

NOTICE ACCOMPANYING THE ELECTRONIC PROSPECTUS OF LGMS BERHAD (“LGMS” OR THE “COMPANY”) DATED 20 MAY 2022 (“ELECTRONIC PROSPECTUS”)

(Unless otherwise indicated, specified or defined in this notice, the definitions in the Prospectus dated 20 May 2022 shall apply throughout this notice)

Website

The Electronic Prospectus can be viewed or downloaded from Bursa Malaysia Securities Berhad’s (“**Bursa Securities**”) website at <https://www.bursamalaysia.com/> (“**Website**”).

Availability and Location of Paper/Printed Prospectus

Any applicant in doubt concerning the validity or integrity of the Electronic Prospectus should immediately request a paper/printed copy of the Prospectus directly from the Company, UOB Kay Hian Securities (M) Sdn Bhd (“**UOBKH**”), or Tricor Investor & Issuing House Services Sdn Bhd. Alternatively, the applicant may obtain a copy of the Prospectus from participating organisations of Bursa Securities, members of the Association of Banks in Malaysia and members of the Malaysian Investment Banking Association.

Prospective investors should note that the Application Forms are not available in electronic format.

Jurisdictional Disclaimer

This distribution of the Electronic Prospectus and the sale of the units are subject to Malaysian law. Bursa Securities, UOBKH and LGMS take no responsibility for the distribution of the Electronic Prospectus and/or the sale of ordinary shares in LGMS (“**Share(s)**”) outside Malaysia, which may be restricted by law in other jurisdictions. The Electronic Prospectus does not constitute and may not be used for the purpose of an offer to sell or an invitation of an offer to buy any Shares, to any person outside Malaysia or in any jurisdiction in which such offer or invitation is not authorised or lawful or to any person to whom it is unlawful to make such offer or invitation.

Close of Application

Applications will be accepted from 10.00 a.m. on 20 May 2022 and will close at 5.00 p.m. on 26 May 2022 or for such further period or periods as the Directors of LGMS in their absolute discretion may decide.

The Electronic Prospectus made available on the Website after the closing of the application period is made available solely for informational and archiving purposes. No securities will be allotted or issued on the basis of the Electronic Prospectus after the closing of the application period.

Persons Responsible for the Internet Site in which the Electronic Prospectus is Posted

The Electronic Prospectus which is accessible at the Website is owned by Bursa Securities. Users’ access to the Website and the use of the contents of the Website and/or any information in whatsoever form arising from the Website shall be conditional upon acceptance of the terms and conditions of use as contained in the Website.

The contents of the Electronic Prospectus are for informational and archiving purposes only and are not intended to provide investment advice of any form or kind, and shall not at any time be relied upon as such.



PROSPECTUS

LGMS BERHAD

(Registration No. 202001039091 (1395412-W))
(Incorporated in Malaysia)

INITIAL PUBLIC OFFERING (“**IPO**”) IN CONJUNCTION WITH THE LISTING OF AND QUOTATION FOR THE ENTIRE ENLARGED ISSUED ORDINARY SHARE CAPITAL OF LGMS BERHAD (“**LGMS**”) ON THE ACE MARKET OF BURSA MALAYSIA SECURITIES BERHAD (“**ACE MARKET**”) COMPRISING:-

- (A) A PUBLIC ISSUE OF 91,395,000 NEW ORDINARY SHARES IN LGMS (“**ISSUE SHARE(S)**”) IN THE FOLLOWING MANNER:-
- (I) 22,800,000 ISSUE SHARES MADE AVAILABLE FOR APPLICATION BY THE MALAYSIAN PUBLIC;
 - (II) 12,500,000 ISSUE SHARES RESERVED FOR APPLICATION BY OUR ELIGIBLE DIRECTORS AND EMPLOYEES AS WELL AS PERSONS WHO HAVE CONTRIBUTED TO THE SUCCESS OF OUR GROUP;
 - (III) 44,695,000 ISSUE SHARES BY WAY OF PRIVATE PLACEMENT TO IDENTIFIED INSTITUTIONAL AND/OR SELECTED INVESTORS; AND
 - (IV) 11,400,000 ISSUE SHARES BY WAY OF PRIVATE PLACEMENT TO IDENTIFIED BUMIPUTERA INVESTORS APPROVED BY THE MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY, MALAYSIA (“**MITI**”);

AND

- (B) AN OFFER FOR SALE OF 45,600,000 EXISTING ORDINARY SHARES IN LGMS (“**OFFER SHARE(S)**”) BY WAY OF PRIVATE PLACEMENT TO IDENTIFIED BUMIPUTERA INVESTORS APPROVED BY THE MITI;

AT AN ISSUE PRICE/OFFER PRICE OF RM0.50 PER ISSUE SHARE/OFFER SHARE, PAYABLE IN FULL UPON APPLICATION.

Principal Adviser, Sponsor, Underwriter
and Placement Agent

UOB KayHian

UOB Kay Hian Securities (M) Sdn Bhd
(Registration No. 199001003423 (194990-K))
(A Participating Organisation of Bursa Malaysia Securities Berhad)

This Prospectus has been registered by the Securities Commission Malaysia (“**SC**”). The registration of this Prospectus should not be taken to indicate that the SC recommends the offering or assumes responsibility for the correctness of any statement made, opinion expressed or report contained in this Prospectus. The SC has not, in any way, considered the merits of the securities being offered for investment.

The SC and Bursa Malaysia Securities Berhad (“**Bursa Securities**”) are not liable for any non-disclosure on the part of LGMS and take no responsibility for the contents of this Prospectus, make no representation as to its accuracy or completeness, and expressly disclaim any liability for any loss you may suffer arising from or in reliance upon the whole or any part of the contents of this Prospectus.

NO SECURITIES WILL BE ALLOTTED OR ISSUED BASED ON THIS PROSPECTUS AFTER 6 MONTHS FROM THE DATE OF THIS PROSPECTUS. INVESTORS ARE ADVISED TO READ AND UNDERSTAND THE CONTENTS OF THIS PROSPECTUS. IF IN DOUBT, PLEASE CONSULT A PROFESSIONAL ADVISER. FOR INFORMATION CONCERNING RISK FACTORS WHICH SHOULD BE CONSIDERED BY PROSPECTIVE INVESTORS, SEE “RISK FACTORS” COMMENCING ON PAGE 36.

THE ACE MARKET IS AN ALTERNATIVE MARKET DESIGNED PRIMARILY FOR EMERGING CORPORATIONS THAT MAY CARRY HIGHER INVESTMENT RISK WHEN COMPARED WITH LARGER OR MORE ESTABLISHED CORPORATIONS LISTED ON THE MAIN MARKET. THERE IS ALSO NO ASSURANCE THAT THERE WILL BE A LIQUID MARKET IN THE SHARES OR UNITS OF SHARES TRADED ON THE ACE MARKET. YOU SHOULD BE AWARE OF THE RISKS OF INVESTING IN SUCH CORPORATIONS AND SHOULD MAKE THE DECISION TO INVEST ONLY AFTER CAREFUL CONSIDERATION.

THE ISSUE, OFFER OR INVITATION FOR THE OFFERING IS A PROPOSAL NOT REQUIRING APPROVAL, AUTHORISATION OR RECOGNITION OF THE SC UNDER SECTION 212(8) OF THE CAPITAL MARKETS AND SERVICES ACT 2007.

THIS PROSPECTUS IS DATED 20 MAY 2022



LGMS BERHAD

(Registration No. 202001039091 (1395412-W))
(Incorporated in Malaysia)

Email: invest@lgms.global
Website: www.lgms.global

RESPONSIBILITY STATEMENTS

OUR DIRECTORS, PROMOTERS AND SELLING SHAREHOLDER (AS DEFINED HEREIN) HAVE SEEN AND APPROVED THIS PROSPECTUS. THEY COLLECTIVELY AND INDIVIDUALLY ACCEPT FULL RESPONSIBILITY FOR THE ACCURACY OF THE INFORMATION CONTAINED IN THIS PROSPECTUS. HAVING MADE ALL REASONABLE ENQUIRIES, AND TO THE BEST OF THEIR KNOWLEDGE AND BELIEF, THEY CONFIRM THAT THERE IS NO FALSE OR MISLEADING STATEMENT OR OTHER FACTS WHICH IF OMITTED, WOULD MAKE ANY STATEMENT IN THIS PROSPECTUS FALSE OR MISLEADING.

UOB KAY HIAN SECURITIES (M) SDN BHD (“**UOBKH**”), BEING OUR PRINCIPAL ADVISER, SPONSOR, UNDERWRITER AND PLACEMENT AGENT IN RELATION TO OUR IPO, ACKNOWLEDGES THAT, BASED ON ALL AVAILABLE INFORMATION, AND TO THE BEST OF ITS KNOWLEDGE AND BELIEF, THIS PROSPECTUS CONSTITUTES A FULL AND TRUE DISCLOSURE OF ALL MATERIAL FACTS CONCERNING OUR IPO.

STATEMENTS OF DISCLAIMER

APPROVAL HAS BEEN OBTAINED FROM BURSA SECURITIES ON 26 JANUARY 2022 FOR THE LISTING OF AND QUOTATION FOR OUR SHARES BEING OFFERED. ADMISSION TO THE OFFICIAL LIST OF BURSA SECURITIES IS NOT TO BE TAKEN AS AN INDICATION OF THE MERITS OF OUR IPO, LGMS OR OUR SHARES.

THIS PROSPECTUS, TOGETHER WITH THE APPLICATION FORMS (AS DEFINED HEREIN), HAS ALSO BEEN LODGED WITH THE REGISTRAR OF COMPANIES OF MALAYSIA, WHO TAKES NO RESPONSIBILITY FOR ITS CONTENTS.

OTHER STATEMENTS

YOU SHOULD NOTE THAT YOU MAY SEEK RECOURSE UNDER SECTIONS 248, 249 AND 357 OF THE CAPITAL MARKETS AND SERVICES ACT 2007 (“**CMSA**”) FOR BREACHES OF SECURITIES LAWS INCLUDING ANY STATEMENT IN THIS PROSPECTUS THAT IS FALSE, MISLEADING, OR FROM WHICH THERE IS A MATERIAL OMISSION, OR FOR ANY MISLEADING OR DECEPTIVE ACT IN RELATION TO THIS PROSPECTUS OR THE CONDUCT OF ANY OTHER PERSON IN RELATION TO LGMS.

OUR SHARES LISTED ON BURSA SECURITIES ARE OFFERED TO THE PUBLIC ON THE PREMISE OF FULL AND ACCURATE DISCLOSURE OF ALL MATERIAL INFORMATION CONCERNING OUR IPO, FOR WHICH ANY PERSON SET OUT IN SECTION 236 OF THE CMSA, IS RESPONSIBLE.

OUR SHARES ARE CLASSIFIED AS SHARIAH COMPLIANT BY THE SHARIAH ADVISORY COUNCIL (“**SAC**”) OF THE SC. THIS CLASSIFICATION REMAINS VALID FROM THE DATE OF ISSUE OF THE PROSPECTUS UNTIL THE NEXT SHARIAH COMPLIANCE REVIEW UNDERTAKEN BY THE SAC OF THE SC. THE NEW STATUS IS RELEASED IN THE UPDATED LIST OF SHARIAH-COMPLIANT SECURITIES, ON THE LAST FRIDAY OF MAY AND NOVEMBER.

THIS PROSPECTUS HAS BEEN PREPARED IN THE CONTEXT OF AN IPO UNDER THE LAWS OF MALAYSIA, AND OUR IPO WILL NOT BE MADE IN ANY COUNTRY OR JURISDICTION OTHER THAN MALAYSIA OR TO PERSONS WHO ARE SUBJECT TO THE LAWS OF ANY COUNTRY OR JURISDICTION OTHER THAN THE LAWS OF MALAYSIA. OUR IPO TO WHICH THIS PROSPECTUS RELATES IS ONLY AVAILABLE TO PERSONS RECEIVING THIS PROSPECTUS ELECTRONICALLY OR OTHERWISE WITHIN MALAYSIA. WE AND OUR PRINCIPAL ADVISER HAVE NOT AUTHORISED AND TAKE NO RESPONSIBILITY FOR THE DISTRIBUTION OF THIS PROSPECTUS (IN PRELIMINARY OR FINAL FORM) OUTSIDE MALAYSIA. ACCORDINGLY, THIS PROSPECTUS MAY NOT BE USED FOR THE PURPOSE OF AND DOES NOT CONSTITUTE AN OFFER FOR SUBSCRIPTION OR PURCHASE OR INVITATION TO SUBSCRIBE OR PURCHASE, ANY SECURITIES UNDER OUR IPO IN ANY JURISDICTION IN WHICH SUCH OFFER OR INVITATION IN ANY JURISDICTION OR IN ANY CIRCUMSTANCES IN WHICH SUCH AN OFFER IS NOT AUTHORISED OR LAWFUL OR TO ANY PERSON TO WHOM IT IS UNLAWFUL TO MAKE SUCH OFFER OR INVITATION. THE DISTRIBUTION OF THIS PROSPECTUS AND THE SALE OF OUR IPO SHARES (AS DEFINED HEREIN) IN CERTAIN JURISDICTIONS MAY BE RESTRICTED BY LAW. PERSONS WHO MAY BE IN POSSESSION OF THIS PROSPECTUS ARE REQUIRED TO INFORM THEMSELVES OF AND TO OBSERVE SUCH RESTRICTIONS.

WE WILL NOT MAKE OR BE BOUND TO MAKE ANY ENQUIRY BEFORE ANY ACCEPTANCE IN RESPECT OF OUR IPO AS TO WHETHER YOU HAVE A REGISTERED ADDRESS IN MALAYSIA. WE WILL NOT ACCEPT ANY LIABILITY WHETHER OR NOT ANY ENQUIRY OR INVESTIGATION IS MADE IN CONNECTION WITH IT. IT IS YOUR SOLE RESPONSIBILITY TO CONSULT YOUR LEGAL AND/OR OTHER PROFESSIONAL ADVISERS AS TO WHETHER OUR IPO WOULD RESULT IN THE CONTRAVENTION OF ANY LAWS OR JURISDICTIONS OTHER THAN MALAYSIA TO WHICH YOU MAY BE SUBJECTED.

FURTHER, IT SHALL ALSO BE YOUR SOLE RESPONSIBILITY TO ENSURE THAT YOUR APPLICATION FOR OUR SHARES WOULD BE IN COMPLIANCE WITH THE TERMS OF OUR IPO AND WOULD NOT BE IN CONTRAVENTION OF ANY LAWS OF COUNTRIES OR JURISDICTIONS OTHER THAN MALAYSIA TO WHICH YOU MAY BE SUBJECTED TO. WE WILL FURTHER ASSUME THAT YOU HAD ACCEPTED THIS IPO IN MALAYSIA AND WILL AT ALL APPLICABLE TIMES BE SUBJECTED ONLY TO THE LAWS OF MALAYSIA CONNECTED TO IT.

HOWEVER, WE RESERVE THE RIGHT, IN OUR ABSOLUTE DISCRETION, TO TREAT ANY ACCEPTANCE AS INVALID IF WE BELIEVE THAT SUCH ACCEPTANCE MAY VIOLATE ANY LAW OR APPLICABLE LEGAL OR REGULATORY REQUIREMENTS.

THIS PROSPECTUS IS PREPARED AND PUBLISHED SOLELY FOR OUR IPO IN MALAYSIA UNDER THE LAWS OF MALAYSIA. OUR SHARES ARE ISSUED IN MALAYSIA SOLELY BASED ON THE CONTENTS OF THIS PROSPECTUS. WE AND OUR PRINCIPAL ADVISER HAVE NOT AUTHORISED ANYONE TO PROVIDE YOU WITH INFORMATION, WHICH IS NOT CONTAINED IN THIS PROSPECTUS.

ELECTRONIC PROSPECTUS

THIS PROSPECTUS CAN ALSO BE VIEWED OR DOWNLOADED FROM BURSA SECURITIES' WEBSITE AT www.bursamalaysia.com. THE CONTENTS OF THE ELECTRONIC PROSPECTUS ARE AS PER THE CONTENTS OF THE PROSPECTUS REGISTERED WITH THE SC.

YOU ARE ADVISED THAT THE INTERNET IS NOT A FULLY SECURE MEDIUM AND THAT YOUR INTERNET SHARE APPLICATION (AS DEFINED HEREIN) IS SUBJECT TO THE RISKS OF PROBLEMS OCCURRING DURING DATA TRANSMISSION, COMPUTER SECURITY THREATS SUCH AS VIRUSES, HACKERS AND CRACKERS, FAULTS WITH COMPUTER SOFTWARE AND OTHER EVENTS BEYOND THE CONTROL OF THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS (AS DEFINED HEREIN). THESE RISKS CANNOT BE BORNE BY THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS.

