SEA-VET.net
TVET Platform for SEA

SEA-VET.NET - GOOD PRACTICE

3u1i Experiential Work-based Learning (WBL):

Developing Cybersecurity Skills and Competencies for Industry Readiness

August 2026

Layout by :
SEA-VET.NET

Photos :
©Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA)

OVERVIEW

Implementing institution(s)	Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA)
Country and / or localities where practice has been implemented	Pahang, Malaysia
Timeline (first year of implementation - last year of implementation)	2022 - ongoing
Target group	Undergraduate students enrolled in Bachelor of Computer Science (Cybersecurity) with Honours program
Total cost incurred / Resources required	Existing staff & resources / 3 labs fully equipped with cybersecurity software & tools with virtual machines (VM) to support the core program courses.

INTRODUCTION

Artificial intelligence is rapidly redefining cyber threats and defenses worldwide and transforming career growth, multiskilling and new job creation in the field of cybersecurity. This has led to the prioritization of critical skill gaps over mere headcount shortages (ISC2, 2025).

Cybersecurity skills shortages and gaps could be addressed through higher education working closely with industry to plan structured, experiential, and hands-on curriculum that focuses on real emerging cybersecurity needs and hyper-accelerated nature of digital threats (Crawford, 2025).

THE PRACTICE

Context

The 3u1i program (also in other variations such as 2u2i) in Malaysian higher education is a work-based learning mode in which students spend three years studying at a university and one full year gaining hands-on experience working in industry. The program's primary goal is to enhance local graduate employability by making students industry-ready.

Aims

A persistent challenge in higher education is bridging the gap between academic theory and dynamic industry requirements. Thus, the Cybersecurity 3u1i Work-based Experiential Learning aims to provide a transformative, experiential learning approach in which students spend 3 years in university studying jointly formulated subject areas with industry partners, mapped to MBOT standards and cyber professional certifications, and a year immersed in cybersecurity firms. The primary goal is to develop industry-specific skills, enhance graduate employability, and provide a "learn and earn" opportunity for students.

Implementation of the Practice

3u1i Experiential WBL

The curriculum structure for the course programme (see Figure 2) entails:

- First 3 Years (On Campus):
  - Students complete core university classes, 17 core faculty courses (51 credits), and 9 core program courses (27 credits) to build foundational computer science and cybersecurity skills
- Final 1 Year (In Industry):
  - First 6 Months: Students complete their Undergraduate Project (PSM) alongside 3 elective courses - Risk Factors in Security, Security Management in Practices and Security Trends and Technology.
  - Second 6 Months: Students complete full-time Industrial Training (LI) in an industry partner organization

Roles and Responsibilities

The successful implementation of this WBL practice relies on active stakeholder engagement and clear delineation of roles among the 4 main drivers (see Figure 1).

i. *WBL Coordinator*

The responsible person who manages placements, bridges communication between the university and industry, and ensures MoU/MoA agreements are established.

ii. *Faculty Teaching Staff (TP)*

The academic staff conduct guided learning (online), monitor student progress, and evaluate performance using the LMS KALAM

iii. *WBL Students*

Enrolled students in their final year actively participate in industry tasks, maintain weekly logbooks, and comply with industry safety and non-disclosure regulations.

iv. *Industry Coach (IC)/Mentor*

A qualified industry professional (e.g., possessing a bachelor's degree with 3 years of relevant experience) who provides day-to-day industry Guidance and conducts formative assessments.

