ADDITIONAL INFORMATION NEEDED FOR THE APEL Q MASTER IN CYBER SECURITY PROGRAM

NAME OF APPLICANT:
DATE:

- For Table 1, please state **YES** or **NO** in the respective space under Source of My Knowledge in Table 1. You may also provide a short explanation, but it is optional.
- For Table 2, if you have knowledge or experience in other cyber security related subjects, you may provide a brief description or keywords. (optional)

TABLE 1: MAIN SUBJECTS

Core Subjects	**Synopsis of the subject**	**Source of My Knowledge**		
		Previous or current Job specification or project	**Previous formal learning (course, training and/or seminar)**	**Non-formal learning (community, online forum, etc)**
Computer Security	This course presents the basic paradigms and principles of computer security technology and mechanism in modern computer systems. At the end of this course, students should be able to treat computer security problems in a structured way. The course has been structured so that the formal prerequisites only require a minimal knowledge in computer science and mathematics. It is designed to serve as a general introduction to the following topic: computer security fundamentals, security models, cryptography and security issues related to these topics.			
Network Security	This course covers the basic and intermediate topics in network security. The aim of this course is to prepare students with the concept and knowledge of using network security protocols and applications to provide security over networks and the Internet. Topics covered include the low level frame packet analysis, analyze			

	each layer in TCP/IP (and the equivalent OSI layer) protocol, as well as the possible threats that come in each layer, network security design, email security, web security, wireless security, and honeypot. Hence the use of important network security tools and applications are introduced such in the lab sessions. The course will also look into vulnerabilities of existing network protocols and the way to overcome them. Students are required to accomplish hands-on lab exercises, practical security assessment as problem-based learning and /report assignments.			
Information Security Management	The course covers methodology, technique, and tools for monitoring events in computer or network for preventing and detecting unwanted process activity, recognizing and recovering from malicious behaviour. This course covers the fundamental concepts and design implications required to develop and implement intrusion detection and prevention systems that address security violations in computer systems. The course explains how to detect and prevent unauthorized accesses of networked computers and minimize the damage intruders can do. It emphasizes on techniques and methods for recognizing and handling attacks both automatically and manually. The case studies, large and/or small scales will be covered in this course. Topics to be covered include: main classes of attacks against computer systems, taxonomy and architecture of intrusion detection and prevention systems, network traffic analysis and feature extraction for intrusion detection, signature and anomaly based techniques and machine learning based techniques for intrusion detection. Intrusion detection and prevention systems performance evaluation, issues related to security and defense and network software tools such as bro, Wireshark and Snort will also be discussed.			
Cyber Law and Ethics	This course analyses the phenomena of cybercrime, legal, and investigation/evidential issues, to enable students to relate the evolution of criminal behaviour in parallel with the advancement of technology. Such knowledge would make students always inculcate the culture of cyber security and ethics. Moreover, the course aims to equip students with knowledge on criminal behaviour and social engineering towards mitigating the risk of cyber threats apart from preparing the students as the planner for computer related activities emphasising or ethics, conventions, and laws. On the whole, the course is geared at producing manpower			

	who will serve as reference in matters pertaining to the organisation, initiation, monitoring and supervision of cyber security acculturation and ethics continuously.			

TABLE 2: OTHER SUBJECTS

(Candidate may share their knowledge in other area of cyber security which is not covered above)

Other Subjects (you can modify, remove or add your subjects)	**Synopsis of the subject**	**Source of Knowledge**		
		Previous or current Job specification or project	**Previous formal learning (Course, Training and/or Seminar)**	**Non-formal learning**
Intrusion Detection and Prevention	The course covers methodology, technique, and tools for monitoring events in computer or network for preventing and detecting unwanted process activity, recognizing and recovering from malicious behaviour. This course covers the fundamental concepts and design implications required to develop and implement intrusion detection and prevention systems that address security violations in computer systems. The course explains how to detect and prevent unauthorized accesses of networked computers and minimize the damage intruders can do. It emphasizes on techniques and methods for recognizing and handling attacks both automatically and manually. The case studies, large and/or small scales will be covered in this course. Topics to be covered include: main classes of attacks against computer systems, taxonomy and architecture of intrusion detection and prevention systems, network traffic analysis and feature extraction for intrusion detection, signature and anomaly based techniques and machine learning based techniques for intrusion detection. Intrusion detection and prevention systems performance			