IF YOU DOUBT THE VALIDITY OR THE INTEGRITY OF AN ELECTRONIC PROSPECTUS, YOU SHOULD IMMEDIATELY REQUEST FROM US OR THE ISSUING HOUSE (AS DEFINED HEREIN), A PAPER/PRINTED COPY OF THIS PROSPECTUS. IF THERE IS ANY DISCREPANCY BETWEEN THE CONTENTS OF THE ELECTRONIC PROSPECTUS AND THE CONTENTS OF THE PAPER/PRINTED COPY OF THIS PROSPECTUS FOR ANY REASON WHATSOEVER, THE CONTENTS OF THE PAPER/PRINTED COPY OF THIS PROSPECTUS WHICH ARE IDENTICAL TO THE COPY OF THIS PROSPECTUS REGISTERED WITH THE SC SHALL PREVAIL.

IN RELATION TO ANY REFERENCE IN THIS PROSPECTUS TO THIRD-PARTY INTERNET SITES (REFERRED TO AS "**THIRD-PARTY INTERNET SITES**"), WHETHER BY WAY OF HYPERLINKS OR BY WAY OF DESCRIPTION OF THE THIRD-PARTY INTERNET SITES, YOU ACKNOWLEDGE AND AGREE THAT:-

- I. WE AND OUR PRINCIPAL ADVISER DO NOT ENDORSE AND ARE NOT AFFILIATED IN ANY WAY TO THE THIRD-PARTY INTERNET SITES AND ARE NOT RESPONSIBLE FOR THE AVAILABILITY OF, OR THE CONTENT OR ANY DATA, INFORMATION, FILES OR OTHER MATERIAL PROVIDED ON THE THIRD-PARTY INTERNET SITES. YOU SHALL BEAR ALL RISKS ASSOCIATED WITH THE ACCESS TO OR USE OF THE THIRD-PARTY INTERNET SITES;
- II. WE AND OUR PRINCIPAL ADVISER ARE NOT RESPONSIBLE FOR THE QUALITY OF PRODUCTS OR SERVICES IN THE THIRD-PARTY INTERNET SITES, PARTICULARLY IN FULFILLING ANY OF THE TERMS OF YOUR AGREEMENTS WITH THE THIRD-PARTY INTERNET SITES. WE AND OUR PRINCIPAL ADVISER ARE ALSO NOT RESPONSIBLE FOR ANY LOSS OR DAMAGE OR COST THAT YOU MAY SUFFER OR INCUR IN CONNECTION WITH OR AS A RESULT OF DEALING WITH THE THIRD-PARTY INTERNET SITES OR THE USE OF OR RELIANCE ON ANY DATA, INFORMATION, FILES OR OTHER MATERIAL PROVIDED BY SUCH PARTIES; AND
- III. ANY DATA, INFORMATION, FILES OR OTHER MATERIAL DOWNLOADED FROM THE THIRD-PARTY INTERNET SITES IS DONE AT YOUR OWN DISCRETION AND RISK. WE AND OUR PRINCIPAL ADVISER ARE NOT RESPONSIBLE, LIABLE OR UNDER OBLIGATION FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA RESULTING FROM THE DOWNLOADING OF ANY SUCH DATA, INFORMATION, FILES OR OTHER MATERIAL.

WHERE AN ELECTRONIC PROSPECTUS IS HOSTED ON THE WEBSITES OF THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS, YOU ARE ADVISED THAT:-

- I. THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS ARE ONLY LIABLE IN RESPECT OF THE INTEGRITY OF THE CONTENTS OF AN ELECTRONIC PROSPECTUS, TO THE EXTENT OF THE CONTENTS OF THE ELECTRONIC PROSPECTUS ON THE WEB SERVERS OF THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS WHICH MAY BE VIEWED VIA YOUR WEB BROWSER OR OTHER RELEVANT SOFTWARE. THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS ARE NOT RESPONSIBLE IN ANY WAY FOR THE INTEGRITY OF THE CONTENTS OF AN ELECTRONIC PROSPECTUS WHICH HAS BEEN DOWNLOADED OR OBTAINED FROM THE WEB SERVERS OF THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS AND SUBSEQUENTLY, COMMUNICATED OR DISSEMINATED IN ANY MANNER TO YOU OR OTHER PARTIES; AND
- II. WHILE ALL REASONABLE MEASURES HAVE BEEN TAKEN TO ENSURE THE ACCURACY AND RELIABILITY OF THE INFORMATION PROVIDED IN AN ELECTRONIC PROSPECTUS, THE ACCURACY AND RELIABILITY OF AN ELECTRONIC PROSPECTUS CANNOT BE GUARANTEED BECAUSE THE INTERNET IS NOT A FULLY SECURE MEDIUM.

THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS ARE NOT LIABLE (WHETHER IN TORT OR CONTRACT OR OTHERWISE) FOR ANY LOSS, DAMAGE OR COST, YOU OR ANY OTHER PERSON MAY SUFFER OR INCUR DUE TO, AS A CONSEQUENCE OF OR IN CONNECTION WITH ANY INACCURACIES, CHANGES, ALTERATIONS, DELETIONS OR OMISSIONS IN RESPECT OF THE INFORMATION PROVIDED IN AN ELECTRONIC PROSPECTUS WHICH MAY ARISE IN CONNECTION WITH OR AS A RESULT OF ANY FAULTS WITH WEB BROWSERS OR OTHER RELEVANT SOFTWARE, ANY FAULTS ON YOUR OR ANY THIRD-PARTY'S PERSONAL COMPUTER, OPERATING SYSTEM OR OTHER SOFTWARE, VIRUSES OR OTHER SECURITY THREATS, UNAUTHORISED ACCESS TO INFORMATION OR SYSTEMS IN RELATION TO THE WEBSITES OF THE INTERNET PARTICIPATING FINANCIAL INSTITUTIONS, AND/OR PROBLEMS OCCURRING DURING DATA TRANSMISSION WHICH MAY RESULT IN INACCURATE OR INCOMPLETE COPIES OF INFORMATION BEING DOWNLOADED OR DISPLAYED ON YOUR PERSONAL COMPUTER.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

INDICATIVE TIMETABLE

The indicative timetable for our IPO is set out below:-

Events	Date
Opening of Applications	20 May 2022
Closing of Applications	26 May 2022
Balloting of Applications	30 May 2022
Allotment/Transfer of our IPO Shares to successful applicants	7 June 2022
Listing	8 June 2022

If there are any changes to this timetable, we will advertise a notice of the changes in a widely circulated English and Bahasa Malaysia newspaper within Malaysia, and make an announcement of such changes on Bursa Securities' website accordingly.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

DEFINITIONS

The following terms in this Prospectus have the same meaning as set out below unless the term is defined otherwise or the context requires otherwise:-

“ACE Market”	: ACE Market of Bursa Securities
“Acquisitions”	: Acquisition of the entire equity interest of each of LE Global, LGMS Advanced Tech, Credence Defender and LGMS Academy by our Company for a total purchase consideration of RM22,299,000, all of which were fully satisfied by the issuance of 22,299,000 new Shares at an issue price of RM1.00 per Share. The Acquisitions, which were part of the Pre-IPO Restructuring, were completed on 30 August 2021
“Act”	: Companies Act 2016 of Malaysia
“ADA(s)”	: Authorised Depository Agent(s)
“AGM”	: Annual general meeting
“Application(s)”	: The application for the Issue Shares by way of Application Form, Electronic Share Application or Internet Share Application
“Application Form(s)”	: Application form(s) for the application of the Issue Shares accompanying this Prospectus
“ATM(s)”	: Automated teller machine(s)
“Authorised Financial Institution(s)”	: Authorised financial institution(s) participating in the Internet Share Application in respect of the payments for the Issue Shares
“BNM”	: Bank Negara Malaysia
“Board”	: Board of Directors of our Company
“Bonus Issue”	: Bonus issue of 342,305,000 LGMS Shares on the basis of 15.35 new LGMS Shares for every 1 existing LGMS Share. The Bonus Issue, which was part of the Pre-IPO Restructuring, was completed on 6 September 2021
“Bumiputera Investor(s)”	: Bumiputera investors as approved and recognised by the MITI
“Bursa Depository”	: Bursa Malaysia Depository Sdn Bhd (Registration No. 198701006854 (165570-W))
“Bursa Securities”	: Bursa Malaysia Securities Berhad (Registration No. 200301033577 (635998-W))
“CAGR”	: Compound annual growth rate
“CDS”	: Central Depository System
“CDS Account(s)”	: Securities account(s) established by Bursa Depository for a depositor pursuant to the SICDA and the rules of Bursa Depository for the recording of deposits of securities and dealings in such securities by the depositor
“CMSA”	: Capital Markets and Services Act 2007
“Constitution”	: Constitution of our Company
“COVID-19”	: Coronavirus disease, an infectious disease caused by the SARS-CoV-2 virus
“Director(s)”	: Directors of our Company and within the meaning given in Section 2(1) of the CMSA

DEFINITIONS (cont'd)

“DQS GmbH”	:	DQS GmbH through DQS Certification (M) Sdn Bhd (Registration No. 200501012268 (689316-X))
“EBIT”	:	Earnings before interest and taxation
“EBITDA”	:	Earnings before interest, taxation, depreciation and amortisation
“Electronic Prospectus”	:	A copy of this Prospectus that is issued, circulated or disseminated via the Internet, and/or an electronic storage medium, including but not limited to compact disc read-only memory (CD-ROMs)
“Electronic Share Application(s)”	:	Application(s) for the Issue Shares through a Participating Financial Institution’s ATM
“Eligible Person(s)”	:	Eligible Directors and employees of our Group as well as persons who have contributed to the success of our Group
“EPF”	:	Employees Provident Fund Board
“EPS”	:	Earnings per share
“FYE”	:	Financial year ended/ending, as the case may be
“Gilbert Chu”	:	Chu Kim Foong, our Group’s Chief Operating Officer who is one of the key senior management personnel and key technical personnel of our Group
“IDC”	:	International Data Corporation, a global provider of market intelligence, advisory services, and events for the IT, telecommunications, and consumer technology markets
“IFRS”	:	International Financial Reporting Standards
“IMR” or “Protégé”	:	Protégé Associates Sdn Bhd (Registration No. 200401037256 (675767-H)), the independent market researcher appointed for our IPO
“Industry Overview Report”	:	Industry overview report of the cybersecurity market in Malaysia prepared by Protégé, as set out in Section 7 of this Prospectus
“Internet Participating Financial Institution(s)”	:	Participating financial institution(s) for the Internet Share Application
“Internet Share Application”	:	Application for the Issue Shares through an Internet Participating Financial Institution
“IPO”	:	Initial public offering comprising the Public Issue and the Offer for Sale
“IPO Share(s)”	:	Collectively, the Issue Share(s) and the Offer Share(s)
“Issue Price” or “Offer Price” or “IPO Price”	:	The issue price/offer price of RM0.50 per Issue Share/Offer Share
“Issue Share(s)”	:	91,395,000 new LGMS Share(s) to be issued pursuant to the Public Issue
“Issuing House”	:	Tricor Investor & Issuing House Services Sdn Bhd (Registration No. 197101000970 (11324-H))
“IT”	:	Information technology
“LGMS” or our “Company”	:	LGMS Berhad (Registration No. 202001039091 (1395412-W))
“LGMS Group” or our “Group”	:	Collectively, LGMS and its subsidiaries and associate company

DEFINITIONS (cont'd)

“LGMS Reporter”	: The software developed by our Group known as LGMS Security Assessment Report Generator v1.0.0
“LGMS Share(s)” or “Share(s)”	: Ordinary share(s) in our Company
“Listing”	: Admission of our Company to the Official List and the listing of and quotation for the entire enlarged issued share capital of LGMS comprising 456,000,000 LGMS Shares on the ACE Market
“Listing Requirements”	: ACE Market Listing Requirements of Bursa Securities
“LPD”	: 22 April 2022, being the latest practicable date prior to the registration of this Prospectus
“Malaysian Public”	: Citizens of Malaysia and companies, societies, co-operatives and institutions incorporated and organised under the laws of Malaysia
“Market Day(s)”	: A day(s) on which Bursa Securities is open for trading of securities
“MASB”	: Malaysian Accounting Standards Board
“MCO”	: Movement control order imposed by the Malaysian Government
“MFRS”	: Malaysian Financial Reporting Standards
“MIA”	: Malaysian Institute of Accountants
“MICPA”	: Malaysian Institute of Certified Public Accountants
“MITI”	: Ministry of International Trade and Industry, Malaysia
“NA”	: Net assets
“Offer for Sale”	: Offer for sale of 45,600,000 Offer Shares at the Offer Price by the Selling Shareholder by way of private placement to identified Bumiputera Investors
“Offer Share(s)”	: 45,600,000 existing LGMS Share(s) to be offered by the Selling Shareholder pursuant to the Offer for Sale
“Official List”	: A list specifying all securities listed on Bursa Securities
“Participating Financial Institution(s)”	: Participating financial institutions for the Electronic Share Application
“PAT”	: Profit after taxation
“PBT”	: Profit before taxation
“Pink Application Form(s)”	: Application form(s) for the application of Issue Shares by our Eligible Person(s) accompanying this Prospectus
“Pink Form Allocations”	: Allocation of 12,500,000 Issue Shares to our Eligible Persons, which forms part of our Public Issue
“Placement Agreement(s)”	: The placement agreements dated 27 April 2022 entered into between (i) our Company and the Placement Agent; and (ii) the Selling Shareholder and the Placement Agent in relation to the placement of the Issue Shares and Offer Shares
“Pre-IPO Restructuring”	: Collectively, the Acquisitions and the Bonus Issue
“Promoter(s)”	: Collectively or individually, Fong Choong Fook and Goh Soon Sei

DEFINITIONS (cont'd)

“Prospectus”	:	This prospectus dated 20 May 2022 issued by our Company in respect of our IPO
“Prospectus Guidelines”	:	Prospectus Guidelines issued by the SC
“Public Issue”	:	Public issue of 91,395,000 Issue Shares at the Issue Price, comprising the following:- (a) 22,800,000 Issue Shares made available for application by the Malaysian Public through a balloting process, of which 11,400,000 Issue Shares will be set aside for Bumiputera individuals, companies, societies, co-operatives and institutions; (b) 12,500,000 Issue Shares reserved for application by our Eligible Persons; (c) 44,695,000 Issue Shares by way of private placement to identified institutional and/or selected investors; and (d) 11,400,000 Issue Shares by way of private placement to identified Bumiputera Investors
“R&D”	:	Research and development
“ROC”	:	Registrar of Companies of Malaysia
“SAC”	:	Shariah Advisory Council of the SC
“SC”	:	Securities Commission Malaysia
“Selling Shareholder”	:	Fong Choong Fook, who is one of our Promoters, the Executive Chairman and a substantial shareholder of our Company
“Share Registrar”	:	Tricor Investor & Issuing House Services Sdn Bhd (Registration No. 197101000970 (11324-H))
“SICDA”	:	Securities Industry (Central Depositories) Act, 1991
“SOCISO”	:	Social Security Organisation
“SST”	:	Self-service terminal
“TÜV TRUST IT”	:	TÜV Trust IT GmbH Unternehmensgruppe TÜV Austria (Company VAT No. DE266780629)
“Underwriting Agreement”	:	Underwriting agreement dated 27 April 2022 between our Company and the Underwriter in relation to 22,800,000 Issue Shares under the Public Issue as set out in Section 3.3.1(i) of this Prospectus, and 12,500,000 Issue Shares under the Pink Form Allocation as set out in Section 3.3.1(ii) of this Prospectus
“UOBKH” or “Principal Adviser” or “Sponsor” or “Underwriter” or “Placement Agent”	:	UOB Kay Hian Securities (M) Sdn Bhd (Registration No. 199001003423 (194990-K))
“USA”	:	United States of America
“White Application Form(s)”	:	Application form(s) for the application of Issue Shares by the Malaysian Public accompanying this Prospectus

DEFINITIONS (cont'd)

Currencies and Unit

“EUR”	:	Euro
“RM” and “sen”	:	Ringgit Malaysia and sen
“SGD”	:	Singapore Dollar
“sq ft”	:	Square feet
“USD”	:	United States dollar

Our Subsidiaries:

“Applied Security”	:	Applied Security Intelligence Sdn Bhd (Registration No. 202001035047 (1391368-M))
“Credence Defender”	:	Credence Defender Sdn Bhd (Registration No. 201201037480 (1021962-T))
“LE Global”	:	LE Global Services Sdn Bhd (Registration No. 200501018357 (700472-M))
“LGMS Academy”	:	LGMS Academy Sdn Bhd (Registration No. 202001042702 (1399023-X))
“LGMS Advanced Tech”	:	LGMS Advanced Tech Sdn Bhd (Registration No. 201501042813 (1168134-M)) (formerly known as LGMS Group Sdn Bhd)

Our Associate Company:

“TUV Austria Cybersecurity Lab”	:	TUV Austria Cybersecurity Lab Sdn Bhd (Registration No. 201701002152 (1216302-X))
---------------------------------	---	---

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

GLOSSARY TERMS

The following commonly used terms in the Group's business and operations shall apply throughout this Prospectus unless the term is defined otherwise or the context otherwise requires:-

"ACFE"	:	Association of Certified Fraud Examiners An anti-fraud organisation and provider of anti-fraud training and education
"CIS"	:	Center for Internet Security An independent non-profit organisation, responsible for the CIS Controls and CIS Benchmarks, which are globally recognised best practices for security IT systems and data
"CISSP"	:	Certified Information Systems Security Professional An information security certification for security analysts granted by the (ISC) ²
"Cloud"	:	Software and services that run on the Internet instead of the computer
"COBIT"	:	Control Objectives for Information and Related Technology A framework for enterprise governance of information and technology that is created by the ISACA
"Common Criteria"	:	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408:2009) An internationally recognised standard for computer security certification which is recognised by all the signatories of the Common Criteria Recognition Arrangement, namely Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Republic of Korea, Singapore, Spain, Sweden, Turkey, USA, Austria, Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Indonesia, Israel, Pakistan, Poland, Qatar, Slovak Republic and United Kingdom
"CREST"	:	The Council for Registered Ethical Security Testers An international not-for-profit accreditation and certification body that represents and supports the technical information security market
"CSA"	:	Cloud Security Alliance An organisation dedicated to defining and raising awareness of best practices to help ensure a secure computing environment
"CSP"	:	Customer Security Programme (by SWIFT) A programme which helps financial institutions ensure their defences against cyber attacks are up to date and effective, to protect the integrity of the wider financial network
"Cyber attack"	:	A deliberate and malicious attempt or exploitation of computer systems (including computing devices) and networks to steal controlled information, disrupt, disable, destroy or control the computing environment or infrastructure, and/or destroying the integrity of the data
"Cybersecurity"	:	The application of technologies, processes and practices to help protect the availability, confidentiality and integrity of computer systems, networks and data against cyber attacks
"EAL"	:	Evaluation Assurance Level A numerical grade assigned to an IT product or system after the completion of the Common Criteria security evaluation

GLOSSARY TERMS (cont'd)

“GIAC”	:	Global Information Assurance Certification An information security certification entity which provides skill-specific certifications that are directly aligned with critical information security job duties
“Hacktivist”	:	Someone who attacks computer systems for socially or politically motivated purpose(s)
“ICT”	:	Information and communications technology Communication technologies including the Internet, computers, software, smartphones and other media applications and services that enable users to access, transmit, store, retrieve and manipulate information in digital form
“IEC”	:	International Electrotechnical Commission A global non-profit organisation involved in the preparation and publication of international standards for all electrical, electronic and related technologies, collectively known as “electrotechnology”
“Information security”	:	The processes or practices that protect information from unauthorised access, use, disclosure, disruption, modification or destruction to preserve the availability, confidentiality and integrity of the information
“IoT”	:	Internet of Things A system of interrelated physical objects with embedded computing technology (including software and sensors) that are able to collect and share data over the Internet
“IRCA”	:	International Register of Certificated Auditors A certification for systems audit professionals offered by the professional body known as Chartered Quality Institute (CQI)
“ISACA”	:	A global association (previously known as the Information Systems Audit and Control Association) that provides IT professionals with knowledge, credentials, training and community in audit, governance, risk, privacy and cybersecurity
“(ISC) ² ”	:	International Information Systems Security Certification Consortium, Inc An international non-profit membership association that specialises in training and certifications for cybersecurity professionals
“ISMS”	:	Information security management system A set of policies and procedures for systematically establishing, operating, monitoring, reviewing, maintaining and improving an organisation’s information to ensure its availability, confidentiality and integrity
“ISO”	:	International Organisation for Standardisation An independent, non-governmental international organisation that develops voluntary, consensus-based, market-relevant International Standards
“IT”	:	Information technology The technology involving the development, maintenance, and the use of computer technology for creating, processing, storing, securing, transmitting and retrieving information in digital form
“MyCC Scheme”	:	Malaysian Common Criteria Evaluation and Certification Scheme A scheme for evaluating and certifying the security functionality of ICT products against ISO/IEC 15408 standard (which is known as Common Criteria)

GLOSSARY TERMS (cont'd)

“OWASP”	:	Open Web Application Security Project A non-profit foundation that works to improve the security of software
“PCI”	:	Payment Card Industry
“PCI ASV”	:	Payment Card Industry Approved Scanning Vendor A selected group of organisation with a set of security services and tools (which are tested and approved by the PCI SSC) to conduct external vulnerability technical scanning services to validate adherence with external scanning requirements of PCI DSS Requirement 11.2.2
“PCI DSS”	:	PCI Data Security Standard
“PCI SSC”	:	PCI Security Standards Council A global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide
“PECB”	:	Professional Evaluation and Certification Board (legal name “PECB Group, Inc”) A certification body which provides education and certification under ISO/IEC 17024 for individuals on a wide range of disciplines
“QSA”	:	Qualified Security Assessor Qualified Security Assessor companies are independent security organisations that have been qualified by the PCI SSC to validate an entity’s adherence to PCI DSS while Qualified Security Assessor employees are individuals who are employed by a Qualified Security Assessor company and have satisfied and continue to satisfy all Qualified Security Assessor requirements
“SSCP”	:	Systems Security Certified Practitioner A beginner certification that evaluates, tests and certifies an individual’s abilities in implementing and managing information security which was developed, maintained and monitored by (ISC) ² for entry-level candidates seeking a career or skills in information security
“SWIFT”	:	Society for Worldwide Interbank Financial Telecommunication (legal name “S.W.I.F.T. SCRL”)
“Threat actor”	:	A person, group or entity that is partially or wholly responsible for a cybersecurity incident that impacts or has the potential to impact the safety or security of a targeted person, group or entity
“TISAX”	:	Trusted Information Security Assessment Exchange An assessment and exchange mechanism for the information security of enterprises and allows recognition of assessment results among the participants in the automotive industry

PRESENTATION OF INFORMATION

Words incorporating the singular shall, where applicable, include the plural and vice versa. Words incorporating the masculine gender shall, where applicable, include the feminine and neuter genders and vice versa. References to persons shall include natural persons, firms, companies, body corporates and corporations.

References in this Prospectus to any provisions of statutes, rules, regulations, enactments or rules of stock exchange shall (where the context admits), be construed as reference to provisions of such statutes, rules, regulations, enactments or rules of stock exchange (as the case may be) as modified by any written law or (if applicable) amendments or re-enactment to the statutes, rules, regulations, enactments or rules of stock exchange for the time being in force. References to a time of day in this Prospectus shall be a reference to Malaysian time, unless otherwise stated.

References to “our Company” or “the Company” or “LGMS” in this Prospectus are made to LGMS Berhad (Registration No. 202001039091 (1395412-W)), references to “our Group” or “the Group” or “LGMS Group” are made to our Company and our subsidiaries and associate company and references to “we” or “us” or “our” or “ourselves” are made to our Company, and where the context requires, our Company and our subsidiaries and associate company. Unless the context otherwise requires, references to “management” are to our Directors and key senior management and key technical personnel as at the date of this Prospectus, and statements as to our beliefs, expectations, estimates and opinions are those of our management.

This Prospectus includes statistical data provided by us and various third parties and cites third-party projections regarding growth and performance of the industry in which we operate. This data is taken or derived from information published by industry sources and from our internal data. In each such case, the source is stated in this Prospectus, provided that where no source is stated, it can be assumed that the information originated from us. In particular, certain information in this Prospectus is extracted or derived from report(s) provided by Protégé for inclusion in this Prospectus. We have appointed Protégé to provide an independent market and industry review relating to an overview of the economy and industry in which we operate in. In compiling their data for the review, Protégé relied on its research methodology, industry sources, published materials, its private databanks and direct contacts within the industry. We believe that the statistical data and projections cited in this Prospectus are useful in helping you to understand the major trends in the industry in which we operate. However, neither we nor our advisers have independently verified these data. Neither we nor our advisers make any representation as to the correctness, accuracy or completeness of such data. Similarly, third-party projections cited in this Prospectus are subject to significant uncertainties that could cause actual data to differ materially from the projected figures. We give no assurance that the projected figures will be achieved. You should not place undue reliance on the statistical data and third-party projections cited in this Prospectus.

The information on our website, or any website directly or indirectly linked to our website does not form part of this Prospectus and you should not rely on it.

Any discrepancy in the tables between the amounts listed and the totals in this Prospectus are due to rounding.

FORWARD-LOOKING STATEMENTS

This Prospectus contains forward-looking statements. All statements other than statements of historical facts included in this Prospectus, including, without limitation, those regarding our financial position, business strategies, plans and objectives of our management for future operations, are forward-looking statements. Such forward-looking statements involve known and unknown risks, uncertainties, contingencies and other factors which may cause our actual results, our performance or achievements, or industry results, to be materially different from any future results, performance or achievements expressed or implied by such forward-looking statements. Such forward-looking statements are based on numerous assumptions regarding our present and future business strategies and the environment in which we will operate in the future. Such forward-looking statements reflect our management's current view with respect to future events and are not a guarantee of future performance.

Forward-looking statements can be identified by the use of forward-looking terminology such as the words "expect", "believe", "plan", "intend", "estimate", "anticipate", "aim", "forecast", "may", "will", "would", and "could" or similar expressions and include all statements that are not historical facts. Such forward-looking statements include, without limitation, statements relating to:-

- i. demand for our services;
- ii. our business strategies and potential growth opportunities;
- iii. our management's plans and objectives for future operations;
- iv. our financial position;
- v. our future earnings, cash flows and liquidity; and
- vi. our ability to pay future dividends.

Our actual results may differ materially from information contained in the forward-looking statements as a result of a number of factors beyond our control, including, without limitation:-

- i. the general economic, business, social, political and investment environment in Malaysia; and
- ii. government policy, legislation and regulation affecting us or the industry in which we operate.

Additional factors that could cause our actual results, performance or achievements to differ materially include, but are not limited to those discussed in **Section 4** of this Prospectus on risk factors and **Section 11.3** of this Prospectus on management's discussion and analysis of the financial condition and financial performance. We cannot give any assurance that the forward-looking statements made in this Prospectus will be realised. These forward-looking statements are based on information made available to us as at the LPD.

In light of these uncertainties, the inclusion of such forward-looking statements should not be regarded as a representation or warranty by us or our advisers that such plans and objectives will be achieved.

Should we become aware of any subsequent material change or development affecting a matter disclosed in this Prospectus arising from the date of registration of this Prospectus but before the date of allotment of Issue Shares, we shall further issue a supplemental or replacement prospectus, as the case may be, in accordance with the provision of Section 238(1) of the CMSA and Paragraph 1.02, Chapter 1 of Part II (Division 6) of the Prospectus Guidelines (Supplementary and Replacement Prospectus).

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

	Page
CORPORATE DIRECTORY	1
1. INTRODUCTION	4
1.1 Approvals and conditions	4
1.2 Moratorium on our Shares	5
2. PROSPECTUS SUMMARY	7
2.1 Principal details of our IPO	7
2.2 History and business	7
2.3 Competitive strengths	8
2.4 Future plans and business strategies	9
2.5 Risk factors	9
2.6 Our Directors, key senior management and key technical personnel	12
2.7 Our Promoters and substantial shareholders	13
2.8 Use of proceeds	13
2.9 Financial highlights	14
2.10 Dividend policy	16
2.11 Impact of COVID-19	16
3. DETAILS OF OUR IPO	17
3.1 Opening and closing of Applications	17
3.2 Indicative timetable	17
3.3 Details of our IPO	17
3.4 Basis of arriving at the price of our IPO Shares	23
3.5 Dilution	24
3.6 Use of proceeds	25
3.7 Brokerage, underwriting commission and placement fee	33
3.8 Underwriting arrangement	33
4. RISK FACTORS	36
4.1 Risks relating to our business and operations	36
4.2 Risks relating to the industry in which we operate	44
4.3 Risks relating to investment in our Shares	47
4.4 Other risks	49
5. INFORMATION OF OUR GROUP	50
5.1 Our Company	50
5.2 Share Capital	50
5.3 Pre-IPO Restructuring	51
5.4 Our Group structure	53
5.5 Our subsidiaries and associate company	55
5.6 Public take-overs	59
5.7 Material investments and material divestitures	60

TABLE OF CONTENTS (cont'd)

	Page
6. BUSINESS OVERVIEW	61
6.1 History and Background	61
6.2 Description of our business	65
6.3 Competitive strengths	82
6.4 Impact of COVID-19 on our Group	86
6.5 Operational process and facilities	88
6.6 Technology used	90
6.7 Our business segments and markets	90
6.8 Marketing and sales activities	95
6.9 Seasonality	97
6.10 Employees	97
6.11 Insurance	98
6.12 Major customers	99
6.13 Major suppliers	102
6.14 Types, sources and availability of supplies	103
6.15 Major licenses and permits	103
6.16 Certifications and qualifications	104
6.17 Material trademarks and other intellectual property rights	109
6.18 Material properties, machinery and equipment.....	110
6.19 Governing laws and regulations.....	112
6.20 Dependency on contracts, agreements, documents or other arrangements	113
6.21 Productive capacity and extent of utilisation	113
6.22 Research and development	113
6.23 Interruptions to business and operations	114
6.24 Environmental matters	114
6.25 Future plans and business strategies	114
7. INDUSTRY OVERVIEW.....	117

TABLE OF CONTENTS (cont'd)

	Page
8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL	128
8.1 Promoters and substantial shareholders	128
8.2 Directors	133
8.3 Board practice	143
8.4 Key senior management	148
8.5 Key technical personnel	151
8.6 Remuneration of Directors and key senior management.....	152
8.7 Involvement of our key senior management and key technical personnel in other businesses and corporations outside our Group	154
8.8 Declaration from our Promoters, Directors, key senior management and key technical personnel	155
8.9 Family relationships and/or associates	155
8.10 Service agreements	155
8.11 Management reporting structure	156
9. RELATED PARTY TRANSACTIONS	157
9.1 Related party transactions	157
9.2 Related party transactions that are unusual in their nature or conditions.....	157
9.3 Outstanding loans and/or financial assistance (including guarantees of any kind) made to or for the benefit of related parties.....	157
9.4 Monitoring and oversight of related party transactions.....	158
10. CONFLICT OF INTEREST	159
10.1 Interest in businesses which carry on similar trade as our Group or businesses of our customers or suppliers.....	159
10.2 Declaration by advisers for our IPO	159
11. FINANCIAL INFORMATION	160
11.1 Historical statements of profit or loss and other comprehensive income.....	160
11.2 Reporting Accountants' report on the compilation of the pro forma consolidated statement of financial position as at 31 December 2021	163
11.3 Management's discussion and analysis of the financial condition and financial performance	175
11.4 Liquidity and capital resources	202
11.5 Trend information	219
11.6 Dividend policy	219
12. ACCOUNTANTS' REPORT	221

TABLE OF CONTENTS (cont'd)

	Page
13. STATUTORY AND OTHER GENERAL INFORMATION	312
13.1 Share capital	312
13.2 Extracts of our Constitution	312
13.3 Limitation on the rights to hold securities and/or exercise voting rights	319
13.4 Deposited securities and rights of Depositors	320
13.5 Material contracts	320
13.6 Material litigation	320
13.7 Repatriation of capital and remittance of profit	320
13.8 Letters of consent	321
13.9 Documents available for inspection	321
13.10 Responsibility statements	321
14. SUMMARISED PROCEDURES FOR APPLICATION AND ACCEPTANCE	322
14.1 Opening and closing of Applications	322
14.2 Methods of Application	322
14.3 Eligibility	323
14.4 Application by way of Application Forms	324
14.5 Application by way of Electronic Share Application	325
14.6 Application by way of Internet Share Application	325
14.7 Authority of our Board and Issuing House	325
14.8 Over/under-subscription	326
14.9 Unsuccessful/partially successful applicants	326
14.10 Successful applicants	327
14.11 Enquiries	328

