acs.org.au/content/dam/acs/acs-publications/aadp2018.pdf.
[2] AISA, *Australian Cyber Security Skills and Jobs Study, 2020*, https://aisa.org.au/common/Uploaded%20files/Research/AISA_NSW%20Report_2020_Final.pdf
[3] ASPI, *Too Few Indigenous People in Tech, 2021,* https://ia.acs.org.au/article/2021/too-few-indigenous-people-in-tech.html.
[4] DISR, *Second National Data Report on Girls and Women in STEM, 2021,* https://www.industry.gov.au/news/second-national-data-report-on-girls-and-women-in-stem.

CRITICAL SUCCESS FACTORS FOR A COMPELLING, INDUSTRY SUPPORTED PROFESSIONALISATION SCHEME

In seeking to establish a successful professionalisation scheme, Government, Industry and Academia will need to consider the current cyber security ecosystem as it currently stands. It will be critical for the any future scheme to incorporate the best, most recognised, and most valuable attributes of the existing ecosystem and use those attributes to advance and accelerate progression to the desired end state – which is to establish a scheme where the Australian cyber security workforce is better skilled, experienced, and competent to handle current, new, and emerging cyber threats.

In this paper, it is contended that a professionalisation scheme needs to be founded and guided by the following core principles:

1. The scheme needs to be delivered at minimal cost to individuals.
2. The scheme must not hinder or block emerging new entrants into the marketplace, regardless of their status as a school leaver or career changer.
3. The scheme must not create an additional set of certifications or accreditations, but rather, must leverage existing and respected market certifications and accreditations.
4. The scheme must incorporate methods that recognises professional competency in cyber security. This includes recognition of hands on, paid work experience, as well as educational background an individual has attained.
5. The scheme needs to embed a strong set of professional standards and a code of ethics that strengthens, protects, and promotes public faith in the sector.
6. The scheme should incorporate an element of background / character / ethical standing verification.
7. The scheme must cater for different career pathways within cyber security, both technical as well as non-technical cyber security roles.
8. The scheme must set clear objectives, outcomes, and value for industry stakeholders.

STEPS TO DEVELOPING A SUCCESSFUL AUSTALIAN CYBER SECURITY PROFESSIONALISATION SCHEME

STEP ONE: ESTABLISHING A WORKING GROUP OF RELEVANT GOVERNMENT, INDUSTRY AND ACADEMIA STAKEHOLDERS

As part of developing a professionalisation scheme, it is proposed that a Professionalisation Industry Working Group be established to discuss a proposed scheme, utilising this whitepaper as a basis for discussions. For the purposes of ensuring relevance of any future scheme to government, industry, and academia, it is recommended that the working group consists of 10-15 persons and consists of individuals representing the following key industry stakeholders:

1) **The Australian Information Security Association (AISA)** representing the Australian cyber security profession.
2) **The Australian Cyber Security Growth Network (AustCyber)** representing industry and government views.
3) **The Australian Computer Society (ACS)** representing the broader views of ICT.
4) **Representatives from Academia** including Universities and TAFEs
5) **The Australian Women in Security Network (AWSN)** representing the views of women in the cyber security sector.
6) **The Technology Council of Australia (TCA)** representing the collective views of the private sector and industry in the proposed scheme.
7) **Representatives from the Federal Government**, specifically the Department of Industry, Science and Resources (DISR), the Australian Signals Directorate (ASD), the Department of Home Affairs (DHA) and/or the Australian Cyber Security Centre (ACSC)

STEP TWO: APPOINTING OR ESTABLISHING A GUIDANCE BODY FOR CAREER PATHWAYS IN CYBER SECURITY

To facilitate the establishment of a professionalisation scheme, it will be necessary to appoint or establish a body to administer the scheme. Such a body might be an existing, willing, and suitable organisation, such as the Australian Information Security Association (AISA) or could be a body set up for the sole purpose of administering such a scheme.

The guidance body must operate cooperatively and consultatively across industry with the sole and overriding mission of upholding professional standards and ethics within the Australian cyber security sector.

Any such body that is appointed or established will need to be tasked with administering the scheme, establishing criteria for accreditation, recognising accreditation, and supervising any affiliated organisations for which the professionalisation scheme will rely on to recognise competency.

AISA's relevance and prominence as a peak industry body and association of cyber security professionals within the Australian cyber value chain offers it the ideal, tangible, and immediate opportunity to function as this guidance body. The recognised guidance body should be tasked with establishing precisely what a career in cyber security could look like for individuals looking to become accredited professionals.

