DIGITAL SKILLS ORGANISATION

Summary

Digital Skills Organisation June 2023

NODE NETWORK OF DIGITAL EXCELLENCE

Summary of NoDE Papers

Paper 1 addresses the increasing demand for digital skills and the challenges faced by the current training system in Australia. It proposes the establishment of Networks of Digital Excellence (NoDE) to bridge the gap between the skills demanded by industry and training provider's current capabilities. The paper introduces seven principles for designing and scaling NoDE, emphasising collaboration, job-specific skilling, industry-tailored training, and adaptable learning. It also highlights successful examples of NoDE approaches and suggests an activation plan.

Paper 2 provides a 'playbook' to guide the development of effective training programs in collaboration with stakeholders. It outlines six steps for creating employer-co-designed training solutions, including pilot establishment, workforce needs analysis, design workshops, training solution development, implementation workshops, as well as program implementation and management. The paper promotes a collaborative approach and offers practical examples, case studies, and guidance to support the development of impactful training programs.

Paper 3 offers guidance for practice-based learning in employer-led training with a focus on Networks of Digital Excellence, trainers, and teachers. It prioritises a skills-based approach and uses digital skills standards as the key mechanism to align teachers with workplace skill requirements. The guide covers various elements, such as elaborating on the purpose of each micro-credential that makes up the designed training solution, documenting the learning objective of skills clusters, formulating digital skills standards, developing practice-based projects and associated artifacts, and selecting appropriate training topics to guide learning. It facilitates mapping acquired digital skills to formal qualifications and offers room for further development and enhancement by the teachers to suit the context of each workplace.

Paper 4 provides detailed case studies which show real-world examples of the employer-led co-designed training solutions presented in Paper 2. It outlines the step-by-step approach the Digital Skills Organisation and its partners themselves followed in implementing the co-design process. The paper showcases successful implementation examples from the Canberra Cyber Pilot and the Cremorne Software Development Pilots, emphasising the importance of holistic implementation of all six steps. It is a practical guide for organisations and stakeholders interested in using employer-led co-design methods to develop effective training solutions in the digital skills landscape.

DIGITAL SKILLS ORGANISATION

Building a Collaborative Network of Digital Excellence

Principles for Designing and Scaling Employer-Led Digital Skills Training.

Digital Skills Organisation June 2023

NODE NETWORK OF DIGITAL EXCELLENCE

Table of Contents

Executive Summary

Demand for digital skills has increased by more than 15 percent across the economy since 2016, and is expected to continue rising. There is a projected 47 percent increase in demand for expert digital workers by 2026, highlighting the growing need for individuals with advanced digital skills. However, if current training trends continue, Australia will see a shortfall of 370,000 digital workers during this period (Digital Skills Organisation, 2023).

The current training and education system is struggling to keep up with this demand. Employer satisfaction with graduates utilising the national training system has experienced a steady decline, dropping from 83.1 percent in 2013 to 78.7 percent in 2021, according to NCVER data. This reflects employers' mounting concerns regarding the mismatch between graduates' skills and industry requirements, which presents a pressing challenge for the future of Australia's professional training system.

The challenges faced by the system are broad and complex. The rapid pace of technological change, coupled with a lack of curriculum and training package agility, low levels of teacher capability to deliver relevant skills, and inadequate supporting infrastructure, hinder the effectiveness of training programs. Moreover, the training system's complexity and fragmentation restrict industry engagement at local, state, and national levels.

While there are 1,519 Registered Training Organisations (RTOs) registered to deliver various ICT qualifications and skillsets there is significant variations in their capability to deliver digital skills programs across the country. All RTOs should be able to deliver some type of digital skills training on behalf of their learners.

In response to these challenges, this paper proposes the establishment of Networks of Digital Excellence (NoDE).

A NoDE seeks to augment the existing digital skills training provided by RTOs, bridging the gap between evolving industry demands and the skills currently provided. The approach aims to create an ecosystem of digital skills training that aligns with industry needs and can be delivered across various training providers.

The approach is based on seven principles: fostering collaboration and connectivity to create a cooperative network, committing to act as a consortium, a focus on job-specific digital skilling solutions, providing industry-tailored training, offering industry-specific credentials, and promoting adaptable learning.

These principles are based on data gathered from successful collaboration initiatives such as the Institute of Applied Technology (IAT) Digital, Wyndham Tech School, TAFEcyber, the AWS Skills to Tech Alliance, and the National Consortium for Data Science.

Activation of the NODE approach could be achieved over a 3-year period (pilot, trial and scale). Throughout this period, stakeholders should seek to build on successes around discreet and bounded opportunities such as digital literacy or cyber skills training.

Introduction

In today's rapidly evolving digital landscape, the demand for digital skills is growing at an unprecedented rate. Equipping the workforce with essential digital skills has become crucial in an era where technology continually reshapes industries.

To address this requirement it is proposed a network of training providers is created to focus on the development and sharing of excellence in digital skills training.

Networks of Digital Excellence (NoDEs) are a dynamic collaborative network that brings together training and industry stakeholders to deliver employer-led digital skilling solutions.

They are an evolution of the traditional approach to skills training, as they place employer needs at the centre of digital skills development, fostering collaboration and knowledge-sharing amongst stakeholders.

Drawing on best practice this paper proposes 7 principles on which a NODE should be based and identifies a potential way forward to operationalise the approach.

NoDE Functions

NoDE has three primary functions:

1. Design

NoDE is not a physical platform, but rather an approach that facilitates collaboration between training providers and employers to address specific digital skills gaps within the local workforce. This collaboration takes place in a physical or virtual environment where all stakeholders can come together to create tailored training solutions that meet the needs of both large and small to medium-sized enterprises (SMEs).

2. Develop

Within the NoDE approach, collaborative partners work together to align a core set of training outcomes with agreed-upon practice-based skills standards. This alignment serves as the foundation for developing training products that collectively yield the desired outcomes, ensuring maximum relevance, transferability, and mobility of skills. Through joint efforts, NoDE enables the creation of comprehensive and robust training offerings that address industry requirements while promoting seamless skill integration and portability across various contexts.

3. Share

NoDE facilitates the establishment of communities of practice (COPs) that develop relevant, agile digital learning pathways to jobs through collaborative co-design, which can be shared across multiple NoDE.

Operating Principles

To ensure a successful implementation of the Network of Digital Excellence (NoDE), the paper outlines seven principles that serve as guiding pillars. These principles form the cornerstone of the NoDE approach to addressing the dynamic challenges of the digital landscape.

Principle 1: Collaborate, Connect and Cooperate

Collaboration, connection, and cooperation lie at the heart of the NoDE approach, forming the foundation for addressing skill shortages and industry needs. By fostering collaboration amongst diverse stakeholders, NoDE creates a vibrant ecosystem that is responsive to the ever-evolving digital landscape.

One of the key aspects of collaboration in NoDE is the integration of various entities, including registered and non-registered training providers, universities, industry partners, and industry and vendor certification providers. This collective effort ensures a wide range of perspectives, expertise, and resources are brought to the table. By actively engaging these stakeholders, NoDE promotes a comprehensive and holistic approach to addressing digital skill gaps.

Within this collaborative environment, knowledge exchange becomes a driving force. NoDE encourages the sharing of knowledge, expertise, best practices, and resources amongst its stakeholders. By doing so, valuable insights are disseminated, enabling stakeholders to learn from one another and adopt effective strategies to bridge the digital skills gap. This knowledge-sharing aspect is integral to the success of NoDE, as it allows for the continuous improvement, upskilling of teachers, and refinement of skilling initiatives.

In addition, the interconnectedness fostered by NoDE ensures industry demands are met efficiently. By establishing strong connections between employers and training providers, NoDE ensures the digital skills being imparted align closely with industry requirements. This proactive approach enables individuals to acquire the most relevant and up-to-date digital skills, equipping them to meet the requirements of the job market.

Principle 2: Willingness to Act as a Consortium

To enhance the effectiveness of the NoDE, it is suggested training providers operate as a consortium, collaborating towards a shared goal. This consortium-based approach forms the foundation of NoDE, instilling greater confidence in the training sector's ability to effectively address the demands of the job market.

By acting as a consortium, the NoDEs foster a spirit of cooperation and coordination amongst diverse stakeholders within the training sector. This collaborative effort brings together the expertise, resources, and perspectives of multiple organisations, creating a synergy that is instrumental in meeting the evolving needs of industry.

The consortium approach offers several benefits.

It enables a more cohesive and unified response to the skills requirements of the job market, ensuring the training sector is better equipped to deliver necessary digital skills and qualifications.

NoDEs also makes it easier for employers to engage with training providers. This streamlined process simplifies the process of integrating employers into training, making it easier for them to take a proactive role in process.

Principle 3: Co-design

Underpinning the consortium approach is the shared commitment to the co-design of solutions. Collaboration as a principle promotes knowledge sharing and best practices amongst participating organisations. This collaborative environment encourages the exchange of ideas, innovative teaching methods, and effective training techniques, leading to an overall improvement in the quality and relevance of digital skills programs through the co-design process.

Co-design within the NoDE presents a unified front to industry stakeholders, employers, and learners. This unity enhances credibility and trust in the training sector's ability to address the skills gap and deliver graduates with the skills required by the job market.

Principle 4: Focussing on job-specific Digital Skilling Solutions for industry

A crucial aspect is to prioritise industry-oriented digital skills solutions that address the specific skill requirements of job roles within those industries. Whether centred around location, theme, and/or industry, NoDEs can play a pivotal role in creating tailored training solutions that depart from the conventional “one size fits all” approach.

The objective is to provide comprehensive digital skilling solutions that closely align with industry demands, thereby providing skills that are both relevant and transferable.

This active involvement directly benefits not only employers and training providers - particularly within the Vocational Education and Training (VET) system - but also employees and learners.

Principle 5: Industry-specific training with short-form credentials

Short-form credentials are offered to meet the specific demands of various sectors and job roles. Recognising the ever-changing nature of the digital landscape, NoDE places great importance on actively involving industry stakeholders and training providers in the development and delivery of short-form credentials.

A collaborative approach ensures the credentials offered through NoDE are not only relevant but also directly aligned with current industry requirements.

Formalising relationships with industry through the NoDE helps to create a feedback loop that informs the design and development of targeted micro-credentials, reflecting the rapidly evolving digital skill sets demanded by the economy.

Principle 6: A commitment to the design of scalable solutions

One of the key benefits of industry-specific short-form credentials is the ability to provide training solutions which are agile and can be easily scaled within a short timeframe.

These credentials can then be used to quickly validate learners' specific skills and knowledge in high-demand areas, enhancing their employability.

Digital badges serve as portable representations of achievement, allowing learners to easily showcase their credentials to employers and industry professionals. These digital badges enable learners to demonstrate their skills in a verifiable and accessible manner, making it easier for potential employers to assess their capabilities and match them with relevant job opportunities.

Traditionally, an aspect of scale is the importance of recognition of prior learning (RPL) and previous experience. RPL enables individuals to gain credit for skills and knowledge they have acquired through non-traditional means, such as work experience, life experience or self-directed learning. This recognition ensures that individuals' prior achievements, skills and competencies are acknowledged and can contribute towards obtaining full qualifications.

This includes the role played by industry certifications, which are widely recognised and valued. The NoDE approach acknowledges the expertise embedded within established certifications and allows learners to benefit from the rigour and industry recognition associated with these credentials.

Principle 7: Agile and Adaptive Learning for Digital Professionals

The approach recognises the importance of staying ahead of the rapidly evolving digital landscape and seeks to offer a hybrid learning model that combines accredited training programs with non-accredited training, higher education subjects, industry certifications, and informal learning opportunities. This approach helps to ensure relevant skills are imparted.

In addition to agility, NoDE recognises the importance of providing a pathway for continuous professional development. The hybrid approach offered by NoDE not only equips individuals with targeted skills but also promotes ongoing learning and growth. Short-form credentials serve as milestones along this pathway, recognising achievements and encouraging professionals to continually build upon their skills and knowledge.

By emphasising continuous learning and professional development, NoDE empowers digital professionals to enhance their employability opportunities and remain competitive in the ever-evolving world of technology.

Showcasing NoDE Principles in Action: Consortiums Promoting Digital Skilling Solutions

IAT Digital, Wyndham Tech School, TAFEcyber, the AWS Skills and Tech Alliance, and the National Consortium for Data Science (NCSD) are prime examples of consortiums that exemplify the principles of the Network of Digital Excellence (NoDE). These collaborative initiatives bring together training providers, industry partners, and educational institutions to deliver industry-specific digital skilling solutions.

Institute of Applied Technology – Digital (IAT Digital)

'IAT Digital' (Institute of Applied Technology - Digital, 2023) embodies the principles of NoDE through its collaborative and industry-focused approach to digital skilling. In partnership with reputable institutions like TAFE NSW, Microsoft, the University of Technology Sydney, and Macquarie University, 'IAT Digital' offers comprehensive courses in data analytics, cybersecurity, cloud computing, software development, and artificial intelligence.

The consortium ensures that its training offerings align closely with the evolving demands of industry, ensuring that learners acquire the specific skills needed to excel in their desired job roles. By tailoring their courses to address industry-specific skill requirements, IAT Digital effectively bridges the gap between the skills provided by training providers and the demands of the digital job market.

Notably, IAT Digital recognises the importance of industry-specific training through short-form credentials. The consortium understands that traditional long-form qualifications may not always capture the rapidly changing skill needs of the digital landscape. Therefore, IAT Digital offers targeted short-form credentials that are industry-recognised and reflect the most up-to-date and in-demand skills. This approach enables learners to quickly acquire relevant skills and enhance their employability in the digital economy.

Collaboration between training providers and industry partners is fundamental to NoDE's success, and IAT Digital exemplifies this principle. By partnering with reputable institutions and industry leaders, IAT Digital leverages their expertise and resources to develop industry-relevant training programs. This collaborative approach ensures that learners gain practical knowledge and skills that are directly applicable to real-world industry scenarios.

Wyndham Tech School

Wyndham Tech School (Wyndham Tech School, 2023) showcases the principles of collaboration and connectivity which could be replicated through the NoDEs. Through its innovative approach, the Tech School fosters collaboration between educational institutions and industry partners to address real-world challenges and provide students with valuable exposure to industry problem-solving.

The principle of collaboration is at the core of the Tech School's operations. By bringing together learners from various schools and projects established by industry partners, the Tech School creates a dynamic learning environment where students can actively engage with and gain practical insights into the digital landscape. This collaborative approach ensures that students are exposed to real-world scenarios and industry practices, enhancing their understanding of industry-specific challenges and requirements.

Moreover, the Tech School promotes connectivity by establishing strong partnerships with local businesses. These partnerships enable the Tech School to offer students unique opportunities to work on projects that address real-world challenges using digital technologies. By connecting students with industry professionals and providing them with hands-on experiences, the Tech School facilitates the development of practical skills and problem-solving abilities, aligning with the agile and adaptive learning principle of NoDE.

TAFECyber

TAFEcyber (TAFECyber, 2020) is an exemplary consortium that aligns with the principles of the Network of Digital Excellence (NoDE). TAFEcyber embodies several NoDE principles:

TAFEcyber places a strong emphasis on job-specific digital skilling solutions for the cybersecurity industry. By offering industry-specific training in cybersecurity, TAFEcyber equips students with the essential knowledge and technical skills needed to excel in the field. The consortium ensures that its programs are closely aligned with the skill needs of employers, preparing graduates to enter the workforce with the specific skills required by the industry.

Collaboration and connectivity are key principles embraced by TAFEcyber. The consortium actively engages industry stakeholders in the development and delivery of its cybersecurity programs. By collaborating with government and industry partners, TAFEcyber ensures that its training offerings remain relevant and up-to-date. The consortium leverages the expertise and best practices of each of the participating TAFE Colleges, creating a consistent learning experience for students and fostering collaboration among all stakeholders.

TAFEcyber demonstrates a willingness to act as a consortium, pooling resources and expertise from TAFE Colleges across Australia. This collective approach allows TAFEcyber to effectively address the challenges posed by rapidly changing technology and evolving industry requirements. By operating as a unified consortium, TAFEcyber ensures that its training remains responsive to the dynamic cybersecurity landscape.

Additionally, TAFEcyber serves as a single intersection point for industry and employers across all TAFE Institutes throughout Australia. This unique position enables TAFEcyber leaders to represent cybersecurity training on behalf of all TAFEs in various government initiatives, roundtable discussions, and advisory committees. By actively participating in these forums, TAFEcyber ensures that the interests and needs of cybersecurity training in all TAFEs are effectively represented. This subsequently strengthens the collective voice of all TAFEs and contributes to the advancement of cybersecurity training across the country.

TAFEcyber embraces the concept of industry-specific training with short-form credentials. By actively involving industry stakeholders and sharing training materials developed across all participating TAFE Institutes, TAFEcyber ensures that its offerings are agile and responsive to evolving industry demands. This approach allows teachers to quickly acquire the specific skills and resources they need to deliver high-quality cybersecurity training. It also enables students to stay competitive in the digital job market by continuously enhancing their skills and adapting to the ever-changing industry landscape.

AWS Skills to Jobs Tech Alliance

The AWS Skills to Jobs Tech Alliance (Amazon Web Services Launches Global Skills to Tech Alliance, 2023) recently announced a coalition of employers, global government agencies, workforce development organisations, and education leaders that aims to address the skills gap present in many training systems and better prepare learners for tech careers. The program will work with institutions to develop training curricula and activities aimed at upskilling students for jobs in cloud support, software development and data integration, and to integrate AWS training content into existing curricula.

Participants in the alliance have joined forces with Amazon Web Services (AWS) to leverage their collective strength, knowledge, and influence to drive change in the tech skills landscape. The alliance aligns with NoDE principles by connecting employers, educational institutions, and government agencies to foster cooperation and coordination in digital training.

National Consortium for Data Science (NCDS)

The National Consortium for Data Science (National Consortium for Data Science, 2023) exemplifies the principles of NoDE through its collaborative and industry-specific approach to data science education and skills development.

The consortium operates as a collaborative initiative that brings together universities, research institutions, and industry partners. By connecting diverse stakeholders, the Data Science Consortium leverages their collective expertise, resources, and perspectives to develop comprehensive data science training programs and credentials that meet the specific needs of the industry.

By actively involving industry partners in the development and design of training programs, the consortium ensures that its offerings are tailored to address the specific data science skills required by the industry. This industry-specific approach enhances the relevance and applicability of the training programs, equipping individuals with the necessary data science skills to excel in the digital economy.

The collaborative nature of the Data Science Consortium fosters connectivity between universities, research institutions, and industry partners. This interconnectedness creates a dynamic learning environment where knowledge and expertise are shared, and industry practices are incorporated. By actively engaging diverse stakeholders, the consortium ensures that learners have access to the latest advancements and best practices in data science, enhancing their skills and keeping them at the forefront of the field.

Way Forward

Across Australia, there are several examples of training providers acting as centres of excellence to develop and share best practices in the delivery of digital skills training. While their collaborative efforts have been exemplary, they have limited capacity to scale on a state or national basis. Building on this experience, the Network of Digital Excellence (NoDE) concept has the potential to provide a practical and scalable approach to building capacity and capability for the delivery of digital skills training across the national VET sector.

The activation of NODEs could be achieved over a 3-year period. To utilise this approach effectively, users need to consider how best to identify and integrate key internal and external stakeholders, gain a shared understanding of skilling opportunities, the co-design of the training solution, the creation of training materials that can be shared freely across other RTOs, staff upskilling to deliver training, and the tracking of success. To achieve this, human and financial resources must be mobilised to ensure universal access to digital infrastructure, tools, and modern learning technologies. Additionally, policymakers should design and implement digital skills and learning strategies aimed at developing innovative curricula, allowing flexibility and individualization of delivery.

