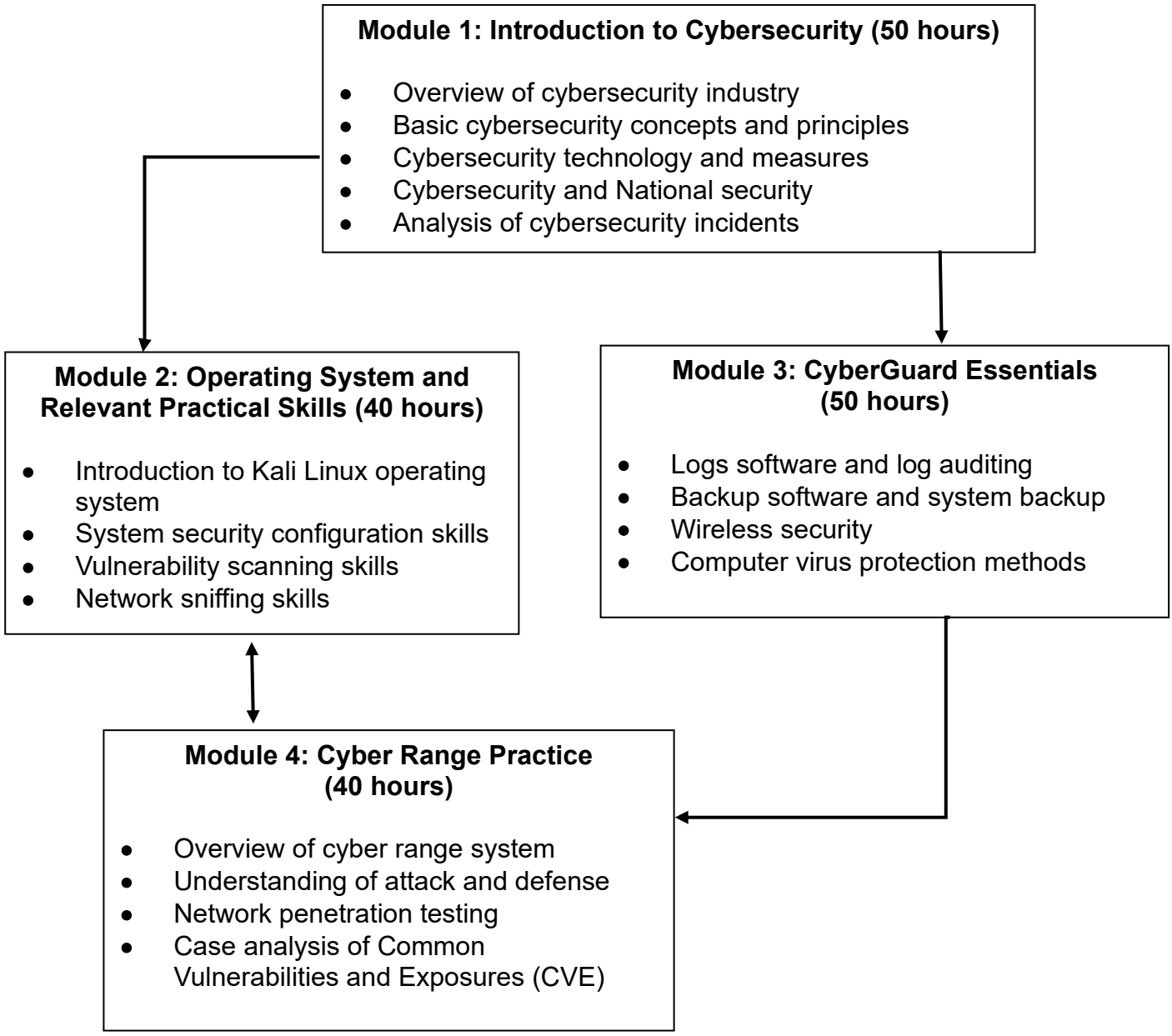
Applied Learning

2025-27 Cohort; 2027 HKDSE

Item	Description
1. Course Title	Cybersecurity
2. Course Provider	Hong Kong College of Technology
3. Area of Studies/ Course Cluster	Engineering and Production/ Information Engineering
4. Medium of Instruction	Chinese or English
5. Learning Outcomes	Upon completion of the course, students should be able to: (i) locate the threats, risks and response strategies of cybersecurity; (ii) illustrate the basic concepts, principles and methods of cybersecurity; (iii) apply basic professional skills in cybersecurity, be familiar with the basic operating environment, tools and techniques of cybersecurity, and be able to response simple tasks, reaching a certain professional standard; (iv) interpret work ethics and proper values related to cybersecurity and be able to make reasonable judgments, and demonstrate respect and responsibility in practical environments; and (v) enhance self-understanding and explore directions on further studies and career pursuits.

