Journal of Systems Thinking

Understanding First, Solutions Second

A Systems Thinking Analysis of the Proposed Australian Cybersecurity Professionalization Scheme

MICHAEL COLLINS [a, b, @]
a: Independent Researcher
b: Melbourne, Australia
@: michael@cybercognition.com.au

ABSTRACT:
This paper applies rigorous systems thinking methodologies to critically evaluate Australia's proposed Cybersecurity Professionalization Scheme within the context of Australia's projected workforce shortages. Through the analytical frameworks of DSRP Theory (Distinctions, Systems, Relationships, Perspectives) and Agent-Based Approach (ABA), this research interrogates the complex adaptive system of cybersecurity workforce development. Meta-analysis of empirical evidence across industries reveals a consistent pattern: while professionalization schemes increase practitioner earnings and potentially enhance service quality in high-risk domains, they simultaneously create significant market entry barriers and can reduce workforce growth. The study identifies that Australia's proposed scheme exhibits strengths in its industry-led design philosophy and integration with existing certification frameworks, but raises concerns regarding systemic impacts on cost inflation, industry adoption rates, and workforce diversity. The ABA analysis identifies emergent properties that may undermine the scheme's objectives and proposes design principles to mitigate unintended consequences.

This paper contributes to the critical discourse on professionalization by demonstrating how a systems thinking approach can reveal dynamics invisible to traditional policy analysis. This research provides stakeholders with an evidence-based evaluation framework to assess the scheme's effectiveness and sustainability, while offering specific recommendations aligned with systems design principles that could enhance positive outcomes while mitigating negative systemic impacts.

As a result, the fundamental question emerges: does Australia have an adequate understanding of the cybersecurity workforce system prior to implementing solutions?

KEYWORDS: Systems Thinking | DSRP | Agent-based Approach | Complex Adaptive Systems | Cybersecurity | Professionalization | Occupational Licensing | Workforce Development | Australia

---

Statement of Significance

This paper expands upon prior research applying DSRP-483 theory within the domain of cybersecurity. Utilizing DSRP and ABA methodologies in national policy discourse illustrates the significance of comprehending the dynamic and adaptive characteristics of complex adaptive systems and the consequences of policy decisions that may impact entire industries.

Background

According to a report published by the Australian government in 2023, the projected shortage of workers in the cybersecurity industry by the year 2026 is estimated to range significantly from 3,000 to 25,000 individuals (18). In response the Australian Government has proposed a ‘Growing and Professionalizing the Cybersecurity Industry Program’ as part of its 2023-2030 Australian Cybersecurity Strategy, allocating $1.9 million over two years (2024-2026) to design, promote, and pilot a professionalization scheme for Australia's cybersecurity workforce (5).

This initiative responds to industry calls for greater clarity around how cybersecurity qualifications and skills map to industry requirements. The stated objectives include establishing a pilot industry-led cybersecurity professionalization scheme, providing clear career pathways, reducing entry barriers, attracting diverse talent, enhancing domestic capabilities, and increasing industry confidence in the workforce (4).

The professionalization of an occupation can be characterized as a social process in which an association is established to supervise the behavior of its members and to establish a method for distinguishing between qualified (professionals) and unqualified (amateurs) members (14). The Australian Professional Standards Council, which regulates professional associations and promotes consumer protection, describes it more explicitly as “the emergence of regulatory bodies with powers to admit and discipline members, and some degree of monopoly rights” (16).

Occupational licensing is a comparable approach that has many similarities with professionalization, including licensing, a code of ethics, industry impacts, and a variety of similar benefits and drawbacks. It is important to recognize that occupational licensing is typically regulated by the government, rather than self-regulation by industry (17). The question of whether there is a tangible benefit to professionalizing Cybersecurity practitioners continues to divide senior cybersecurity leaders in Australia (1,7), raising concerns about whether it would significantly improve either Australia's cyber resilience or cybersecurity workforce shortages.

Research indicates that while the cybersecurity workforce currently lacks formal professionalization, industry standards are maintained through certifications, education requirements, and extensive experience prerequisites. Each of the certification bodies noted in the grant document have a code of ethics (31,32,33,34) that holds members accountable for their conduct. Regarding the significance of certifications in obtaining employment in the market, an analysis of job postings revealed that 64% require industry certifications (particularly CISSP), 82% demand at least a bachelor's degree, and 95% require prior experience, with a median requirement of five years (20, 21).

Professionalization metrics in cybersecurity currently focus on certification rates and workforce retention indicators. Studies report that 67% of companies require vendor-specific or vendor-neutral certifications, with 94% of respondents confirming that certifications facilitate employment and 80% noting their value for career progression (19). Retention metrics emphasize non-technical skills development, professional identity enhancement, and job satisfaction. Across a variety of industries and geographies, both

professionalization and occupational licensing schemes have yielded mixed results. Therefore, understanding the experiences of other industries with similar schemes provides vital context.

Economic research demonstrates that occupational licensing consistently raises practitioner earnings by 4-15% across industries and increases service prices (22). While quality improvements are documented in healthcare, with licensing linked to reduced mortality rates, similar quality benefits are less evident in other sectors (25). Licensing also reduces market competition and can decrease employment by up to 29%, with stronger adverse effects in lower-risk occupations (22). Without a thorough understanding of the industry's dynamics, the potential consequences of professionalizing Australia's cybersecurity industry could have far-reaching implications, necessitating additional research to determine whether it presents opportunities or risks.

This paper represents the initial step in that process, by applying established systems thinking frameworks, to conduct a systematic analysis of the cybersecurity workforce in the context of the proposed professionalization scheme. It examines its potential effects on workforce dynamics, service quality, market competition, implementation challenges, and factors that influence success.

Methodology

Scope

It is important to highlight that certain constraints were purposefully imposed on this analysis to ensure timeliness and to prevent scope creep. Because we are dealing with a complex adaptive system, it is critical to understand that any changes to the system's state or updates to the information used during the analysis may have an impact on the outcomes, so those predictions must always be revisited to determine any potential changes.

This should not be interpreted as a weakness in the analysis, or the approach used, but rather as an acknowledgement of the difficulties of working with a complex and changing system. In fact, this is a significant benefit of using this method, which distinguishes it from other methodologies that ignore the inherent nature of complex adaptive systems (3). It also emphasizes the significance of establishing measures for tracking the system's behavior over time to understand whether it is serving its intended goal.

This analysis employed “Fropping”, a combination of framing and stopping rules designed to limit the analysis and address questions regarding what is essential, when to cease, and what or where to investigate (24).

Framing Rules

1. Utilize evidence-based methodologies to substantiate the validity of the approach.
2. Conduct the analysis to;
    a. Educate stakeholders about the complex nature of the initiative.

    b. Inform stakeholders of proposed policy recommendations.
3. Analysis based on publicly available research and information.