To establish early momentum, it will be important to build on success around discreet and bounded opportunities such as digital literacy or cyber skills training. The first step would be to develop the NoDE operating principles by working closely with a specified provider who is willing to become the nexus for the network. This could be delivered as a pilot program designed to test the approach and identify issues which could then be used to inform a follow-on trial prior to broader scaling. Both state and federal government funding is likely to be required.

Conclusion

The establishment of Networks of Digital Excellence (NoDE) represents a tangible and scalable approach for addressing the digital skills gap and building capacity and capability across the training network. By bringing together training providers, employers, and industry stakeholders, NoDE creates a collaborative ecosystem where best practices can be developed and shared.

NoDEs foster dynamic learning environments where stakeholders actively collaborate to share knowledge and resources. This collaborative approach ensures training programs are tailored to meet the specific needs of industries, making the acquired skills more relevant and applicable in real-world contexts. A prime example of this collaboration is seen in the success of the Wyndham Tech School, where partnerships with industry expose students to authentic challenges and hands-on projects, equipping them with practical skills for the digital workforce.

The second NoDE paper describes a step-by-step framework for establishing collaborative networks, incorporating industry-specific training, fostering connectivity, and promoting agility.

References

Amazon. (2023, June 7). Amazon Web Services Launches Global Skills to Tech Alliance. Retrieved from: https://www.aboutamazon.com

https://www.aboutamazon.com/news/aws/amazon-web-services-launches-global-skills-to-tech-alliance

Digital Skills Organisation. (2023). Growing Australia's Digital Workforce - Final Report. Melbourne: Digital Skills Organisation.

National Centre for Vocational Education Research. (2021). Employers' use and views of the VET system. Adelaide: NCVER.

National Consortium for Data Science. (2023). National Consortium for Data Science. Retrieved from National Consortium for Data Science: https://datascienceconsortium.org/

TAFE NSW. (2023). Institute of Applied Technology - Digital . Retrieved from TAFE NSW: https://store.training.tafensw.edu.au/product-category/iat/iat-digital/

TAFECyber. (2020). TAFECyber. Retrieved from TAFECyber: https://www.tafecyber.com.au/

Victoria University. (2023). Wyndham Tech School. Retrieved from Vicrtoria University: https://www.wyndhamtechschool.vic.edu.au/

DIGITAL SKILLS ORGANISATION

The NoDE Playbook: Six Steps for Employer Co-Designed Training Solutions

Digital Skills Organisation June 2023

NODE NETWORK OF DIGITAL EXCELLENCE

Table of Contents

Executive Summary

This document is a guide to employer co-designed training solutions based on the Digital Skills Development Model, which is informed by best practice and has been developed through multiple DSO trials and training programs.

The 'Playbook' describes six steps for developing effective training programs in collaboration with stakeholders:

- **Step 1: Pilot Establishment -** In this phase, the focus is on determining the broad purpose the training to be delivered, setting clear objectives, and forming necessary partnerships.
- **Step 2: Workforce Needs Analysis -** Research and data collection are crucial in understanding specific digital skills development requirements. Reports, sector scans, employer surveys, and other relevant sources are analysed to inform the co-design process.
- **Step 3: Design Workshops -** This step involves collaboration between employers and training providers to co-design necessary solutions. A digital skills pathway is identified to address the skill needs, outlining the broad process by which the required digital skills should be acquired, along with a training and assessment strategy.
- **Step 4: Training Solution Development -** Building upon the strategy outlined in Step 3, this phase focuses on developing a tangible training solution. It leverages the capabilities of available training providers to deliver the required skills that meet the employers' needs.
- **Step 5: Implementation Workshops -** The overall training solution is presented to training providers and employers in these workshops, in order to seek their feedback and approval before proceeding with program implementation.
- **Step 6: Program Implementation and Management -** This phase requires documenting the developed solution and implementing the training program. Continuous evaluation and management ensure the program's effectiveness and address any necessary adjustments.

Steps 2 to 5 form the core co-design process, which fosters a collaborative approach to developing training solutions tailored to the specific needs of employers and workforce.

This combined framework provides a practical guide to creating impactful and successful training programs that bridge the digital skills gap and empower the workforce to thrive in the digital era.

Introduction

This Playbook aims to formalise the employer-led and skills-based approach that has been developed through several DSO trials and training programs, utilising elements from the DSO's Digital Skills Development Model.

It brings together best-practice training and assessment solutions from various exemplary pilot projects involving employers, government organisations, training providers, and industry bodies. This document therefore aims to be a guide for designing and delivering such training programs while fostering collaboration with stakeholders.

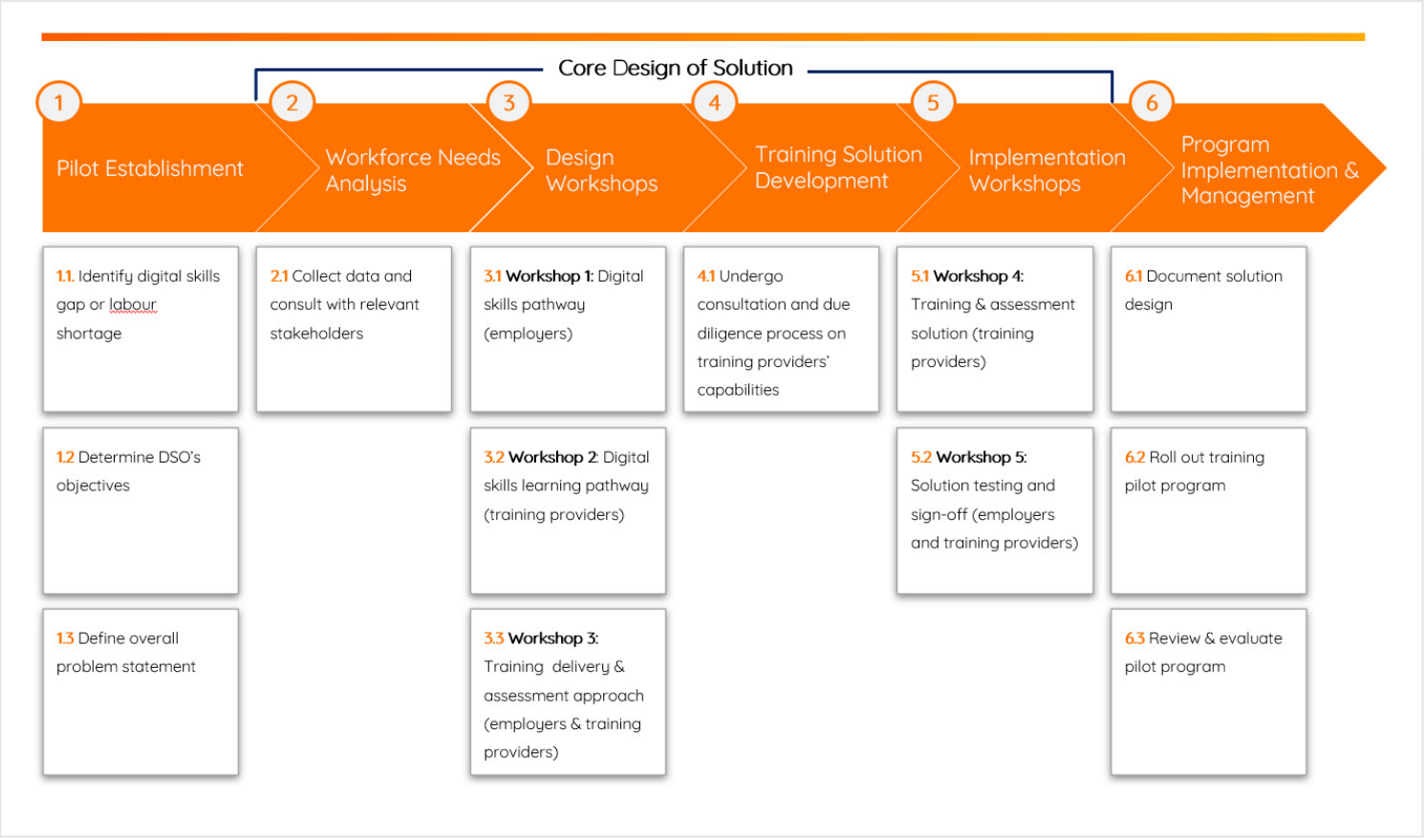
The Playbook was created through the DSO's Pilot Codification Project (undertaken by Generation Australia). This project set out to capture the 'skills based' approach by examining several DSO trials through diverse research methods, including direct observation, walkthroughs, document analysis, and stakeholder interviews. The active involvement of DSO staff throughout the process ensured the accuracy and validation of the codification outcomes.

The outcome of this report brings together the culmination of these learnings and experience, organising them into a number of repeatable steps.

Pilot Project Design and Delivery Process: User Guide

The overall process is summarised in Diagram 1. Please note that the following process may need to be adapted for different contexts, dependent upon stakeholder objectives. For example, some pilots may not involve employers, in which case the pilot partner, such as a government organisation, may take on the role of identifying the needs of the learners.

Figure 1: *Overall Process Map.*



Step 1. Pilot Establishment

1.1: Identifying the Training Solution's Purpose

- The driving force behind establishing a training solution is the recognition of a digital skills gap or labour shortage in a specific geographic region, industry, or organisation.
- Typically, organisations seeking support or guidance approach the entity responsible for the training solution (referred to as the 'partner'). However, in some cases, the organisation offering the training solution may independently reach out to a particular employer or industry body.

1.2: Determining Objectives

- Clearly outline the objectives for both the pilot partners and the organisation providing the training solution. Examples of partner objectives include:
  - Upskilling the existing workforce to enhance productivity.
  - Expanding the available workforce with the required digital skills.
- Examples of the organisation's (training solution provider) objectives include:
  - Implementing the Digital Skills Development Model.
  - Testing Digital Skills Standards, such as Digital Literacy, Digital Fluency, Critical Core Skills, Data Analytics, Software Development, Digital Executive, or Cyber Security.
  - Creating new Skills Standards based upon identified digital skills gaps or labour shortages.

1.3: Defining the Problem Statement

- Thoroughly clarify the context of the problem, including the specific industry, organisation, geography, or target demographic.
- Evaluate the magnitude and urgency of the digital skills gap or labour shortage, considering factors such as the number of vacant positions that need filling and the timeline for upskilling workers.
- Identify the underlying factors driving the need to upskill the existing workforce, as well as those contributing to the labour shortage.

1.4: Identifying Stakeholders

- Engage and incorporate relevant stakeholders in the process, including organisations, industry representatives, government bodies, and potential trainees. Their participation and collaboration are vital to the success of the training solution.

Step 2. Workforce Needs Analysis (WNA)

2.1: Collect data and consult with relevant stakeholders

- Send out employer and/or learner surveys to:
  - Gauge interest in training programs;
  - Understand the current digital skill levels of potential learners;
  - Identify the context in which learners will utilise their digital skills (e.g., jobs or future jobs); and/or
  - Analyse the digital skills gaps identified by employers and industry.
- Study local jobs data (such as advertisements) to quantify the types and number of roles available in the specific industry and/or location.
- Perform additional research and stakeholder consultation as required.

Step 3. Design Workshops

3.1: Workshop 1: *Digital Skills Pathway*

Attendees	Activities	Outcomes
Employer(s) (or similar) and/or pilot partner	• Deep-dive on digital skills needs: e.g., skills gaps for target learners (e.g., current and incoming employees), labour shortages (specific job roles in the highest demand), etc., based on findings from Workforce Needs Analysis. • Group problem-solving on specific digital skills most needed (and not met by current education credentials).	• Attendees identify the specific digital skills needs in the target learners. Example might include the upskilling requirements for existing employees, or the top 1-2 in-demand job roles from a shortlist of 5-10, as well as their major digital skills requirements.

3.2: Workshop 2:[1] *Digital Skills Learning Pathway*

Attendees	Activities	Outcomes
Training provider(s) - pilot partner representatives may wish to attend in an advisory capacity.	• Training providers identify what they believe to be the best 'learning pathways' for the digital skills identified in Workshop 1. This will involve outlining which micro-credentials are most relevant, and the ideal order in which they should be acquired.	• A comprehensive draft learning pathway for the chosen digital skills or job roles, based upon an identified number of micro-credentials.

1 . The default pilot methodology is for the Digital Skills Pathway (employer) workshop to come before the Digital Skills Learning Pathway (training provider) workshop. Unfortunately, for the Canberra Cyber Hub pilot, due to scheduling challenges this order was reversed. On reflection, DSO would recommend keeping the employer workshop first, as the former directly informs the content focus for the latter: the employer-focused perspective on the current labour and skills shortages helps narrow the focus and direction of the training provider workshop.

3.3: Workshop 3: *Training delivery and assessment approach*

Attendees	Activities	Outcomes

Employer(s), training provider(s), and pilot partner	• Discussions with employers about their preferences regarding the learning approach (e.g., formal classroom on-ramp training vs. informal work-integrated, practice-based training).
	• Self-assessment report by employers concerning how much time can be devoted to work-integrated training and how much internal expertise is available, vs. need for external training providers.
	• Problem-solving sessions with training providers on how to adapt existing content to best meet individual employers specific skill-demands.
	• Discussion and problem-solving between employers and training providers regarding:
	  • The training delivery model (breakdown of on-ramp vs. work-integrated).
	  • Capacity for talent pipeline (e.g., employers' willingness to commit to a paid or unpaid internship model, traineeship program or employment-after-graduation agreement).
		• Agreement in principle between employers and training providers to co-operate in the development and implementation of the digital skills training program.
		• Training providers agree to adaptations of course content according to the micro-credentials required for chosen digital skills. This will require providers to self-identify the compatibility and incompatibility between the needed skills and existing content in training courses.

Step 4. Training Solution Development

4.1: Undergo consultation and due diligence process on training providers' capabilities

- Share summary of the learnings and training solution needs identified at Design Workshops with training providers.
- Interview training providers concerning their capability to meet micro-credential requirements (e.g., teaching availability, relevant courses that can be immediately utilised or adapted).
  - Collect their curriculum responses (self-mapping of micro-credential requirements to their courses).
- Pilot partner should also *independently* map micro-credential requirements to existing training provider courses, informed by the training providers' own self-mapping.
- Identify learning pathway gaps (i.e., where training providers' courses do not meet micro-credential requirements).
  - Confirm whether additional existing or newly developed courses will be required from main training providers to meet both relevant standards - such as the Australian Qualifications Framework (AQF) – and the additional non-accredited skills requested by employers in the Design Workshops.
- Conduct due diligence on training providers concerning:
  - Scope of content they can deliver;
  - Assessment/certification processes they can offer; and
  - Delivery models for course content (e.g., online, instructor-led, self-paced or structured assessment regimes)
- Select one or more training partners. A typical model might involve one main partner and incorporate additional training providers to fill content gaps [2] where needed.
- Reach a consensus between training and industry stakeholders regarding the strategy for implementing work-integrated digital skilling as detailed in the practice-based learning guide.

[2] *For example, for the Canberra Cyber Hub, to meet Micro-credential 1 for the Threat Operations Analyst, DSO decided that beyond the core AQF-standard courses provided by the Canberra Institute of Technology (the main training provider partner), additional bespoke training skills gaps could be met by Risk2Solutions, DDLS, and Australian National University.*

Step 5. Implementation Workshops

5.1: Workshop 4: *Training & assessment solution*

Attendees	Activities	Outcomes
Training provider(s), and possible pilot partner (1-2 employers may also join to provide steering)	• Discussion on how training will be separated into on-ramp and work-integrated training. • Group problem-solving to identify what additional skills beyond relevant standards that learners need. This might include people skills, OH&S, and technical skills. • Whiteboarding to build exhaustive training framework, including content, providers, and timelines.	**Finalisation of training and assessment solutions for on-ramp and work-integrated micro-credentialing:** • Learning pathway map finalised for "integrated solution" between training providers for all micro-credentials. • Responsibilities for content delivery assigned to stakeholders. A typical example might outline that Training Provider X must deliver 4 units of competency at RTO skillset Level A for micro-credential 1, Training Provider Y will deliver bespoke module for Skill B, whilst Training Provider Z will also provide certification for Skill C.

5.2: Workshop 5: *Solution testing and sign-off*

Attendees	Activities	Outcomes
Employer(s), training provider(s), pilot partner	• Employers presented with the learning program and training model and asked to provide feedback	**Finalisation of training schedule and employer commitments:** • Employers provide formal sign-off to participate in the pilot and indicate the number of graduates/trainees they can accommodate, as well as confirmation they understand their commitments during training. • Agreement on delivery plan specifics

Step 6. Program Implementation and Management

6.1: Document solution design

- Record all design details, such as curriculum, training and assessment strategy, delivery method, and assessments.
- Codify agreements between training providers and employers.

6.2: Roll out training program pilot

- Commence the pilot program rollout, putting the carefully designed solution into action.
- Monitor the progress of the pilot program closely, keeping a close eye on how well the training is being delivered, and ensuring that any challenges or issues are addressed promptly.

6.3: Review and evaluate pilot program

- Agree to review pilot program with all stakeholders at set intervals.
- Evaluate pilot program with stakeholders and suggest amendments.
  - Implement program adjustments.
- Scale up and expand program, if applicable.

Conclusion

The NoDE Playbook presented in this document offers a valuable and comprehensive guide for establishing co-designed training solutions in response to identified digital skills gaps and labour shortages. Based on the Digital Skills Development Model developed through multiple DSO trials and training programs, this guide encapsulates best-practice training and assessment solutions from various pilots involving employers, government organisations, training providers, and industry bodies.

The step-by-step process outlined in the Playbook facilitates a collaborative approach to designing and delivering training programs, emphasising close cooperation with employers and stakeholders to address specific skill needs. The six essential steps - Pilot Establishment, Workforce Needs Analysis, Design Workshops, Training Solution Development, Implementation Workshops, and Program Implementation and Management - create a structured framework to develop impactful and effective training solutions.

By offering concrete examples and case studies, the appendices further enhance the Playbook's utility, providing practical guidance and insights for employers and stakeholders interested in implementing co-designed training solutions. The combination of the main content and the appendices creates a comprehensive resource to foster successful collaboration and address the evolving digital skills landscape.

As the digital landscape continues to fluctuate, the insights and guidance provided in the Playbook will remain relevant and adaptable to various industries and contexts. By embracing co-design principles and collaborating with stakeholders, organisations can foster innovation, creativity, and sustainable growth in the ever-changing digital world.

DIGITAL SKILLS ORGANISATION

Implementing Practice-Based Learning Supporting Guide

Digital Skills Organisation June 2023

NODE NETWORK OF DIGITAL EXCELLENCE

Table of Contents

Executive Summary

Practice based learning is an important part of delivering employer led training. This supporting guidance has been drafted to support Networks of Digital Excellence (NoDE), trainers and teachers. The complete application of this guidance as illustrated in the Practice-Based Learning Guide for Cyber Analysts - originally developed within the Canberra Cyber NoDE and packaged into a SCORM product - is available on request.

Together they are a resource which trainers and teachers can use to help improve contemporary training programs to ensure they can meet the actual needs of employers in a rapidly evolving workplace (AIIA, 2023).

The guidance focuses on a skills-based approach and utilises the digital skills standards framework which outlines the practical requirements for various job roles and their respective proficiency levels via transferable skills clusters.