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

CORPORATE DIRECTORY**DIRECTORS**

Name/(Designation)	Gender	Address	Nationality
Fong Choong Fook <i>(Executive Chairman)</i>	Male	63, Jalan DU 5/4 Kinrara Residence Taman Damai Utama 47180 Puchong Selangor Darul Ehsan	Malaysian
Goh Soon Sei <i>(Executive Director)</i>	Female	63, Jalan DU 5/4 Kinrara Residence Taman Damai Utama 47180 Puchong Selangor Darul Ehsan	Malaysian
Chan Kam Chiew <i>(Independent Non-Executive Director)</i>	Male	29 Bukit Kiara Residences Jalan Sri Hartamas 1 50480 Kuala Lumpur	Malaysian
Dr Teh Chee Ghee <i>(Independent Non-Executive Director)</i>	Male	15 Jalan Kenanga SD9/3C Bandar Sri Damansara 52200 Kuala Lumpur	Malaysian
Antonius Sommer <i>(Independent Non-Executive Director)</i>	Male	Kerbecke 27 D-45529 Hattingen Germany	German
Ts. Lim Mei Shyan <i>(Independent Non-Executive Director)</i>	Female	6, Jalan Jati SD 4/2 Bandar Sri Damansara 52200 Kuala Lumpur	Malaysian

AUDIT COMMITTEE

Name	Designation	Directorship
Chan Kam Chiew	Chairman	Independent Non-Executive Director
Dr Teh Chee Ghee	Member	Independent Non-Executive Director
Ts. Lim Mei Shyan	Member	Independent Non-Executive Director

REMUNERATION COMMITTEE

Name	Designation	Directorship
Dr Teh Chee Ghee	Chairman	Independent Non-Executive Director
Chan Kam Chiew	Member	Independent Non-Executive Director
Ts. Lim Mei Shyan	Member	Independent Non-Executive Director

CORPORATE DIRECTORY (cont'd)

NOMINATION COMMITTEE

Name	Designation	Directorship
Chan Kam Chiew	Chairman	Independent Non-Executive Director
Dr Teh Chee Ghee	Member	Independent Non-Executive Director
Ts. Lim Mei Shyan	Member	Independent Non-Executive Director

RISK MANAGEMENT COMMITTEE

Name	Designation	Directorship
Dr Teh Chee Ghee	Chairman	Independent Non-Executive Director
Chan Kam Chiew	Member	Independent Non-Executive Director
Antonius Sommer	Member	Independent Non-Executive Director
Fong Choong Fook	Member	Executive Chairman

COMPANY SECRETARIES

: **Siew Suet Wei**

Professional qualification: Malaysian Institute of Chartered Secretaries and Administrators (“**MAICSA**”) Chartered Secretary and Chartered Governance Professional, Fellow of the MAICSA
(MAICSA 7011254 / SSM PC No. 202008001690)

Lim Yen Teng

Professional qualification: Masters in Business Administration from Universiti Tunku Abdul Rahman
(LS 0010182 / SSM PC No. 201908000028)

5-9A, The Boulevard Offices
Mid Valley City
Lingkaran Syed Putra
59200 Kuala Lumpur

Tel : (03) 2282 6331

Fax : (03) 2201 9331

REGISTERED OFFICE

: 5-9A, The Boulevard Offices
Mid Valley City
Lingkaran Syed Putra
59200 Kuala Lumpur

Tel : (03) 2282 6331

Fax : (03) 2201 9331

HEAD OFFICE

: A-11-01, Empire Office Tower
Jalan SS 16/1
47500 Subang Jaya
Selangor Darul Ehsan

Tel : (03) 8605 0155

Website : <https://lgms.global/>

Email : invest@lgms.global

CORPORATE DIRECTORY (cont'd)

- AUDITORS AND REPORTING ACCOUNTANTS** : Baker Tilly Monteiro Heng PLT
(LLP No. 201906000600 (LLP0019411-LCA))
(Firm No. AF 0117)
- Baker Tilly MH Tower
Level 10, Tower 1, Avenue 5
Bangsar South City
59200 Kuala Lumpur
- Tel : (03) 2297 1000
Fax : (03) 2282 9980
- Partner in charge: Paul Tan Hong
Professional qualifications: Chartered Accountant - Member of MIA (MIA Membership No.: 40209), Fellow Member of the Association of Chartered Certified Accountants (Approval No. 03459/11/2023 J)
- LEGAL ADVISER** : Rahmat Lim & Partners
Suite 33.01, Level 33
The Gardens North Tower
Mid Valley City, Lingkaran Syed Putra
59200 Kuala Lumpur
- Tel : (03) 2299 3888
Fax : (03) 2287 1616
- PRINCIPAL ADVISER, SPONSOR, UNDERWRITER AND PLACEMENT AGENT** : UOB Kay Hian Securities (M) Sdn Bhd
Suite 19.03, 19th Floor
Menara Keck Seng
203 Jalan Bukit Bintang
55100 Kuala Lumpur
- Tel : (03) 2147 1888
Fax : (03) 2147 1950
- INDEPENDENT MARKET RESEARCHER** : Protégé Associates Sdn Bhd
Suite C-09-12, Plaza Mont' Kiara
2, Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur
- Tel : (03) 6201 9301
- Managing Director's name: Seow Cheow Seng
Professional qualification: Masters in Business Administration from Charles Sturt University, Australia and Bachelor of Business majoring in Marketing from RMIT University, Australia
- ISSUING HOUSE AND SHARE REGISTRAR** : Tricor Investor & Issuing House Services Sdn Bhd
Unit 32-01, Level 32
Tower A, Vertical Business Suite
Avenue 3, Bangsar South
No. 8, Jalan Kerinchi
59200 Kuala Lumpur
- Tel : (03) 2783 9299
Fax : (03) 2783 9222
- LISTING SOUGHT** : ACE Market of Bursa Securities
- SHARIAH STATUS** : Approved by the SAC

1. INTRODUCTION

1.1 Approvals and conditions

We have obtained the approvals from the following authorities in relation to our Listing:-

(i) Bursa Securities

Bursa Securities had, vide its letter dated 26 January 2022, approved our admission to the Official List and listing of and quotation for our entire enlarged issued share capital comprising 456,000,000 Shares on the ACE Market of Bursa Securities ("**Bursa Securities' Approval**"). The Bursa Securities' Approval is subject to the following conditions:-

Details of conditions imposed	Status of compliance
(i) Submit the following information with respect to the moratorium on the shareholdings of the Promoters to Bursa Depository:- <ul style="list-style-type: none"> - Name of shareholders; - Number of Shares; and - Date of expiry of the moratorium for each block of Shares; 	To be complied
(ii) Approvals from other relevant authorities have been obtained for implementation of the Listing proposal;	Complied
(iii) Make the relevant announcements pursuant to paragraphs 8.1 and 8.2 of Guidance Notes 15 of the Listing Requirements of Bursa Securities;	To be complied
(iv) Furnish to Bursa Securities a copy of the schedule of distribution showing compliance with the public shareholding spread requirements based on the entire issued share capital of LGMS on the first day of Listing;	To be complied
(v) In relation to the public offering to be undertaken by LGMS, to announce at least 2 Market Days prior to the Listing date, the result of the offering including the following:- <ul style="list-style-type: none"> - Level of subscription of public balloting and placement; - Basis of allotment/allocation; - A table showing the distribution for placement tranche as per the format in Appendix I of Bursa Securities' Approval; and - Disclosure of placees who become substantial shareholders of LGMS arising from the public offering, if any. The overall distribution of LGMS's securities shall be properly carried out to mitigate any disorderly trading in the secondary market; and	To be complied
(vi) LGMS/UOBKH to furnish Bursa Securities with a written confirmation of its compliance with the terms and conditions of Bursa Securities' Approval upon the admission of LGMS to the Official List of the ACE Market.	To be complied

(ii) SC

Our Listing is an exempt transaction under Section 212(8) of the CMSA and is therefore not subject to the approval of the SC.

1. INTRODUCTION (cont'd)

The SC had, vide its letter dated 16 February 2022, approved the resultant equity structure of our Company pursuant to the Listing under the Bumiputera equity requirement for public listed companies, subject to LGMS allocating Shares equivalent to 12.50% of its enlarged number of issued Shares at the point of Listing to Bumiputera Investors. In addition, LGMS is to make available at least 50.00% of the Shares offered to the Malaysian public investors via balloting to Bumiputera public investors at the point of Listing.

The effects of the Listing on the equity structure of LGMS are as follows:-

Category of shareholders	As at 6 September 2021		After the Listing	
	No. of Shares	% of issued Shares	No. of Shares	% of enlarged issued Shares
Bumiputera				
- Bumiputera Investors	-	-	⁽¹⁾ 57,000,000	12.50
- Bumiputera public investors via balloting	-	-	⁽²⁾ 11,400,000	2.50
Total Bumiputera	-	-	68,400,000	15.00
Non-Bumiputera	364,605,000	100.00	387,600,000	85.00
Malaysians	364,605,000	100.00	456,000,000	100.00
Foreigners	-	-	-	-
Total	364,605,000	100.00	456,000,000	100.00

Notes:-

- (1) Based on the assumption that the Shares allocated to Bumiputera Investors shall be fully subscribed.
- (2) Based on the assumption that the Shares allocated to Bumiputera public investors via balloting shall be fully subscribed.

(iii) SAC

The SAC had vide its letter dated 28 October 2021, classified our securities as Shariah-compliant based on our audited financial statements for the FYE 31 December 2020.

(iv) MITI

The MITI had vide its letter dated 12 November 2021, taken note and had no objection to the listing of our Company on the ACE Market of Bursa Securities.

1.2 Moratorium on our Shares

In accordance with Rule 3.19(1) of the Listing Requirements, a moratorium will be imposed on the sale, transfer or assignment of Shares held by our Promoters as follows:-

- (i) the moratorium applies to the entire shareholdings of our Promoters for a period of 6 months from the date of our admission to the Official List of the ACE Market ("**First 6 Months Moratorium**");
- (ii) upon the expiry of the First 6 Months Moratorium, we must ensure that our Promoters' aggregate shareholdings amounting to at least 45% of the total number of issued Shares remain under moratorium for another period of 6 months ("**Second 6 Months Moratorium**"); and

1. INTRODUCTION (cont'd)

- (iii) upon the expiry of the Second 6 Months Moratorium, our Promoters may sell, transfer or assign up to a maximum of 1/3rd per annum (on a straight-line basis) of our Shares held under moratorium.

Details of our Promoters and their Shares which will be subject to moratorium are as follows:-

Promoters	Shares under the First 6 Months Moratorium		Shares under the Second 6 Months Moratorium	
	No. of Shares ('000)	⁽¹⁾ (%)	No. of Shares ('000)	⁽¹⁾ (%)
Fong Choong Fook	245,600	53.86	157,983	34.65
Goh Soon Sei	73,405	16.10	47,217	10.35
Total	319,005	69.96	205,200	45.00

Note:-

- (1) Based on our enlarged issued share capital comprising 456,000,000 Shares after our IPO.

In addition, our Promoters have also provided an undertaking that they will comply with the said moratorium conditions relating to the sale of the Shares as set out above.

The above moratorium, which is fully acknowledged and accepted by our Promoters, will be specifically endorsed on the share certificates representing the entire shareholdings of our Promoters to ensure that our Share Registrar does not register any transfer that contravenes the above moratorium restrictions.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

2. PROSPECTUS SUMMARY

This Prospectus Summary only highlights the key information from other parts of this Prospectus. It does not contain all the information that may be important to you. You should read and understand the contents of the whole Prospectus prior to deciding on whether to invest in our Shares.

2.1 Principal details of our IPO

Our IPO comprises the following:-

(a) Public Issue

91,395,000 Issue Shares at the IPO Price in the following manner:-

- (i) 22,800,000 Issue Shares made available for application by the Malaysian Public through a balloting process, of which 11,400,000 Issue Shares will be set aside for Bumiputera individuals, companies, societies, co-operatives and institutions;
- (ii) 12,500,000 Issue Shares reserved for application by our Eligible Persons;
- (iii) 44,695,000 Issue Shares by way of private placement to identified institutional and/or selected investors; and
- (iv) 11,400,000 Issue Shares by way of private placement to identified Bumiputera Investors.

(b) Offer for Sale

45,600,000 Offer Shares at the Offer Price by way of private placement to identified Bumiputera Investors.

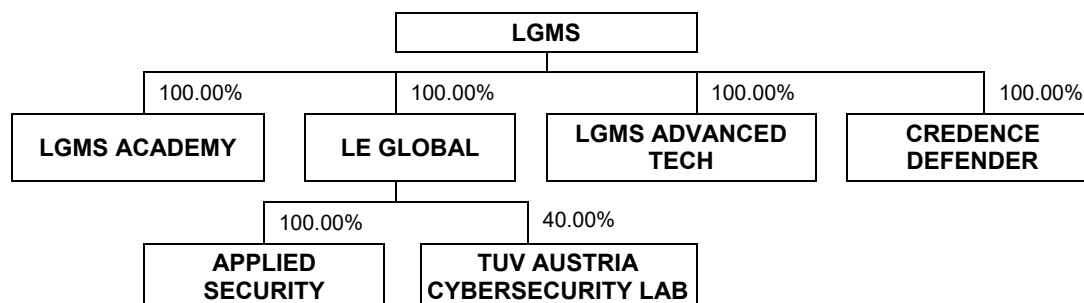
(c) Moratorium on our Shares

In accordance with Rule 3.19(1) of the Listing Requirements, a moratorium will be imposed on the sale, transfer or assignment of Shares held by our Promoters. Further details of the moratorium are set out in **Section 1.2** of this Prospectus. Save for the moratorium imposed on the Shares held by our Promoters, there is no other moratorium imposed on our Shares.

Please refer to **Section 3.3** of this Prospectus for further details on our IPO.

2.2 History and business

Our Company was incorporated in Malaysia on 30 November 2020 as a public limited company under the name of LGMS Berhad. Our Group structure as at the LPD is set out below:-



We are an independent provider of professional cybersecurity services, primarily involved in cybersecurity assessment and penetration testing, cyber risk management and compliance, and the provision of digital forensics and incident response services. We provide our professional cybersecurity services predominantly in Malaysia, being our primary market.

Please refer to **Section 6** of this Prospectus for further details on our history and business.

2. PROSPECTUS SUMMARY (cont'd)

2.3 Competitive strengths

Our competitive strengths are summarised as follows:-

2.3.1 Established track record and industry-wide recognitions

Our Group has been providing professional cybersecurity services since 2005 and we have been recognised by CyberSecurity Malaysia, IDC and other industry bodies (including accreditation and certification bodies) for our services as well as our contribution to the cybersecurity market. LE Global was awarded the 'Cyber Security Company of The Year' in 2017 by CyberSecurity Malaysia in recognition of its innovativeness, commitment, industry/product/service leadership and sound business strategies. LE Global had also been named as one of the key IoT penetration testing vendors in the 2018 IDC Report titled 'Asia/Pacific IoT Security Landscape and Key Vendors' by IDC, a global provider of market intelligence, advisory services, and events for the IT, telecommunications, and consumer technology markets.

2.3.2 Experienced senior management team with certified cybersecurity expertise

Our Group is spearheaded by our founders, our Executive Chairman, Fong Choong Fook and Executive Director, Goh Soon Sei, who are both veteran cybersecurity experts, and have participated in the cybersecurity market for more than 20 years and 15 years respectively. Other members of our key senior management team which consist of our Chief Operating Officer, Gilbert Chu and our Senior Director, Professional Services, Fow Chee Kang, have more than 10 years of working experience each in the cybersecurity market. Our team holds various key internationally recognised cybersecurity related certifications, which are highly regarded in the cybersecurity market. Most of the members of our key senior management team have been with us for more than 10 years and have been instrumental towards growing and sustaining our competitiveness in the cybersecurity market. Please refer to **Sections 8.1.3, 8.4.2 and 8.5.2** of this Prospectus for further details of the credentials of our Promoters and our key senior management and key technical personnel.

2.3.3 Strategic partnership with TÜV Austria Group

In 2019, we established a joint venture with TÜV TRUST IT via TUV Austria Cybersecurity Lab in which we have a 40% stake. The strategic partnership allows us to leverage on the established TÜV methodologies and branding in the business of providing testing and certification services. TÜV TRUST IT is a part of the TÜV Austria Group and is recognised in the field of information security and data protection as an objective, independent partner for consulting and certification services with an international customer base from across a wide range of industries. This collaboration was a key milestone for our Group.