Stopping Rule

1. Complete the analysis within 4-6 weeks

Rapid Literature Review

To comply with the fropping rules, a rapid literature review was conducted using the AI research tool Elicit (29), with the goal of reducing the time required for evidence synthesis while maintaining a methodology comparable to human-based synthesis without sacrificing accuracy.

In order to identify any difference in effects between the two approaches a similar research question was asked for both the occupational licensing and professionalization schemes.

Using the research questions;

1. “What is the comparative impact of occupational licensing on economic performance, quality of service, workforce growth and retention, and consumer protection across different industries?”

2. What is the comparative impact of industry professionalization on economic performance, quality of service, workforce growth and retention, and consumer protection across different industries?

A search was conducted across over 126 million academic papers from the Semantic Scholar Corpus, with 50 papers being identified as the most relevant to each of the queries.

Screening

Screening was performed to narrow down the relevant research to those that were most closely aligned to the research question. Papers that met the following criteria were then selected:

1. **Empirical Analysis of Licensing**: Does the study empirically examine occupational licensing or professionalisation requirements in any industry or profession?

2. **Relevant Outcomes**: Does the study measure at least one of the following outcomes: economic performance (wages, prices, market competition), service quality metrics, workforce characteristics, or consumer protection outcomes?

3. **Comparative Analysis**: Does the study include a comparison between licensed and unlicensed periods, jurisdictions, or professions?

4. **Research Design**: Does the study employ one of the following quantitative research designs: quasi-experimental studies, longitudinal analyses, cross-sectional comparative analyses, or

systematic reviews/meta-analyses?

5. **Geographic Scope**: Does the study examine licensing requirements within a defined geographic jurisdiction (national, state, or local level)?

6. **Original Research**: Is the paper an original research study (not an opinion piece, commentary, theoretical paper, or policy recommendation without original research)?

Results – Occupational Licensing

Study	Study Design	Industry Sector	Outcomes Measured	Geographic Scope	Full Text Retrieved
Anderson et al., 2016	Empirical quantitative	Healthcare (Midwifery)	Maternal mortality, infant mortality	United States	Yes
Anderson et al., 2020	Empirical quantitative	Healthcare (Midwifery)	Maternal mortality, infant mortality	United States	Yes
Blair and Fisher, 2022	Mixed methods	Home Services	Service provider surplus, platform surplus, consumer surplus, accept rate	United States	Yes
Carollo, 2020	Empirical quantitative	Various licensed occupations	Worker earnings, employment	United States	No
Deyo, 2017	Empirical quantitative	Four unspecified occupations	Number of firms, service quality (Yelp ratings)	United States (implied)	No
Farronato et al., 2020	Empirical quantitative	Home Improvement Services	Service prices, competition, consumer satisfaction	United States	Yes
Johnson and Loucks, 1986	Empirical quantitative	Real Estate	Number of licensees, earnings, service quality	No mention found	No
Kleiner and Kudrle, 1997	Empirical quantitative	Healthcare (Dentistry)	Service prices, practitioner earnings	United States	No
Kleiner and Kudrle, 1999	Empirical quantitative	Healthcare (Dentistry)	Service prices, practitioner earnings	United States	No

Kleiner and Soltas, 2019	Mixed methods	Various licensed occupations	Wages, employment, service prices, total surplus	United States	No

Table 1- Characteristics of the included studies

Quantitative Effects of Licensing

Impact Measure	Effect Size Range	Industry Variation	Key Findings
Practitioner Earnings	+4% to +15%	Consistent across industries	Licensing generally increases earnings
Wages Employment	-29% to slight positive	Varies by industry and risk level	Mixed effects, with some studies showing significant negative impacts
Service Prices	Increase (magnitude not specified)	Consistent across studied industries	Licensing tends to increase prices
Market Competition	Decrease (magnitude varies)	Consistent across studied industries	Licensing reduces competition and number of firms
Consumer Surplus	No significant increase to decrease	Limited data across industries	Mixed effects, with some showing no benefit or negative impacts
Platform / Provider Surplus	-27.8% to -36.8%	Specific to digital platforms	Significant negative impact to home services industry

Table 2- Economic Performance Metrics

Key Findings of Occupational Licensing Studies

Licensing typically increases practitioner earnings. Employment effects differed, with some studies indicating significant negative effects. Studies consistently show that licensing raises prices. Licensing reduced the number of firms and competition in the industries being studied. Some studies found no positive or negative effects from consumer surplus. Occupational licensing can have a complex and multifaceted impact on economic performance, with potential trade-offs between outcomes.

Workforce effects

These findings imply that occupational licensing may alter workforce dynamics, reducing employment and market entry while increasing job stability for licensed professionals.

Consumer Protection Outcomes

Several studies have found varying links between occupational licensing and service quality or consumer protection. Whilst licensing seemed to be a promising solution in healthcare-related fields, it was unclear whether it resulted in higher quality in fields other than healthcare. All the studies suggest a potential

trade-off between quality/protection outcomes and economic consequences (such as higher prices and reduced competition).

Issues in Measuring Quality Outcomes

Because there are so many ways to measure quality (such as death rates, consumer ratings, and an undefined concept known as "quality of service"), it is difficult to determine the impact of licensing on service quality across all industries. This variation in how results are measured demonstrates how difficult it is to assess quality and the importance of exercising caution when interpreting results in various business settings.

Barriers to Entry

Several studies have consistently reported across industries that licensing creates barriers to entry, reducing the number of practitioners or firms in the market, which in turn translated into less competition in those licensed industries (27). The reduced competition associated with licensing was often reported to be accompanied by higher prices for services (28, 22), which may impact market dynamics and consumer access to services. While licensing was generally reported to increase earnings for those in the profession, some studies reported that it may reduce overall employment in the sector (22). This suggests a potential trade-off between benefits for licensed practitioners and overall market participation.

Conclusion

Together, these results imply that occupational licensing has a significant documented influence on market structure and competition in several industries, typically resulting in more competitive, limited markets with fewer players and higher prices. These differences underline the need to take industry-specific elements into account while assessing the effects of occupational licensing.