6. Curriculum Map – Organisation and Structure



7. The Context

- The information on possible further study and career pathways is provided to enhance students' understanding of the wider context of the specific Applied Learning course.
- The recognition of Applied Learning courses for admission to further studies and career opportunities is at the discretion of relevant institutions. Students who have successfully completed Applied Learning courses have to meet other entry requirements as specified by the institutions.

Possible further study and career pathways

Further studies

- e.g. courses related to cybersecurity, information technology, computer science, engineering

Career development

- e.g. junior cybersecurity engineer, information security engineer, cybersecurity officer, IT security officer, system administrator

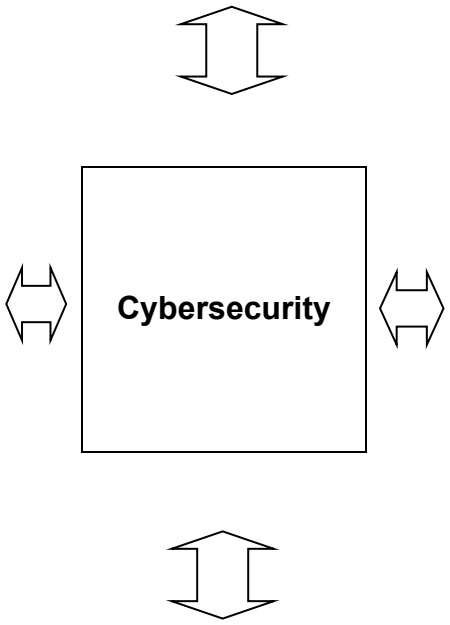
Complementarity with core subjects and other elective subjects

Enhancing and enriching**,** e.g.

- enhance the awareness and application of threats and security on the internet among students taking **Information and Communication Technology** through practices

Expanding horizons**,** e.g.

- expand students' horizons of the technology application in risk management for taking **Business, Accounting and Financial Studies**



Relations with other Areas of Studies/ courses of Applied Learning

e.g.

Business, Management and Law

- enhance students' understanding of the importance and application of cybersecurity in nowadays business environment

Foundation knowledge developed in junior secondary education

The course is built upon the foundation knowledge students acquired in, e.g.

- **Chinese Language Education** and **English Language Education** – verbal, reading and writing skills
- **Mathematics** – logical thinking ability, computational ability, analytical and inductive ability
- **Technology Education** – use the appropriate hardware, software and computer systems to perform various tasks

8. Learning and Teaching

In this course, student-centred learning and teaching activities are designed to enable students to understand fundamental theories and concepts, develop their generic skills, and address their career aspirations in cybersecurity/information technology.

Different modes of activities are employed to provide students with a systematic understanding about the context (e.g. cybersecurity role-playing – students take on roles such as network administrators and attackers, participating in scenario simulations to deepen their understanding of offense and defense) and eye-opening opportunities to experience the complexity of the context (e.g. cyber range simulated experiment – students simulate CVE vulnerabilities in cyber range, gaining hands-on experience in the process of discovering and fixing vulnerabilities).

Students acquire an understanding of the requirements, fundamental knowledge and skills essential for further learning within the area through learning-by-practising opportunities in an authentic or near-authentic environment (e.g. wireless network security configuration practice - students practically configure wireless network security protocols to ensure data confidentiality).

Students are given opportunities to consolidate their learning and demonstrate entrepreneurship and innovation (e.g. vulnerability report writing – students select a CVE vulnerability case in groups, and write a detailed vulnerability report including discovery, analysis, and remediation methods).

9. Curriculum Pillars of Applied Learning

Through related contexts, students have different learning opportunities, for example:

(i) Career-related Competencies

- understand the career paths and industry terminology in the field of cybersecurity;
- develop essential skills on teamwork and problem-solving; and
- understand the latest development trends in cybersecurity.

(ii) Foundation Skills

- familiarise with basic cybersecurity concepts such as protocols and network services;
- understand the basic applications of cybersecurity tools;
- understand the principles and protection skills of computer viruses; and
- learn to analyse and recover vulnerabilities of systems.

(iii) Thinking Skills

- evaluate and mitigate risks related to cybersecurity;
- effectively handle cybersecurity incidents; and
- understand and comply with regulations and ethical requirements related to cybersecurity.

(iv) People Skills

- demonstrate communication skills by conveying cybersecurity problems and solutions to others effectively throughout the process of handling cybersecurity incident; and
- collaborate within a team to solve cybersecurity challenges.

(v) Values and Attitudes

- respect the privacy of individuals and refrain from engaging in illegal activities;
- adhere to legal and ethical standards while conducting cybersecurity-related activities;
- recognise the social responsibility in the digital space; and
- cultivate a perpetual learning mindset to adapt to evolving cybersecurity technologies.