2.3.4 A diversified customer base and long-term customer relationships help to drive customer retention, broaden revenue stream and maximise recurring income opportunities

With more than 15 years of operating history, we have an established local and international customer base across a broad range of industries. Our customers include major local banks and insurance companies, multinational companies and government agencies, some of whom have decade-long-standing relationships with us and are recurring or repeat customers that believe in our professional cybersecurity services.

2. PROSPECTUS SUMMARY (cont'd)

2.3.5 Independent cybersecurity provider focused on vulnerability assessment and penetration testing

We are an independent cybersecurity professional services provider that offers cybersecurity assessment, penetration testing, cyber risk management and compliance, and professional advice and recommendations to organisations on cybercrime and cybersecurity threats. We offer a wide range of vulnerability assessment and penetration testing services to our customers, using industry best practices as well as internationally recognised and accepted methodologies and cybersecurity tools. We also assist our customers to investigate cybersecurity incidents and undertake the necessary digital forensics and compromise assessment works.

Please refer to **Section 6.3** of this Prospectus for further information on our competitive strengths.

2.4 Future plans and business strategies

Our future plans and business strategies are summarised as follows:-

2.4.1 Purchasing an office premise in Klang Valley

We intend to purchase an office unit or building with a built-up area of at least 20,000 sq ft from the property market in Klang Valley to house our business operations including our digital forensics and IoT labs. This will allow us to save on our rental expenses of up to RM557,000 annually. The new facilities will allow us to scale up our operations and accommodate a larger workforce to support our growing customer base. As at the LPD, we have viewed 6 properties located in Ara Damansara, Bangsar and Petaling Jaya and have yet to identify a suitable property and will continue our search for a suitable property that meets our operational requirements.

2.4.2 Scaling up our operations by expanding our capability and developing our human capital

We want to scale up our operations to support our growing customer base and to continue developing the right professionals for our business. As part of our growth expansion, we plan to hire at least an additional 70 technical personnel in the next 2 years. We will provide them with on-the-job training and continue to support them to obtain internationally recognised cybersecurity certifications. We are also enhancing our capability in undertaking digital forensics as well as IoT assessments and testing.

2.4.3 Increasing our geographical footprint

We are embarking on an international expansion strategy and plan to have a localised direct presence in selected countries within the Southeast Asia region within the next 2 years. This is aimed to broaden our customer base, mitigate country-specific risk and allow us to ride on the potential growth in demand for cybersecurity services in the region. The countries identified for our initial international expansion are Singapore, Vietnam and Cambodia. We intend to set up a branch office in Singapore to provide direct operational and sales support to our existing customers. We will also be pursuing potential tie-ups and joint-ventures with local partners in Vietnam and Cambodia.

Please refer to **Section 6.25** of this Prospectus for further information on our future plans and business strategies.

2.5 Risk factors

Before investing in our Shares, you should carefully consider, along with the other matters set out in this Prospectus, the risks and investment considerations.

The following are some of the key risks affecting our business, operations and industry that we are currently facing or that may develop in the future.

2. PROSPECTUS SUMMARY (cont'd)

2.5.1 Risks relating to our business and operations

- (a) **Our business could suffer if we are unable to attract, train, motivate and retain senior management and other qualified technical personnel.** The cybersecurity market is growing and fast-changing with an overall shortage of skilled and experienced talent. Our technical teams are staffed with individuals with information technology and/or cybersecurity qualifications and professional certifications and given that there are limited number of individuals with the education, training and qualifications necessary to fill these roles, such individuals are in high demand. A high turnover and/or any reduction in numbers to the headcount of our senior management or other critical technical personnel may be disruptive to our business and may result in loss of crucial and confidential knowledge about our customers which, in turn, could lead to the loss of our customers. It may be difficult for us to find suitable and timely replacement(s) given the talent shortage.
- (b) **Real or perceived defects, errors or negligence in the provision of our services or any failure of our services to prevent a security breach could harm our reputation and cause us to lose customers.** While our vulnerability assessment and penetration testing services is done on a best effort basis to uncover all known vulnerabilities at the time of testing, there is no guarantee that our services will be able to detect other unknown vulnerabilities or vulnerabilities that are announced after the date of testing. There is also no assurance that our customers will implement our recommendations to address identified vulnerabilities. Although in general most of our customers would implement our recommendations, such implementation would be based on each customer's prioritised approach, which may not necessarily coincide with the risk levels which we have assigned to the identified vulnerabilities and may be affected by budget constraints and technological limitations faced by the customer. Any real or perceived defects, errors or negligence in the provision of our services, or any failure of our recommended preventive actions in detecting or preventing a cybersecurity threat, could harm our reputation and result in our customers delaying or withholding payment to us or electing not to renew their service agreements with us or to further engage us for our services.
- (c) **Our reputation may be harmed if the security of confidential information or personal information of our customers is breached or otherwise subject to unauthorised access or disclosure.** In the course of performing our services and with the consent of our customers, we will have access to confidential information of our customers. Notwithstanding our stringent policies and protocols, there is no guarantee that inadvertent disclosure or unauthorised disclosure or loss of personal or confidential information will not occur or that third parties will not gain unauthorised access to such information. Any data leakage, loss of data or security breaches to our IT infrastructures, whether actual or perceived, could adversely affect market perception of our services and our reputation. We could also be exposed to significant liability if we are subject to litigation or other action resulting in monetary damages and legal fees.
- (d) **Our business is dependent on the achievement and/or maintenance of certain certifications or standards and partnerships.** Our technical teams hold various internationally recognised cybersecurity related certifications (some of which are held by the Group while some are held personally by members of our technical team) and our Group has also established partnerships with certain international cybersecurity organisations to conduct training and examinations in Malaysia. In order to maintain these certifications and/or partnerships, we are required to comply with certain standards and/or obligations under the relevant partnership agreements such as annual audits.

2. PROSPECTUS SUMMARY (cont'd)

If our Group and/or our employees are late in achieving or fail to achieve or maintain compliance with these certifications and standards, we may be disqualified from selling our services to our customers. In addition, if our competitors achieve similar standards and certifications, we may lose our competitive advantage.

- (e) **If our services fail to help our customers achieve and maintain compliance with regulations and/or industry standards, our business, financial condition and financial performance could be harmed.** If we are unable to adapt our services to changing legal and regulatory standards or other requirements in a timely manner, or if our cybersecurity advisory services fail to assist with, or expedite, our customers' cybersecurity prevention and compliance efforts, our customers may lose confidence in our services. In addition, if laws, regulations or standards related to data security, vulnerability management and other IT security and compliance requirements are relaxed or the penalties on the non-compliances are amended to be less onerous, our customers may deprioritise government and industry best practice cybersecurity compliance as they may consider such compliance to be less critical to their businesses.
- (f) **We are dependent on customers within the financial services and telecommunications and media industries.** Our customers from the financial services and telecommunications and media industries in aggregate accounted for approximately 72.76%, 66.63%, 67.29% and 55.03% of our total revenue for the past 4 FYEs 2018, 2019, 2020 and 2021 respectively. Any variety of changes in the financial services and/or the telecommunications and media industries could adversely affect our business, financial condition and financial performance such as reduction in expenditure on technology and cybersecurity based on changes in economic conditions and other factors.

2.5.2 Risks relating to the industry in which we operate

- (a) **We operate in a highly competitive environment and competitive pressures are expected to increase in the future, which could adversely affect our business, financial conditions and financial performance.** The cybersecurity market is highly competitive, fragmented and characterised by rapid changes in technology, heightening industry standards and best practices, changing customer requirements, increasingly sophisticated cyber attacks, and frequent introduction of new or improved products and/or services to combat cybersecurity threats. Competitive pressures or our failure to compete effectively may result in price reductions, reduced margins, loss of market share and inability to gain market share, and a decline in revenue.
- (b) **The lack of sophistication of the regulatory landscape and customer awareness on the evaluation criteria for selection of cybersecurity service providers in Malaysia.** The regulatory landscape and the level of customer awareness in Malaysia on the evaluation criteria for selection of cybersecurity service providers lack sophistication compared to other developed nations. There are currently no detailed local guidelines or regulatory standards for assessing the credibility and track record of cybersecurity players in the local cybersecurity market in Malaysia. As customers are often left to their own devices to conduct due diligence on their cybersecurity service providers, there is no assurance that we will be able to successfully differentiate ourselves in the local cybersecurity market and leverage on our cybersecurity accreditations.

2. PROSPECTUS SUMMARY (cont'd)

- (c) **Our financial performance will suffer if we fail to anticipate changing customer requirements or industry and market developments, or we fail to adapt our business model to keep pace with the evolving cybersecurity threats from a variety of increasingly sophisticated cyber attacks.** Due to the challenges of ever changing customer requirements, rapid technological development, dynamics and evolving market trends as well as the emergence of new cybersecurity threats, we may be unable to keep abreast with the latest technologies and the ever evolving threats. We may also experience unanticipated delays in the offering of new solutions that would meet customer expectations. If our service offerings are not viewed by our customers as necessary or effective in addressing their cybersecurity needs, this may have an adverse impact on our business, financial condition and financial performance.
- (d) **Fluctuating economic conditions may have an adverse effect on demand for our services.** Economic weakness, customer financial difficulties, and constrained spending on cybersecurity may result in a decrease in our revenue and earnings and could make it difficult to ascertain and accurately forecast our operating results. If our customers are not convinced that our services should be an integral part of their overall approach to cybersecurity or if there is a general reduction in IT spending by our customers due to economic pressures, this will affect our business, financial condition and financial performance.
- (e) **Our business is dependent on the level of awareness of cybersecurity threats.** Based on our market observation, the majority of spending on cybersecurity in Malaysia to date has been on threat protection products which organisations may believe are considered sufficient to safeguard the access to sensitive business data. Premised on such notions, organisations may hence continue to deprioritise cybersecurity services such as ours and allocate their budget towards threat protection products and may not adopt our vulnerability assessment and penetration testing services in addition to, or in lieu of, such traditional products. If the number of cyber attacks were to decline, or companies or governments perceive that the general level of cyber attacks have declined, our ability to attract new customers and expand our offerings within existing customers could be materially and adversely affected.
- (f) **Our business operations and the use of technology are subject to evolving legal requirements regarding privacy throughout the world.** We currently operate our business in jurisdictions where we are subject to data protection or privacy laws and regulations, including but not limited to the Personal Data Protection Act 2010 in Malaysia (being our primary market) and we may also be subject to privacy and data protection laws and regulations in those jurisdictions in which our customers operate. There can be no assurance that such requirements will not change or that we will not otherwise be subject to legal or regulatory actions.

Please refer to **Section 4** of this Prospectus for further details on our risk factors.

2.6 Our Directors, key senior management and key technical personnel

Our Directors, key senior management and key technical personnel are set out as follows:-

Name	Designation
<u>Directors</u>	
Fong Choong Fook	Executive Chairman
Goh Soon Sei	Executive Director
Chan Kam Chiew	Independent Non-Executive Director

2. PROSPECTUS SUMMARY (cont'd)

Name	Designation
Dr Teh Chee Ghee	Independent Non-Executive Director
Antonius Sommer	Independent Non-Executive Director
Ts. Lim Mei Shyan	Independent Non-Executive Director
<u>Key senior management</u>	
Gilbert Chu	Chief Operating Officer
Fow Chee Kang	Senior Director, Professional Services
Lum Pui Yee	Financial Controller
<u>Key technical personnel</u>	
Fong Choong Fook	Executive Chairman
Goh Soon Sei	Executive Director
Gilbert Chu	Chief Operating Officer
Fow Chee Kang	Senior Director, Professional Services

Please refer to **Sections 8.1.3, 8.2.2, 8.4.2 and 8.5.2** of this Prospectus for further details of our Directors, key senior management and key technical personnel.

2.7 Our Promoters and substantial shareholders

Our Promoters and substantial shareholders, as well as their respective shareholdings in our Company, are set out as follows:-

Promoters and substantial shareholders	Nationality	Before the IPO				After the IPO			
		Direct		Indirect		Direct		Indirect	
		No. of Shares ('000)	(¹) (%)	No. of Shares ('000)	(%)	No. of Shares ('000)	(²) (%)	No. of Shares ('000)	(²) (%)
Fong Choong Fook	Malaysian	291,200	79.87	⁽³⁾ 73,405	20.13	245,600	53.86	⁽³⁾ 73,405	16.10
Goh Soon Sei	Malaysian	73,405	20.13	⁽³⁾ 291,200	79.87	73,405	16.10	⁽³⁾ 245,600	53.86
Total		364,605	100.00			319,005	69.96		

Notes:-

- (1) Based on our existing issued share capital comprising 364,605,000 Shares after the Pre-IPO Restructuring but before the Public Issue.
- (2) Based on our enlarged issued share capital comprising 456,000,000 Shares upon Listing.
- (3) Deemed interested by virtue of his or her spouse's interest pursuant to Section 8 of the Act.

Please refer to **Section 8.1.3** of this Prospectus for further details of our Promoters and substantial shareholders.

2.8 Use of proceeds

The gross proceeds from the Public Issue amounting to RM45.70 million based on the Issue Price of RM0.50 per Issue Share are expected to be used in the manner as set out below:-

2. PROSPECTUS SUMMARY (cont'd)

Details of use	Estimated timeframe for use upon Listing	RM'000	Percentage of gross proceeds (%)
1. Business expansion			
• Purchase of office	Within 12 to 24 months	18,000	39.39
• Expansion of workforce	Within 24 months	6,500	14.22
• Capital expenditure on equipment and tools	Within 24 months	6,000	13.13
• Strategic business expansion	Within 24 months	7,698	16.85
		38,198	83.59
2. Working capital	Within 12 months	3,500	7.66
3. Estimated listing expenses	Within 3 months	4,000	8.75
Total		45,698	100.00

Our Company will not receive any proceeds from the Offer for Sale as such proceeds will go directly to our Selling Shareholder. The gross proceeds from the Offer for Sale is approximately RM22.80 million based on the Offer Price of RM0.50 per Offer Share.

Please refer to **Section 3.6** of this Prospectus for further details on the use of proceeds from the Public Issue.

2.9 Financial highlights

The historical financial information presented below should be read in conjunction with the management's discussion and analysis of the financial condition and financial performance as set out in **Section 11.3** of this Prospectus and the Accountants' Report, together with the accompanying notes, assumptions and bases as set out in **Section 12** of this Prospectus. There were no audit qualifications on our audited financial statements for the past 4 FYEs 31 December 2018, 2019, 2020 and 2021.

Historical statements of profit or loss and other comprehensive income

The following table sets out a summary of the audited financial information for the past 4 FYEs 31 December 2018, 2019, 2020 and 2021.

	Audited			
	FYE 31 December			
	2018	2019	2020	2021
	(RM'000)	(RM'000)	(RM'000)	(RM'000)
Revenue	17,387	20,563	20,649	28,262
Operating profit	8,042	8,466	10,573	14,337
PBT	8,018	8,441	10,611	14,285
PAT	5,991	6,329	8,074	10,305
EBITDA ⁽¹⁾	8,601	9,656	11,983	15,486
EBITDA margin (%) ⁽²⁾	49.47	46.96	58.03	54.79
Operating profit margin (%) ⁽³⁾	46.25	41.17	51.20	50.73
PBT margin (%) ⁽⁴⁾	46.11	41.05	51.39	50.54
PAT margin (%) ⁽⁵⁾	34.46	30.78	39.10	36.46
Basic and diluted EPS (sen) ⁽⁶⁾	1.31	1.39	1.76	2.26

2. PROSPECTUS SUMMARY (cont'd)**Notes:-**

- (1) The table below sets out a reconciliation of our PBT to EBITDA:-

	Audited			
	FYE 31 December			
	2018	2019	2020	2021
	(RM'000)	(RM'000)	(RM'000)	(RM'000)
PBT	8,018	8,441	10,611	14,285
Adjusted for:-				
Finance costs	60	174	168	132
Interest income	(16)	(66)	(18)	(8)
Depreciation	539	1,107	1,222	1,077
EBITDA	8,601	9,656	11,983	15,486

- (2) EBITDA margin is computed based on the EBITDA over revenue of our Group.
- (3) Operating profit margin is computed based on the operating profit over revenue of our Group.
- (4) PBT margin is computed based on the PBT over revenue of our Group.
- (5) PAT margin is computed based on the PAT over revenue of our Group.
- (6) Basic and diluted EPS is computed based on PAT attributable to the owners of our Company divided by the number of issued Shares of 456,000,000 after our IPO. There are no dilutive instruments as at the end of the respective financial years.

Pro forma consolidated statement of financial position

We have prepared the pro forma consolidated statement of financial position below for illustrative purposes only, to show the effects of the IPO on the NA and gearing of our Group assuming that the IPO had been effected on 31 December 2021.