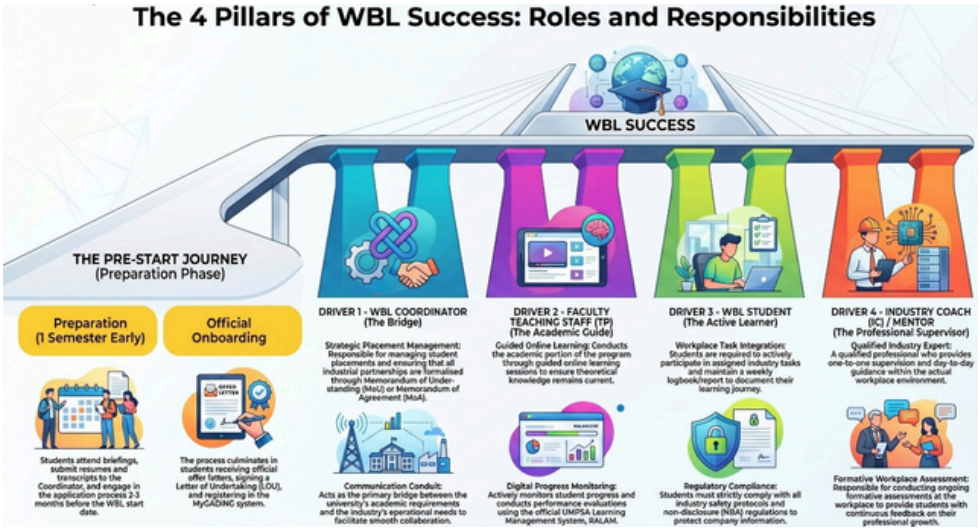


Figure 1. The 4 pillars of WBL Success

Curriculum Co-Design and Development

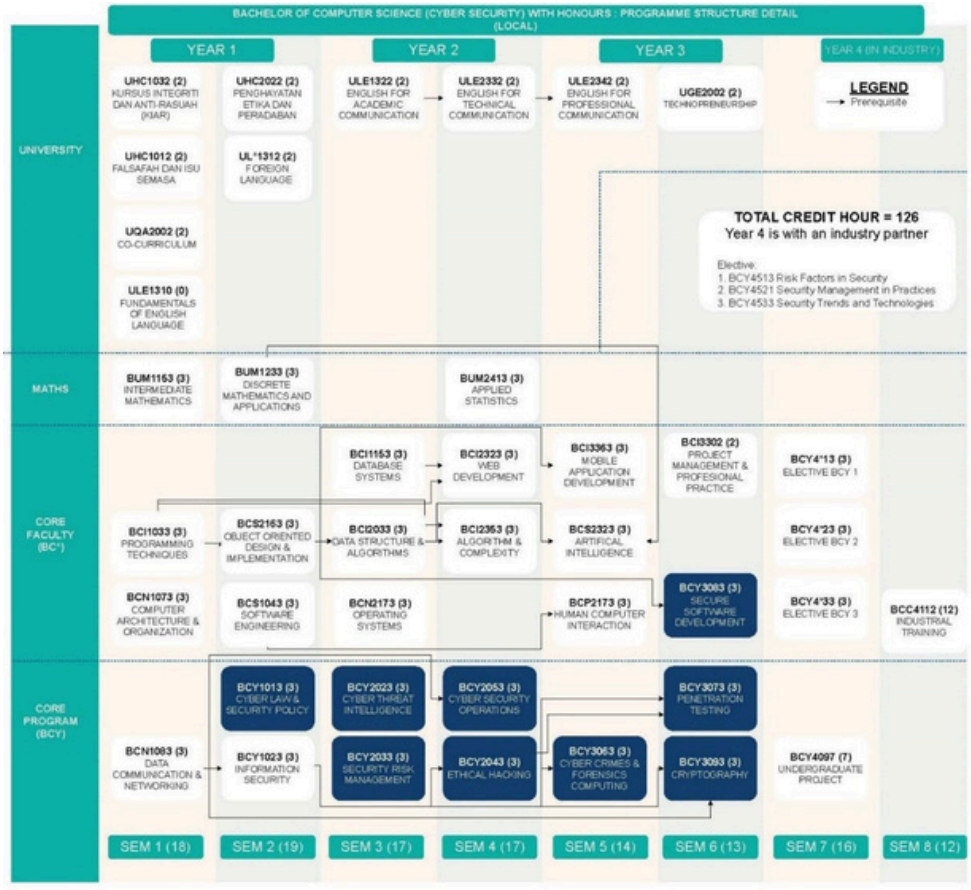
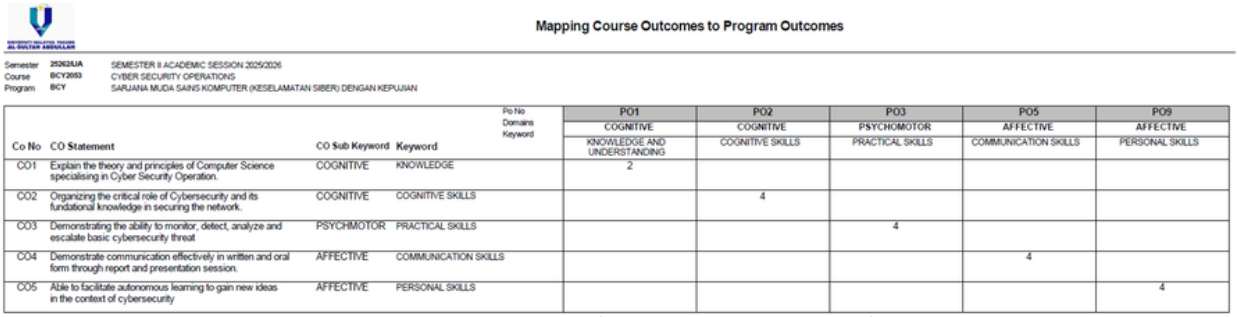