On SCORM, there are an exemplar set of practice-based projects based on the cyber security skills standards and their related artifacts that align with a cyber analyst role, which were developed for the Canberra Cyber project.

Key elements covered in this guide:

- Identifying relevant micro-credentials.
- Understanding skills clusters.
- Formulating digital skills standards.
- Developing practice-based projects to enhance skills and associated artifacts.
- Selecting appropriate facilitated training topics that align with projects.
- Offering monitoring and support tools to track progress.

Together this guide facilitates the mapping of acquired digital skills to accredited qualifications, micro-credentials, or units of competency, allowing training providers to align their offerings with government funding and formal accreditation benefits.

The guidance herein should not be taken as strictly prescriptive and may be further developed by those using it depending on their specific needs.

Introduction

This document details the ‘Practice-based Learning Guide‘ within the Network of Digital Excellence (NoDE). They are an important part of the NoDE approach which aims to align training components with digital skills standards.

The content presented in this document is based on the best-practice guide for practice-based learning designed by DSO as part of the “Closing the Cyber Skills Gap in Canberra” project.

The guidance and supporting templates have been widely embraced by training providers, employers, and learners for its standardized framework, addressing the industry’s digital skills requirements.

The notes are presented alongside a SCORM package which can be seamlessly integrated into any learning management system, ensuring unparalleled accessibility and adaptability.

Practice-based Learning Programmes

SCORM Package

The SCORM package - available with this guide - serves as a comprehensive toolkit, aimed at supporting the implementation of the Practice-Based Learning Guide for Cyber Analysts within the Networks of Digital Excellence (NoDE). This package contains a diverse range of valuable resources designed to align with the specific aim of each micro-credential and the learning objectives associated with different skills clusters.

Central to the SCORM package are the practice-based learning projects, carefully curated to correspond to the relevant cybersecurity skills standard. These projects are structured to guide learners through a series of hands-on activities that allow them to apply their theoretical knowledge in practical scenarios. Each project is described in detail, providing learners with clear instructions on the activities they need to undertake to successfully complete the project.

Within each activity, learners are presented with a set of tasks that facilitate step-by-step progression, ensuring a systematic and immersive learning experience. These tasks are designed to challenge learners, helping them develop critical problem-solving and analytical skills, which are crucial for excelling in the role of cyber analysis.

The SCORM package goes beyond just providing tasks and activities; it also offers an array of supplementary materials to scaffold the learning process effectively. Learners can access best-practice guides, templates, and real-world examples that serve as valuable references, aiding them in comprehending the concepts and their practical applications.

Moreover, the package includes facilitated training topics encompassing a wide range of skills, knowledge, and activities relevant to the cyber analyst role. These training topics are expertly crafted to offer learners a structured and organised work-integrated learning path, ensuring they acquire the necessary skills step by step.

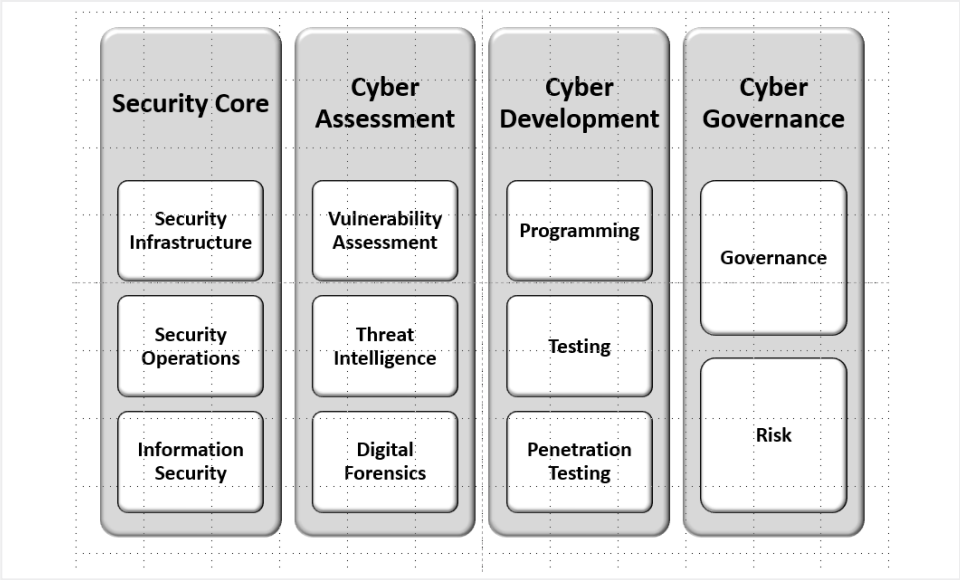
By utilising the SCORM package, learners can engage in an interactive learning journey, gaining hands-on experience, and deepening their understanding of cybersecurity concepts. The wealth of resources within the package empowers learners to develop their expertise in a systematic manner, with the flexibility to adapt their learning to suit their individual needs and workplace.

Supporting Guidance

Understand the Purpose of each Micro-Credentials

In the development of the workplace practice learning guide it is important to clearly define the purpose and scope of each micro-credential. An example of co-designed micro-credentials and the associated skills clusters for cyber analyst role is given in **Figure 1.**

Figure 1: *Four Micro-credentials within Cyber Analyst role.*



As an example, consider “cyber assessment” depicted in Figure 1.

This micro-credential seeks to enable individuals to proficiently assess the security of digital assets, systems, and networks. It involves developing skills related to threat intelligence analysis, conducting vulnerability assessments, performing digital forensics investigations, analysing evidence related to security incidents, responding to and mitigating security incidents, and implementing preventive measures against cyber threats. By completing this micro-credential, individuals can demonstrate their proficiency in these critical areas, enhancing their suitability for cyber analyst roles and other relevant positions in the field of cybersecurity.

The purpose of this micro-credential is described as:

...to enable individuals to proficiently assess the security of digital assets, systems, and networks. This includes developing the skills necessary to identify potential vulnerabilities through threat intelligence analysis, vulnerability assessments, conduct thorough digital forensics investigations to analyse collected evidence related to security incidents, and respond to and mitigate security incidents.

Identify the learning objectives for each skills cluster that will be met within any Micro-credential.

In the development of the workplace learning guide it is important to identify which learning objectives will be met through the delivery of a micro credential.

As an example consider the “Threat Intelligence” skills cluster within the cyber assessments micro-credential.

Figure 2. *Analysis of Digital Skilling Objectives for Cyber Analyst Skills Pathway.*

Microcredential 1 **Security Core**	**Microcredential 2** **Cyber Assessment**	**Microcredential 3** **Cyber Development**	**Microcredential 4** **Cyber Governance**
This is an introduction module to Cyber Security and provides the fundamental skills for those entering the Cyber Security Workforce.	This module focuses on the strategies that can be implemented to access an organisation's cybersecurity measures it has in place to protect its information and systems from cyber-threats	This module will provide the skills to implement policy, procedures and processes that will building and maintain cybersecurity capabilities within an organisation.	This module will develop skills in developing, implementing, and evaluating frameworks to ensure information and systems are secure.
Microcredential 1 **Security Core**	**Microcredential 2** **Cyber Assessment**	**Microcredential 3** **Cyber Development**	**Microcredential 4** **Cyber Governance**
The following skills clusters are included: • **Information security** is the practice of protecting information and information systems from unauthorised used. • **Security Infrastructure** is the security provided to protect infrastructure and seeks to limit vulnerability and recommends remediation or mitigation. • **Security Operations** groups key applications into scalable package that will prioritise and response to security threats using workflows and automation.	The following skills clusters are included: • **Digital Forensics** is the process of using techniques and tools to examine and analyse digital devices, such as computers, in order to identify and analyse evidence for use in a court of law or other legal proceedings. • **Threat Intelligence** is the planning, collecting, analysing, and disseminating information that poses a threat to applications and systems. • **Vulnerability Assessment** is a systematic review of security weaknesses in an information system. The skills will enable the evaluation of a system being susceptible to any known vulnerabilities.	The following skills clusters are included: • **Penetration Testing** is the simulation of a cyberattack that tests a computer system, network, or application for security weaknesses. • **Software development/programming/ testing** – develop and test software components	The following skills clusters are included: • **Cyber-Strategy** defines the approach to cyber security. This includes vision, mission, statement, and alignment with organisational policies, directions, and goals. • **Risk Management** refers to the process of identifying, evaluation, and mitigating risks to an organisation's information and system Program Stakeholders.

Figure 3 outlines how the digital skilling objectives for this cluster focuses on equipping participants with the necessary knowledge, skills, and hands-on experience to proficiently identify, analyse, and mitigate cybersecurity threats.

Figure 3. *Digital Skilling Objective for Threat Intelligence Skills Cluster.*

What does it involve:

Threat intelligence involves the process of gathering and analysing information about potential or existing cyber threats to an organisation's assets, including its networks, systems, and data. It involves monitoring and analysing a variety of data sources to identify potential threats and to provide actionable insights to security teams to prevent or mitigate attacks.

Learning Objectives

Provide participants with the necessary knowledge, skills, and practical experience to effectively identify, analyse, and mitigate cybersecurity threats.

As a cyber analyst intern, you will be responsible for analysing and assessing potential cyber and information security threats to our organisation. Your work will involve reviewing and interpreting threat intelligence data from various sources, including open-source intelligence, dark web monitoring, and threat feeds. Your goal will be to identify potential threats and vulnerabilities, and to recommend strategies to mitigate those risks.

Establishing Digital Skills Standards and Proficiency Levels

Training which relies on the delivery of multiple micro credentials is brought together under a 'digital skills standard' which specifies the skills and proficiency levels to be achieved within a particular digital skills pathway.

These digital skills standards delineate the specific competencies within each skills cluster and articulate the corresponding levels of performance using the well-regarded Dreyfus Skill Acquisition model. Proficiency levels are determined based upon the identified job role an individual is pursuing. This information enables effort to be at a level appropriate to the job role/s that the learner is preparing to enter.

Given the necessity that the skills being taught are relevant to a particular real job, it is crucial that this standard be co-designed with input from employers.

As an example, consider the threat intelligence skills cluster in **Figure 4**.

Figure 4. *Digital Skills Standards for Threat Intelligence - Cybersecurity Job Family.*

Skills Section Title	Skills Statement	Level 1 Novice	Level 2 Advanced Beginner	Level 3 Adept	Level 4 Proficient	Level 5 Lead
Plan Threat Intelligence	Develop threat intelligence program and plans.			Collect data, create an information dissemination plan, analyse threat intelligence programs, and determine the intelligence requirements.	Manage recourses and set up communication channels/processes to effectively operationalize the cyber intelligence program. Evaluate and identify the threat intelligence requirements and plan the threat intelligence strategy.	Evaluate and develop threat intelligence strategies and programs. Build a threat intelligence team by formulating roles/ responsibilities. Create a training plan, policies, and procedures for the intelligence program.
Threat Intelligence Data Management	Collect, analyse, assess, and disseminate threat intelligence data.	Collect threat intelligence data from various sources. Process, collate, and exploit threat data on its relevance and reliability to develop and maintain the organisation's "situational awareness".	Cleanse, convert, label, validate the intelligence data (collected data from alerts, logs, and reported events) to make it suitable for analysis. Assess and validate information from several sources on current and potential cyber and information security threats to the organisation.	Analyse threat intelligence data (collected from a wide range of internal & external sources) and prepare actions and make recommendations.	Manage, interpret, and assess the threat data (collected from different internal & external sources). Prepare and disseminate threat intelligence report.	Determine and confirm the strategy and processes to collect threat intelligence data. Establish governance for the effective collection, implementation, utilization and improvement of threat intelligence data management tasks,

Skills Section Title	Skills Statement	Level 1 Novice	Level 2 Advanced Beginner	Level 3 Adept	Level 4 Proficient	Level 5 Lead
Threat Assessment and Mitigation	Threat Assessment Identify information management risks and mitigation techniques.	Scan external environment as per provided instructions for known threats and report the threats. Implement specified information security controls to mitigate the risks, as per provided instructions	Identify and document the assets, associate vulnerabilities, and threats that exploit vulnerabilities. Implement specified information security controls as per the provided instructions.	Prioritise threats, and develop threat intelligence system, and operating model. Design, plan, and evaluate the implementation of cyber and information security controls to mitigate identified risks.	Analyse the threats and plan threat hunting activities to proactively search for malicious activities. Manage the threat assessment activities within the estimated resources (time, coast and other resources). Develop an implementation and evaluation plan for implementing and evaluating the security controls. Evaluate and improve the security controls, resourcing plan and communication strategies.	Establish governance for identifying and analysing threats and related risk. Establish security governance process for the effective implementation of security controls, and improve the security posture.
Threat Modelling	Perform threat modelling.	Identify the assets and potential threats as per the provided guidelines, and threat modelling tools.	Recommend and utlise an appropriate threat modelling tool for threat assessment of the organisation.	Prioritise identified threats and maintain a register of potential threats to recommend mitigation capabilities.	Prioritise the identified threats, and maintain a register of potential threats to recommend mitigation capabilities.	Analyse and evaluate the threat landscape. Apply the security controls, and monitor the performance of applied controls to mitigate the threats.

Consider entry-level cyber analysts, participating in a training program such as an internship, workplace traineeship, or formal training at an educational institution. These learners will embark on their practice-based projects at the 'Advanced Beginner' level as described in **Figure 5**. By the completion of the training program, they will attain the competencies aligned with the 'Adept' skill level, equipping the participants to enter the workforce with confidence.

Figure 5. *Training will be aligned to the 'Advanced Beginner' level.*

DSO Skills Statements – Advanced Beginner	
1.1	**Threat Intelligence Data** • Cleanse, convert, label, validate the intelligence data (collected data from alerts, logs, and reported events) to make it suitable for analysis. • Assess and validate information from several sources on current and potential cyber and information security threats to the organisation.
1.2	**Assessment** • Identify and document the assets, associated vulnerabilities, and threats that exploit vulnerabilities.
1.3	**Risks & Mitigation** • Implement specified information security controls as per the provided instructions
1.4	**Threat Modelling** • Identify the assets and potential threats as per the provided guidelines, and threat modelling tools.

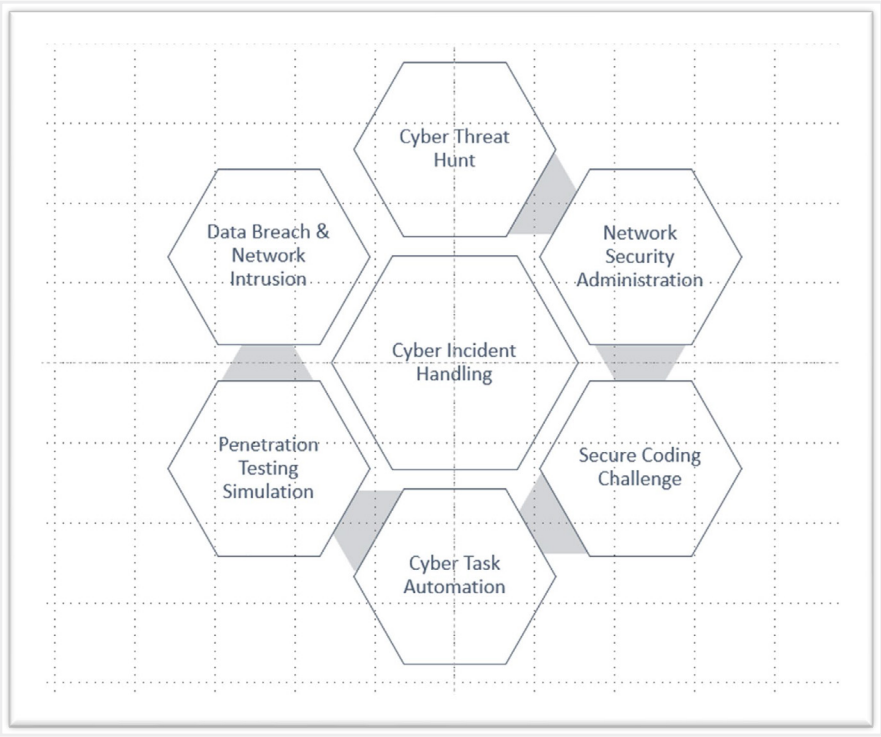
A Focus on the Foundational Skills Required for Success

In the delivery of any training programme, it will be important to ensure the learners have the base skills necessary to be successful during the ongoing work integrated training.

By appreciating the desired outcomes of the training process it is possible to identify the essential skills learners should have in place to maximise their chances of success during full training.

Figure 6. shows the result of collaborative brainstorming between training providers to identify the scenario-based project topics for the ONRAMP learning program, which forms the digital foundations bootcamp for the workplace. The topics were carefully derived through an analysis of the learning objectives in each skills cluster, enabling the identification of essential pre-requisite skills and knowledge necessary for a successful transition into practice-based learning.

Figure 6. *Brainstorming Results - Topic for ONRAMP Learning.*



A bootcamp was designed to prepare learners for the full practice-based experience by helping them to acquire the essential foundational skills determined as being necessary to complete the practice-based learning projects. In this case four scenario-based projects were created to provide an immersive learning experience, engaging learners fully while accelerating their skill development through hands-on activities, interactive sessions, and practical experiences.

In the design of such scenarios it is important to balance the need for technical skills and the development of enterprise and human skills such as collaboration, effective communication, and adaptability in dynamic work environments.

Figure 7. *Digital Foundations Bootcamp for Cyber Analyst - Scenario-based Projects.*

DSO Skills Statements – Advanced Beginner	
Student Guide	• Week 1 – Cyber Incident Management • Week 2 – Network Security Administration • Week 3 – Cyber Development • Week 4 – Data Encryption
Teacher guide	Teacher Guide Overview • Week 1- Cyber Incident Management • Week 2 – Network Security Administration • Week 3 – Cyber Development • Week 4 – Cyber Analyst Role
Lab Configuration Guide	• Sand Box Environment – Configuration Requirements

Figure 7 shows the scenarios created for the Canberra Cyber project bootcamp. These scenarios closely simulate real-world security incidents or challenges that learners might encounter in the work place.

In the design of these scenarios the following guidelines should be considered:

Practical experience

The scenarios should incorporate hands-on activities and practical exercises that closely resembles actual practice to encourage learners to actively participate in gathering and analysing digital evidence; and solving basic network, cyber, and security related problems.

Collaboration

The scenarios also should be designed to promote teamwork and collaboration. Learners should have opportunities to work together, sharing insights, and collectively solving complex challenges. Collaboration enhances their ability to work effectively within a team, a critical skill in cybersecurity roles.

Communication

Communication challenges should also be integrated within the scenarios, requiring learners to articulate their findings, insights, and proposed solutions. Communication skills are essential for conveying technical information to stakeholders and fellow team members.

Adaptability

Introduce dynamic elements in the scenarios, reflecting the ever-changing nature of information technology, networking, and cybersecurity challenges. This encourages learners to adapt quickly to new situations, fostering resilience and versatility.