The pro forma consolidated statement of financial position should be read in conjunction with the Reporting Accountants' report on the pro forma consolidated statement of financial position as at 31 December 2021 and the notes thereon as set out in **Section 11.2** of this Prospectus.

The pro forma effects of the IPO on the NA and gearing of our Group are set out below:-

	Audited as at 31 December 2021 (RM'000)	Pro forma I (⁽³⁾After the Offer for sale (RM'000)	Pro forma II After the Public Issue (RM'000)	Pro forma III (⁽⁴⁾After the IPO and utilisation of proceeds (RM'000)
Share capital	22,300	22,300	67,998	(⁽⁵⁾ 66,364)
Reorganisation reserve	(20,649)	(20,649)	(20,649)	(20,649)
Retained earnings	26,423	26,423	26,423	(⁽⁵⁾ 25,391)
Total Equity	28,074	28,074	73,772	71,106
No. of Shares in issue ('000)	364,605	364,605	456,000	456,000
NA per Share (RM)⁽¹⁾	0.08	0.08	0.16	0.16
Total borrowings (RM'000)	2,238	2,238	2,238	2,238
Gearing (times)⁽²⁾	0.08	0.08	0.03	0.03

Notes:-

- (1) Computed based on our NA attributable to owners of the Company divided by total number of issued Shares.
- (2) Computed based on our total borrowings divided by total equity as at 31 December 2021.
- (3) The Offer for Sale will not have any effect on the NA and gearing of our Group.
- (4) As at the LPD, there are no purchase orders, sale and purchase agreements or contractually binding agreements in relation to the utilisation of proceeds for the business expansion.

2. PROSPECTUS SUMMARY (cont'd)

- (5) *Out of the total estimated listing expenses of RM4.00 million, a total of RM1.33 million had already been incurred and charged to retained earnings account of LGMS as at 31 December 2021. Out of the remaining estimated listing expense to be incurred of RM2.67 million, RM1.63 million is assumed to be directly attributable to the Public Issue and will be capitalised under share capital upon Listing, whilst the balance of RM1.04 million will be charged to the profit or loss statement.*

Please refer to **Sections 11.2 and 12** of this Prospectus for further information on our financial information and the Reporting Accountants' letter on the pro forma consolidated statement of financial position as at 31 December 2021.

2.10 Dividend policy

At this juncture, our Board has not adopted a formal dividend payout policy. Any dividend declared will be subject to the recommendation of our Board, taking into consideration our Group's capital structure and ensuring sufficient funds for our future growth. Any final dividends declared will be subject to the approval of our shareholders at our AGM. The dividends declared and paid for the past 4 FYEs 2018, 2019, 2020 and 2021 are as follows:-

	FYE 2018 (RM'000)	FYE 2019 (RM'000)	FYE 2020 (RM'000)	FYE 2021 (RM'000)
Dividend declared in respect of	-			
• FYE 2019		3,583	-	-
• FYE 2020		-	5,500	-
• FYE 2021		-	-	3,800
Dividend paid in respect of	-			
• FYE 2019		2,000	1,583	-
• FYE 2020		-	4,500	1,000
• FYE 2021		-	-	3,800

Our Board does not intend to declare any further dividends prior to our Listing.

Please refer to **Section 11.6** of this Prospectus for further details on our dividend policy.

2.11 Impact of COVID-19

COVID-19 was officially declared a health pandemic by the Director-General of the World Health Organisation on 11 March 2020. Throughout 2020 and 2021, several phases of the MCO were implemented in the country to curb the spread of the COVID-19 pandemic with varying levels of restrictions. On 16 March 2020, the Malaysian Government announced the MCO under the Prevention and Control of Infectious Diseases Act 1988 and the Police Act 1967 effective from 18 March 2020 to 3 May 2020. During the MCO period, all government and private premises (saved for those involved in essential services or industries which had special permission) are required to be closed. Thereafter, the MCO was relaxed in stages to allow all economic sectors and businesses to resume operations on a staggered basis, subject to compliance with the prescribed standard operating procedures.

We closely monitor the development of the pandemic through the various levels of lockdown measures imposed in Malaysia and the jurisdictions in which our customers operate. As we have adopted flexible working arrangements even prior to the COVID-19 pandemic, our business operations have not been adversely impacted as our employees are able to operate at full capacity and just as effectively, working from home (remotely). As for overseas engagements, we have been able to work remotely despite the travel restrictions. We have been able to enjoy savings on operational expenses due to reduced spending on business travels. As Malaysia transitions to the "Endemic" phase on 1 April 2022, all restrictions limiting business operating hours and number of employees in a workplace based on vaccination coverage has been uplifted. As such, we do not expect any further closures or restrictions to impact our business operations. Please refer to **Section 6.4** of this Prospectus for further details on the impact of COVID-19 on our Group.

3. DETAILS OF OUR IPO

3.1 Opening and closing of Applications

Applications for our IPO Shares will open at 10.00 a.m. on 20 May 2022 and will remain open until 5.00 p.m. on 26 May 2022. **Late applications will not be accepted.**

3.2 Indicative timetable

The indicative timetable for our IPO is set out below:-

Events	Date
Opening of Applications	20 May 2022
Closing of Applications	26 May 2022
Balloting of Applications	30 May 2022
Allotment/Transfer of our IPO Shares to successful applicants	7 June 2022
Listing	8 June 2022

If there are any changes to this timetable, we will advertise a notice of the changes in a widely circulated English and Bahasa Malaysia newspaper within Malaysia, and make an announcement of such changes on Bursa Securities' website accordingly.

3.3 Details of our IPO

Our IPO is subject to the terms and conditions of this Prospectus and upon acceptance, our IPO Shares are expected to be allocated in the manner described below, subject to the clawback and reallocation provisions as set out in **Section 3.3.3** of this Prospectus:-

	No. of IPO Shares	Percentage of our enlarged issued share capital (%)
Public Issue		
(i) Malaysian Public ⁽¹⁾	22,800,000	5.00
(ii) Eligible Persons	12,500,000	2.74
(iii) Private placement to identified institutional and/or selected investors	44,695,000	9.80
(iv) Private placement to identified Bumiputera Investors	11,400,000	2.50
	91,395,000	20.04
Offer for Sale		
Private placement to identified Bumiputera Investors	45,600,000	10.00
Total	136,995,000	30.04

Note:-

(1) Out of the 22,800,000 Issue Shares, 11,400,000 Issue Shares will be set aside for Bumiputera individuals, companies, societies, co-operatives and institutions.

3. DETAILS OF OUR IPO (cont'd)**3.3.1 Public Issue**

We are offering 91,395,000 Issue Shares at an Issue Price of RM0.50 payable in full on application, representing approximately 20.04% of our enlarged issued share capital after the IPO, in the following manner:-

(i) Malaysian Public

22,800,000 Issue Shares, representing 5.00% of the enlarged issued share capital of our Company, are available for application by the Malaysian Public through a balloting process, of which 11,400,000 Issue Shares, representing 2.50% of the enlarged issued share capital of our Company, will be set aside for Bumiputera individuals, companies, societies, co-operatives and institutions. Any Issue Shares not subscribed by such Bumiputera investors will be made available for application by other Malaysian Public.

(ii) Eligible Persons

12,500,000 Issue Shares, representing 2.74% of the enlarged issued share capital of our Company ("**Pink Form Shares**") have been reserved and set aside for the Eligible Persons under the Pink Form Allocation.

The details of the number of Pink Form Shares set aside for the Eligible Persons are as follows:-

Eligible Persons	No. of Eligible Persons	Aggregate number of Pink Form Shares allocated
Directors of our Company ⁽¹⁾	4	950,000
Eligible employees of our Group ⁽²⁾	73	8,946,700
Persons who have contributed to our success ⁽³⁾	28	2,603,300
Total	105	12,500,000

Notes:-

- (1) *The criteria for allocation to our Directors is based on, amongst others, their respective roles and responsibilities in, and contribution to our Group. The number of Pink Form Shares to be allocated to our Directors are set out as follows:-*

Name	Designation	No. of Pink Form Shares to be allocated
<i>Chan Kam Chiew</i>	<i>Independent Non-Executive Director</i>	<i>250,000</i>
<i>Dr Teh Chee Ghee</i>	<i>Independent Non-Executive Director</i>	<i>250,000</i>
<i>Antonius Sommer</i>	<i>Independent Non-Executive Director</i>	<i>250,000</i>
<i>Ts. Lim Mei Shyan</i>	<i>Independent Non-Executive Director</i>	<i>200,000</i>
Total		950,000

- (2) *The basis and criteria for allocation of the Pink Form Shares to the eligible employees of our Group (excluding the Directors and employees of our associate company), as approved by our Board, is based on, amongst others, the following factors:-*

- (i) *the eligible employee must be a full time confirmed employee and be on the payroll of our Group; and*
- (ii) *the number of Pink Form Shares allocated to the eligible employees is based on their staff grade, length of service, past performance and level of contributions made to our Group, including any other factors considered relevant to our Board.*

3. DETAILS OF OUR IPO (cont'd)

The allocation to our eligible employees includes the allocation to the following key senior management:-

Name	Designation	No. of Pink Form Shares to be allocated
Gilbert Chu	Chief Operating Officer	1,800,000
Fow Chee Kang	Senior Director, Professional Services	800,000
Lum Pui Yee	Financial Controller	400,000
Total		3,000,000

(3) The allocation to persons who have contributed to our success, as approved by our Board, is determined based on amongst others, the length of business relationship with our Group, their current and past contributions and support to our business. The persons who have contributed to our success may include our customers, suppliers and business associates (including the Directors and employees of our associate company). For avoidance of doubt, these eligible persons are not parties related to our Promoters, substantial shareholders and Directors.

(iii) Private placement to identified institutional and/or selected investors

44,695,000 Issue Shares, representing approximately 9.80% of the enlarged issued share capital of our Company, allocated by way of private placement to identified institutional and/or selected investors.

(iv) Private placement to identified Bumiputera Investors

11,400,000 Issue Shares, representing approximately 2.50% of the enlarged issued share capital of our Company, allocated by way of private placement to identified Bumiputera Investors.

Any Issue Shares not taken up by the Malaysian Public or Eligible Persons under the Pink Form Allocation will be subject to the clawback and reallocation as set out in **Section 3.3.3** of this Prospectus, and the balance thereof will be underwritten. Please refer to **Section 3.8** of this Prospectus for further details of our underwriting arrangement. Applicants who subscribe for the Pink Form Shares under **Section 3.3.1(ii)** above may also apply for the Issue Shares available under the Malaysian Public portion.

Save for the allocation made available for application by Eligible Persons as disclosed in **Section 3.3.1(ii)** above, it is not known to our Company as to whether any of our substantial shareholders, Directors or member of the key senior management have the intention to apply for the Issue Shares allocated under the Malaysian Public portion.

Meanwhile, the 44,695,000 Issue Shares under **Section 3.3.1(iii)** above will be placed out to institutional and/or selected investors identified by our Placement Agent. These Issue Shares will be subject to irrevocable undertakings to be procured from such investors. The 11,400,000 Issue Shares under **Section 3.3.1(iv)** above will be placed out by our Placement Agent to identified Bumiputera Investors.

To the best of our knowledge and belief, there is no person who intends to subscribe for more than 5.00% of our IPO Shares.

3. DETAILS OF OUR IPO (cont'd)

3.3.2 Offer for Sale

Our Selling Shareholder will undertake an offer for sale of 45,600,000 Offer Shares at an Offer Price of RM0.50 per Offer Share, representing approximately 10.00% of the enlarged issued share capital of our Company, by way of private placement to identified Bumiputera Investors.

Details of our Selling Shareholder and the Shares offered for sale are set out as follows:-

Name and address	Nature of relationship with our Group for the past 3 years up to the LPD	Before our IPO		Shares offered pursuant to the Offer for Sale		After the Offer for Sale and the IPO ⁽³⁾	
		No. of Shares	(1)%	No. of Shares	(2)%	No. of Shares	(2)%
Fong Choong Fook 63, Jalan DU 5/4 Kinrara Residence Taman Damai Utama 47180 Puchong Selangor Darul Ehsan	Our Executive Chairman, Promoter and a substantial shareholder	291,200,040	79.87	45,600,000	10.00	245,600,040	53.86

Notes:-

- (1) Based on our existing issued share capital comprising 364,605,000 Shares after the Pre-IPO Restructuring but before the Public Issue.
- (2) Based on our enlarged issued share capital comprising 456,000,000 Shares upon Listing.
- (3) Assuming all 45,600,000 Offer Shares are fully placed out to identified Bumiputera Investors.

The 45,600,000 Offer Shares under the Offer for Sale will be placed out by our Placement Agent.

In the event of under-subscription of the Offer Shares, the remaining Offer Shares will then be clawed-back and reallocated to the identified institutional investors under **Section 3.3.1(iii)** of this Prospectus, and thereafter to the Bumiputera public investors under **Section 3.3.1(i)** of this Prospectus.

3. DETAILS OF OUR IPO (cont'd)

3.3.3 Clawback and reallocation

Our IPO Shares shall be subject to the following clawback and reallocation provisions:-

- (i) In the event there are Issue Shares not subscribed by the Malaysian Public and the Eligible Persons, the remaining portion will be made available for application by way of private placement to identified institutional and selected investors under **Section 3.3.1(iii)** of this Prospectus;
- (ii) In the event of over-subscription by the Malaysian Public and a corresponding undersubscription under **Sections 3.3.1(ii), 3.3.1(iii) and 3.3.1(iv)** of this Prospectus, the remaining portion will be clawed-back and be reallocated to the Malaysian Public; and
- (iii) If the Issue Shares and Offer Shares allocated to identified Bumiputera Investors are not fully subscribed, the remaining portion will be clawed-back and reallocated firstly, to the identified institutional investors under **Section 3.3.1(iii)** of this Prospectus, and thereafter to the Bumiputera public investors under **Section 3.3.1(i)** of this Prospectus.

The clawback and reallocation shall not apply in the event of over-subscription under **Sections 3.3.1(i), 3.3.1(ii), 3.3.1(iii), 3.3.1(iv) and 3.3.2** of this Prospectus. Any balance unsubscribed Issue Shares under **Section 3.3.3(i)** of this Prospectus (arising after the reallocation to the identified institutional investors) will not be subject to any further clawback and reallocation. Such Issue Shares will hence be fully underwritten by the Underwriter.

The basis of allocating the IPO Shares shall take into account the desirability of distributing the IPO Shares to a reasonable number of applicants with a view of broadening our shareholding base, to meet the public spread requirements of Bursa Securities as well as to establish a liquid and adequate market for our Shares. The applicants will be selected in a fair and equitable manner to be determined by our Board.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

3. DETAILS OF OUR IPO (cont'd)**3.3.4 Share capital**

Upon completion of our IPO, our share capital will be as follows:-

	No. of Shares	RM
Issued share capital before the IPO	364,605,000	22,300,000
New Shares to be issued under the Public Issue ⁽¹⁾	91,395,000	⁽²⁾ 45,697,500
Enlarged issued share capital upon Listing prior to utilisation of proceeds	456,000,000	67,997,500
Less: Estimated listing expenses	-	(1,633,000)
Enlarged issued share capital upon Listing and after utilisation of proceeds	456,000,000	⁽³⁾66,364,500
Shares to be offered under Offer for Sale	45,600,000	22,800,000
IPO Price per Share (RM)	-	0.50
Market capitalisation upon Listing (based on the IPO Price and enlarged number of issued Shares after our IPO) (RM)	-	228,000,000
Pro forma NA per Share (based on the pro forma consolidated statement of financial position as at 31 December 2021) (RM)	-	0.16

Notes:-

- (1) *The Offer for Sale and the Listing will not have any effect on the issued share capital of our Company.*
- (2) *Calculated based on the IPO Price.*
- (3) *After deducting the estimated listing expenses of approximately RM1.63 million which is directly attributable to the Public Issue and deducted against the share capital of our Company.*

3.3.5 Price stabilisation mechanism

We will not be employing any price stabilisation mechanism (which is in accordance with the Capital Markets and Services (Price Stabilisation Mechanism) Regulations 2008) for our IPO.

3.3.6 Classes of shares and ranking

There is only 1 class of shares in our Company, namely ordinary shares.

Our Issue Shares will, upon allotment and issue, rank equally in all respects with our other existing Shares, including voting rights, and will be entitled to all rights, dividends and distributions that may be declared subsequent to the date of allotment of the Issue Shares, subject to any applicable rules of Bursa Depository.

Our Offer Shares rank equally in all respects with our existing Shares, including voting rights, and will be entitled to all rights, dividends and distributions that may be declared subsequent to the date of transfer of the Offer Shares, subject to any applicable rules of Bursa Depository.