Results – Professionalization

Study	Study Design	Industry Sector	Outcomes Measured	Geographic Scope	Full Text Retrieved
Barone and Cingano, 2008	Empirical quantitative	Professional services, retail trade, network sectors	Effects of anticompetitive service regulation on economic performance	Organisation for Economic Co-operation and Development (OECD) countries	Yes
Canton et al., 2014	Empirical quantitative	Legal, accounting, architectural, engineering activities	Economic impact of professional services liberalization	European Union	No
Deyo, 2017	Empirical quantitative	Four unspecified occupations	Relationship between licensing and service quality	No mention found	No
Farronato et	Empirical	Home	Impact of	United States	Yes

al., 2020	quantitative	improvement services	occupational licensing on demand and supply		
Johnson and Loucks, 1986	Empirical quantitative	Real Estate	Effect of state licensing regulations on real estate brokerage industry	No mention found	No
Kawaguchi et al., 2014	Quasi-experimental; Empirical quantitative	Large-scale building construction	Effects of stricter quality standards on architects and building market	Japan (Tokyo metropolitan area)	Yes
Kleiner and Kudrle, 1999	Empirical quantitative	Healthcare (Dentistry)	Impact of licensing stringency on dental services	No mention found	No
Morris et al., 2023	Comparative analysis	Various licensed occupations	Methods to improve care worker recruitment, retention, safety, and education	Not limited to specific region or country	Yes
Paterson et al., 2007	Comparative analysis	Legal services, accountancy services, technical services, pharmacy services	Comparison of regulations governing professional services	European Union member states	No
Zhang and Gunny, 2006	Comparative analysis	Accounting industry	Comparison of self-regulation vs. private sector regulation	No mention found	No

Table 3 - Characteristics of the included studies

Quantitative Effects of Professionalization

Impact Measure	Effect Size Range	Industry Variation	Key Findings
Practitioner Earnings	Up to 30% increase	Construction and Dental	Limited data suggests a tendency toward increased earnings for licensed practitioners, though the evidence base is relatively small and focused on specific sectors
Employment	-2.2% to slight positive	Varies by industry and risk level	Mixed effects, with some studies showing slight negative impacts
Service Prices	3.2% to 15% increase in prices	Consistent across studied industries	While the evidence is limited to three studies, all findings consistently showed that stricter licensing or regulation was associated with higher prices for consumers.
Market Competition	Negative relationship (magnitude varies)	Consistent across studied industries	Licensing reduces competition and number of firms
Consumer Surplus	Price effects suggest negative impacts on consumers	Not mentioned	While consumer surplus isn't explicitly measured, the combination of higher prices, reduced competition, and inconsistent quality improvements suggests that stricter licensing and regulation may negatively affect consumer welfare overall.
Platform / Provider Surplus	Negative impacts	Not mentioned	Reduced market participation suggests that the overall effect on provider surplus may be mixed. However, the report's limited data and lack of direct surplus measures makes it difficult to draw definitive conclusions about total platform/provider surplus.

Table 4- Economic Performance Metrics

Key Findings of Professionalization Studies

The research report identified several key findings across different domains which were broadly consistent with the previous stated findings related to the occupational licensing model.

Economic Effects
Prices consistently increased with stricter licensing, competition decreased, evidenced by fewer firms and less regulated services showed better efficiency outcomes, including faster value added and productivity growth.

Workforce Effects
Earnings typically increased for licensed practitioners, employment effects were generally negative, with fewer firms operating and reduced service quotes.

Service Quality
Evidence was mixed, with one study finding licensing lowered quality, another showing no significant quality improvement, and one reporting higher quality with pre-licensing regulation.

Barriers to Entry
While the research doesn't explicitly use the term "barriers to entry", it provides several indicators suggesting that stricter licensing and regulation created entry barriers. These findings consistently suggest that stricter licensing and regulation reduce market participation and new entry. However, it's worth noting that only 3 of the 10 studies provided data related to market entry effects, and the report doesn't provide detailed analysis of specific entry barrier mechanisms.

Rapid Literature Review Summary

Although this was not a comprehensive study, the rapid literature review offers focused, high-quality, and authoritative resources for time-sensitive decision-making. The research demonstrates that more stringent licensing and regulation typically resulted in diminished market competition and less efficient market structures, regardless of the model employed. Less stringent regulation seems correlated with accelerated value addition, enhanced productivity, and increased allocative efficiency, indicating that producers meet consumer demand effectively.

A separate but related report written for the Victorian Government to consider the use of occupational licensing noted, "there are countless studies that have examined the potential for occupational licensing to cost more in terms of higher prices, reduced competition, and poorer consumer choice and options, than the schemes actually resolve in terms of protecting consumers and addressing market failures" (17). The report identifies several criteria that must be met to determine whether licensing has the potential to address specific issues and is justified. The Australian Government grant scheme document made no explicit mention of any of these market conditions, implying that occupational licensing would not be a consideration in this scenario.

Analysing the Australian Cybersecurity Workforce System

DSRP

DSRP theory (Distinctions, Systems, Relationships, Perspectives) is the universal pattern for how information is organized in both the mind and nature and is used to help make meaning of the world (30). Applying DSRP helps overcome the biases inherent in our mental models of reality. DSRP is predictive in nature and is used to interrogate the system and explore elements that might be overlooked during the analysis phase (2,3). The importance of comprehending the complexities of any system should be evident, particularly in decision-making and policy formulation. However, a common bias is the tendency to immediately seek solutions. A DSRP analysis allows the analyst to identify knowledge gaps, consider potential biases, and gain a better understanding of any system before attempting to fix perceived problems within it. This analysis contributes to the creation of a mental model aimed at improving our understanding of the real-world system of the Australian cybersecurity workforce in relation to the implementation of a professionalization scheme.

Systems Thinking Loop (ST-Loop)

Throughout the analysis, the analyst compares the information received with the current model. Where new understanding emerges, this mental model is updated to better reflect reality and provide the closest approximation to the real world. The model should be regularly tested against real-world developments, such as industry feedback, regulatory changes, and workforce trends.

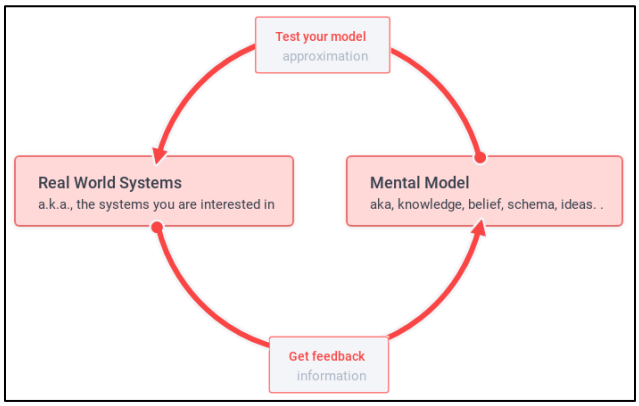

Figure 1- Systems Thinking Loop

DSRP Analysis

Establishing the Mental Model

The initial starting point for the mental model was derived from information provided from the grant document and other publicly available information. DSRP analysis helps the practitioner identify and map the system's distinctions, systems, relationships, and perspectives. To better understand any system, you must first understand what is included and excluded, as well as the individual parts and how they can be

combined to form a whole. Then, by understanding the relationships between and among those parts and wholes, you can look at how they're related, as well as how your decisions may lead to actions and reactions between them. This enables you to make structural predictions about the system's behavior based on your choices and actions. Finally, identifying the system's various perspectives allows you to gain a better understanding of the various points of view about the system and how each perspective may reflect a different mental model of the situation.