Figure 2: Curriculum structure for Cybersecurity course

The curriculum and teaching methods are jointly formulated by the university and industry partners to ensure they address current market needs, comply with MS ISO 9001:2015, and are formally mapped to the Malaysia Board of Technologists (MBOT) standards.

All course outcomes (COs) are mapped to program outcomes and by the time students are deployed for their final year in the industry, they would have achieved program outcomes (POs), which include not only technical competencies but soft skills such as Practical Skills & High Technology, Analytical and Critical Thinking, Ethics & Professionalism, and Technopreneurship.

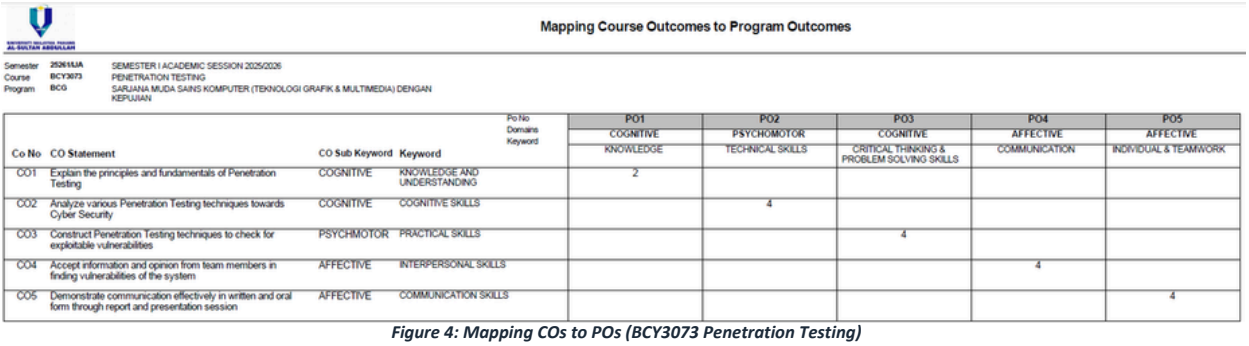


Mapping Course Outcomes to Program Outcomes

Semester 2526201A SEMESTER II ACADEMIC SESSION 2025/2026
Course BCY2053 CYBER SECURITY OPERATIONS
Program BCY SARJANA MUDA SAINS KOMPUTER (KESELAMATAN SIBER) DENGAN KEPUJIAN

Co No	CO Statement	CO Sub Keyword	Keyword	Po No / Domains / Keyword	PO1	PO2	PO3	PO5	PO9
					COGNITIVE	COGNITIVE	PSYCHOMOTOR	AFFECTIVE	AFFECTIVE
					KNOWLEDGE AND UNDERSTANDING	COGNITIVE SKILLS	PRACTICAL SKILLS	COMMUNICATION SKILLS	PERSONAL SKILLS
CO1	Explain the theory and principles of Computer Science specialising in Cyber Security Operation.	COGNITIVE	KNOWLEDGE		2				
CO2	Organizing the critical role of Cybersecurity and its fundational knowledge in securing the network.	COGNITIVE	COGNITIVE SKILLS			4			
CO3	Demonstrating the ability to monitor, detect, analyze and escalate basic cybersecurity threat	PSYCHMOTOR	PRACTICAL SKILLS				4		
CO4	Demonstrate communication effectively in written and oral form through report and presentation session.	AFFECTIVE	COMMUNICATION SKILLS					4	
CO5	Able to facilitate autonomous learning to gain new ideas in the context of cybersecurity	AFFECTIVE	PERSONAL SKILLS						4