STEP THREE: ESTABLISHING A CYBER CAREERS PATHWAY FOR AUSTRALIAN CYBER SECURITY PROFESSIONALS

One of the tasks that the working group will need to definitively establish is for the creation, documentation, and promulgation of a formal cyber career's pathway for existing and future cyber security professionals. Significant ambiguity remains even with seasoned cyber professionals as to the steps required to be deemed a competent professional. This ambiguity is then reflected with potential cyber security professionals, who often rely on anecdotal or self-serving sources of information from institutions financially vested in signing up trainees for their own programs.

An indicative cyber careers pathway for Australian cyber security professionals which the working group should consider is detailed below.

Figure 1 – A Potential Career Roadmap for Cyber Security Professionals

STEP FOUR: ESTABLISHING AN AUSTRALIAN PROFESSIONAL RECOGNITION SCHEME LEVERAGING EXISTING QUALITY CERTIFICATIONS, WORK EXPERIENCE AND TERTIARY EDUCATION

It will be necessary of course to establish an agreed cross-industry professionalisation scheme. It is recommended that any such scheme recognise existing and past work experience, tertiary education, recognised industry certifications and quality training and vendor-led accreditations to minimum levels of competency pursuant to the level of professional recognition being sought, aligned to the following framework.

Figure 2 – Elements of a Proposed Professional Recognition Scheme for Australian Cyber Security Professionals

Under the proposed scheme contained within this whitepaper:

- New and/or early-stage entrants to cyber security would be graded as an **Associate Cyber Security Professional**.
- Established practitioners with formal education and some work experience would be graded as a **Principal Cyber Security Professional**.
- A senior practitioner with extensive work experience would be designated as a **Chartered Cyber Security Professional.**

Professionalisation levels would be based on competency assessed against candidate knowledge, skills, and experience, with this model following from the work currently being considered by the UK Government through the UK Cyber Security Council[5] in the proposed professionalisation scheme being considered for the UK.

The proposed scheme includes a 'fast track' approach using AS / NZS / ISO / IEC 17024 recognised industry certifications which validate knowledge, skills and experience attributes would be included. Additionally, a points-based approach for those who do not hold such certifications would form part of the scheme, which would see points awarded based on tertiary education, vendor certifications / accreditations, hands on work experience and a background / character check through law enforcement. The number of points or value attributed to tertiary education courses would be based on the quality of the course and its relevance to the needs of industry and the community, courses which would be recognised and assessed by the guidance body. This will help ensure tertiary courses continually improve and are responsive to the needs of industry, responding to rapid changes in cyber security. Such a scheme would see industry reward education providers who deliver valuable, relevant, and current education courses for the cyber security sector. Years of service in cyber security roles would also be attributed points based on type of service and length of service.

Proposed Professional Recognition Level	Description of Recognition Level with Career Stage	Equivalent Years of Demonstrated Work Experience
Associate Cyber Security Professional	New Entrant to Early Career	0 to 2 Years
Principal Cyber Security Professional	Early Career to Mid-Career	2 to 5 Years
Chartered Cyber Security Professional	Mid-Career to Senior Career	5 Years +

Table 1 – Proposed Professional Recognition Levels to Career Stage and Equivalent Years of Demonstrated Work Experience

STEP FIVE: EVALUATING THE ROLE OF EXISTING INDUSTRY CERTIFICATIONS IN THE PROPOSED PROFESSIONAL RECOGNITION SCHEME

An essential element of professional recognition will be to consider the numerous education offerings available as well as personnel accreditation schemes that already exist and operate successfully within the Australian cyber security ecosystem. While these offerings differ in nature and quality, many, particularly recognised certifications, enjoy broad industry appeal, with prestige in some of these schemes anchored in independent and verifiable quality control standards such as AS / NZS / ISO / IEC 17024, the international standard which governs and formalised accreditation and certification of individuals. Under this standard, accreditation is based on a candidate's levels of competency, including demonstrated levels of knowledge, skills, and relevant work experience; endorsement by an existing certified professional or by the certification body itself; adherence to a strict and professional code of ethics; and maintenance of the certification by the individual through earning continuing professional education. Additionally, a formalised process in determining credential knowledge areas and updating accredited certifications on a periodic basis are core to the AS / NZS / ISO / IEC 17024 standard. For these reasons, AS / NZS / ISO / IEC 17024 certifications have been recognised and are incorporated into numerous accreditation, certification, and recognition schemes, here in Australia as well as globally.