3. DETAILS OF OUR IPO (cont'd)

Subject to any special rights (amongst others, taking priority over our Shares in terms of the distribution of dividends or other profits) attaching to any Shares which we may issue in the future, our shareholders are, in proportion to the amount paid on the Shares held by them, entitled to share in the profits paid out by us in the form of dividends or other distributions. Similarly, if our Company is liquidated, our shareholders are entitled to the surplus (if any), in accordance with our Constitution after the satisfaction of any preferential payments in accordance with the Act and our liabilities.

At any general meeting of our Company, each shareholder is entitled to vote in person, by proxy, by attorney or by other duly authorised representative. Any resolution set out in the notice of any general meeting, or in any notice of resolution, is to be voted on by poll. On a poll, each shareholder present either in person, by proxy, by attorney or by other duly authorised representative shall have one vote for each Share held or represented. A proxy may but need not be a member of our Company. On a show of hands, each shareholder presents either in person, by proxy, by attorney or by other duly authorised representative shall have one vote.

3.3.7 Minimum level of subscription

There is no minimum subscription in terms of the proceeds to be raised from the IPO. However, in order to comply with the public shareholding spread requirement under the Listing Requirements, the minimum subscription level in terms of the number of Shares will be the number of Shares required to be held by public shareholders for our Company to comply with the public shareholding spread requirement under the Listing Requirements or as approved by Bursa Securities.

Under the Listing Requirements, we are required to have a minimum of 25.00% of our Shares held by at least 200 public shareholders, each holding not less than 100 Shares at the point of our Listing.

If the aforesaid public shareholding spread requirement is not met, our Company may not be permitted to proceed with the Listing. Please refer to **Section 4.3.2** of this Prospectus for the details in the event there is a delay in or cancellation of our Listing.

3.4 Basis of arriving at the price of our IPO Shares

3.4.1 IPO Price

Our IPO Price of RM0.50 per IPO Share was determined and agreed upon between our Directors, Selling Shareholder and our Principal Adviser, after taking into consideration the following factors:-

- (i) our Group's pro forma EPS of 2.26 sen for the FYE 2021 is based on our Group's PAT attributable to owners of our Company of RM10.32 million and our enlarged issued share capital comprising 456,000,000 Shares, which translates into a price-to-earnings multiple of 22.12 times. After adjusting for listing expenses incurred in the FYE 2021 of approximately RM0.74 million, our PAT would be approximately RM11.06 million which would translate into a price-to-earnings multiple of approximately 20.61 times;
- (ii) our financial performance and operating history as described in **Sections 11 and 12** of this Prospectus;
- (iii) the pro forma consolidated NA as at 31 December 2021 attributable to owners of the Company, after the IPO and subsequent to the utilisation of proceeds from our Public Issue of approximately RM0.16 per Share based on our enlarged issued share capital upon Listing comprising 456,000,000 Shares;

3. DETAILS OF OUR IPO (cont'd)

- (iv) our competitive strengths as outlined in **Section 6.3** of this Prospectus;
- (v) our future plans and business strategies as outlined in **Section 6.25** of this Prospectus;
- (vi) the overview and future outlook of the industry which we operate in, as described in the Industry Overview Report in **Section 7** of this Prospectus; and
- (vii) the prevailing market conditions, which include current market trends and investors' sentiment.

Applicants should also note that the market price of our Shares upon Listing is subject to the vagaries of market forces and other uncertainties which may affect the trading volatility of our Shares.

3.4.2 Market capitalisation upon Listing

Based on our IPO Price of RM0.50 per IPO Share and our enlarged issued share capital comprising 456,000,000 Shares, our market capitalisation upon Listing is RM228.00 million.

3.5 Dilution

Dilution is the amount by which the price paid by the investors of our IPO Shares exceeds our pro forma consolidated NA per Share after our IPO.

The following table illustrates the dilution on a per Share basis:-

	Details	(RM)
IPO Price	(A)	0.50
Audited consolidated NA per Share as at 31 December 2021, before adjusting for the IPO	(B)	0.08
Pro forma consolidated NA per Share as at 31 December 2021, after giving effect to the IPO (after the IPO and subsequent to the utilisation of proceeds from our Public Issue)	(C)	0.16
Increase in the pro forma consolidated NA per Share to existing shareholders	(C - B)	0.08
Dilution in the pro forma consolidated NA per Share to new public investors	(A - C)	0.34
Dilution in the pro forma consolidated NA per Share to new public investors as a percentage of the IPO Price (%)	(A - C)/(A)	68.00

Save for the Pre-IPO Restructuring and as disclosed below, there has been no direct acquisition and/or subscription of any existing Shares in our Company by our Directors, key senior management, substantial shareholders or persons connected with them (assuming full subscription under the Pink Form Allocation), or in which they have the right to acquire since the incorporation of our Company up to the date of this Prospectus:-

3. DETAILS OF OUR IPO (cont'd)

	No. of Shares before IPO	⁽²⁾ No. of Shares from IPO	Total consideration (RM)	Average effective cash contribution per Share (RM)
<u>Promoters, Directors and substantial shareholders</u>				
Fong Choong Fook	⁽¹⁾ 291,200,040	-	17,810,400	0.06
Goh Soon Sei	⁽¹⁾ 73,404,960	-	4,489,600	0.06
<u>Directors</u>				
Chan Kam Chiew	-	250,000	125,000	0.50
Dr Teh Chee Ghee	-	250,000	125,000	0.50
Antonius Sommer	-	250,000	125,000	0.50
Ts. Lim Mei Shyan	-	200,000	100,000	0.50
<u>Key senior management</u>				
Gilbert Chu	-	1,800,000	900,000	0.50
Fow Chee Kang	-	800,000	400,000	0.50
Lum Pui Yee	-	400,000	200,000	0.50

Notes:-

- (1) Shares issued to them pursuant to the Pre-IPO Restructuring.
- (2) Assuming full subscription of our Issue Shares allocated to our Directors, key senior management and key technical personnel under the Pink Form Allocation.

3.6 Use of proceeds

The total gross proceeds of approximately RM45.70 million from the Public Issue will be utilised by our Group in the following manner:-

Details of use	Estimated timeframe for use upon Listing	RM'000	Percentage of gross proceeds (%)
1. Business expansion			
• Purchase of office	Within 12 to 24 months	18,000	39.39
• Expansion of workforce	Within 24 months	6,500	14.22
• Capital expenditure on equipment and tools	Within 24 months	6,000	13.13
• Strategic business expansion	Within 24 months	7,698	16.85
		38,198	83.59
2. Working capital	Within 12 months	3,500	7.66
3. Estimated listing expenses	Within 3 months	4,000	8.75
Total		45,698	100.00

3. DETAILS OF OUR IPO (cont'd)

Details of our use of gross proceeds from the Public Issue are as follows:-

3.6.1 Business Expansion**(i) Purchase of office**

We have earmarked RM18.00 million or 39.39% of our total Public Issue proceeds to purchase a new office premise to support our growing customer base. We are currently operating from 2 rented office units located in Empire Office Tower in Subang, Selangor Darul Ehsan ("**Current Office**"), for which the tenancy of the units will expire on 31 May 2022 and 30 November 2023 respectively. The aggregate built-up area of our Current Office is approximately 14,748 sq ft, housing, amongst others, our corporate office (with a limited number of meeting rooms), 7 test labs (of which 3 are mini sized labs), 1 forensic lab and 6 training classrooms.

The workstations at our Current Office can accommodate up to 85 employees. As at the LPD, we have a total of 90 employees, of which 66 are technical personnel, including our key technical personnel as set out in **Section 8.5** of this Prospectus. Further details of our Current Office are set out in **Section 6.18.2** of this Prospectus.

In view of our growing customer base and business expansion plans (which include the expansion of our workforce and increasing our technical capacity (via the setting up of new labs), our existing floor space is insufficient to cater for such plans and strategies. Given the space constraints and our intention to scale up our operations in the near term, we intend to purchase an office premise with a larger built-up area of at least 20,000 sq ft from the property market in the Klang Valley ("**New Office**").

The New Office will encompass, amongst others, the following:-

- a larger number of workstations to accommodate the expansion of our workforce given that we intend to hire at least an additional 70 technical personnel in the next 2 years to cater to the rising demand for cybersecurity services;
- a dedicated training centre with 6 sizeable training classrooms for our Group to conduct cybersecurity related training;
- a higher number of labs (i.e. at least 9 new sizeable labs) to be set up at the New Office ("**New Labs**") to enhance the Group's technical capability to scale up its operations, in particular, in undertaking, amongst others, digital forensics and IoT assessments. These New Labs will be equipped with new IT equipment and software forensic tools, including amongst others, forensic imagers and custom built hardware for IoT assessments; and
- the corporate office with at least 6 meeting rooms for our technical personnel to hold meetings with existing and potential customers. Currently, due to floor space constraints, our Current Office only has 4 small sized rooms available for meetings. The new corporate office will also serve to enhance our corporate image amongst our customers, employees and stakeholders.

3. DETAILS OF OUR IPO (cont'd)

The estimated size of the new facilities are set out below:-

	Existing size based on Current Office (sq ft)	*Indicative size at the New Office (sq ft)
Client Meeting Rooms	4 small-sized discussion rooms with floor space ranging from 145 sq ft to 150 sq ft (Total floor space: 585 sq ft)	6 meeting rooms with total floor size of 1,300 sq ft
Test Labs	7 test labs, comprising 3 mini-sized labs (of 77 sq ft each) and 4 test labs with floor space ranging from 113 sq ft to 268 sq ft (Total floor space: 966 sq ft)	8 test labs with total floor size of 2,000 sq ft
Forensic Lab	1 forensic lab with floor space of 361 sq ft	1 forensic lab with floor space of 500 sq ft
Training Classrooms	6 training classrooms with floor space ranging from 105 sq ft to 340 sq ft (Total floor space: 1,407 sq ft)	6 training classrooms with floor space of 2,000 sq ft

Note:-

* Floor space of the respective facilities are indicative as at this juncture and may be subject to further changes depending on the layout of the identified New Office.

We intend to purchase the office by the second half of 2022 and have accordingly requested for property agents to identify a suitable office premise, taking into consideration, amongst others, our floor space requirements, potential office layout with our preference for a strategic location with good connectivity such as Subang Jaya, Glenmarie, Ara Damansara, Bangsar or Petaling Jaya. At this juncture, we have viewed 6 properties ("**Viewed Properties**") located in Ara Damansara, Bangsar and Petaling Jaya. However, after further deliberation with our management, we are of the view that the Viewed Properties do not fulfil our operational and business expansion requirements. As such, we will continue to search for a suitable property that meets our operational requirements.

We have estimated the indicative costs for the purchase of our New Office (after taking into consideration, amongst others, the management's market estimates of commercial properties located in its preferred locations) together with renovation and fit out works to amount to approximately RM18.00 million.

The earmarked proceeds of the Public Issue is expected to be allocated between the purchase cost and the cost of renovation and fit out works (collectively referred to as "**Total Property Costs**") as follows:-

Indicative costs	RM'000
Purchase of New Office ⁽¹⁾	15,000
Renovation and fit out works ⁽²⁾	3,000
Total	18,000

3. DETAILS OF OUR IPO (cont'd)**Notes:-**

- (1) Based on the management's estimates of the average property market value of commercial properties of RM750 per sq ft, after taking into consideration, the market value of similar commercial properties located in our preferred locations.
- (2) Based on the management's estimates of the renovation and fit out works, after taking into consideration, the indicative quotations for amongst others, the office workstations, furniture and fittings.

We anticipate that the process to identify, acquire and renovate the New Office will be carried out in stages over a period of up to 2 years, and the indicative timeframe for such process is set out as follows:-

Stage(s)	Event(s)	Indicative timeframe
1.	<ul style="list-style-type: none"> Identify suitable properties located in Klang Valley Undertake preliminary assessment on the office layout to cater to our office requirements and needs 	Up to August 2022
2.*	<ul style="list-style-type: none"> Commence negotiations for the purchase of the property Appointment and commencement of discussions with the interior designer and/or contractor on the design of the office layout of the property 	Up to October 2022
3.	<ul style="list-style-type: none"> Execution of the sale and purchase agreement ("SPA") and/or financing agreements (if required) for the acquisition of the New Office 	Up to November 2022
4.	<ul style="list-style-type: none"> Completion of the acquisition of the New Office (assuming 3 months from the date of the SPA) 	Up to January 2023
5.	<ul style="list-style-type: none"> Commence renovation of the New Office 	February 2023
6.	<ul style="list-style-type: none"> Completion of the renovation of the New Office Relocation from the Current Office to New Office 	Up to June 2023

Note:-

- * The tenancy of 1 of the units at our Current Office (which will expire on 31 May 2022) has been renewed for an additional 12 months from 1 June 2022 to 31 May 2023 pending a relocation to the New Office.

In the event the actual cost for the New Office, including the renovation works are higher than budgeted, the shortfall will be funded from our internally generated funds and/or bank borrowings. Conversely, should the amount allocated be more than the actual cost, such surplus will be channelled towards the strategic business expansion purposes as set out in **Section 3.6.1(iv)** below.

We do not foresee any major obstacles in identifying and acquiring a suitable property for our New Office within the proposed timeframe in view of the large and readily available supply of commercial properties in the Klang Valley. Nevertheless, in the event that we are unable to identify a suitable property for our New Office within the proposed timeframe, we may explore the option of purchasing our Current Office and any available units within the same office tower.

3. DETAILS OF OUR IPO (cont'd)**(ii) Expansion of workforce**

We intend to scale up our operations to support our growing customer base and to continue developing our human resources capabilities and recruiting the right professionals for our business. We aim to achieve this by increasing our headcount and hiring at least an additional 70 technical personnel in the next 2 years, including to support our plans for strategic business expansion in the Southeast Asian region (in particular Singapore, Cambodia and Vietnam) as more particularly described in **Section 3.6.1 (iv)** of this Prospectus. We intend to hire at least 60 technical personnel for our local operations and up to 10 technical personnel to be based in Singapore, Cambodia and Vietnam for our strategic business expansion. Although we are able to undertake overseas cybersecurity projects remotely from Malaysia, our intention to hire up to 10 technical personnel to be based in Singapore, Cambodia and Vietnam is with the aim to provide localised support to better serve our existing and potential customers. As at the LPD, we have 66 technical personnel including our key technical personnel, all of which are based in Malaysia.

We have therefore earmarked RM6.50 million or 14.22% of our total Public Issue proceeds towards the expansion of our technical workforce. We believe that our new recruits will enhance our capacity to service the growing number of new purchase orders and contracts. For the past 4 FYEs 2018, 2019, 2020 and 2021 and up to the LPD, we have serviced more than 400 customers across various end user industries. We also expect the number of our support staff from our commercial, finance and human resource department to increase in tandem with the increase in the headcount of our technical workforce. The staff cost of these new recruits will be fully funded through internally generated funds.

The breakdown of utilisation is envisaged as follows:-

Details		RM'000
(i)	Staff salaries of new technical recruits	(1)5,500
(ii)	Relevant training and certification costs to enhance the technical skill and competence of the new recruits	1,000
Total		6,500

Note:-

(1) To fund the staff salaries of 70 new technical recruits for an estimated period of 12 months.

If the actual amount required for our workforce expansion is lower than estimated, the excess will be used for working capital purposes. Conversely, any excess amount required for workforce expansion will be funded from our working capital.

(iii) Capital expenditure on equipment and tools

In line with our business expansion strategies disclosed above, we also intend to utilise the earmarked Public Issue proceeds of RM6.00 million or 13.13% of our total Public Issue proceeds towards the purchase of new IT equipment, tools, and software forensic tools for our operations and to support the expansion of our workforce as well as for our New Labs and training centre (at the New Office).

3. DETAILS OF OUR IPO (cont'd)

The breakdown of utilisation is envisaged as follows:-

Details	RM'000
Purchase of laptops (with high specifications suited primarily to undertake cybersecurity projects) ⁽¹⁾	1,000
Software related costs (which are primarily utilised for cybersecurity projects, such as threat intelligence platforms and security scanning software) ⁽¹⁾	3,000
Equipment and tools for the New Labs and training centre at the New Office (which include servers and network devices as well as assessment and software forensic tools (such as forensic imager kits and customised IoT assessment tools)) ⁽¹⁾	2,000
Total	6,000

Note:-

(1) *Based on the management's estimates of the prices of the identified equipment and software after taking into consideration, amongst others, the indicative quotes of certain equipment and management's research on the prices of the said equipment and software.*

If the actual amount required for the above capital expenditure is lower than estimated, the excess will be used for working capital purposes. Conversely, any excess amount required for such capital expenditure will be funded from our working capital.