Figure 3: Mapping COs to POs (BCY2053 Cybersecurity Operations)



Mapping Course Outcomes to Program Outcomes

Semester 2526103A SEMESTER I ACADEMIC SESSION 2025/2026
Course BCY3073 PENETRATION TESTING
Program BCG SARJANA MUDA SAINS KOMPUTER (TEKNOLOGI GRAFIK & MULTIMEDIA) DENGAN KEPUJIAN

Co No	CO Statement	CO Sub Keyword	Keyword	Po No / Domains / Keyword	PO1	PO2	PO3	PO4	PO5
					COGNITIVE	PSYCHOMOTOR	COGNITIVE	AFFECTIVE	AFFECTIVE
					KNOWLEDGE	TECHNICAL SKILLS	CRITICAL THINKING & PROBLEM SOLVING SKILLS	COMMUNICATION	INDIVIDUAL & TEAMWORK
CO1	Explain the principles and fundamentals of Penetration Testing	COGNITIVE	KNOWLEDGE AND UNDERSTANDING		2				
CO2	Analyze various Penetration Testing techniques towards Cyber Security	COGNITIVE	COGNITIVE SKILLS			4			
CO3	Construct Penetration Testing techniques to check for exploitable vulnerabilities	PSYCHMOTOR	PRACTICAL SKILLS				4		
CO4	Accept information and opinion from team members in finding vulnerabilities of the system	AFFECTIVE	INTERPERSONAL SKILLS					4	
CO5	Demonstrate communication effectively in written and oral form through report and presentation session	AFFECTIVE	COMMUNICATION SKILLS						4

Figure 4: Mapping COs to POs (BCY3073 Penetration Testing)

Next, industry partners assist in mapping coursework to professional certifications. The foundational courses (Years 1-3) are also explicitly mapped to the knowledge domains of major industry-standard certifications such as:

- Cisco CCNA / CyberOps: The course Cyber Security Operations (BCY2053) utilizes the official Cisco CyberOps Associate CBROPS 200-201 curriculum and textbooks, equipping students for Security Operation Centre (SOC) monitoring.
- CEH (Certified Ethical Hacker) & CompTIA PenTest+: Dedicated course in Ethical Hacking (BCY2043) and Penetration Testing (BCY3073) map directly to practical offensive skills.
- CompTIA Security+: Courses like Security Risk Management (BCY2033) and Cyber Threat Intelligence (BCY2023) provide the baseline for high-level risk assessments.

Students are not required to officially hold the external vendor certifications before deployment. However, their successful completion of these professionally mapped academic courses are able to show their theoretical and technical readiness for industry tasks.

IMPACT

By spending a full year immersed in industry settings, students are exposed to real-world cybersecurity equipment and facilities provided and able to solve authentic cybersecurity challenges, such as mitigating ransomware attacks, evaluating remote-work risks via VPNs, and managing cloud and IoT security in real time, which helped to bridge the gap between theoretical knowledge and practical application. In real high-pressure corporate environments, students absorbed technical concepts faster because they could apply theories to live corporate problems. They also showed professional maturity, resilience, and problem-solving capabilities in a highly competitive digital landscape.

For participating industry partners, this initiative establishes a reliable, customised talent pipeline that delivers clear economic benefits. Rather than expanding extensive resources to train fresh graduates from scratch, companies benefit from pre-trained students who actively contribute to the organisation's daily operations and strategic goals during their placement. For instance, final-year students already conducted Security Penetration Assessments (SPAs), run phishing awareness campaigns, and propose mitigation strategies to address real-time security breaches. The one-year corporate onboarding via their final year would mean they do not require additional entry-level training and students could secure full-time employment offers from their host companies as soon as they graduate, bypass traditional post-graduate hiring delays and could accelerate the industry's urgent market demand for skilled cybersecurity professionals.

In terms of operational and financial impact on the university, by fully utilizing the advanced technological infrastructure, software, and real-world data environments provided by industry partners, the university significantly reduces the financial burden of purchasing and continuously upgrading expensive in-house cybersecurity laboratories.