As a result, using DSRP ensures that we prioritize thinking over acting, and thus understanding over solutioning.

1. Distinctions Analysis (Identity - Other)

The grant document includes definitions for the following key identities in the Cybersecurity licensing ecosystem. It is equally important to define what they are (identity) and what they are not (other), to identify what may be intentionally or unintentionally excluded from the program. This helps to avoid biases that arise from focusing solely on one element, such as 'identity' at the expense of 'other'.

Identity	Other(s)
Professionalisation scheme	Ad hoc industry practices, unstructured professional development, varied employer expectations, inconsistent job requirements
Certified professionals	Uncertified professionals
Career pathways	Fragmented career progression; ambiguous skill requirements
Cybersecurity industry bodies	
Industry standards	Sub-standard, non-standard, unconventional practices
Domestic cybersecurity workforce	New entrants, excluded minorities, non-cybersecurity professionals, international candidates
Professional certification schemes	On the job experience, tacit knowledge
Educational institutions	Non-formal education; Self-taught professionals

Table 5- Distinctions Analysis

2. Systems Analysis (Part-Whole)

The cybersecurity workforce system can be organized into several part-whole systems, each with multiple parts, and recognizes each system may also be a part of a larger system.

Cybersecurity Workforce

- Domestic
    - Certified
    - Non-Certified

Cybersecurity Industry Organizations

- Australian Computer Society
- Australian Information Security Association

Eligible Grant Recipient

- Industry-led Co-design Team
- Existing Consortium

International Best Practice Skills Frameworks

- Skills Framework for the Information Age (SFIA)
- National Initiative for Cybersecurity Education (NICE)
- Cybersecurity Body of Knowledge (CyBok)
- Chartered Institute of Information Security (CIISec)

Professional Certification Schemes

- Information Systems Audit and Control Association (ISACA)
    - Certified Information Security Manager (CISM)
- International Information System Security Certification Consortium (ISC2)
    - Certified Information Systems Security Professional (CISSP)
- Australian Computer Society
    - Certified Professional in Cybersecurity
    - Certified Technologist in Cybersecurity

Educational Institutions

- Universities
- Technical colleges
- Private training providers

Relevant Stakeholders

- Future Skills Organisation
- Executive Cyber Council Workforce
- Accreditation Bodies
- Government Bodies
    - Federal
    - State
    - Local

New Market Entrants

- Job Seekers
- Minority Groups

Employers

- Government
- Large Enterprise
- Small Medium Enterprise
- Not for Profit
- Cybersecurity Providers

3. Relationships Analysis (Action - Reaction)

Identifying key relationships between identities is required when considering the potential consequences of actions taken within the system. Does one action cause or influence another part of the system, and what reaction could be caused by actions taken during the implementation process? These reactions may be delayed and emerge over time, therefore failing to understand the relationships between the parts may result in "surprises" later on in the form of unintended consequences. While these surprises may seem to occur unexpectedly in the system and appear to be unavoidable, they are frequently the result of insufficient analysis of the system's relationships and were simply hidden within relationships that were not identified during the initial analysis.

Key relationships between these identities include:

- Cybersecurity Workforce <> Business / Employers
- Cybersecurity Workforce <> Educational Institutions
- Cybersecurity Workforce <> Cybersecurity Industry Organizations
- Cybersecurity Workforce <> Professionalization Body
- Cybersecurity Workforce <> Threat Landscape
- Cybersecurity Workforce <> New Entrants
- Professionalization Body <> Cybersecurity Industry Organizations
- Professionalization Body <> Business / Employers
- Professionalization Body <> Professional Certification Schemes
- Professionalization Body <> Educational Institutions
- Threat Landscape <> Business / Employers
- Grantee <> Eligible Grant Recipient
- Grantee <> Relevant Stakeholders
- Eligible Grant Recipient <> Relevant Stakeholders
- Eligible Grant Recipient <> Existing Consortium
- Cybersecurity Industry Organizations <> Professionalization Framework (co-design and validation)
- Professionalization Framework <> Educational Pathways (alignment requirements)
- Diversity Initiatives <> Entry Barriers (tension/balance)
- Industry Adoption <> Economic Impacts (feedback loop)
- Standards Rigor <> Accessibility (inverse relationship)
- Government funding > Self-sustainability (transition requirement)

The professionalization scheme fits into the larger cyber workforce system that includes educational institutions, employers, government agencies, and local and international certification bodies. This vast interconnected system introduces a level of complexity that must be considered when determining what consequences may result from any actions taken to influence the desired outcomes.