	evaluation, issues related to security and defense and network software tools such as bro, Wireshark and Snort will also be discussed.			
Ethical Hacking and Penetration Testing	Ethical hacking, or also known as penetration testing, is a disciplined and methodological approach to test a computer security in a computer network, a wireless environment, web applications and online services. In this course, the students can compare, and evaluate the techniques needed for the purpose of ethical hacking and penetration testing specific systems. The students also can demonstrate practical competence in a number of hacking techniques: social engineering, reconnaissance, scanning, enumeration, exploiting Linux and Windows applications, client side attacks, web application attacks, password attacks, and denial of service attacks. Finally, the students can integrate their knowledge and skills into evolving techniques in information security.			
Security Audit and Assessment	This course introduces the concept of information system audit and security assessment. It involves techniques in internal audit, and security control in ICT environment, consisting of network, application and operating systems. Students should understand the importance of internal control in an organisation, thus information system auditing. It also discusses audit objectives and procedures for internal controls (management and applications). The use of Computer Assisted Auditing Techniques and Tools (CAATTs) using ACL.			
Fundamental of Digital Forensics	This course introduces the fundamental of digital forensics domain. It covers introduction to forensic science, basics and management of investigation, quality assurance and countermeasures. Students would also learn the processes of investigation conducted by an investigator officer or first responder in managing and solving contemporary forensic digital problem related to digital evidence. It covers phases of identification, seizure at the crime scene, preservation, analysis and presentation of findings to stakeholders and court. Additionally, this course also explains management digital forensic lab including process of building a forensic laboratory, and the management of people, technology and activities.			

Data Recovery and Analysis	This course introduces the methods of data recovery and digital forensic on data evidence related to computer and embedded systems such as smartphones and Cloud. Prior to that, students will learn basic concept about file system of computer and smartphones, Operating System, File signature and computer architecture. Then, student will also be taught on the techniques of data recovery on computer, memory and latest technology. Nevertheless, the student will be equipped with techniques on analysis of computer, latest devices and technology, writing and presenting findings from analysis of specific digital evidence. Finally, this course will generate expert witness for the forensic cases related to computer, memory and latest technology.			
Software Security	This course aims to provide skills and knowledge to produce secure software. It starts with the discussion about possible threats on software and its technical cause. In order to reduce this treats, secure software development lifecycle should be in place, hence a few standard lifecycle are presented. Two important software products that are database and web application will be then thoroughly explored in term of its security. Finally, methods to justify that software product has embedded certain level of security aspect are examined.			
Financial Technology Security and Risk	Financial technology (FinTech) is a new technology and innovation that aims to make financial services more efficient. This technology covers the areas of big data analytic, online financial services and payment card technology. However, big data analytic will not be covered in this module. The module begins with a discussion on various type of FinTech and its differences. Then, architectures of e-commerce platform with payment gateway and digital wallet, payment card, Secure Electronic Transaction protocol which underpinning the online payment services, blockchain and cryptocurrency will be discussed. The discussion continues with Regulations and standards that FinTech has to comply. After that, students will be challenged to identify security risks in the discussed technology based on accepted security risk management model. Following that, mitigation and control elements that can be applied to manage the risks will be discussed. Throughout the module, real financial crime cases based on the technology vulnerabilities will be used as a case study.			

Cyber Threat Intelligence	Cyber threat intelligence represents a force multiplier for organizations looking to empower their response and detection mechanisms to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary’s tool, but the real threat is the human, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders. This course will teach the student in the tactical, operational and strategic level of cyber threat intelligence skills. Further, through this course, it able to create better security teams, more efficient and accurate incident response and the student more aware of the evolving threats landscape.			
//You can add more				