Progression

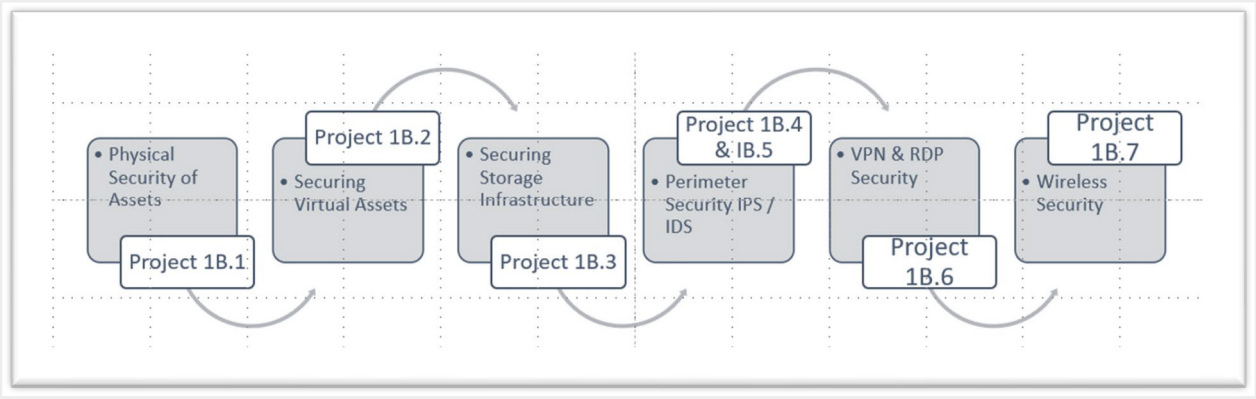
Arrange the scenarios in a logical sequence, gradually increasing the complexity and difficulty level as learners advance. This sequential approach allows learners to build upon their skills and knowledge systematically.

The Use of Job-Aligned Practice-Based Projects

Training should be supported by a collection of job-aligned practice-based projects which will help learners to access to engaging, relevant, and purposeful learning experiences.

These projects not only allow learners to apply their skills but also provide the necessary structure, guidance, and support to foster their development and success in the workplace.

Figure 8. *Practice-based Project Collection for Security Infrastructure Skills Cluster*



As per the example provided in **Figure 8**, projects serve as practical applications that allow learners to apply their acquired knowledge and skills in a real or simulated work environment. Projects should be selected that not only reflect the type of work expected from interns or employees but also align with the digital skills standards established for the respective skills clusters.

Figure 9. *Scenario and activities for a Security Infrastructure Project.*

Project 1B.1: Physical Security of Assets	
Skills Cluster	Security Infrastructure.
Skills Standard	Classify assets based on mission criticality. Assist in the implementation and management of the cyber defence measures for physical assets.
Project	As part of this project, you will be working on two physical assets within our organisation, which have been identified as critical to our mission. Your objective will be to assist in the implementation and management of cyber defence measures for these assets. The project will involve identifying and classifying these assets based on their mission criticality and implementing appropriate security controls to protect them from cyber threats.
Activity 1	Classify Mission Criticality of Physical Assets
Activity 2	Create a plan for implementing cyber defence measures for each asset
Activity 3	Discuss the recommended cyber defence measures with your supervisor and assist in implementation as required.

As shown in **Figure 9**, each practice-based project within the collection includes a carefully designed scenario that simulates real workplace situations. The scenario is crafted to provide learners with meaningful and relevant context for their learning experience. It encapsulates the activities and responsibilities that learners would typically encounter in their desired job roles, enabling them to develop practical skills that are directly applicable in the workplace.

To facilitate effective learning, it is important to develop not only the scenario but also provide comprehensive support for learners. This includes furnishing all the necessary information, tools, processes, and procedures aligned with the workplace context that learners would require to successfully execute the projects. A few examples of these are provided in **Figure 10**, **Figure 11**, and **Figure 12**.

A step-by-step breakdown of activities that learners should undertake to complete each project will help to ensure clarity and guidance throughout the learning process.

Figure 10. *Project execution steps and supporting material.*

Activity 1: Classify Mission Criticality of Physical Assets

1. Identify two physical assets within the organisation that are critical to its operations.
2. Gather information about the assets such as their location, usage, and importance to the organisation's mission.
3. Conduct a mission criticality assessment for each asset by answering the following questions:

- What would be the impact to the organisation's mission if the asset were to be damaged, destroyed, or made unavailable?
- What are the consequences to the organisation in terms of financial losses, reputation damage, or legal liabilities?
- Are there any regulations or compliance requirements that mandate protection of the asset?
- Are there any alternative assets or systems that can be used if the asset becomes unavailable?

4. Use a scoring system or a scale to rank the mission criticality of each asset based on the assessment.
5. Prepare a report summarising the results of the mission criticality assessment for each asset, including the scores and the justifications for the ranking.

Note: The intern should work closely with the organisation's security team or management and follow established policies and procedures for conducting the mission criticality assessment. The report should be completed under the guidance and supervision of the employer supervisor, security team or management.

Example of Physical Assets

1. **Servers:** These are physical computers that store and manage an organisation's data and applications.
2. **Network devices:** These include routers, switches, and firewalls that connect devices within an organisation's network and provide access to the internet.
3. **Storage devices:** These are physical devices that store data, such as hard disk drives, solid-state drives, and network-attached storage devices.
4. **Peripherals:** These include physical devices such as printers, scanners, and other input/output devices that are connected to an organisation's computers.
5. **Data centres:** These are facilities that house an organisation's servers, storage devices, and other IT infrastructure components.
6. **Power and cooling systems:** These are systems that ensure the stable and continuous operation of the organisation's IT infrastructure by providing uninterrupted power supply and regulating the temperature in the data centre.
7. **Physical security systems:** These are systems that protect an organisation's IT infrastructure assets from physical threats such as theft, vandalism, or environmental disasters.

As illustrated in **Figure 12**, specific tasks are outlined within each activity, providing learners with clear objectives and expectations. It is advised to provide finished products or deliverables with best-practice examples aligned with industry standards to help learners better understand and complete the tasks. These items should also contain pertinent links to frameworks or instructions to help students complete the tasks successfully.

Figure 11. *Instructions for Work Supervisors and Training Managers included when relevant.*

Activity 2: Create a firewall rule to protect a company database or another application

NOTE: As this is a practical hands-on activity, the supervisors may consider providing a sandbox environment or a test network for this activity. Alternatively, the interns may assist a member from the security team in configuration, monitoring, or management of a tool for securing virtual assets.

INSTRUCTIONS FOR SUPERVISORS AND TRAINING MANAGERS

Depending on the resources at hand and the security posture of the organisation, the intern may carry out one or more of the following tasks that align with the skills standard for this project. Other tasks that align with the goal of this activity may also be assigned by the supervisor.

There is a number of options available:

1. **Virtual Machines (VMs):** One way to create a safe sandbox environment for interns to practice configuring firewall rules is by setting up virtual machines. VMs can be set up on the interns' own personal computers or on a dedicated server or workstation. There are several free or low-cost virtualization platforms available such as Oracle VirtualBox or VMware Player that can be used to create multiple virtual machines for testing firewall configurations.
2. **Firewall Emulators:** Another option is to use a firewall emulator, which is a software-based tool that can emulate the functionality of a real firewall. Emulators such as GNS3 or EVE-NG can be used to simulate a range of firewall types and configurations, allowing interns to test different rule sets and configurations without affecting live systems.
3. **Cloud-Based Sandbox Environments:** Several cloud providers such as AWS, Azure, and Google Cloud offer free or low-cost sandbox environments for testing and development purposes. These cloud-based environments can provide access to virtual machines, networks, and other resources that can be used to test firewall configurations and other security measures.

Note: It's important to note that interns should be provided with clear guidelines and instructions on how to use these sandbox environments safely and responsibly. They should also be instructed not to use the same passwords or credentials used in the production environment and to avoid using any sensitive data in the sandbox environment.

Activity Details

1. S1. Write a firewall rule to stop an outsider from accessing a back-end product database to block all traffic from external IP addresses to the specific port on which the database is running.
   - A. Identify the IP address or range of IP addresses from which external traffic should be blocked. This could be a specific IP address or a range of IP addresses. Record the IP Address or the Range: _____
   - B. Determine the port on which the database is running. By default, most database management systems run on port 3306. Port: _____
   - C. Create Firewall Rule to achieve the above (see instructions below)

Figure 12. *Examples of finished products incorporated within the project collection.*

Activity 1: Data Collection

Collect threat intelligence data from various sources, such as alerts, logs, and reported events.

Tasks:

1. Identify the Sources:

   The intern should identify the sources from which they can collect the threat intelligence data. These sources may include alerts generated by security tools, logs generated by servers and network devices, and reports of suspicious activity or incidents reported by employees or customers.

   You can record the different types of sources from which you will collect the threat intelligence data, such as alerts, logs, and reports. For each source, you can provide a name, description, and data collection method, which could be automated or manual. This table will help you keep track of the different sources of threat intelligence data and how they are collected, which will be useful for future analysis and reporting.

Example of Data Sources Table

Source Type	Source Name	Description	Data Collection Method
Alerts	Security Tool 1	Alerts generated by Security Tool 1	Automated
Alerts	Security Tool 2	Alerts generated by Security Tool 2	Automated
Logs	Server 1	Logs generated by Server 1	Automated
Logs	Server 2	Logs generated by Server 2	Automated
Logs	Network Device 1	Logs generated by Network Device 1	Automated
Reports	Employee 1	Suspicious activity or incident reported by Employee 1	Manual
Reports	Employee 2	Suspicious activity or incident reported by Employee 2	Manual
Reports	Customer 1	Suspicious activity or incident reported b Customer 1	Manual
`Reports	Customer 2	Suspicious activity or incident reported by Customer 2	Manual

The Use of Facilitated Training and Just-in-Time Learning Topics

Teachers can be supported to deliver relevant training by providing them with guidance on the essential knowledge topics, skills topics, and activities that learners will need to effectively execute their projects.

Facilitated Training Topics

To support learners in their journey, the requirements for specific knowledge and skills topics have been described. Additionally, suggested classroom activities that are critical for their understanding and application of the project requirements are provided.

These facilitated training topics encompass the theoretical foundations, industry practices, and relevant concepts that learners need to grasp to succeed in their projects. As illustrated in **Figure 13**, the guide offers detailed guidance and resources for teachers and trainers to effectively deliver these training topics, fostering a comprehensive education experience for learners.

Figure 13. *Facilitated Training for Security Infrastructure Skills Cluster.*

Facilitated Training			
Project	**Knowledge Lessons**	**Skills Lessons**	**Practical Activities**
Securing physical assets	• Understanding physical security risks and threat landscape. • Identifying and classifying physical assets based on mission criticality. • Understanding security controls and their implementation.	• Classifying mission criticality of physical assets. • Creating a plan for implementing cyber defence measures for each asset. • Discussing recommended cyber defence measures with the supervisor. • Assisting in the implementation of cyber defence measures.	• Secure selected physical assets.
Securing virtual assets	• What are virtual assets? • Understanding virtual security risks and the threat landscape. • Identifying tools and techniques used in organisation to secure virtual assets. • Understanding security controls and their implementation.	• Creating a firewall rule to protect virtual assets. • Conduct vulnerability assessments on virtual assets.	• Implement a basic security control to protect a virtual asset (eg: web server).

Facilitated Training			
Project	**Knowledge Lessons**	**Skills Lessons**	**Practical Activities**
Securing storage infrastructure	• Understanding access control and authentication mechanisms. • Understanding storage infrastructure and its role in organisation. • Understanding security controls and their implementation.	• Configuring user accounts and access rights. • Configuring authentication mechanisms. • Monitoring and reviewing access logs. • Enforcing access control policies.	• Implement access control and Authentication Measures for storage infrastructure.
Perimeter security using IPS/IDS	• Understanding perimeter security and intrusion detection/prevention systems. • Understanding the configuration and operation of IDS/IPS.	• Installing and configuring an IDS/IPS on a sandbox environment. • Testing IDS/IPS configurations. • Troubleshooting IDS/IPS issues.	• Install and configure an IDS/IPS, test, & troubleshoot.
VPN / RDP security	• Understanding Virtual Private Networks and Remote Desktop Protocols. • Understanding VPN/RDP technologies and their security implications. • Understanding security controls and their implementation.	• Analysing workplace requirements. • Installing and configuring remote access solutions. • Testing remote access solutions.	• Configuring and securing remote access solutions, ensuring that they meet the security requirements of the organization.
Wireless security	• Understanding wireless security risks and the threat landscape. • Identifying wireless security solutions. • Understanding security controls and their implementation.	• Workstation configuration for wireless security solutions. • Installing and configuring wireless security solution. • Testing wireless security solution.	• Configure a Security Wi-Fi Network.

Self-Paced Learning Topics

In addition to facilitated training, the importance of self-paced learning is also recognised. It identifies self-paced learning topics that allow learners to explore specific areas of interest or dive deeper into certain skills or concepts related to their projects. **Figure 14** provides an example of a collection of self-paced learning projects aligned to the security infrastructure skills cluster.

Figure 14. *Self-paced learning guide - Security+ for Security Infrastructure Skills Cluster.*

CompTIA SECURITY+ LEARNING PROGRAM	
CompTIA Security+ Lessons	**CompTIA Security+ Labs**
• Lesson 3: Performing Security Assessments • Lesson 9: Implementing Secure Network Configuring a firewall, Scanning and Identifying Network Nodes, Intercepting and Designs • Lesson 10: Implementing Network Security Appliances • Lesson 11: Implementing Secure Network Protocols • Lesson 12: Implementing Host Security Solutions • Lesson 13: Implementing Secure Mobile Solutions • Lesson 15: Implementing Secure Cloud Solutions • Lesson 16: Explaining Data Privacy and Protection Concepts	• Managing Incident Response • Mitigation and Recovery • Identifying Application Attacks • Security Network Infrastructure • Configuring a System for Auditing Policies • Interpreting Network Traffic with Packet Sniffing Tools • Managing Centralised Authentication • Managing Access Controls in Windows Server • Securing the Network Infrastructure • Managing Access Controls in Linux • Configuring Identity and Access Management Controls • Implementing a Virtual Private Network • Configuring an Intrusion Detection System • Implementing a Secure SSH Server • Implementing Endpoint Protection

Just-in-Time Learning

To enhance the learning experience further it is important to integrate just-in-time learning resources into the delivery of training as shown in **Figure 15**.

Figure 15. *Just-in-time training for programming skills cluster projects.*

Basics of PowerShell – Further Study

PowerShell is a scripting language developed by Microsoft for use with Windows operating systems. It is designed to automate administrative tasks and can be used to manage various aspects of the Windows operating system, including system settings, file systems, registry settings, and network configurations.

How do you open the PowerShell Prompt?

1. **Using the Start menu search bar:** On Windows 10, you can open the Start menu and type "PowerShell". This will display a list of search results, including "Windows PowerShell" and "Windows PowerShell (x86)". Select one of these options to open the PowerShell prompt.
2. **Using the Run dialog:** You can also open the PowerShell prompt using the Run dialog by pressing the Windows key + R and typing "powershell". Then press Enter or click OK to open the PowerShell prompt.
3. **Using the Command Prompt:** If you have the Command Prompt open, you can switch to the PowerShell prompt by typing "powershell" and pressing Enter.
4. **Using Windows Terminal:** If you have Windows Terminal installed, you can open the PowerShell prompt by selecting the PowerShell option in the dropdown menu.

Once you have opened the PowerShell prompt, you can start entering PowerShell commands and executing PowerShell scripts. By default, the PowerShell prompt displays the current directory and the user context, indicated by the command prompt. You can use the cd command to change the current directory and the dir command to list the files and folders in the current directory.

Here are some basics of PowerShell that you need to be familiar for executing the projects:

1. **Command structure:** PowerShell commands are structured in the form of cmdlets, which are small, single-purpose commands that can be combined together to create more complex scripts. The syntax for a cmdlet is as follows: Verb-Noun. For example, the Get-Process cmdlet is used to retrieve information about running processes on a system.
2. **Variables:** PowerShell allows you to store values in variables, which can then be used in scripts. Variables in PowerShell are denoted by a dollar sign ($). For example, $ComputerName = "Server01" creates a variable called $ComputerName and sets its value to "Server01".
3. **Loops:** PowerShell supports various types of loops, including foreach, while, and do-while. Loops are used to repeat a block of code a certain number of times or until a certain condition is met.
4. **Conditionals:** PowerShell supports if, elseif, and else statements, which are used to test conditions and execute different blocks of code depending on the result of the test.
5. **Functions:** PowerShell allows you to define custom functions, which are blocks of code that can be reused in different parts of a script or in different scripts altogether. Functions are defined using the function keyword and can accept parameters and return values.
6. **Modules:** PowerShell modules are collections of cmdlets, functions, and other scripts that can be imported and used in your scripts. PowerShell comes with a number of built-in modules, and you can also create your own modules to share with others.
7. **PowerShell ISE:** PowerShell ISE (Integrated Scripting Environment) is an integrated development environment that provides a graphical interface for writing, testing, and debugging PowerShell scripts. It also includes features such as syntax highlighting, auto-completion, and code snippets.

These resources can be accessed by learners through industry certification platforms or dedicated just-in-time learning management systems. By leveraging these resources, learners can acquire specific knowledge or skills on demand, precisely when they need them during their project execution. Just-in-time learning (see **Figure 15** and **Figure 16**) ensures that learners have immediate access to relevant and up-to-date information, empowering them to overcome challenges and achieve optimal outcomes in real-time.

Figure 16. *Additional Reading Material & Suggestions Provided.*

Additional Reading
Topic 1 Cyber Incident Management

What is a cyber incident?

The Australian Cyber Security Centre (ACSC) defines a cyber incident as an unwanted or unexpected cyber security event or a series of such events that have a significant probability of compromising business operations. (ACSC, 2023)

Why do we need a cyber incident response plan?

All organisations should have a cyber incident response plan to ensure an effective response and prompt recovery in the event security controls don't prevent an incident from occurring. This plan should be tested and regularly reviewed to ensure risk mitigation in case of an incident, and minimize the risk of future incidents. (Cyber Incident Response Plan, ACSC 2023).

What is a cyber incident response plan?

A cyber incident plan is a set of documented procedures and protocols an organisation has to manage and respond to cybersecurity incidents. The plan outlines the steps an organisation should take in the event of a security breach or other cyber incident, such as a data breach, ransomware attack, or denial-of-service (D.O.S) attack.

A typical cyber incident plan includes the following key components:

1. **Roles and Responsibilities:** Defines the roles and responsibilities of incident response team members, including their specific duties and decision-making authority.
2. **Incident Detection and Reporting:** Describes the process for detecting and reporting security incidents, including who is responsible for monitoring and analysing system logs and alerts.
3. **Incident Analysis and Triage:** Outlines the procedures for analysing the incident and determining its severity, scope, and impact.
4. **Incident Containment and Mitigation:** Details the steps to be taken to contain the incident and prevent further damage, such as isolating affected systems or networks, disabling compromised user accounts, or blocking malicious traffic.
5. **Incident Investigation and Remediation:** Describes the process for investigating the incident, identifying the root cause of the problem, and implementing corrective actions to prevent similar incidents from occurring in the future.
6. **Communication and Notification:** Outlines the procedures for communicating with stakeholders, including employees, customers, law enforcement, and regulatory bodies, and notifying them of the incident.
7. **Recovery and Restoration:** Describes the process for recovering systems and data, restoring normal operations, and conducting post-incident reviews to identify areas for improvement.

Additional Reading

Topic 1 Cyber Incident Management

How do I respond to a Ransomware Attack?

As the name suggests, Ransomware is malware by which hackers encrypt user data and then demand a certain price to provide the encryption key to the user. User can be individual business organisation or government. (Beaman. et al, 2021)

Here is an example of how you can respond to a ransomware attack.