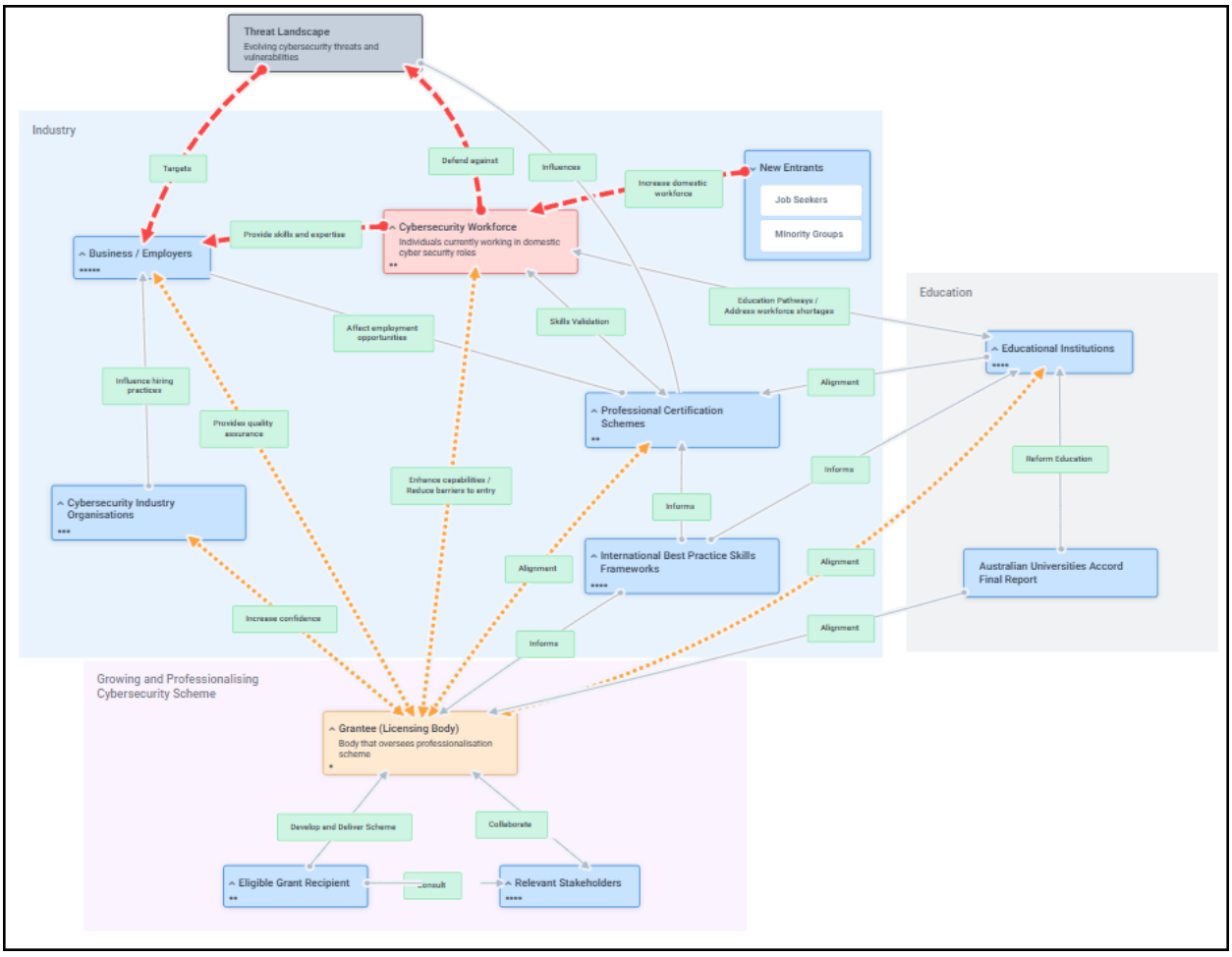

Figure 2- Australian cybersecurity workforce system map

4. Perspectives Analysis (View – Point)

Every observation comes from a particular point seeing a particular view. No single perspective provides complete understanding of the entire system. A DSRP analysis deliberately integrates multiple perspectives, asking not just "What do I see?" but "What would this view look like from another point?" This shift in perspectives dynamically alters distinctions, systems, and relationships in ways that other perspectives may miss. Perspectives do not have to be limited to 'eyes', which means that considering conceptual (non-human) viewpoints can also reveal important insights.

Key perspectives in the cybersecurity professionalization program:

- Government
- Cybersecurity Workforce

- Business / Employer
- Educational Institutions
- Diversity, Equity, Inclusion
- Economic
- Industry Bodies

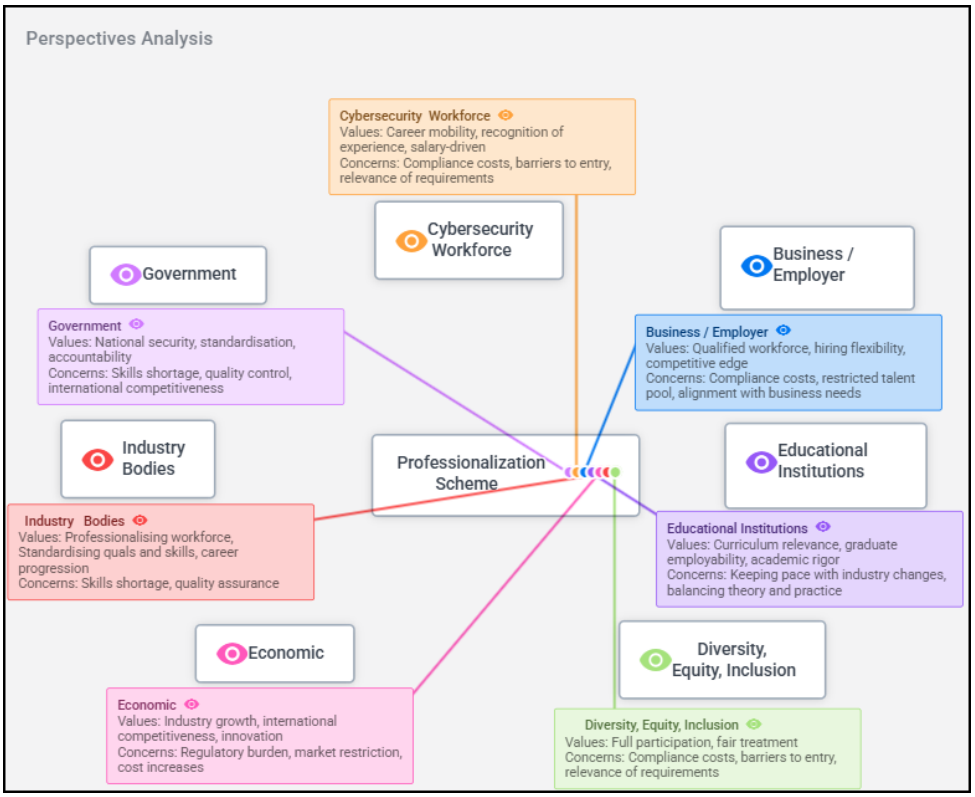

Figure 3- Perspectives analysis

These perspectives reveal significant differences in how the scheme may be perceived and valued, highlighting the importance of inclusive design and stakeholder alignment for successful implementation.

Agent Based Analysis

The Agent-Based Approach (ABA) is a methodology for understanding and dealing with complex challenges by looking at systems as collections of interacting agents. It is founded on the principles of Complex Adaptive Systems (CAS), where individual agents, adhering to simple local rules, collectively generate emergent properties and behaviors. It has been applied in multiple domains to help analyze and inform policy decisions (2,12). By identifying the agents within the system and establishing their predicted behaviors, one can infer the types of actions that may modify such behaviors and subsequently "codify" those generalizable actions into specific recommendations.

The ABA analysis follows a sequential process of understanding system behavior, analysing agents and rules, conducting POSIWID (Purpose Of a System Is What It Does) assessments, and developing

principles-based recommendations.

The analysis process involved:

1. Careful review of the grant opportunity guidelines and background materials
2. Application of DSRP mapping to identify key elements and relationships
3. Structure-determines-behavior analysis to understand system behaviors
4. POSIWID comparison of current versus desired future states
5. Analysis of agents and their simple rules within the cybersecurity workforce system
6. Development of principles-based recommendations for consideration

Given the fropping rules, this methodology ensures that the analysis adheres to empirical evidence where available, while providing systematic insights into the proposed scheme's potential impacts, challenges, and success factors. This does not preclude the use of additional empirical evidence to supplement and strengthen the analysis as needed.

Structure Determines Behavior (SdB) Analysis

The phrase "structure determines behavior" tells us that the way a system is organized has a significant impact on its overall performance. This means that the way things are organized within a system influences how the system functions and the results it produces. Understanding the structure of a system (for example, the relationships between its parts) can aid in predicting its overall behavior.

Current System Understanding

The current cybersecurity workforce system has the following structural attributes that contribute to its overall behavior.