It must be noted that in Australia, the ASD Independent Registered Assessors Program (IRAP) program recognises such certifications as prequalifiers to IRAP accreditation. Additionally, AS / NZS / ISO / IEC 17024 accredited certifications are recognised by international partners in the U.S. via the US Department of Defence 8570.01-M / 8140.01 standards, the UK Government endorsed Certified Cyber Professional (CCP) Assured Service administered by the British Computer Society (BCS) and the Chartered Institute of Information Security (CIISec).

STEP SIX: EVALUATING THE ROLE OF TERTIARY EDUCATION IN THE PROPOSED PROFESSIONAL RECOGNITION SCHEME

A traditional route into the cyber security sector involves individuals completing a recognised degree program via an Australian (or overseas) university or via a TAFE accreditation. At university, this can often involve a Computer Science, Information Technology, or a dedicated Cyber Security degree, either at undergraduate or postgraduate level. At TAFE, a Certificate III/IV in Information Technology, Networking or Cyber Security is also well recognised. This whitepaper contends that a professional recognition scheme needs to incorporate recognition of such programs, coupled with the requirement that an individual seeking accreditation possess a minimum amount of paid and verifiable work experience as a cyber security practitioner.

STEP SEVEN: ESTABLISHING THE ROLE OF PAID AND VERIFIABLE WORK EXPERIENCE IN THE PROPOSED PROFESSIONALISATION RECOGNITION SCHEME

A concern often vocalised by industry is that it requires competent individuals who possess paid and verifiable work experience with cyber security. It is for this reason that AS / NZS / ISO / IEC 17024 industry accreditations which require paid and verifiable work experience have earned considerable respect as an indicator of an individual's competency in the field, and why many job descriptions include a desired listing of industry certifications. It is validly noted and recognised that for those who do not have, or have very limited work experience, this is a limiting factor in terms of employment prospects. As part of the proposed recognition scheme, it is contended that the formal recognition of paid work experience is an essential element for individuals who may or may not possess academic qualifications or AS / NZS / ISO / IEC 17024 industry accreditations.

[5] https://www.ukcybersecuritycouncil.org.uk/

THE PROPOSED METHODOLOGY TO BE EMPLOYED IN ASSESSING INDIVIDUALS TO ATTAIN PROFESSIONAL RECOGNITION UNDER THIS SCHEME

It is proposed that two specific pathways to cyber security professionalisation are incorporated as part of a future Australian cyber security professionalisation scheme.

Under both pathways, an appointed and recognised Australian cyber security industry body would become the recognised guidance body and authority for Australian cyber security professionals.

PATHWAY 1 – FAST TRACK USING AS / NZS / ISO / IEC 17024 ACCREDITATIONS

The recognised Australian cyber security industry authority and guidance body would formally accredit relevant international certification bodies to issue professional recognition to Australian cyber security professionals in line with the professionalisation scheme. This would be limited to relevant not-for-profit industry bodies that issue AS / NZS / ISO / IEC 17024 certifications and can demonstrate that they follow a verifiable and structured process for individuals to accredit against. The approved Australian guidance body would then categorise certifications issued by these international bodies according to the level of competence each certification demonstrates and bestow the title of **Associate**, **Principal** or **Chartered** pursuant to that level of certification.

For individuals using AS / NZS / ISO / IEC 17024 certifications as a basis for their professional recognition, individuals would need to remain compliant and current with their internationally issued industry certifications to maintain currency under the proposed Australian professionalisation scheme.

In seeking to create a professionalisation scheme, in the immediate term, it would be wise to take into consideration the existing accreditation landscape, particularly those administered under AS / NZS / ISO / IEC 17024. This will ensure that the new scheme can be rapidly adopted by an existing and significantly sized cohort of individuals who are already certified in internationally recognised, industry-respected, and quality-controlled certifications. Crucially, the strict and formalised process which each certification body must adhere to for the regular updating of the bodies of knowledge underpinning each certification ensures that the both the certification as well as any scheme that relies on those certifications remains futureproofed. Similarly, the requirement that certified individuals accredited under AS / NZS / ISO / IEC 17024 maintain their certifications through a formalised process of continuing professional development and education ensures that individuals who maintain their certifications can demonstrate currency of knowledge, skills, experience, and overall competency, providing an additional layer of validity and relevance to any schemes that use AS / NZS / ISO / IEC 17024 accreditations as a basis for recognition.