1. Isolate the infected systems: The first step is to isolate the affected system or systems from the network to prevent the ransomware from spreading. This can be done by disconnecting affected systems from the network, shutting down affected servers, or disabling network connections.
2. Alert the incident response team: Notify the incident response team immediately to investigate the incident, contain it, and minimize the attack's impact.
3. Assess the scope of the attack: Conduct a thorough assessment of the scope of the attack, including which systems are affected and what data may have been encrypted or compromised. This can help inform decisions about how to proceed with the response.
4. Contact law enforcement: Consider contacting law enforcement to report the attack, particularly if there is evidence of criminal activity.
5. Restore data from backups: If possible, restore data from backups to minimize the attack's impact. It's important to ensure that backups are not also infected with ransomware before restoring them.
6. Do not pay the ransom: While it may be tempting to pay the ransom to regain access to encrypted data, this can encourage further attacks and is not guaranteed to restore data.
7. Conduct a post-incident review: After the incident is resolved, conduct a post-incident review to identify any areas for improvement in the incident response plan or in the organization's overall security posture.

What should be in a critical incident management communication plan?

The communication plan should specify the procedures for notifying relevant parties, such as internal teams, customers, partners, and regulatory authorities, about the breach and its impact. This could include specifying the information to be communicated (based on the investigation), the channels to be used, and the timeline for communication.

The guide provides comprehensive guidance and suggestions for the selection and integration of facilitated training topics, self-paced learning topics, and just-in-time learning resources. It assists teachers and trainers in curating a well-rounded training program that addresses the diverse learning needs of learners, while ensuring that they have access to the necessary knowledge, skills, and support throughout their project-based learning journey (see **Figure 17** and **Figure 18**).

Figure 17. *Documents and Templates provided as required.*

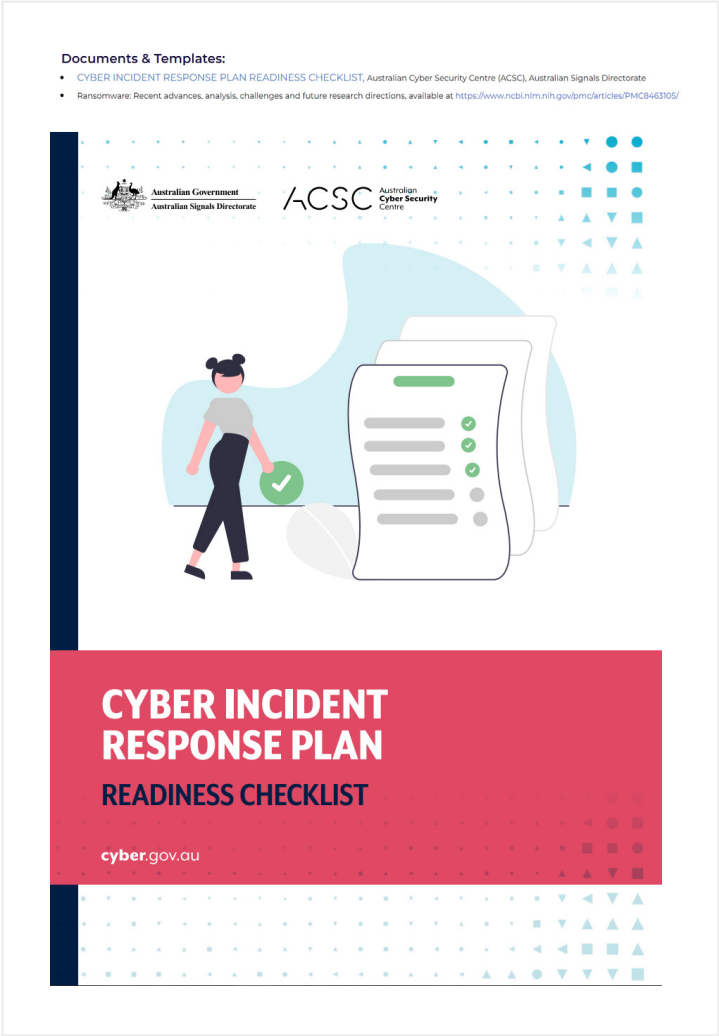


Figure 18. *Instructions for configuring sandbox environments for practical components.*

Sandbox Environment Bootcamp

1. **Hardware Requirements:**
   The sandbox environment should consist of at least one server and one workstation for each group of students.
   - Server: Minimum of 8GB RAM, quad-core CPU, and at least 500GB of storage.
   - Workstation: minimum of 4GB RAM, dual-core CPU, and at least 250GB of storage.
2. **Virtualization Software:**
   - The sandbox environment should use virtualization software such as VirtualBox or VMware to create virtual machines for the server and workstation.
3. **Network Configuration:**
   - The server and workstation should be connected to a virtual network that is isolated from the host network. This can be achieved by configuring the virtual network adapter as “host-only” or “internal network” in the virtualization software.
4. **Operating System:**
   - The server and workstation should run a supported operating system such as Windows Server 2016 or 2019, and Windows 10, respectively.
5. **IDS/IPS Software:**
   - The sandbox environment should have at least one IDS/IPS software package such as Snort or Suricata installed and configured on the server.
6. **Firewall Software:**
   - The sandbox environment should have at least one firewall software package such as pfSense or iptables installed and configured on the server.
7. **Remote Access Solutions:**
   - The sandbox environment should have remote access solutions such as RAS, RDP, and wireless configured on the server and workstation. This can be achieved by configuring the built-in Windows Server Remote Access role, Remote Desktop Services, and configuring the wireless adapter settings on the workstation.
8. **Documentation:**
   - The interns should document the configuration of the sandbox environment, including any changes made to the software, hardware, and network configurations.

Conculsion

This sandbox environment configuration should provide interns with practical experience in configuring and testing IPS/IDS, firewall, RAS, RDP, and wireless solutions in a safe and isolated environment. It will help improve their knowledge and skills in network security, which can be applied in real-world scenarios.

Monitoring and Support Tools for Practice-Based Projects

Throughout the learning pathway it is important to monitor learner progress and provide timely support during the execution of practice-based projects to ensure learners receive the guidance they need to succeed.

Meeting Schedules and Mentor Guidance

It is important to establishing regular meeting schedules between learners, trainers, and workplace supervisors / mentors. These meetings provide valuable opportunities to discuss project progress, address any challenges, as well as provide guidance and support. Trainers and mentors play a pivotal role in offering expert advice, sharing best practices, and facilitating the learning process.

They also provide guidance to employer supervisors on how to support learners effectively within the work environment, ensuring a cohesive learning experience.

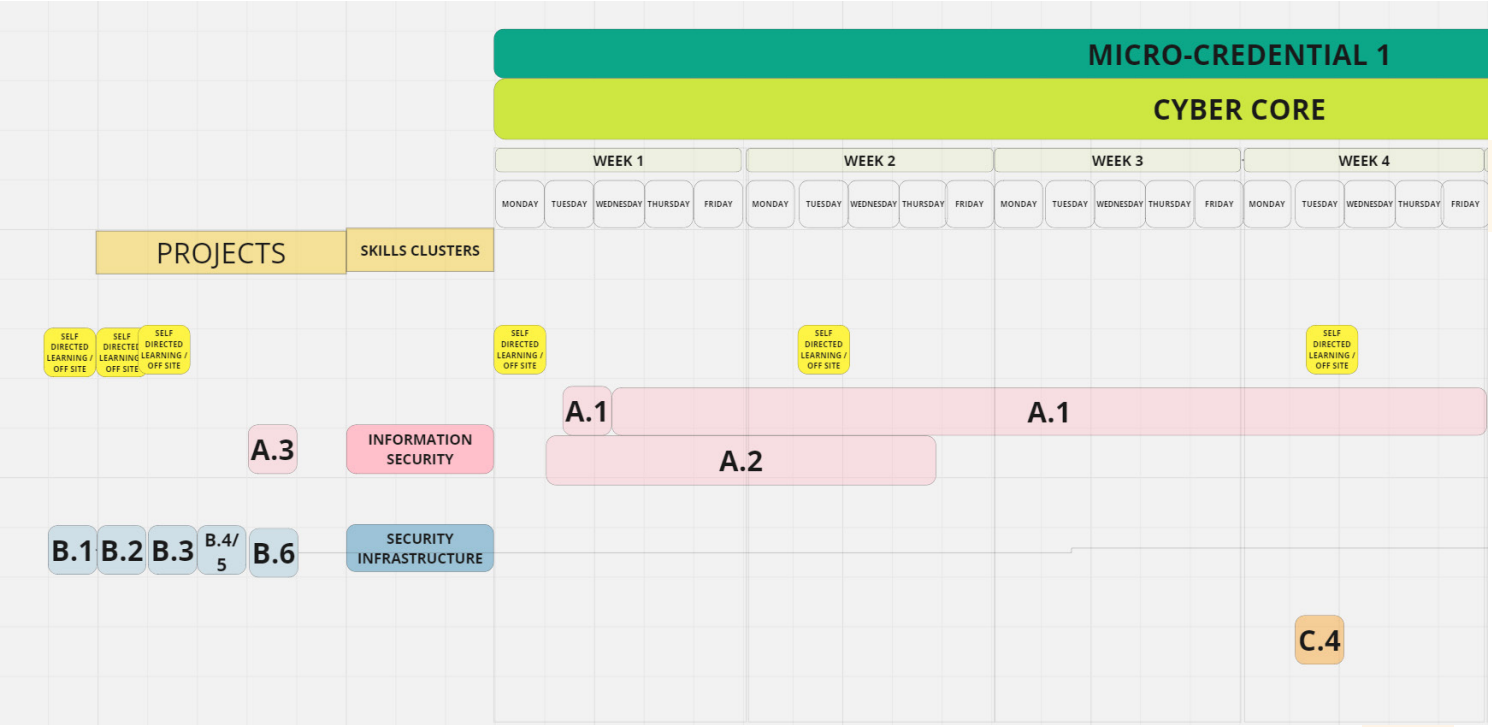
Figure 19. *Meeting Schedule.*

Micro Credential	Focus Day (0.5 – 1 day every six weeks	Skills Clusters	Project Number	Planned Commencement	Planned Completion	Daily Stand Up	Weekly Retrospective Time and Duration (Day and Time)
Cyber Core		• Information Security • Security Infrastructure • Security Operations					
Cyber Assessment							
Cyber Development							
Cyber Governance							

Personalised Learning Plans and Tools

To enhance the learning experience, it is important to introduce tools that supervisors and teachers can utilise to create personalised plans for learners' workplace activities. These tools assist in outlining specific tasks, responsibilities, and time commitments, ensuring that learners receive tailored guidance and support aligned with their specific needs. Personalised learning plans promote a structured approach, enabling learners and supervisors to track their progress, identify areas for improvement, and set goals for development.

Figure 20. *Personalised Practice-based Learning Plan Template.*



Framework for Monitoring Progress

It is important to agree ahead of time on a framework for monitoring learners' progress throughout the duration of their practice-based projects. This framework includes clear guidelines on how to assess project milestones, identify any issues or impediments to progress, and establish mechanisms to address them promptly. It emphasises the importance of creating to-do lists and action plans to ensure timely remediation activities, fostering a proactive approach to learning and development.

Figure 21. *Tools for Monitoring Progress.*

Project Scorecard Template							Weekly Progress		
Skills Cluster	**Project**	**Project Lead/Support**	**Priority**	**Resources**	**Start Date**	**Planned Completion**	**WK 1**	**WK 2**	**WK 3**
			MEDIUM	MARGINAL			20 – 40 %	40 – 80%	80 – 100%
			LOW	INADEQUATE					
			HIGH	MARGINAL					
			HIGH	MARGINAL					

Engagement with Workplace Supervisors

For projects conducted in a workplace setting, such as internships or traineeships, the guide highlights the importance of ongoing engagement between training providers and workplace supervisors. It encourages regular communication and collaboration to ensure that learners' progress is effectively supported within the workplace environment. By establishing strong partnerships and fostering open lines of communication, training providers can address any challenges, provide additional resources, and maintain a cohesive learning experience throughout the project duration.

Mapping Projects to Accredited Units of Competency and Certifications

Learning outcomes which are aligned with practice-based micro-credentials should be recognised within the formal training or industry certification systems to ensure learners gain tangible recognition for their achievements.

The learning journey must be mapped to the practice-based projects and their associated facilitated delivery to accredited units of competency, higher education subjects, industry certifications, or any other credentials.

Customised Mapping for Training Providers and Credential Issuing Organisations

It is recognised that different training providers and credential issuing organisations may have specific requirements for recognition and accreditation. Thus, a flexible approach to mapping projects to accredited units of competency or certifications is required.

Training providers have the flexibility to align the learning outcomes of projects with the specific requirements of their chosen accreditation or certification pathways. This customisation ensures that learners' achievements are appropriately recognised and validated within their chosen educational or industry frameworks.

Table 1 presents the mapping conducted by Canberra Cyber Project training providers. The contribution of practice-based projects to this mapping will be managed by individual training providers, ensuring compliance with relevant legislative requirements as needed.

Table 1. *Mapping of Micro-credentials to Accredited and Non-Accredited Credentials.*

Micro-Credentials	Skills Clusters	Training Program Details	Type Of Training	Provider
Security Core	Information Security	ICTCYS403 Plan and implement information security strategies for an organisation	Accredited	Canberra Institute of Technology (CIT)
	Security Infrastructure	VU23218 - Implement network security infrastructure for an organisation	Accredited	CIT
	Security Infrastructure	ICTCLD401 - Configure cloud services	Accredited	CIT
	Security Infrastructure	VU23220 - Develop and carry out a cyber security industry project	Accredited	CIT
	Security Operations	Security Operations	Non-Accredited	Risk2Solutions
	Security Fundamentals	CompTIA Security+	Industry Certifications	Lumify
	Human Skills Resource	Problem Solving, Communication, Teamwork, Analytical Thinking	Non-Accredited	Maxme
Cyber Assessments	Threat Intelligence	ICTCYS407 Gather, analyse and interpret threat data	Accredited	CIT
	Vulnerability Assessments	VU23222 - Expose website security vulnerabilities	Accredited	CIT
	Digital Forensic	VU23221 - Evaluate and test an incident response plan for an enterprise	Non-Accredited	ACFA
	Security Fundamentals	CompTIA Security+	Industry Certifications	Lumify
	Human Skills Resource	Problem Solving, Communication, Team work, Analytical Thinking	Non-Accredited	MaxMe

Micro-Credentials	Skills Clusters	Training Program Details	Type Of Training	Provider
Cyber Development	Programming	ICTPRG434 - Automate processes	Accredited	CIT
	Testing	ICTPRG433 - Test software developments	Accredited	CIT
	Pen Testing	VU23215 - Test concepts and procedures for cyber security	Accredited	CIT
	Pen Testing	Ethical Hacker Course	Non-Accredited	Lumify
	Security Fundamentals	CompTIA Security+	Industry Certification	Lumify
	Human Skills Resource	Problem Solving, Communication, Team work, Analytical Thinking	Non-Accredited	MaxMe
Cyber Governance	Cyber Governance	Information Security Governance	Non-Accredited	ACFA
	Risk Management	Cyber Risk Management	Non-Accredited	Risk2Solutions
	Security Fundamentals	CompTIA Security+	Industry Certification	Lumify
	Human Skills Resource	Problem Solving, Communication, Team work, Analytical Thinking	Non-Accredited	MaxMe

Alignment of Learning with Formal Training and Certification

Mapping projects and associated facilitated delivery to accredited units of competency or certifications helps to ensure the skills and knowledge acquired through program are recognised and transferable within broader education and industry contexts. It provides learners with a seamless pathway for further education or career progression, as their achievements in practice-based learning are acknowledged and validated through formal accreditation or certification.

Recognition of Micro-Credentials

It will be important to recognise the role played by micro-credentials achieved through practice-based learning to demonstrate learners' specific skills, knowledge, and practical experience relevant to their desired job roles.

By mapping the projects to accredited units of competency or certifications, the guide ensures that micro-credentials align with industry standards and requirements, further enhancing their recognition and value in the job market.

Furthermore, by incorporating this step of mapping projects to accredited units of competency, certifications, or other credentials, the guide provides a clear pathway for learners to have their practice-based learning recognised within formal training and certification systems. This recognition enhances the credibility and portability of their acquired skills, enabling them to progress in their educational and professional journeys with confidence.

Conclusion

The “Practice-Based Learning Guide” within the Network of Digital Excellence (NoDE) presents a holistic approach to digital skills development by aligning training components with digital skills standards.

This guide empowers learners, teachers, and training providers to navigate the process of practice-based learning effectively, ensuring that learners acquire the necessary skills for their desired job roles. By following the eight-step framework outlined in the guide, individuals can identify micro-credentials, skills clusters, and digital skills standards; acquire foundational digital skills, engage in job-aligned practice-based projects, receive facilitated training and just-in-time learning; and benefit from monitoring and support tools. Furthermore, the guide enables the mapping of projects to accredited units of competency and certifications, providing learners with tangible recognition for their achievements.

Overall, the “Practice-Based Learning Guide” serves as a valuable resource in the digital skills development landscape, promoting the acquisition of relevant and practical skills that meet industry demands and prepare individuals for success in the ever-evolving digital workforce.

References

- AIIA. (2023). AIIA Survey Digital State of the Nation 2023. Canberra: AIIA.
- Kudryashova, E., & Chankova, S. (2020). Scenario-based learning: A review of the literature. 13th International Conference on Education and New Learning Technologies (EDULEARN20), (pp. 8653–8662.).

DIGITAL SKILLS ORGANISATION

Process in Practice, End-To-End Implementation

Digital Skills Organisation June 2023

NODE NETWORK OF DIGITAL EXCELLENCE

Table of Contents

Executive Summary

This paper provides a comprehensive overview of the employer-led co-designing of training solutions introduced in Paper 2 of this NoDE series, Six Steps for Employer Co-Designed Training Solutions, as demonstrated in the Canberra Cyber Pilot and the Cremorne Software Development Pilots. The document outlines the step-by-step approach the Digital Skills Organisation (DSO) and its partners take in executing the co-design process for these projects.

By showcasing examples and outcomes, the paper highlights the successful implementation of each step in the design process, emphasising the holistic implementation of all six steps in the Canberra and Cremorne projects. This paper guides organisations and stakeholders interested in leveraging employer-led co-design methods to develop effective training solutions in the digital skills landscape.

Introduction

This paper delves into the experiences of DSO in implementing its step by step process for employer co-design training solutions within two significant DSO pilots: the Canberra Cyber Pilot and the Cremorne Software Development.

The Cremorne project was the first undertaking, providing valuable insights and learnings regarding the co-design process. Building upon this foundation, the Canberra project served as a comprehensive demonstration of all six steps within the NoDE framework. Throughout the paper, examples and outcomes from both projects are presented to showcase the successful application of employer-led co-design process.

Process in Practice, End-To-End Implementation

1. Canberra Cyber Project – Cyber Security

1.1. Overview

Current pilot status

A co-designed solution is currently undergoing testing through an internship program, which involves the active participation of the Canberra Institute of Technology, Risk2Solutions, ACFA, and MaxMe. This initiative is sponsored by the Canberra Cyber Hub.

Background and rationale

In April 2021, the ACT Government committed to establishing the Canberra Cyber Hub (CCH) to strengthen and support the emerging Canberra cyber security ecosystem and to help close the cyber security skills and labour gap:

- Local research indicated that 18,000 cyber security experts will be required in Canberra in the next 4 years;
- In addition, many existing cyber security professionals and providers work in isolation, which means there is a lack of consistency across the industry.

The CCH is also dedicated to working with industry and other stakeholders to help position Canberra as the preeminent destination for talented individuals to establish and build a career in cyber security, as well as highlighting the talent, capability and innovative technology on offer at the companies that are already established in the region.