Attributes	Description
Skill-Based Hiring	Organizations primarily hire based on technical skills and certifications rather than standardized professional credentials
Diverse Entry Pathways	Multiple entry points into cybersecurity (IT professionals, self-taught specialists, university graduates, TAFE, private training providers)
Fragmented Certification Landscape	Numerous competing certifications with varying recognition and value
Limited Industry Standardization	Absence of uniform job descriptions, competency frameworks, and career progression paths
Skills-Experience Paradox	Employers demand experience while new entrants need opportunities to gain experience
Education System	Traditional education, bootcamps, self-learning platforms, and certification programs operating independently
Hiring System	Human resource departments and cybersecurity leaders with different expectations and evaluation criteria

Compensation System	Salary structures favoring experience and specific technical skills
Career Development System	Ad-hoc progression paths varying widely between organizations
Supply-Demand Imbalance	Significant workforce shortages according to various studies (difficult to quantify)
Certification-Employment Nexus	Employers use certifications as proxies for competence, creating demand for certification acquisition
Experience-Opportunity Loop	Work experience is highly valued but difficult for new entrants to obtain
Knowledge Transfer Limitations	Experienced professionals have limited incentives to mentor newcomers
Employers	View cybersecurity talent as a scarce resource; concerned about skills gaps
Experienced Professionals	See market advantages from scarcity; focus on maintaining competitive edge
New Entrants	Experience significant barriers to entry despite apparent workforce shortage
Certification Bodies	Compete for market share and industry recognition
Education Institutions	Struggle to align curricula with rapidly changing industry needs

Table 6- Current cybersecurity workforce system structure and attributes

The current structure of the cybersecurity workforce creates a self-reinforcing system that perpetuates scarcity despite efforts to alleviate it, resulting in several key behavioral patterns:

- The fragmentation of certifications encourages professionals to acquire more credentials to stand out, but it doesn't solve the problem of basic skill shortages.
- The skills-experience paradox encourages risk-averse hiring practices whereby companies contend for the same pool of experienced people instead of investing money into training new entrants.
- Lack of standardised career pathways encourages opportunistic job-hopping as professionals seek advancement through external moves rather than internal development.
- Hiring practices that prioritize technical skills validated through certifications encourage a narrow focus on certifications as a proxy for capability and experience.
- The market's reactive compensation structure drives short-term employment decisions by both employers and employees, limiting investment in long-term professional development.

This analysis demonstrates how the current cybersecurity workforce market structure naturally produces behaviors that perpetuate skills gaps and workforce shortages despite significant efforts to address them. The current system is structured to reward experienced specialists and create barriers for new entrants, making it inherently resistant to achieving workforce equilibrium.

POSIWID Analysis

Stafford Beer coined the abbreviation POSIWID, which stands for "The purpose of a system is what it does". This means that the system's design determines its results. Therefore, while evaluating a system, we must focus on what it really does rather than what its initial intent was, as the two are frequently unrelated. It is critical that the focus of this stage is on embracing the system's reality rather than succumbing to confirmation bias, which occurs when we exclusively look for information that validates our ideas about the system's intended purpose. The POSIWID analysis is unique in that it takes the opposite approach to fault-finding, recognizing that the system is simply performing as expected given its current structure rather than viewing its design as flawed.

After identifying the current system's attributes and structure, the next step is to define the system's future purpose and highlight the key differences between the two states. This establishes the foundation for ABA's subsequent steps.

Current POSIWID: The current cybersecurity workforce system is exceptionally well designed and good at its purpose of maintaining artificial scarcity that benefits established professionals while perpetuating barriers to entry despite chronic workforce shortages.

Future POSIWID: The future cybersecurity workforce system should be exceptionally well designed to provide clear pathways for qualified professionals with verified skills, lower barriers to entry for new entrants, and maintain industry adaptability and workforce equilibrium.

Core Differences:

1. Capability centred vs. Certification centred
2. Supply demand balance vs. Artificial scarcity
3. Clear career pathways vs. Fragmented certification frameworks
4. Experience development vs. Experience privileged
5. Clear entry requirements vs. Barriers to entry

Complex Adaptive System (CAS) Analysis

Where the POSIWID analysis identifies the complex emergent properties of the system in both the current and ideal future states, the CAS analysis identifies the agents within the system and the simple rules they may follow that drive their collective behaviors. Identifying the agents and the simple rules is key to identifying the most effective design principles for effecting change in the system to achieve the desired future state.

Agent Type	Simple Rules	Behaviour
Professionalization Scheme	Establish stakeholder trust	Market adoption; Time-constrained
	Maintain exclusivity to preserve value	
	Ensure scheme sustainability	
Education Institutions	Align curricula with industry needs	

	Maximise enrolment	Market-oriented; competitive positioning
	Seek recognition of credentials	
Professional Certification Schemes	Maintain standards	Market-oriented; competitive positioning
	Generate revenue	
	Align offerings with market demands	
Business / Employers	Access to qualified talent	Resource-driven; Cost-sensitive
	Validate skills of applicants	
	Cost effective resources	
Cybersecurity Workforce	Career mobility	Salary-driven; Certification-conscious
	Seek recognition and career development	
	Individual return on investment	
New Entrants	Overcome barriers to entry	Entry-focused; Cost-sensitive
	Identify minimum viable credentials	
	Secure initial experience	
Government	Enhance national security	Policy-focused; National interest orientation
	Grow cyber workforce	
	Ensure scheme sustainability	

Table 7- Agent Types and Behaviors

This agent-based analysis reveals a complex adaptive system in which individual agent behaviors, particularly those of the cybersecurity workforce, employers, and certification bodies, have a significant impact on the emerging properties of the professionalization scheme. The system's behavior emerges from countless interactions between these agents, with feedback loops between employer adoption, professionalization value, market costs, and accessibility creating complex dynamics that will determine the scheme's ultimate effectiveness in achieving its core objectives of addressing workforce shortages and reducing barriers to entry.

The interactions between these agents create emergent properties that cannot be predicted by analyzing individual components in isolation. For example, if professionalization requirements are overly stringent, the emergent property may be a reduction in workforce diversity, despite explicit diversity goals. Conversely, if the requirements are too lenient, the emergent property may be a lack of employer confidence in the scheme, which may impede its adoption.

Design Principles

To ensure that each recommendation is consistent with the desired future state of the system determined in previous steps, a set of design principles must be established to serve as criteria against which all future recommendations must be measured. This increases the likelihood that the recommendations will result in the desired emergent properties of the system.