Accreditation	Verified Work Experience Requirements	Status Claimable
(ISC)²		
CISSP	5 Years	Chartered
CISSP-ISSAP	6 Years	Chartered
CISSP-ISSEP	6 Years	Chartered
CISSP-ISSAP	6 Years	Chartered
CCSP	5 Years	Chartered
SSCP	1 Year	Associate
CSSLP	4 Years	Principal
ISACA		
CISM	5 Years	Chartered
CISA	5 Years	Chartered
CRISC	3 Years	Principal
CPDSE	3 Years	Principal
CGEIT	5 Years	Chartered
CompTIA		
Security+	1 Year	Associate
CySA+	4 Years	Principal
Pentest+	3 Years	Principal
PECB		
ISO 27001 Implementer	2 Years	Associate
ISO 27001 Lead Implementer	5 Years	Principal
ISO 27001 Senior Lead Implementer	10 Years	Chartered
ISO 27001 Auditor	2 Years	Associate
ISO 27001 Lead Auditor	5 Years	Principal
ISO 27001 Senior Lead Auditor	10 Years	Chartered

Table 2 – Proposed Categorisation of AS / NZS / ISO / IEC 17024 Certifications issued by ISACA, (ISC)², CompTIA and PECB against the proposed Australian Professionalisation Scheme.

Note: This is not an exhaustive or final list of proposed certifications to be used for a 'fast track' scheme, However, any potential certification on the 'fast track' scheme must be AS / NZS / ISO / IEC 17024 to qualify for inclusion by the proposed Guidance Body.

PATHWAY TWO: A DEMONSTRATRATION OF COMPETENCY-BASED ATTRIBUTES FOR PROFESSIONAL RECOGNITION UNDER THE PROPOSED SCHEME.

For individuals seeking professional recognition who may not hold a recognised certification or accreditation under Pathway One, nor seek such an accreditation, the recognised Australian authority and guidance body for Australian cybersecurity professionals would seek to utilise a credit points system whereby credits are awarded based on an individual's verified knowledge, skills, education, and experience. Credits will vary based on the type of education, experience and training being claimed. The approved guidance body would then categorise individuals according to the level of competence demonstrated, and bestow the title of **Associate**, **Principal** or **Chartered** pursuant to that level of competence.

Individuals accredited under this pathway will be required to maintain their professional accreditation by demonstrating ongoing education and currency of skills through a Continuing Professional Education and Development (CPE / CPD) scheme administered by the recognised Australian guidance body, equivalent in nature and rigour to that defined under AS / NZS / ISO / IEC 17024.

It is understood and appreciated that there are numerous routes that an individual could take into the cyber security profession, both conventional as well as non-conventional. Some individuals may create their own career journey and demonstrate an equally valuable set of knowledge, skills, experience, and competency. This pathway caters for such individuals.

For the purposes of illustrating how a potential professionalisation scheme could operate, credits could be assigned for indicators of competency, such as a tertiary education program in or directly related to cyber security. A limited and provisional example schedule of credits for each indicator of competency is listed below.

Indicator of Competency	Credits
Recognised Tertiary Educational Programs	
TAFE Cert III / IV in Cyber Security (or Equivalent)	10
TAFE Cert III / IV in IT	5
Recognised Diploma or Advanced Diploma in Cyber Security	10
Recognised Diploma or Advanced Diploma in IT and IT related fields (such as network and systems administration)	5
Recognised Bachelor's Degree in Cyber Security	30
Recognised Bachelor's Degree in IT	20
Recognised Master's Degree in cyber security	30
Recognised Master's Degree in IT	20
PhD in Cyber Security	20
Recognised and Approved Vendor Accreditations	
AS / NZS / ISO / IEC 17024 accreditations not issued by international not-for-profit industry associations (For example: Cisco CCIE or Microsoft Azure accreditations)	20
Non-ISO issued and recognised credentials (For example: Offensive Security, eLearnSecurity, EC Council etc)	Between 5 and 20 depending on content.
Recognised Work Experience	
Each Equivalent Full Time Year of Paid and Verifiable Work Experience in Cyber Security. Work must include at least *one* element of the following disciplines within the cyber security ecosystem: - Security Risk Management - Asset Security - Security Architecture - Security Engineering - Identity and Access Management - Security Assessment - Security Testing - Security Operations - Software Development Security - Security Auditing - Security Governance	10

Table 3 – Proposed Indicators of Competency with provisional credit weightings for each.
Note: This is not an exhaustive or final list of proposed indicators of competency to be used for a 'credit point' scheme, However, any potential indicator of competency on the 'credit point' scheme must be approved by the proposed Guidance Body to qualify.

Under a proposed scheme operating under the credit point method:

- an individual seeking to attain **Associate** status would require 20 points;
- an individual seeking to attain **Principal** would require 50 points and;
- an individual seeking to attain **Chartered** would require 100 points.