In August 2021, the CCH formally partnered with DSO to help employers close the skills gap, with a primary focus on supporting current and aspiring cyber security professionals in Canberra to develop the skills required to pursue higher competencies in cyber security and advance their career pathways.

Purpose

For DSO, the purpose of the pilot was to build a dynamic and sustainable employer engagement and training model which meets local industry needs today and in the future, in order to:

- Increase the supply of skilled workers in cyber security in Canberra; and
- Create a model that can be replicated nationally to help alleviate the national skills shortage across the cyber security sector.

Scope

The scope of the project, "Closing the Cyber Gaps in Canberra," involved a collaborative effort between the Digital Skills Organisation (DSO) and the Canberra Cyber Hub, with a specific focus on addressing the rapidly growing demands of the cyber security sector in the region. The project aimed to establish a 'Network of Digital Excellence' that brought together employers and training providers in the Canberra region to create targeted and effective training solutions for supporting the cybersecurity workforce in Canberra.

The project involved:

- Articulating and defining the Cyber Security Skills Pathway for an in-demand job type (later agreed as Cyber Analyst);
- Defining the micro-credentials employees will need to meet the requirements of the in-demand job type and identifying the DSO skill clusters within those micro-credentials;
- Mapping existing training programs to those micro-credentials and identifying skills gaps in existing training programs; and
- Empowering employers to work with education providers to drive the design of formal training and support with work-integrated learning.

Location

Workshops and consultations were conducted on-the-ground at the Canberra Innovation Network offices (with some participants joining virtually).

Stakeholders involved

Facilitators	Local employers	Local RTOs/Training providers
• Canberra Cyber Hub • DSO • ACT Government	• Leidos • IBM • CBIT Digital Forensic Services (CDFS) • Accenture • AUKUS • Fifth Domain • Macquarie Telecom Group • Amazon Web Services (AWS) • Tesserent • Microsoft • Castlepoint Systems • Modern Methodologies • Cybermerc • National Institute of Strategic Resilience • Brand Rebellion • Emanate Technology • Department of Defence • Elbit Systems • Blue Eagle Technologies • Independent Tertiary Education Council of Australia	**Primary delivery partner:** • Canberra Institute of Technology (CIT) **Micro-credential skills standards "gap" providers:** • Risk2Solutions • Cybermerc • DDLS • ACFA • Maxme **Other Collaborators:** • UNSW Canberra • University of Canberrra • Australian National University • Modis • ACoP Education and Accreditation Portfolio • WithYouWithMe • TasTAFE • Australian Fraud and Anti-Corruption Academy • National Institute of Strategic Resilience • Ionize • CDFS • Australian Defence Force Academy

Learners

The program was opened to several learner groups including school-leavers, TAFE graduates, University graduates, career-changers, and others interested in a cyber security career.

Funding

All workshops were funded by DSO. The program implementation of the design solution is co-funded by DSO and Canberra Cyber Hub.

1.2. Key activities in design and delivery of pilot

1.2.1. Pilot Establishment

Process step	Activities led by DSO	Outcomes
Establishment of the CCH-DSO partnership *June – August 2021*	• Presentation to CCH and ACT Government on Cyber Security Skills Standards.	• Formal partnership established between CCH, DSO & ACT Government. • MoUs established with CCH and ACT Government.

1.2.2. Workforce Needs Analysis

Process step	Activities led by DSO	Outcomes
Data collection and stakeholder consultation to understand skills shortage in local cyber security sector *June 2021 – February 2022*	• Initial consultations with CCH and employers to confirm scope of workforce skills needs. • Weekly meetings with CCH (from October 2021). • Presentations to prospective employers about CCH's objectives (October 2021). • Preparatory workshop with CCH (November 2021). • Scan of local cyber security job advertisements (to quantify number and types of roles available). • Consultations with and surveys of employers, to identify most in-demand jobs in Canberra for cyber security and thus which 5-10 jobs DSO/CCH should focus on. The results of the survey to employers is given in **Figure 1**, **Figure 2**,and **Figure 3**.	• Employers agreed that the DSO Cyber Security Skills Standard is a good mechanism for aligning the Canberra training ecosystem and employers around a common framework and taxonomy of cyber security skills. • Prospective employers agreed to attend and participate in design workshops to develop a local cyber security training solution.

The Canberra Cyber Hub conducted a survey to collect employer requirements for cyber skilling. The table below presents an overview of the survey, including the questions asked and the tabulated answers. This valuable information has provided the project partners with insights into the high-demand jobs in Canberra, essential industry skills, and the preferred delivery methods.

Figure 1. *Canberra Cyber Employer Survey Data Analysis Part* 1.

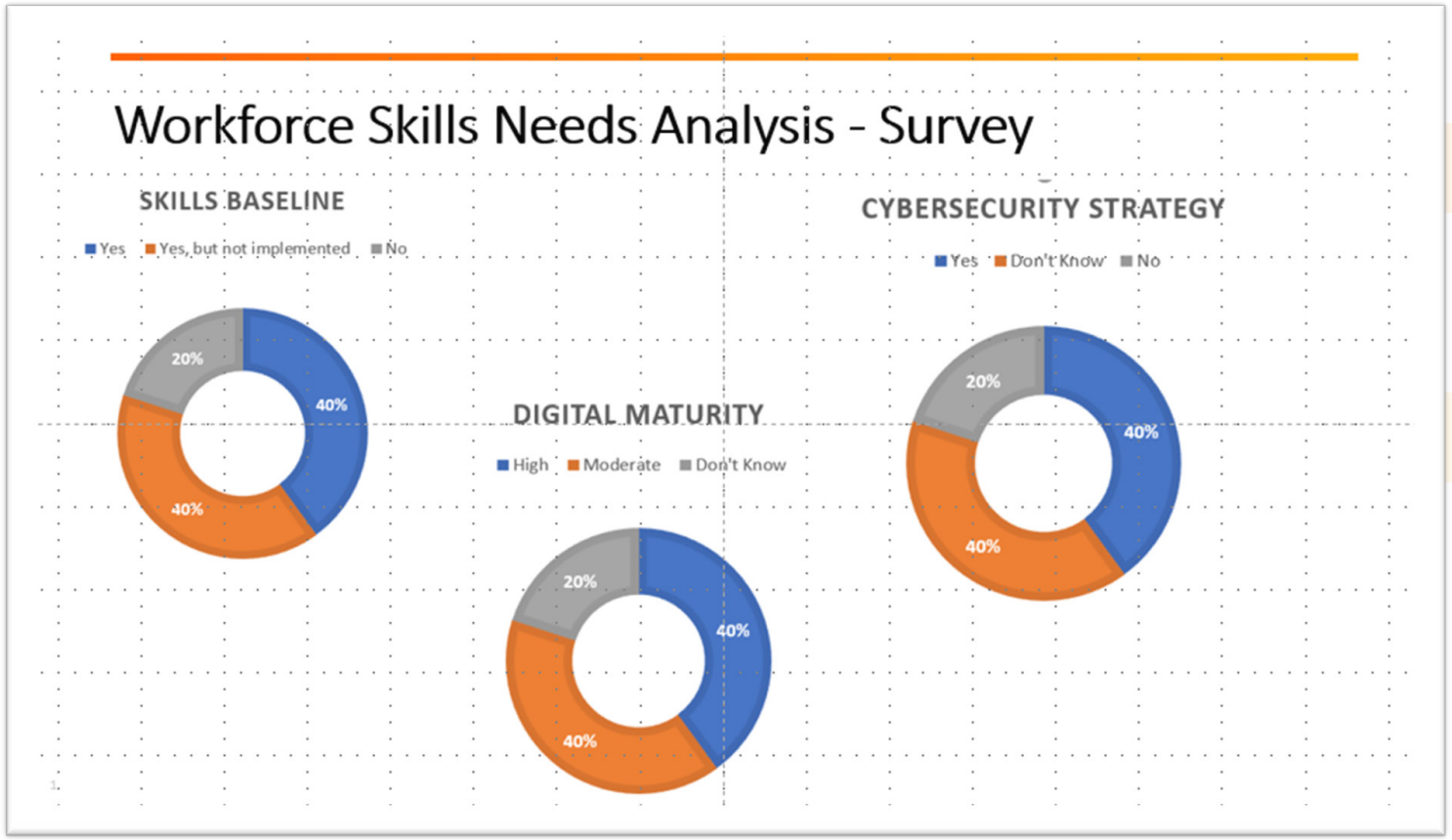


Figure 2. *Canberra Cyber Employer Survey Data Analysis - Part 2.*

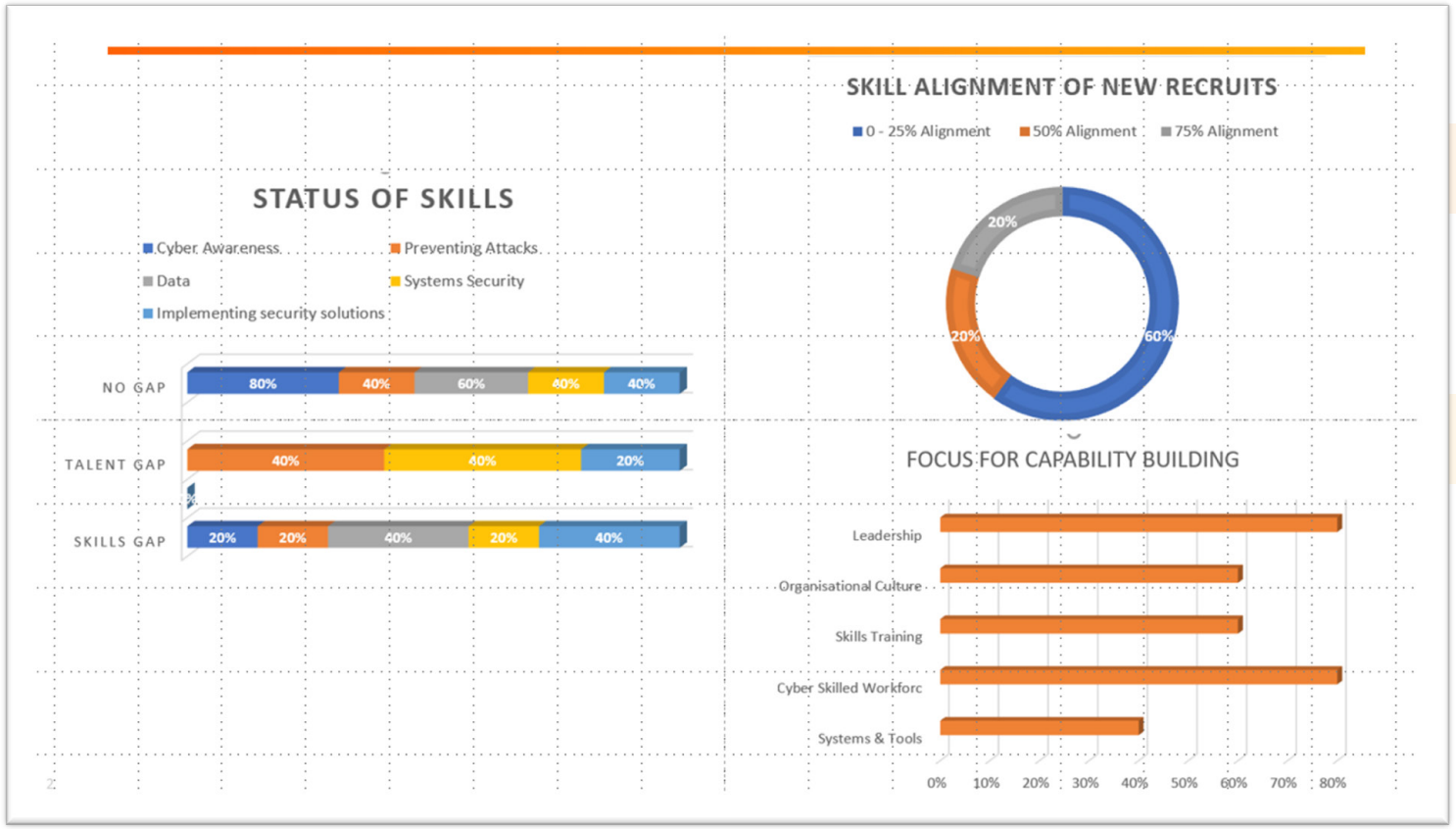
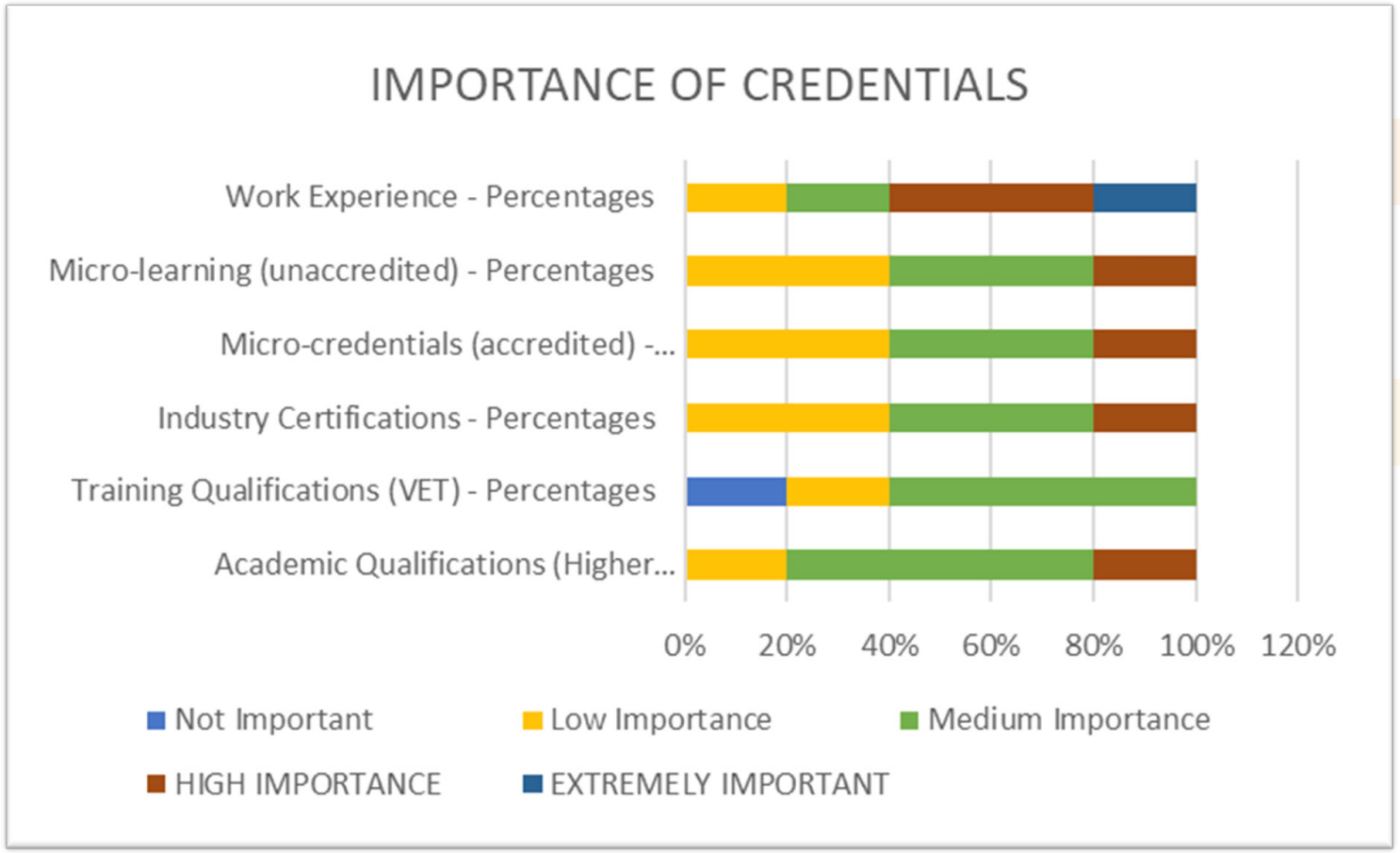


Figure 3. *Canberra Cyber Employer Survey Data Analysis - Part 3.*



1.2.3. Design Workshops

Process step	Activities led by DSO	Outcomes
Workshop 1: Training Strategy for Closing Skills Gaps in Canberra Creation of Cyber Security Skills Learning Pathway for in-demand cyber security jobs in Canberra Attended by CCH, DSO and Employers *28 May 2022*	• A brainstorming session was conducted to identify the job roles that were most in demand by employers for the Canberra Cyber NoDE. Results of a Mentimeter poll ran during the workshop is shown in **Figure 4**. • A deep dive analysis of the survey results was conducted on the cyber skills needs for the target learners, such as current and incoming employees, as well as labour shortages in specific job roles with high demand. This analysis was based on the findings from the Workforce Needs Analysis. • Group problem-solving was done to identify the specific digital skills that were most needed but not currently being met by existing education credentials.	• Target learners' specific digital skills needs were identified, including upskilling requirements for existing employees and the top 1-2 in-demand job roles from a shortlist of 5-10 roles, along with the major digital skills requirements for those top roles. • Skills clusters within job roles were identified through a job role analysis and a Miro board activity conducted during thew workshops (see **Figure 5**).