Recommendation-Rubric Analysis

Based on the ABA analysis recommendations for addressing cybersecurity professionalization in Australia the scheme should adhere to these principles:

Recommendation Rubric:

1. Must address the skills shortage rather than exacerbate it
2. Must include sustainable funding mechanisms that don't increase entry costs
3. Must integrate with, rather than replace, existing recognized certifications
4. Must provide demonstrable value to both employers and professionals
5. Must offer flexible pathways that recognize diverse entry points and experiences
6. Must balance standardization benefits with flexibility needs
7. Must not create perverse market incentives leading to counterproductive outcomes
8. Must establish clear exit criteria if scheme does not meet core objectives.

Specific Recommendations

NOTE: It is important to understand that these are the author's proposed recommendations to demonstrate the approach. While they may be appropriate for addressing the issue, a variety of other recommendations may be equally valid providing they adhere to the design principles.

Recommendation	Principles
1. Conduct further analysis to assess alternative solutions to workforce shortage challenges, given the uncertainty surrounding outcomes, based on existing evidence.	4, 7
2. Create a Multi-Stakeholder Governance Body o Include representation from government, industry, education, professionals, minority representation and independents o Empower this body to develop, review, and update standards o Ensure transparent decision-making processes o Ensure transparent reporting of success measures	1,2,3,4,5,6,7,8
3. Develop a Staged Professionalization Approach o Begin with voluntary registration and standards o Gradually implement mandatory baseline requirements for critical roles o Maintain flexibility for emerging specialisations	1,2,3,5,7
4. Establish Recognition of Prior Learning Pathways	1,3,5

○ Create bridging programs for professionals without formal qualifications ○ Ensure these pathways are accessible and affordable	
5. Implement Tiered Professionalization Approach ○ Basic registration for entry-level positions ○ Intermediate levels for standard cybersecurity roles ○ Advanced levels for critical infrastructure and sensitive positions	1,2,3,5,7
6. Assess co-funding models between industry stakeholders ○ Certification Bodies ○ Educational Institutions ○ Industry Bodies ○ Employers	2,4,7

Table 8- Recommendations rubric

6. Evidence-Based Evaluation Framework

It is critical to have simple and straightforward measures for assessing the program's effectiveness in meeting the agreed-upon outcomes. Similarly, exit criteria should be defined to ensure that the scheme's sustainability is not undermined by the sunk cost fallacy[1]. Since complex adaptive systems are inherently dynamic, these indicators will serve as early warning of the system's actual behavior over time, enabling evidence-based course corrections to guarantee the scheme can adapt to the changing environment if required. The examples provided below are intended to help answer key questions and validate that the system's intended purpose is being met.

Measures of Success

Based on the DSRP and ABA analyses, the following metrics would indicate successful implementation of the scheme:

Economic Indicators

1. **Industry Participation Rate:** Percentage of employers recognizing and requiring scheme credentials, with targets for growth over time.
2. **Professional Enrolment:** Number and growth rate of professionals voluntarily registering with the scheme, segmented by career stage.

[1] the idea that a company or organisation is more likely to continue with a project if they have already invested a lot of money, time, or effort in it, even when continuing is not the best thing to do.

3. **Diversity Demographics:** Number of underrepresented groups at various credential levels, measured against industry baselines.
4. **Cost Efficiency:** Average cost to individuals to obtain and maintain credentials relative to income and compared to international benchmarks.
5. **Credential Wage Premium:** Earnings differential between credentialed and non-credentialed professionals, tracked to ensure value without creating excessive barriers.

Impact Measures

1. **Barrier Reduction:** Changes in time-to-hire and ability to enter the profession for new entrants, compared to baseline measures.
2. **Employer Confidence:** Survey-based measures of employer trust in the credential as a reliable sign of competence.
3. **Workforce Mobility:** Rates of career progression and job mobility for credentialed professionals compared to non-credentialed counterparts.
4. **Skill Alignment:** Employer-reported alignment between credential expectations and actual job performance.
5. **International Recognition:** Formal recognition of Australian credentials by international bodies and multinational employers.

Implementation Quality

1. **Stakeholder Satisfaction:** Satisfaction ratings from key stakeholders including professionals, employers, and education providers.
2. **Pathway Clarity:** Survey-based measures of perceived clarity in career progression routes.
3. **Scheme Sustainability Progress:** Metrics tracking progress toward financial self-sustainability without increasing barriers.
4. **Framework Integration:** Level of integration with existing international frameworks and credentials.

These metrics should be tracked throughout the pilot phase and beyond, with regular evaluation against baseline measures to determine the scheme's effectiveness in achieving its stated objectives. Additionally, they can serve as evidence to stakeholders of the scheme's ongoing efficacy in resolving the original problem statements, thereby bolstering industry support and guaranteeing the scheme's long-term sustainability.

Conclusion

This analysis of the Australian Cybersecurity Professionalization Scheme reveals a fundamental tension between its stated objectives and the empirical evidence regarding professionalization outcomes across industries. The scheme's architects have clearly articulated admirable goals, addressing workforce shortages, creating clear career pathways, and reducing entry barriers. However, the evidence from both occupational licensing and professionalization studies consistently indicates that such initiatives tend to produce outcomes that may directly contradict these objectives.

The rapid literature review demonstrates that while professionalization schemes reliably increase practitioner earnings and may enhance service quality in high-risk domains, they simultaneously create significant market entry barriers, reduce workforce growth, and decrease competition. These findings align with research specifically commissioned by the Victorian Government, which concluded that "there are countless studies" showing that occupational licensing schemes "cost more in terms of higher prices, reduced competition, and poorer consumer choice and options, than the schemes actually resolve." This presents a critical paradox: the very solution selected to address workforce shortages may instead exacerbate them.

The DSRP and ABA analyses further reveal the complexity of the cybersecurity workforce system, highlighting how the current structure already creates substantial entry barriers through certification requirements, experience prerequisites, and fragmented career pathways. The proposed scheme, despite its intent to reduce these barriers, risks introducing additional layers of formalization that could further restrict entry, particularly for underrepresented groups and non-traditional entrants whose inclusion is essential for addressing the projected workforce shortfall.

This is not to suggest that professionalizing the cybersecurity workforce lacks merit entirely. The analysis identifies potential benefits through standardized competency frameworks, clearer career progression, and enhanced industry confidence. However, these benefits appear contingent upon implementation approaches that fundamentally differ from historical professionalization patterns across industries. Without significant design innovations, the scheme risks reinforcing the system's current tendency toward artificial scarcity rather than workforce expansion.

The design principles and specific recommendations proposed in this analysis represent potential mitigating factors but cannot fully resolve the inherent tension between standardization and accessibility. The multi-stakeholder governance body, staged implementation approach, recognition of prior learning pathways, and tiered professionalization structure may mitigate some risks, but evidence suggests these modifications may not be sufficient to overcome the fundamental economic incentives that typically drive professionalization outcomes.