LESSON LEARNT AND REPLICABILITY

A key lesson learned from implementing the 3u1i Experiential WBL model is the need for a highly structured, modular approach to prevent students from becoming overwhelmed during their industry placements. By dividing academic cybersecurity courses into manageable learning blocks sessions via online platforms like KALAM and Microsoft Teams, students can better balance their daily industry operations with their university requirements. Additionally, utilising standardised collaborative rubrics, in which grading responsibilities are systematically shared between the Faculty Teaching Staff (TP) and the Industry Coach (IC), ensures that evaluations remain fair, consistent, and accurately reflect both academic proficiency and practical workplace competencies.

To ensure quality across different stakeholders, consultation discussions should be held transparently and align standards with the Malaysia Qualifications Agency Guidelines to Good Practices: Work-based Learning, Department of Higher Education 2u2i Study Mode Implementation Guidebook, UMPSA Work-Learning Guidelines Garis Panduan and ISO 9001:2015. The placement of students at industry partner sites (such as VulsanX, Cybersecurity Malaysia (CSM), Perodua, and HeiTech Padu) has to be formalized through MoA/MoU agreements and through open rigorous selection.

FUTURE OUTLOOK

Guided by ISO Clause 6.1 (actions to address risks and opportunities), the program continuously evaluates technological shifts. The curriculum dynamically adapts to include emerging trends such as AI-powered surveillance, blockchain technology, and evolving regulatory frameworks (GDPR, PDPA, NIST guidelines). The faculty is pioneering specialized tools such as CyberSecure VR and integrating into future work-based learning curriculum both virtual reality simulations and professional micro-credential modules such as Cisco Ethical Hacker certification.

The program will continue to observe graduate employability and job readiness, in order to channel graduates into critical immediate roles like Cyber Security Executives, Network Penetration Testers, and Security Operations Specialists.

CONCLUSION

The 3u1i Experiential WBL model implemented at UMPSA is an example of future workforce preparation in the field of cybersecurity where academic learning is integrated with industry experience. Through curriculum co-design with industry partners, alignment with Malaysia Board of Technologists (MBOT) standards, and mapping of core courses to internationally recognised professional certifications, students are trained with both technical foundations, industry-relevant competencies and soft skills.

A key takeaway is for close collaboration among universities, industry partners, students, and professional bodies while referencing quality frameworks such as MQA, KPT and MS ISO 9001:2015 to effectively bridge the gap between academic knowledge and rapidly evolving cybersecurity workforce requirements. With continuous curriculum enhancement in emerging areas such as artificial intelligence, virtual reality, blockchain, and evolving cybersecurity regulations, the programme model is hoped to sustainably address the cybersecurity skills gap and strengthen graduate employability for the future.

REFERENCES

Crawford, A. (2025). *The Future of Work-based Learning for Cyber Jobs*. Center for Security and Emerging Technology. https://doi.org/10.51593/20240057

International Information System Security Certification Consortium (2025). *2025 Cybersecurity Workforce Study*. Available at https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

FURTHER INFORMATION

Ts. Dr. Nor Saradatul Akmar Binti Zulkifli
Senior Lecturer
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA), 26600 Pekan, Pahang, Malaysia
saradatulakmar@umpsa.edu.my

Ts. Dr. Syifak Izhar Hisham
Head of Department
Computer Network & Cybersecurity
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA), 26600 Pekan, Pahang, Malaysia
syifakizhar@umpsa.edu.my

Assoc. Prof. Ts. Dr. Adzhar Kamaludin
Associate Professor
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA), 26600 Pekan, Pahang, Malaysia
adzhar@umpsa.edu.my

Assoc. Prof. Ts. Dr. Mohd Faizal Bin Ab Razak
Associate Professor
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA), 26600 Pekan, Pahang, Malaysia
faizalrazak@umpsa.edu.my

SEA-VET.net
TVET Platform for SEA

ABOUT GOOD PRACTICES

"Good Practices" are chosen according to selection criteria that have been created by a working group. They aim to serve as benchmarks for transformation towards quality TVET.However, they reflect on the individual circumstances of the submitting country and may only be adopted with context specific modifications.

CONTACT INFORMATION

SEAMEO VOCTECH, Jalan Pasar Baharu, Gadong BE1318, Brunei Darussalam

team@sea-vet.net

+673 244 7992

FOLLOW US ON

@seavetnet

@seavetnet

Scan for more information

https://sea-vet.net/tvet-in-southeast-asia/good-practices

Copyright © 2026 SEA-VET.NET. All Rights Reserved.