Figure 4. *Output from Canberra Employer Workshop.*

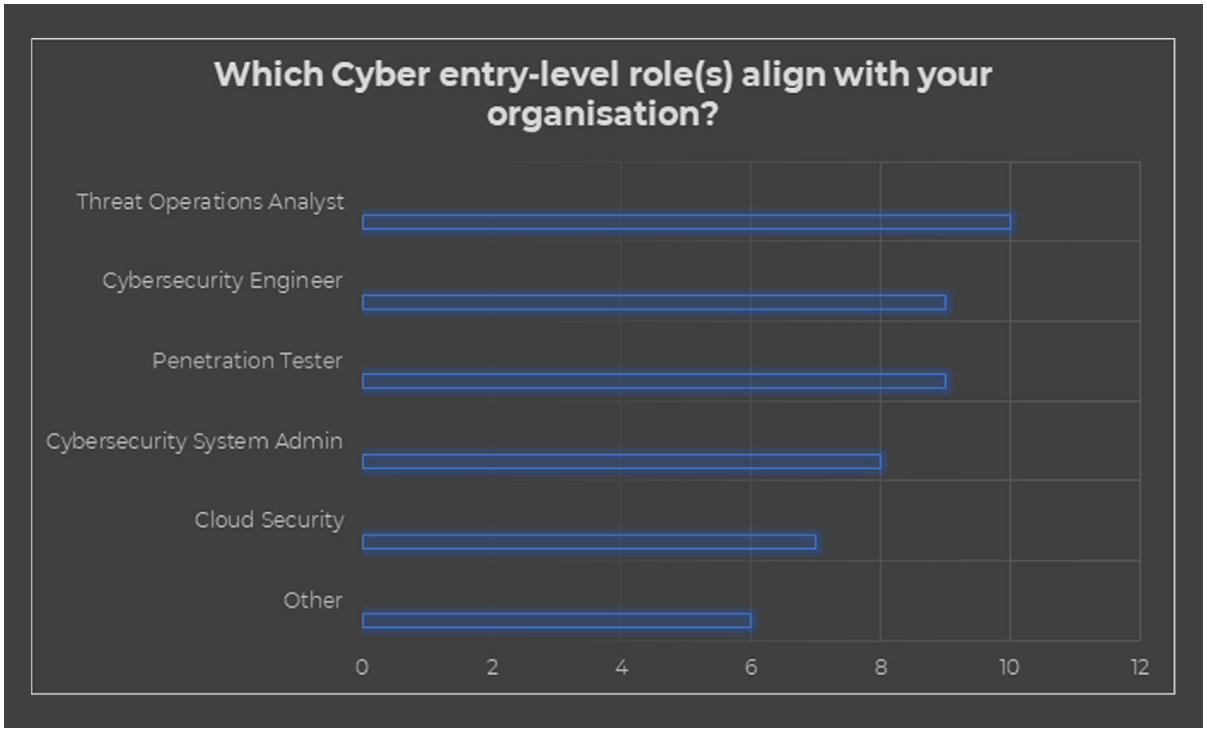


Figure 5. *Digital Skills Pathway Employer co-design.*

Skills Clusters				
		Penetration Testing	Threat Intelligence	Cyber Defense Analysis
		IT Infrastructure	Security Operations	Cyber Defense Infrastructure
	Continuity Management	Digital Forensics	Cyber Incident Response	Cyber Incident Response
		Penetration Testing	Vulnerability Assessment	Vulnerability Assessment
			Solution Architecture	Security Architecture
			Risk Management	Security Control
		Software Testing	Programming / Software Development	Cyber Development
		Emerging Technology Monitoring	Vulnerability Research	Technology Research and Development
	Security Administration	Information Security	Vulnerability Assessment	Information Systems Security
			Personal Data Protection	Compliance
	Strategic Planning	Information Security Governance	Specialist Advice	Strategy and Governance
Collaborate	Critical Thinking	Analytical Thinking	Problem Solving	Critical Core Skills
Decision Making	Emotional Intelligence	Communication Skills	Creative Thinking	

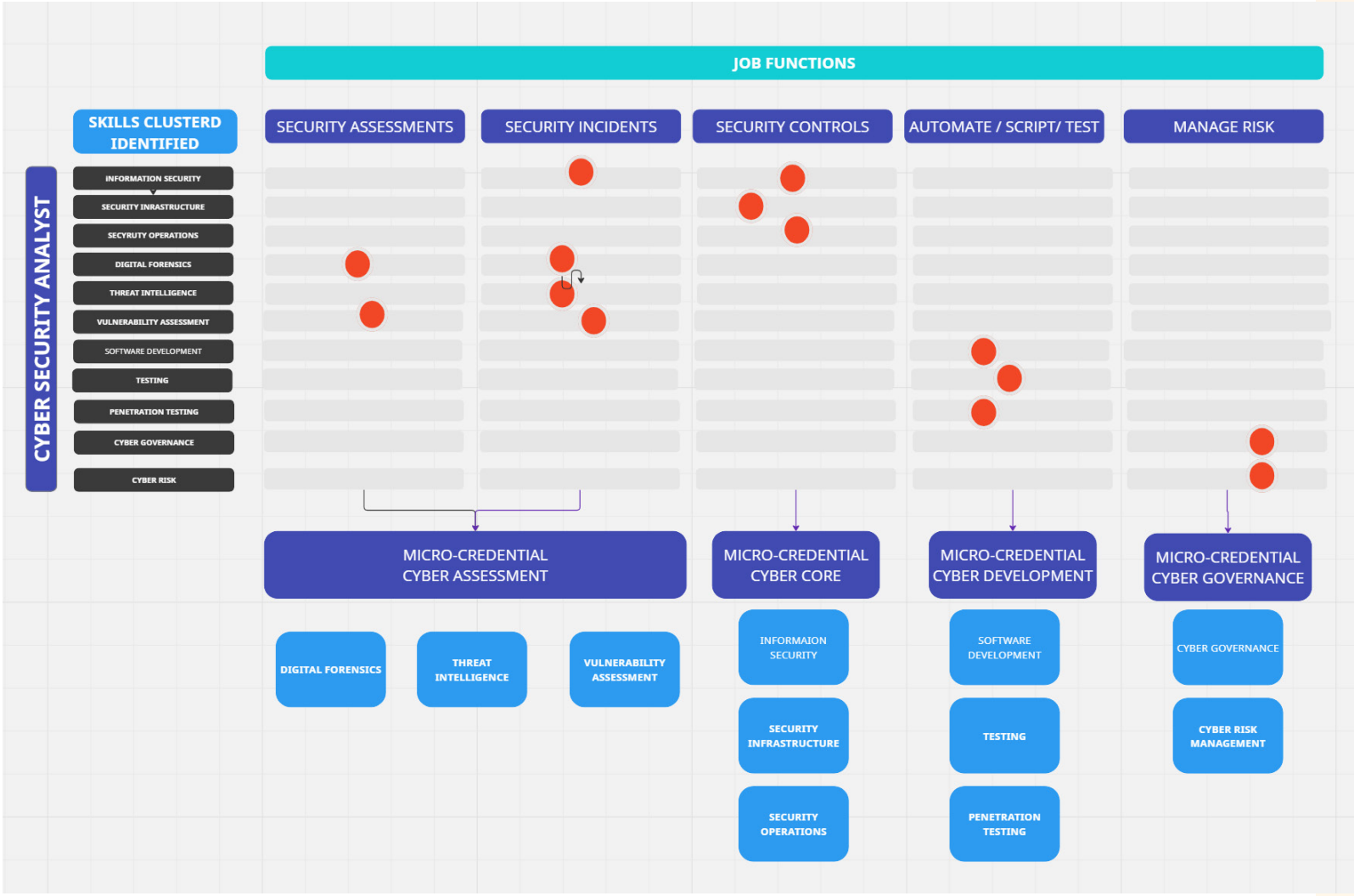
Cyber Analyst

Cyber Defense Analysis			Threat Intelligence
Cyber Defense Infrastructure	IT Infrastructure	Security Operations	
Cyber Incident Response		Digital Forensics	
Vulnerability Assessment	Penetration Testing	Vulnerability Assessment	
Security Architecture			
Security Control	Risk Management		
Cyber Development	Software Testing	Programming / Software Development	
Technology Research and Development			
Information Systems Security	Security Administration	Vulnerability Assessment	Threat Intelligence
Compliance			
Strategy and Governance	Information Security Governance	Specialist Advice	
Critical Core Skills	All Critical Core Skills		

Process step	Activities led by DSO	Outcomes

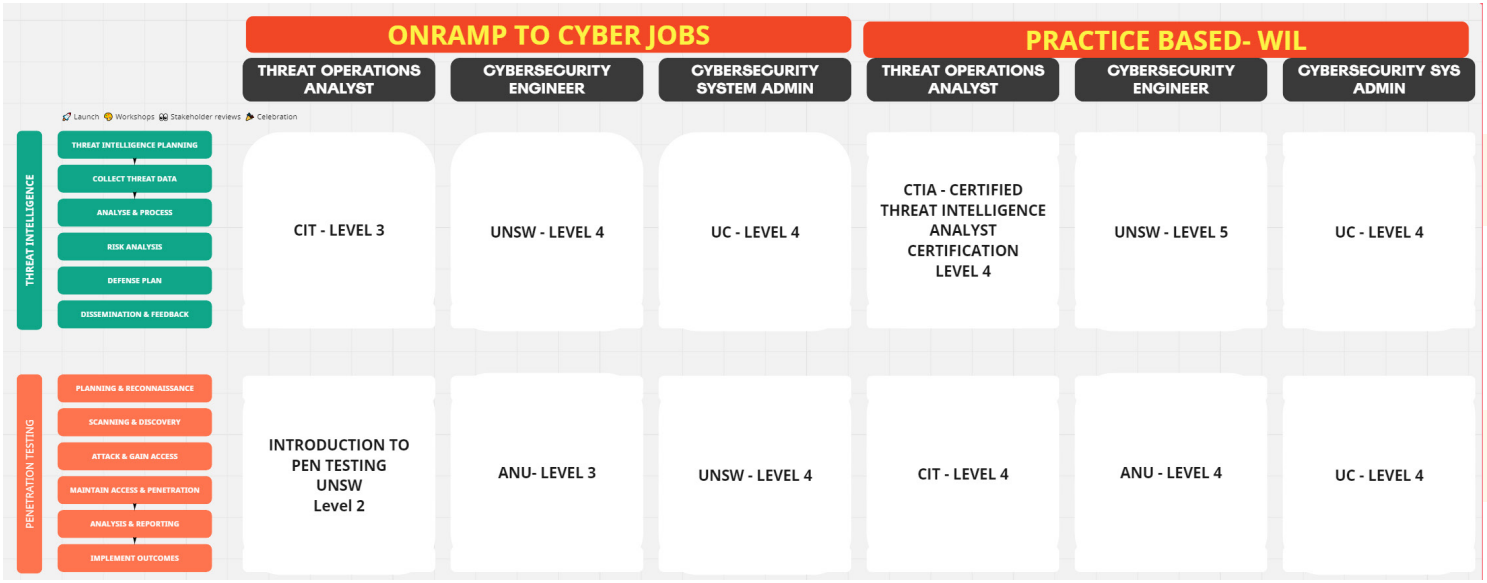
Workshop 2: Digital Skills Learning Pathways
16 June 2022
	• Using the guidelines for establishing the micro-credentials, the workshop groups the skills clusters for cyber analyst job role into Micro-credentials. Miro Board activity that was used to aggregate skills into Micro-credentials in shown in **Figure 6**.	• Framework of micro-credentials aligned to the skills required for cyber analyst job role.
		• The skills clusters that employers need to satisfy the Threat Operations Analyst role were identified and re-categorised into 4 specific micro-credentials:
		  • Security core
		  • Information security
		  • Security infrastructure
		  • Security operations
		  • Cyber assessment
		  • Threat intelligence
		  • Vulnerability assessment
		  • Digital forensics
		  • Cyber development
		  • Programming/software development
		  • Software testing
		  • Penetration testing
		  • Cyber governance
		  • Risk management
		  • Information security governance

Figure 6. *Co-design of Micro-credential-learning pathway.*



Process step	Activities led by DSO	Outcomes
Workshop 3: Work-integrated Training and Assessment Approach This objective is to ensure that learners are able to apply their skills in real-world scenarios and effectively solve problems that they will face on the job. **Participants:** Training providers (CIT, UNSW, UC, ANU, Lumify, Risk2Solutions, ACFA) Pilot Sponsor: Canberra Cyber Hub *22 June 2022*	**Training and Assessment Strategy:** • Develop and implement an ONRAMP approach for entry-level learners, which includes foundational training, hands-on exercises, and job shadowing opportunities. • Adopt a Work Integrated Digital Skilling Approach that combines formal training with on-the-job training and practice-based learning to develop skills needed for the specific job role of a Cyber Analyst. • Initial brainstorming activity shown in **Figure 7** was used to map existing training programs to identified micro-credentials.	• Determination of ONRAMP format and duration, a model for accelerating digital foundations training to prepare learners for job roles. *Outcome: Cyber Foundations Skills Accelerator Bootcamp.* • Adoption of a work-integrated training approach, utilising a practice-based approach for skill development and a just-in-time training approach for structured learning. *Outcome: Internship Model.* • Adoption of a hybrid micro-credential model, offering a range of accredited and non-accredited options including Higher Education and Industry Certifications. *Outcome: To be consulted with individual training providers to confirm availability, capacity, and capability.*

Figure 7. *Initial brainstorming and mapping.*



1.2.4. Training Solution Development

Process step	Activities led by DSO	Outcomes

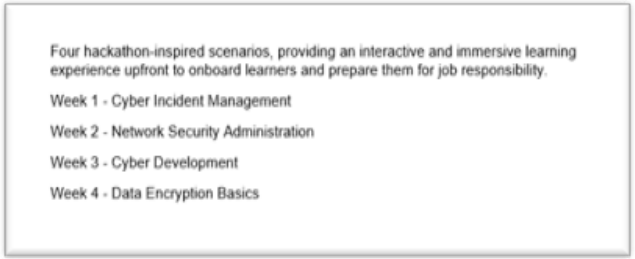
Consultation process with training providers regarding capability to meet Skills Standards for the Skills Clusters comprising each micro-credential
July – September 2022
	• DSO reviewed CIT's post-workshop proposal to meet the requirements for accredited micro-credentials and identified areas where the curriculum needed improvement.
	• DSO examined the library of CIT courses to find existing courses that could fill the gaps in thea curriculum to meet the accredited Skills Standards requirements for each micro-credential.
	• DSO consulted with and shortlisted other training providers capable of offering training that addresses the non-accredited components of the Skills Standards gaps. This process involved:
	  • Sending curriculum surveys to training providers.
	  • Independently evaluating course content from various training providers.
	  • Identifying training providers with existing course content that best aligns with the Skills Standards gaps.
	  • Collaborating with training providers to create new content required for work-integrated learning components, such as:
	  • Designing an assessment rubric for an essay on an employer's cyber security operations.
	  • Creating an assignment on handling cyber incidents that can be adapted for different employers. This assignment requires trainees to identify cyber incidents, handle tickets, and report them to the appropriate person in the employer's cyber security team.
	  • Developing an assignment on cloud security management, where trainees' abilities to set up a cloud, maintain access privileges, and provide other authorizations are assessed by their employers.
		• On-ramp and work-integrated learning (and respective training providers) for each micro-credential mapped and finalised by DSO
		  • Output ONRAMP - Cyber Skills Foundations Accelerator Bootcamp
		 
		Four hackathon-inspired scenarios, providing an interactive and immersive learning experience upfront to onboard learners and prepare them for job responsibility.
		Week 1 - Cyber Incident Management
		Week 2 - Network Security Administration
		Week 3 - Cyber Development
		Week 4 - Data Encryption Basics
		• Training solution that was derived at the end of this workshop is available in **Table 1** below.

Table 1. *Output of Workshop - Training Solution Development.*

Micro-Credentials	Skills Clusters	Training Program Details	Type Of Training	Provider
Security Core	Information Security	ICTCYS403 Plan and implement information security strategies for an organisation	Accredited	Canberra Institute of Technology (CIT)
	Security Infrastructure	VU23218 - Implement network security infrastructure for an organisation	Accredited	CIT
	Security Infrastructure	ICTCLD401 - Configure cloud services	Accredited	CIT
	Security Infrastructure	VU23220 - Develop and carry out a cyber security industry project	Accredited	CIT
	Security Operations	Security Operations	Non-Accredited	Risk2Solutions
	Security Fundamentals	CompTIA Security+	Industry Certifications	Lumify
	Human Skills Resource	Problem Solving, Communication, Teamwork, Analytical Thinking	Non-Accredited	Maxme
Cyber Assessments	Threat Intelligence	ICTCYS407 Gather, analyse and interpret threat data	Accredited	CIT
	Vulnerability Assessments	VU23222 - Expose website security vulnerabilities	Accredited	CIT
	Digital Forensic	VU23221 - Evaluate and test an incident response plan for an enterprise	Non-Accredited	ACFA
	Security Fundamentals	CompTIA Security+	Industry Certifications	Lumify
	Human Skills Resource	Problem Solving, Communication, Team work, Analytical Thinking	Non-Accredited	MaxMe

Micro-Credentials	Skills Clusters	Training Program Details	Type Of Training	Provider
Cyber Development	Programming	ICTPRG434 - Automate processes	Accredited	CIT
	Testing	ICTPRG433 - Test software developments	Accredited	CIT
	Pen Testing	VU23215 - Test concepts and procedures for cyber security	Accredited	CIT
	Pen Testing	Ethical Hacker Course	Non-Accredited	Lumify
	Security Fundamentals	CompTIA Security+	Industry Certification	Lumify
	Human Skills Resource	Problem Solving, Communication, Team work, Analytical Thinking	Non-Accredited	MaxMe
Cyber Governance	Cyber Governance	Information Security Governance	Non-Accredited	ACFA
	Risk Management	Cyber Risk Management	Non-Accredited	Risk2Solutions
	Security Fundamentals	CompTIA Security+	Industry Certification	Lumify
	Human Skills Resource	Problem Solving, Communication, Team work, Analytical Thinking	Non-Accredited	MaxMe

1.2.5. Implementation Workshops

Process step	Activities led by DSO	Outcomes

Workshop 4: Finalisation of training and assessment strategy
Attended by CCH, DSO, and training providers
28 October 2022
	• Testing on-ramp and work-integrated training curriculum with training providers
	  • E.g., presenting flowchart with chronology of courses for each micro-credential, including pathways towards industry certifications or exit-points where trainees can opt out of next micro-credential.
	• Whiteboarding to build delivery framework (e.g., timelines, dates, modality of course delivery)
	  • E.g., each training provider presents course content, duration of training and assessment plan for their respective courses.
	• Discussion regarding assessment strategy, certifications of competency, and other potential qualification options
	  • E.g., AWS industry certification for Cloud Security.
	• Discussion regarding funding model for additional certifications.
		• Sign-off from training providers on training plan, assessment plan and delivery plan
		• Stakeholders agree to assigned responsibilities for content delivery (e.g., for Cyber Core micro-credential, CIT will deliver 4 units of competency (network security, cyber security operations, implementation of cyber security operations, and cyber security response), and Risk2Solutions will deliver 2 units (network infrastructure, networking and systems; and analysis of cyber security events and how to deliver cyber security operations).
		• Stakeholders agree to course funding responsibilities.

Workshop 5: Sign-off on micro-credential solution
Attended by CCH, DSO, and employers
10 November 2022
	• Presented micro-credential training plan and on-ramp delivery plan for Cyber Analyst to employers
	  • Employers were given two options to consider: Option 1 (6.5-month program with 5 months in the workplace) and Option 2 (7-month program with 5.5 months in the workplace).
	• Employers were asked to indicate the number of trainees/ graduates they can accommodate.
	• Employers were asked to finalise the work-integrated Digital Skilling Strategy.
		• Employers provide formal expressions of interest to participate in the pilot and indicate the number of graduates/trainees they can accommodate.
		• Employers align on work-integrated learning curriculum and how it fits into the broader work responsibilities of trainees.
		• Employers agree on time commitments required for work-integrated learning components of each micro-credential.
		• Employers decide on preferred on-ramp learning timeline for trainees
		  • E.g., employers determine which baseline on-ramp micro-credentials are needed before commencing work vs. on-ramp micro-credential components that can be taught concurrently with traineeship.

1.2.6. Program Implementation and Management

Process step	Activities led by DSO	Outcomes
Documentation of solution design	• Codification of agreements between training providers and employers. • Solution design documentation includes the codification of agreements between training providers and employers. Additionally, the creation of the Practice-based Project Learning Kit aims to align with all skills clusters within the four micro-credentials. To ensure implementation, signed agreements have been established with training providers and employers.	• Signed agreements with training providers and employers. • The Practice-Based Project Learning Kit has been converted into SCORM packages and uploaded to the Learning Management System of all partner training providers.
Roll-out of training pilot program	• DSO provides implementation plan to CCH to enable CCH to independently run pilot (including training provider agreements, advice on resource planning, and program promotion). • CCH aligns training providers post-workshops and manages resources for pilot program.	• DSO and CCH jointly spearheaded the program's implementation. DSO took the lead in demonstrating the implementation of the Bootcamp and Micro-credential 1, while CCH assumed the responsibility for overseeing the remainder of the project in collaboration with an appointed training manager.
Review and evaluation of pilot program	• DSO reviews outcomes from pilot program and collects feedback from micro-credential graduates and employers.	• Iteration on DSO Cyber Security Skills Standards according to findings.