Given these tensions, it would be prudent to more thoroughly investigate alternative approaches to addressing cybersecurity workforce challenges before proceeding with the proposed scheme. At minimum, the implementation should incorporate robust monitoring frameworks using the success metrics identified in this analysis to detect early signs of adverse outcomes, with clear exit criteria to

prevent the sunk cost fallacy from perpetuating a potentially counterproductive system.

The evidence presented in this analysis does not support the conclusion that the proposed scheme, as currently conceived, is likely to achieve its stated objectives of expanding the cybersecurity workforce while reducing entry barriers. Rather, it suggests that without significant structural innovations that differentiate it from traditional professionalization approaches, the scheme may inadvertently reinforce the very workforce constraints it aims to resolve. This underscores the importance of understanding first and solutioning second, a systems thinking principle that should guide not only this analysis but the design and implementation of any intervention in complex adaptive systems.

References

1. B. Mosse, “Reconsider the Australian Government’s grant for professionalising the cybersecurity industry” (2025).

2. J. Bond, The Military-Climate Change System: A Case Study Using the Agent Based Approach (ABA). *Journal of Systems Thinking* (2022). https://doi.org/10.54120/jost.pr000003.v1.

3. Y. O. Mulyono, U. Sukhbaatar, D. Cabrera, ‘Hard’ and ‘Soft’ methods in complex adaptive systems (CAS). *Journal of Systems Thinking* 3 (2023).

4. Department of Home Affairs website. *Department of Home Affairs Website*. Available at: https://www.homeaffairs.gov.au/cyber-security-subsite/Pages/cyber-security-act.aspx [Accessed 18 April 2025].

5. Growing and professionalising the Cybersecurity industry program | Business.gov.au. *business.gov.au* (2024). Available at: https://business.gov.au/grants-and-programs/growing-and-professionalising-the-cyber-security-industry-program [Accessed 10 March 2025].

6. “Australia’s Cybersecurity Sector Competitiveness Plan 2023” (AustCyber, 2023).

7. T. Vizza, The Australian Cybersecurity Profession is Broken. (2025). Available at: https://www.linkedin.com/pulse/australian-cyber-security-profession-broken-tony-vizza [Accessed 18 April 2025].

8. ACS certification: Professional recognition. *Australian Computer Society*. Available at: https://www.acs.org.au/professionalrecognition/certification-landing-page.html [Accessed 10 March 2025].

9. 2024 ISC2 Cybersecurity Workforce Study. *ISC2* (2024). Available at: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study [Accessed 10 March 2025].

10. R. Lemos, Licensed to Bill? Nations Mandate Certification & Licensure of Cybersecurity Pros. *Dark Reading* (2024). Available at: https://www.darkreading.com/cyber-risk/licensed-to-bill-nations-mandate-certification-licensure-of-cybersecurity-pros [Accessed 11 March 2025].

11. Singapore Cybersecurity licensing. *International Trade Administration | Trade.gov* (2022). Available at: https://www.trade.gov/market-intelligence/singapore-cybersecurity-licensing [Accessed 28 April 2025].

12. Wen, *et al.*, Framework Effectiveness and Prevalence in Public Policy. *Journal of Systems Thinking* **2** (2022).

13. N. Steinhall, *et al.*, Wicked solutions for wicked problems. *Journal of Systems Thinking* 4 (2024).

14. Wikipedia contributors, Professionalization. *Wikipedia* (2025). Available at: https://en.wikipedia.org/wiki/Professionalization [Accessed 28 April 2025].

15. Australian Government Red Tape Senate Committee, "Effect of red tape on occupational licensing" (Commonwealth of Australia, 2018).

16. Professional Standards Council. Available at: https://www.psc.gov.au/sites/default/files/2021-08/Professionalisation.pdf [Accessed 28 April 2025].

17. The Allen Consulting Group, "A framework for considering the use of occupational licensing" (Consumer Affairs Victoria, 2007).

18. Behavioural Economics Team of the Australian Government, N. Hilderson, H. M. Watkins, S. Copley, A. Willis, "Attracting a diverse Cybersecurity workforce" (Commonwealth of Australia, 2023).

19. B. Tran, K. Benson, L. Jonassen, Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce. *Journal of Cybersecurity Education Research and Practice* **2023** (2023).

20. M. Nkongolo, N. Mennega, V. Z. Izaan, Cybersecurity Career Requirements: A Literature review. *arXiv (Cornell University)* (2023). https://doi.org/10.48550/arxiv.2306.09599.

21. C. Ramezan, P. Coffy, J. Lemons, Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for? *Journal of Cybersecurity Education Research and Practice* 2024 (2023).

22. M. M. Kleiner, E. J. Soltas, A welfare analysis of occupational licensing in U.S. states. *The Review of Economic Studies* 90, 2481–2516 (2023).

23. E. J. Timmons, A. Mills, Bringing the Effects of Occupational Licensing into Focus: Optician Licensing in the United States. *Eastern Economic Journal* 44, 69–83 (2016).

24. D. Cabrera, L. Cabrera, E. Cabrera, The Steps to Doing a Systems Literature Review (SLR). *Journal of Systems Thinking* (2023). https://doi.org/10.54120/jost.pr000019.v1.

25. D. M. Anderson, R. Brown, K. K. Charles, D. I. Rees, Occupational Licensing and Maternal Health: Evidence from Early Midwifery Laws. *Journal of Political Economy* 128, 4337–4383 (2020).

26. C. Farronato, A. Fradkin, B. Larsen, E. Brynjolfsson, "Consumer Protection in an online World: An analysis of Occupational Licensing" (2020).

27. D. Deyo, "LICENSING AND SERVICE QUALITY: EVIDENCE USING YELP CONSUMER REVIEWS" (American Economic Association, 2017).

28. M. M. Kleiner, R. T. Kudrle, Does Regulation Affect Economic Outcomes? the Case of Dentistry. *The Journal of Law and Economics* 43, 547–582 (2000).

29. Elicit: the AI Research Assistant. *Elicit*. Available at: https://elicit.com [Accessed 18 March 2025].

30. D. Cabrera, A mathematical theory of organization. *Journal of Systems Thinking* (2024). https://doi.org/10.54120/jost.00000100.

31. ISC2 Code of Ethics. Available at: https://www.isc2.org/ethics [Accessed 2 May 2025].

32. Australian Information Security Association (AISA) Code of Ethics and Conference Behaviour Rules. (2018). Available at: https://www.aisa.org.au/common/Uploaded%20files/aisa_code_of_ethics_-_final_v2.pdf [Accessed 2 May 2025].

33. Code of Professional Ethics | IS/IT Certifications | ISACA. ISACA. Available at: https://www.isaca.org/code-of-professional-ethics [Accessed 2 May 2025].

34. Professional Ethics, Conduct and Complaints. ACS (Australian Computer Society). Available at: https://www.acs.org.au/memberships/professional-ethics-conduct-and-complaints.html [Accessed 2 May 2025].