MAPPING THE PROPOSED PROFESSIONAL ACCREDITATION SCHEME TO EXISTING AUSTRALIAN GOVERNMENT PROFICIENCY LEVELS

It is noted that the Australian government employs several schemes to indicate competency levels, including the ASD Cyber Skills Framework.[6]

To facilitate better acceptance of the proposed Accreditation Scheme, an indicative mapping of accreditations to existing schemes is as follows:

Proposed Australian Professionalisation Recognition Scheme	ASD Cyber Skills Framework Level	CIISec Skills Framework	SFIA Levels	ASD Streams
Associate	Level 1 – Learner	Level 1 – Knowledge	Level 1 – Follow	N/A
Associate	Level 2 – Novice	Level 2 – Knowledge and Understanding	Level 2 – Assist	Level 1 – Novice
Principal	Level 3 - Practitioner	Level 3 – Apply	Level 3 – Apply	Level 1 – Novice
Principal	Level 4 – Senior Practitioner	Level 4 – Enable	Level 4 – Enable	Level 2 – Practitioner
Chartered	Level 5 – Principal Practitioner	Level 5 – Advise	Level 5 – Advise, Ensure	Level 3 – Expert
Chartered	Level 6 – Expert Practitioner	Level 6 – Expert	Level 6 – Initiate, Influence Level 7 – Set Strategy, Inspire, Mobilise	Level 4 - Leader

Table 4 – Indicative Mapping of Accreditation Scheme Status (Associate, Principled, Chartered) with Australian Cyber Ecosystem Frameworks and Standards

CONCLUSION

The Australian cyber security industry sits at a crossroads, one which more established industries have endured in their own histories. Faced with challenges which have undermined those sectors, visionary professionals in those sectors agreed that reform was needed and established professionalisation schemes to ensure that both industry and members of the public could identify credentialed and competent individuals to assist them with their problems and challenges.

The time for professionalisation of the Australian cyber security sector has come: to provide entrants into the sector a level of certainty as to what is needed to achieve their career goals; to provide academia a pathway to credible and relevant education offerings; to provide industry and the private sector the ability to discern which individuals have achieved a base level of competence in cyber security; to provide a framework and a governance model for cyber professionals and their continuing education requirements; and finally to help achieve a safer and more cyber secure Australia.

[6] ASD, *ASD Cyber Skills Framework,* https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf

ABOUT THE AUTHOR

Tony Vizza has been involved in the information technology, information security and privacy fields for more than 25 years.

Tony has completed a Bachelor of Science in Computing Science from the University of Technology, Sydney and a Global Executive MBA from the University of Sydney which included study at Stanford University in the United States, The London School of Economics in the UK and the Indian Institute of Management, Bangalore in India. Tony is currently studying for a Juris Doctor law degree at the University of New South Wales.

Tony's information security credentials include CISSP (Certified Information Systems Security Professional), CCSP (Certified Cloud Security Professional), CIPP/E (Certified Information Privacy Professional / Europe), CRISC (Certified in Risk and Information Systems Controls), CISM (Certified Information Security Manager) and he is a certified ISO/IEC 27001 Senior Lead Auditor.

Tony is a member of the Board of Directors for the Australian Information Security Association (AISA), a Cyber Security Ambassador for the NSW Government, a member of the Cybersecurity Industry Advisory Committee for the NSW Government, a member of the Technology and Business Services Industry Skills Reference Group for NSW TAFE, a member of the Data Security Standards Committee for Blockchain Australia, the co-chair of the (ISC)^2 Asia-Pacific Advisory Council and has provided expert services to the United States Government Department of Energy (DoE), the United Kingdom Department of Culture, Media and Sport (DCMS), the European Union Cyber Security Organisation (ECSO), the Australian Government's Australian Prudential Regulation Authority (APRA), the Australian Signals Directorate (ASD), the Law Society of NSW, the Australian Security Industry Association Limited (ASIAL), the Australian Institute of Project Management (AIPM) as well as numerous boards.

Tony is an expert speaker on information security regularly speaking across the world on information security matters. He has also taught and mentored young and aspiring information security students through Victoria University, TAFE NSW and TAFE Victoria in association with Infoxchange and has lectured cybersecurity students at the University of Technology, Sydney, the University of New South Wales and the University of Queensland.

Tony is a regular contributor to numerous cyber security and IT industry publications including CSO Magazine, Infosecurity Magazine, Cyber Today Australia, Security Insider Magazine, Australian Reseller News (ARN), Channel Reseller News (CRN) and Lifehacker, amongst others, regarding information security, privacy, business, and channel strategy.

Tony can be contacted through www.tonyvizza.com.