1.3. Certification / accreditation approach

Learners who undertake the Cyber Analyst learning pathway will be eligible for 4 different types of certification/accreditation:

1. DSO endorsed badge for Achievement of Digital Skills Standards

- Accessible through the Learning Vault Platform
- Awarded on completion of each Skills Cluster, Micro-credential and overall completion of Digital Skills Pathway for Cyber Analyst

2. Statement of completion by each training provider

- Each training provider credentials their own programs

3. Completion of practice-based work-integrated digital skilling project

- Summative assessment contributing to delivery by all training providers
- Industry certifications are an option

1.4. Outcomes and key learnings

Key learnings

- Create upfront draft documents ahead of workshops: e.g., Digital Skills Pathways based on findings from Workforce Needs Analysis to present at Design Workshops.
- For future pilots, it would be more expedient for DSO to draft out the initial Digital Skills Pathways and Learning Pathways and then get pathways verified by experts.
- Verified draft pathways can then be used to guide the thinking of workshop attendees (especially employers), rather than encouraging workshop attendees to draft out pathways from scratch without having prior experience doing so.
- DSO ultimately guides and directs this process anyway, and given the limited time available in the workshops, the focus should be on iterating and expanding upon pre-verified draft pathways instead.

- When inviting employers and training providers to attend workshops, DSO should provide a role/expertise description for attendees, to help employers/training providers identify the best representative from within their organisation to attend workshops.
- E.g., participants in the first employer Design Workshop should be ICT professionals who understand the technical requirements of specific jobs and workforce skill needs.
- E.g., participants in the second employer Design Workshop should be senior managers who are able to make organisational decisions.

Artifacts

- Digital Skills Standards for Cyber Security (9 standards)
- Capstone assessment rubrics
- Assessment guidance
- Guidelines and support documentation for work-integrated learning (in development)

2. Cremorne – Software Development

2.1. Overview

Background and rationale

Cremorne is emerging as Victoria's newest and fastest growing technology precinct, with over 700 businesses and 10,000 workers. To power their continued growth, the employers at Cremorne share a common need for talent with relevant digital and technology skills, and in particular, software development skills.

In June 2021, DSO partnered with the Kangan Institute to formalise a collaborative pilot project to address the growing digital skills shortage in the Cremorne area, through targeted digital skills traineeships. In September 2021, DSO launched their first series of design workshops with the Kangan Institute and participating technology employers in the Cremorne area, including Carsales.com, LiveTiles, REA, InfoXchange and MYOB. Kangan Institute then launched their own pilot program (with DSO support).

Purpose

The objective of the pilot was to develop a sustainable, employer-led talent pipeline to create a digitally upskilled, job-ready workforce in Cremorne.

This would be achieved through a bespoke learning program, which would include:

- A doctrinal, cohort-based training program using real-world scenarios; and
- A work-integrated-learning-based traineeship with "on-the-job" experience.

Scope

The original scope of the project involved:

- Creating a 'Network of Excellence' between employers and training providers in the Cremorne area;
- Co-designing an entry-level skills development pathway with employers based on the skills needed to perform an in-demand job (later agreed as Software Development);
- Validating whether learner outcomes were achieved through consultation with students and industry partners (e.g., checking completion rates, surveying learner and employer satisfaction with programs)

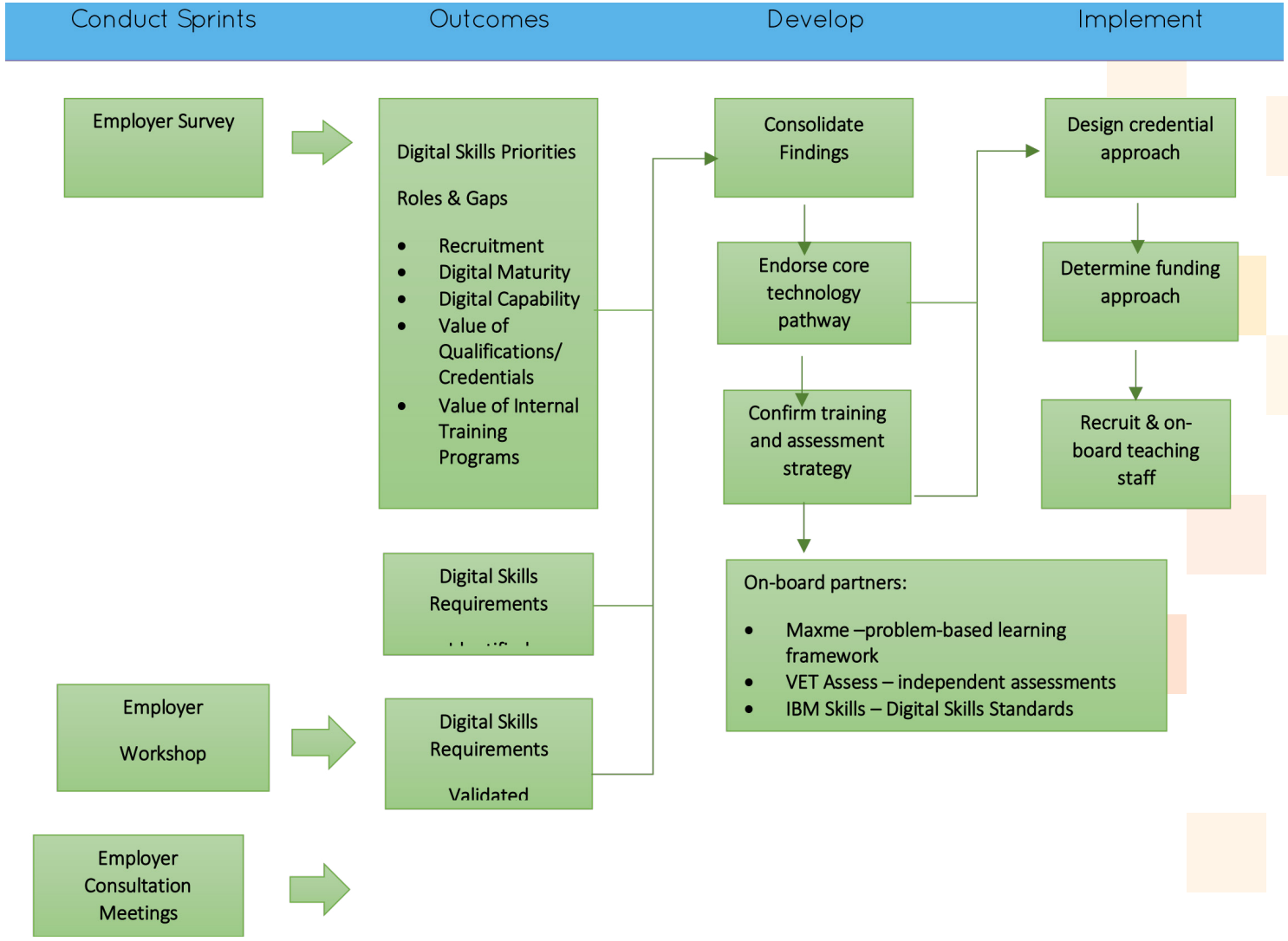
Location

Workshops and consultations were conducted both online and on-the-ground at the Cremorne Digital Hub precinct at the Kangan Institute.

Stakeholders involved

Facilitators	Local employers	Local RTOs/Training providers
• Kangan Institute of TAFE • DSO	**Local tech employers:** • REA Group • InfoXchange • MYOB • LiveTiles • Carsales.com	**Primary training delivery provider:** • Kangan Institute of TAFE

2.2. Overall process methodology



2.3. Key activities in design and delivery of pilot

2.3.1. Pilot Establishment

Process step	Activities led by DSO	Outcomes
Establishment of the Kangan-DSO partnership *June 2021*	• Presentation to Kangan Institute on DSO Model.	• Formal partnership established between Kangan Institute and DSO – MOU Signed.

2.3.2. Workforce Needs Analysis

Process step	Activities led by DSO	Outcomes
Data collection and stakeholder consultation to understand digital skills shortage in local tech sector *July — August 2021*	• Initial consultations with Kangan Institute and employers to confirm scope of workforce skills needs. • Weekly meetings with Kangan Institute (from July 2021). • Presentations to and expressions of interest sought from 7 prospective employers. • Preparatory workshop with Kangan Institute (August 2021). • Scan of local digital job advertisements (to quantify number and types of roles available). • Consultations with and surveys sent out to 20 employers to identify most in-demand digital jobs in Cremorne, and which 5-10 job types DSO and Kangan Institute should focus on.	• Employers agreed that creating a DSO Digital Skills Standard for in-demand digital job types would be a good mechanism for aligning the Cremorne training ecosystem and employers around a common framework and taxonomy of digital skills (applicable DSO Skills Standards had not been developed at this time). • Prospective employers agreed to attend and participate in design workshops to develop a local digital skills training solution.

2.3.3. Design Workshops

Process step	Activities led by DSO	Outcomes

Workshop 1: Identification of most in-demand digital skills needed for Cremorne workforce
Attended by Kangan Institute, DSO, and employers
September 2021
	• **Activity 1:** Employers shortlisted the most in-demand digital jobs within their operations which require specialised training.
	• **Activity 2:** Problem-solving with employers to identify the specific technical and enterprise skills needed from employees to succeed in in-demand roles.
	• **Activity 3:** Employers provided feedback on their preferred training models.
		• **Activities 1 and 2:** Employer skills needs identified – shortlisted critical digital skills clusters.
		  • Software Development identified as the job role for the pilot, to be aligned to a Diploma in Information Technology.
		  • However, Cremorne employers were more focused on developing soft skills (e.g., teamwork) than technical skills (which they believed they were capable of teaching themselves).
		• **Activity 3**: Preferred employer training model identified:
		  • Shorter, just-in-time on-ramp training model to precede traineeship.
		• Learning programs to be sequenced.

Workshop 2: Creation of Digital Skills Pathway for in-demand software development jobs in Cremorne, and preliminary discussions on training strategy, delivery and assessment approach
Attended by Kangan Institute, DSO, employers, and training providers
September 2021
	• Employers mapped SFIA Skills to Digital Pathways (e.g., software engineer, dev-ops engineer, data analyst, UX developer/designer, cloud engineer, developer/programmer)
	• Problem-solving with training providers to identify relevant courses available
	• Analysis and discussion concerning the education requirements (i.e., duration, qualifications needed) for the relevant skills clusters identified
		• Draft solution identified potential curriculum content and training models that could be used to satisfy employer needs
		• Employers agreed that industry must support training initiatives to increase the supply of entry-level workers with software development skills
		• Employers agreed-in-principle that they would offer work-integrated learning-based traineeship positions after trainees undertake initial on-ramp training
		• Employers agreed that they would trial graduates of proposed learning program as trainees.
		• DSO proposed to develop Software Development Skills Standards, which could be used to inform the training program.
		• Kangan Institute and training providers agreed to mapping components of their existing course content to the skills clusters discussed in Workshops 1 & 2
		• Preliminary alignment between stakeholders concerning:
		  • Assessment guidelines;
		  • Training delivery (breakdown of on-ramp vs. work-integrated); and
		  • Talent pipeline capacity (e.g., paid or unpaid internship model, traineeship program, employment-after-graduation)

2.3.4. Training Solution Development

Process step	Activities led by DSO	Outcomes	Status

Consultation process with Kangan Institute and training providers regarding scope of skills training and qualifications required
October 2021 — January 2022
	• Individual meetings with 3 individual employers to validate outcomes from workshops.
	• DSO created new Skills Standards for Software Development.
	• DSO mapped several Skills Clusters to core and elective units of competency in:
	  • ICT40120 – Certificate IV in Information Technology; and
	  • ICT50220 – Diploma of Information Technology; but this mapping wasn't used
	• Discussions with Kangan Institute on scope of training required to accommodate employer needs.
	Decision-making process regarding:
	  • Accredited vs. non-accredited courses
	  • VET/RTO provider vs. other training provider
	  • Duration of course and traineeship
	  • Curriculum mapped to DSO Skills Standards vs. other skill metrics (i.e., VET metrics)
	  • On-ramp training vs. work-integrated learning.
		Training program design completed:
		• 2-month bootcamp and 1-year traineeship, resulting in Certificate IV and Diploma in IT.
		• Due to different needs, Kangan Institute elected to use a different model to DSO's proposed solution: they preferred an accredited training program backed by government funding instead of the micro-credentialing model based on DSO Software Development Skills Standards.
		  • Their proposed bootcamp solution was not based on DSO Skills Standards but based on units of competency from training packages authorised by government (however some of DSO's content and approach was integrated into the final program).
		• Kangan Institute chose pre-traineeship on-ramp bootcamp to be:
		  • 6-week face-to-face bootcamp and online training content (unaccredited)
		  • 6-month Certificate IV in Information Technology (accredited).
		• Funding model finalised and communicated with employers.
			In progress

2.3.5. Implementation Workshops

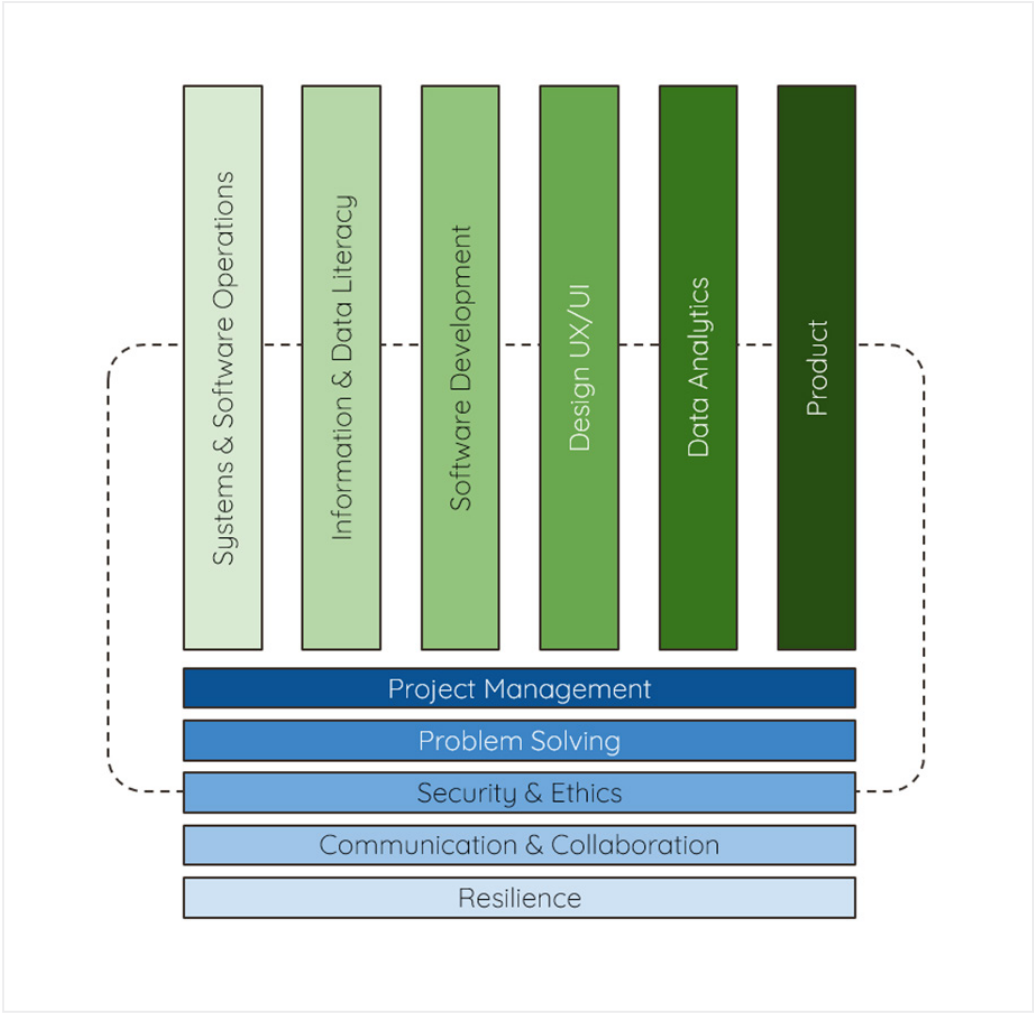
Process step	Activities led by DSO	Outcomes	Status
Workshop 3: Finalisation of Digital Skills Training Pathway and Assessment Strategy Attended by Kangan Institute, DSO, and training providers *February 2022*	Testing on-ramp and work-integrated training curriculum with training providers: • E.g., presenting curriculum, delivery model, and assessment guidelines. • Discussion regarding funding model for additional certifications.	• Sign-off from training providers on training plan, assessment plan, and delivery plan. • Completed workplace supervision, training, assessment and mentoring toolkit. • Developed recruitment Plan.	Complete
Workshop 4: Sign-off on Training Solution Attended by Kangan Institute, DSO, and employers *February 2022*	• Presented complete learning program to employers. • Employers indicated number of trainees/ graduates they can accommodate.	• Employers provided formal expressions of interest to participate in the pilot and indicate number of graduates/trainees they can accommodate. • Employers agreed to support work-integrated learning and understood how it fits into the broader work responsibilities of trainees. • Employers agreed on time commitments required for work-integrated learning components of learning program. • Assessment modes and associated programs finalised and approved.	Complete

2.3.6. Program Implementation and Management

Process step	Activities led by DSO	Outcomes
Documentation of solution design	• Codification of agreements between training provider and employers.	• Signed agreements with training provider Kangan Institute and employers.
Roll-out of training pilot program	• Kangan Institute leads implementation process • DSO provides implementation plan and advice to Kangan Institute (including training provider agreements, resource planning, and program promotion).	• Kangan Institute aligns training providers after workshops and manages resources for pilot program. • A bootcamp based on the Certificate IV has commenced and concluded in 2022. This will lead into work-integrated learning with the Diploma of Information Technology.
Review and evaluation of pilot program	• DSO reviews outcomes from pilot program and collects feedback from traineeship graduates and employers.	• The Cremorne project's DSO evaluation was incorporated into the DSO's final evaluation report.

2.4. Digital Skills Pathway

Digital Skills Pathway co-developed with DSO, focusing on software development skills clusters within Security and Ethics.



2.5. Learning pathway, assessment, and micro-credentialing models

Learning pathway

- On-ramp training delivers the necessary digital skills.
- Learning was sequenced as per the traditional Certificate IV in Information Technology (Programming) delivery.

Assessment

- Traditional Assessment model for Certificate IV Information Technology qualification.

Micro-credentialing model

- N/A.

2.6. Certification / accreditation approach

- Upon successful completion of the bootcamp, students are awarded a Certificate IV in Information Technology (ICT40120).
- Upon successful completion of the traineeship, students are awarded a Diploma of Information Technology (ICT50220).

2.7. Outcomes and key learnings

Key Learnings

- RTOs face more challenges when designing programs to meet employer needs, due to funding constraints (e.g., funding requires course accreditation). Non-RTOs can rapidly develop and scale bespoke programs without the same constraints.

Artifacts

- Digital Skills Standards and Assessment Rubric for Software Development.
- Design Workshop process (which informed the methodology used for other pilots).
- Skills-based capability framework built out into an implementation framework.

Conclusion

The employer-led co-design approach has proven to be a valuable and effective method for developing training solutions in the digital skills landscape. The experiences gained from the Cremorne and Canberra projects highlight the importance of collaboration between employers, industry experts, and training providers to ensure the relevance and effectiveness of the training solutions.

By following the six-step process outlined in the NoDE framework, organisations can achieve successful outcomes in their co-design efforts. The artifacts produced and the outcomes of co-design activities showcased in this paper demonstrate the tangible results that can be achieved through this collaborative approach.

Moving forward, it is essential for organisations to embrace and adapt employer-led co-design methods to meet the evolving demands of the digital workforce. Through continued collaboration and implementation of these methodologies, we can ensure the development of training solutions that align with industry needs, maximise learner outcomes, and drive overall success in the digital skills landscape.