(iv) Strategic business expansion

We have earmarked approximately RM7.70 million or 16.85% of our total Public Issue proceeds towards our strategic expansion plans to further grow our business and revenue streams.

We intend to implement our strategic expansion plans, which include the setting up of overseas branches and/or tie-ups with local partners with existing presence in selected countries within the Southeast Asia region. This strategy will allow our Group to establish a localised direct presence to service our overseas customers as well as a platform to tap into the potential growth in demand for cybersecurity services in the region.

The countries identified for our initial geographical expansion are Singapore, Vietnam and Cambodia. We intend to prioritise our expansion to Singapore ahead of Vietnam and Cambodia as the Singapore market has been the largest contributor to our overseas revenue segment for the past 3 FYEs 2019, 2020 and 2021. We intend to set up a branch office in Singapore (to primarily serve the Singapore market), with up to 6 technical personnel to provide direct operational and service support to our existing customers in the near term. At this juncture, we are currently working with property agents in Singapore to identify a suitable office premise and expect to set up our Singapore branch office latest by the first quarter of 2023.

Our strategic expansion to Vietnam and Cambodia will be by way of potential tie-ups or joint-ventures with local partner(s) in these countries with the aim to primarily serve the local cybersecurity markets. We believe that this is an effective and expedient avenue for our Group to have direct access to the established customer network of our local partners and to tap into the growth of the cybersecurity market in such countries by leveraging on our local partners' key competitive strengths (such as the established brand name, reputation and/or track record of our local partners in such countries).

3. DETAILS OF OUR IPO (cont'd)

Notwithstanding the above, as and when any suitable opportunity arises, we also intend to embark on potential strategic acquisitions of companies within the local and regional cybersecurity market (“**Strategic Acquisitions**”). Such expansion strategies would also potentially broaden our service offerings and customer base, as well as expand our market presence. As at the LPD, we have not identified any specific business for acquisition or tie-ups/joint ventures. Our Company will make the necessary announcements as required under the Listing Requirements as and when we have entered into any material agreement in relation to our Strategic Acquisitions and/or investments. In the event that shareholders’ approval and/or regulatory approvals are required, such approvals will be sought by our Company.

Premised on our above strategic plans, the breakdown of the utilisation of the earmarked proceeds is envisaged to be as follows:-

Details	RM'000
Setting up of new branch in Singapore ⁽¹⁾	2,500
Proceeds allocated to finance the joint ventures/tie-ups with local partners in Vietnam or Cambodia as well as Strategic Acquisitions if any suitable opportunities arise ⁽²⁾	5,198
Total	7,698

Notes:-

- (1) *Includes the rental deposits, rental of the office premise, renovation works and purchase of furniture, equipment and tools. The indicative sum was derived based on the management’s estimate of 6 months office rental of an office unit in Central Business Area of Singapore and the indicative renovation fee for an office unit with floor space of 2,000 sq ft.*
- (2) *Includes deposits, acquisition costs (if applicable) and/or legal fees relating to the acquisitions as well as the associated costs relating to the tie-ups and joint ventures, which may include, legal and advisory fees on the structure and terms of the tie-ups and joint ventures in Cambodia and Vietnam.*

Any shortfall in the actual costs of strategic expansions compared to our budget will be financed through our internally generated funds and/or bank borrowings. Conversely, in the event the actual proceeds utilised to fund our strategic expansion plans is lower than the allocation of RM7.70 million, the excess will be channelled towards working capital purposes.

In the event that we are unable to undertake the above strategic expansions within 2 years from the completion of the Listing, the proceeds earmarked for such purposes will be reallocated for our working capital purposes as disclosed in **Section 3.6.2** below. Failing to undertake the above strategic expansions will materially impact our ability and hinder our business plans to expand our market presence in the identified geographical markets (i.e. Singapore, Vietnam and Cambodia) moving forward as well as potentially affect our strategic business plans to broaden our service offerings and customer base (through tie-ups and/or Strategic Acquisitions). This will potentially affect our business, in particular, in the identified geographical markets, financial performance and prospects moving forward.

3.6.2 Working capital

We also expect our working capital requirements to increase in tandem with the expected growth in scale of operations.

3. DETAILS OF OUR IPO (cont'd)

Hence, we intend to utilise the earmarked Public Issue proceeds of RM3.50 million or 7.66% of the total Public Issue proceeds towards working capital requirements, which include the following:-

Details	RM'000
Sales and marketing expenses, which include media advertisements to promote cybersecurity awareness to the private and public sector as well as to promote the "LGMS" brand as a solutions provider for cybersecurity	2,500
General overheads, which include payment of administration and operational expenses such as for the upkeep of offices and office utilities	1,000
	3,500

3.6.3 Estimated listing expenses

The estimated expenses and fees incidental to our Listing amounting to RM4.00 million shall be borne by our Company, the details of which are as follows:-

Expenses	RM'000
Professional fees ⁽¹⁾	2,200
Brokerage, placement fees and underwriting commission	1,200
Other fees and expenses such as printing, advertising, travelling and roadshow expenses incurred in connection with the IPO	200
Contingencies and other incidental expenses in connection with the IPO such as translation fees, regulatory fees, public or investor relation consultant, service tax, and funds reserved for contingency purposes	400
Total	4,000

Note:-

(1) Includes advisory and professional fees for, amongst others, our Principal Adviser, Legal Adviser, Reporting Accountants, and IMR.

If the actual listing expenses are higher than the estimated amount as set out above, the deficit will be funded out of the portion from the IPO proceeds allocated for working capital. Conversely, if the actual listing expenses are lower than the estimated amount, the excess will be utilised for the general working capital requirements of our Group.

We intend to place the proceeds raised from the Public Issue (including accrued interest, if any) or the balance thereof as deposits with licensed financial institutions or short-term money market instruments prior to the use of the proceeds from the Public Issue for the above intended purposes.

Our Company will not receive any proceeds from the Offer for Sale as such proceeds will go directly to our Selling Shareholder. The gross proceeds from the Offer for Sale is approximately RM22.80 million based on the Offer Price of RM0.50 per Offer Share. Our Selling Shareholder will bear all the expenses, including the registration and transfer fees, placement fees and miscellaneous expenses relating to the Offer for Sale, which is estimated to be approximately RM0.51 million.

3. DETAILS OF OUR IPO (cont'd)

3.7 Brokerage, underwriting commission and placement fee

(i) Brokerage

We will pay brokerage fees in respect of the Issue Shares allocated to the Malaysian Public, at the rate of 1.00% (exclusive of applicable tax) of the Issue Price in respect of all successful applications which bear the stamp of the participating organisations of Bursa Securities, members of the Association of Banks in Malaysia, members of the Malaysian Investment Banking Association and/or the Issuing House.

(ii) Underwriting commission

As stipulated in the Underwriting Agreement, we will pay the underwriting commission at the rate of 2.25% (exclusive of applicable tax) of the total value of the underwritten Shares based on the Issue Price.

(iii) Placement fee

Our Placement Agent, UOBKH, has agreed to place out 44,695,000 Issue Shares to be offered to identified institutional and/or selected investors as set out in **Section 3.3.1(iii)** of this Prospectus, 11,400,000 Issue Shares to identified Bumiputera Investors as set out in **Section 3.3.1(iv)** of this Prospectus, as well as 45,600,000 Offer Shares to identified Bumiputera Investors. We will pay our Placement Agent a placement fee at the rate of 2.25% of the total value of the 56,095,000 Issue Shares placed out to investors identified by our Placement Agent at the Issue Price and a placement fee at the rate of 0.75% of the total value of the Issue Shares placed out to investors identified by our Company at the Issue Price.

The Selling Shareholder will pay the Placement Agent a placement fee at the rate of 2.25% of the total value of the Offer Shares placed out to investors identified by our Placement Agent at the Offer Price and a placement fee at the rate of 0.75% of the total value of the Offer Shares placed out to investors identified by our Company at the Offer Price.

3.8 Underwriting arrangement

We have entered into the Underwriting Agreement with the Underwriter to underwrite 22,800,000 Issue Shares under the Public Issue as set out in **Section 3.3.1(i)** of this Prospectus, and 12,500,000 Pink Form Shares under the Pink Form Allocation as set out in **Section 3.3.1(ii)** of this Prospectus, both of which are subject to the clawback and reallocation provisions as set out in **Section 3.3.3** of this Prospectus.

(The capitalised terms used in this section shall have the respective meanings as ascribed in the Underwriting Agreement or as defined herein unless the context otherwise requires)

“Closing Date”	Means the last day and time for the acceptance of and payment for the retail offering in accordance with the Prospectus and the Application Forms or any such date as may be extended from time to time by our Company with the agreement of the Underwriter in writing
“Material Adverse Effect”	Means a material adverse effect on:- <ul style="list-style-type: none"> (a) the condition (financial or otherwise), earnings, business or operations of our Company or our Group taken as a whole; or (b) the ability of our Company to perform in any material respect its respective obligations under the Underwriting Agreement or the Placement Agreements

3. DETAILS OF OUR IPO (cont'd)

“Offer Documents” Means the Prospectus and the Application Forms and where the context permits, can be either one of these documents

Pursuant to the Underwriting Agreement, the Underwriter may at any time before the listing date by notice in writing to our Company terminate the Underwriting Agreement upon the occurrence of any of the following:-

- (i) the IPO is stopped or delayed by our Company for any reason whatsoever (unless such delay has been approved by the Underwriter);
- (ii) there occurs any misrepresentation or breach of warranties or failure to perform the undertakings by our Company set out in the Underwriting Agreement in any material respect;
- (iii) the Placement Agreements shall have been terminated in accordance with their terms or either our Company or the Selling Shareholder shall have failed to perform their obligations under the Placement Agreements;
- (iv) the SC or Bursa Securities suspends or revokes any approval for the IPO or makes any ruling (or revokes any ruling previously made), the effect of which is to prevent the IPO and the Listing;
- (v) trading of all securities on Bursa Securities has been suspended or materially limited on, or by Bursa Securities, as the case may be;
- (vi) any new law or regulation or change in law, directive, policy or ruling in Malaysia which in the reasonable opinion of the Underwriter (after having consulted our Company) may prejudice the success of the Listing or which would have or the effect of making it impracticable to enforce contracts to allot the shares or making any obligation under the Underwriting Agreement incapable of performance in accordance with its terms;
- (vii) there shall have been any other material adverse change in national monetary, financial (including stock market, foreign exchange market, inter-bank market or interest rates or money market or currency exchange rates or foreign exchange controls) conditions which in the reasonable opinion of the Underwriter (after having consulted our Company) is likely to have a Material Adverse Effect. For the avoidance of doubt, if the FTSE Bursa Malaysia Kuala Lumpur Composite Index (“**Index**”) is, at the close of normal trading on Bursa Securities, on any Market Day:
 - (a) on or after the date of the Underwriting Agreement; and
 - (b) prior to the Closing Date,

lower than 85% of the level of the Index at the last close of normal trading on the relevant exchange on the Market Day immediately prior to the date of the Underwriting Agreement and remain at or below that level for at least 3 consecutive Market Days, it shall be deemed a material adverse change in the stock market condition;
- (viii) our Company withholds any material information from the Underwriter which, in the reasonable opinion of the Underwriter (after having consulted our Company), is likely to have a Material Adverse Effect;

3. DETAILS OF OUR IPO (cont'd)

- (ix) there shall have occurred any outbreak or escalation of hostilities, epidemic, acts of terrorism, acts of God, accidents or interruptions, or any calamity or crisis or other event or series of events in the nature of force majeure that, in the reasonable opinion of the Underwriter (after having consulted our Company), makes it impracticable or inadvisable to proceed with the offer, sale or delivery of the Issue Shares on the terms and in the manner contemplated in each Offer Documents;
- (x) any government requisition or other occurrence of any nature whatsoever in the reasonable opinion of the Underwriter (after having consulted our Company), is likely to have a Material Adverse Effect; or
- (xi) the Listing does not take place within 3 months from the date of the Underwriting Agreement or such other extended date as may be agreed by the Underwriter.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

4. RISK FACTORS

YOU SHOULD CAREFULLY CONSIDER THE FOLLOWING KEY RISK FACTORS WHICH MAY HAVE A MATERIAL ADVERSE IMPACT ON OUR BUSINESS OPERATIONS, FINANCIAL POSITION AND THE FUTURE PERFORMANCE OF OUR GROUP, IN ADDITION TO OTHER INFORMATION CONTAINED ELSEWHERE IN THIS PROSPECTUS, BEFORE INVESTING IN OUR COMPANY.

4.1 Risks relating to our business and operations**4.1.1 Our business could suffer if we are unable to attract, train, motivate and retain senior management and other qualified technical personnel**

The cybersecurity market is growing and fast-changing with an overall shortage of skilled and experienced talent. Our success depends, to a large extent, on our ability to attract and retain senior management and qualified personnel with the right technical expertise, professional integrity and commitment that is aligned with our business core values. Our technical teams are staffed with individuals with IT and/or cybersecurity qualifications and professional certifications and given that there are limited number of individuals with the education, training and qualifications necessary to fill these roles, such individuals are in high demand. To this end, we take an active approach towards talent recruitment and management. We create internship opportunities for students from IT faculty of local colleges and universities that meet our requirements and also participate in career fairs and talks organised by such educational institutions. In order to identify suitable recruits, we engage the services of professional recruitment agencies and also actively conduct talent searches on online professional networking platforms and job portals. We also promote our attractive incentives, employee benefits and our positive corporate culture as part of our talent acquisition strategy. In relation to talent management, we have in place structured training and mentoring programmes for all our technical employees, we also sponsor/subsidise the fees for their professional examinations, qualifications and accreditations and also the fees for them to maintain their qualifications and accreditations. We prefer to develop internal candidates to fill key positions. Our ability to operate and compete could be adversely affected if we are unable to attract, train, motivate and retain qualified individuals. This, in turn, could negatively impact our business and financial results.

We could also lose our senior management or other qualified technical personnel to our competitors, our customers or other participants in the cybersecurity market and it may be difficult for us to find suitable and timely replacement(s) given the talent shortage. A high turnover and/or any reduction in numbers to our headcount of senior management or other critical technical personnel may be disruptive to our business and may result in loss of crucial and confidential knowledge about our customers which, in turn, could lead to the loss of our customers.

As at the LPD, we have not experienced any material turnover in our senior management. We have put in place competitive remuneration packages and attractive incentives to reward and motivate our performing personnel and to retain their services in our Group. We also believe that effective succession planning such as ensuring effective transfer of knowledge and smooth transitions involving key positions, is vital to the long-term success of our business. However, despite our efforts, there is no assurance that we will be able to attract, integrate or retain personnel with the necessary skills to fulfil our current or future needs. If we are unable to do so, this could adversely affect our business, financial condition and financial performance.

4. RISK FACTORS (cont'd)

4.1.2 Real or perceived defects, errors or negligence in the provision of our services or any failure of our services to prevent a security breach could harm our reputation and cause us to lose customers

We provide vulnerability assessment and penetration testing services to our customers to identify the vulnerabilities of their IT infrastructure to cyber attacks. Our revenue from vulnerability assessment and penetration testing services accounted for approximately 48.83%, 56.22%, 58.79% and 56.98% of our total revenue for the past 4 FYEs 2018, 2019, 2020 and 2021, respectively. While all testing is done on a best effort basis to uncover all known vulnerabilities at the time of testing, there is no guarantee that our services will be able to detect other unknown vulnerabilities or vulnerabilities that are announced after the date of testing, especially in light of the rapidly changing cybersecurity landscape to which we must respond. As at the LPD, we have not encountered any major failure in detecting or preventing any cybersecurity attack on our customer's systems and operations. In addition, there is also no assurance that our customers will implement all our recommendations to address identified vulnerabilities. Although in general most of our customers would implement our recommendations, such implementation would be based on each customer's prioritised approach, which may not necessarily coincide with the risk levels which we have assigned to the identified vulnerabilities and may be affected by budget constraints and technological limitations faced by the customer.

Typically, the implementation of our recommendations will be carried out by the internal IT department of our customers. External third parties or specialists such as system network integrators may be brought in by our customers to implement these recommendations in cases where the customer's internal IT department lacks the technical expertise, or if the maintenance of the customer's IT systems has been outsourced. Certain customers may also face technological limitations in the implementation due to the customer continuing to operate on legacy IT systems for their businesses which are unable to run or support the software or solutions recommended. Hence, if any of our customers experience a security breach arising from a cyber attack not due to our negligence but which could be perceived by the general public or our other customers to be as such, this could result in damage to our reputation and loss of confidence in the quality of our services, which in turn, could adversely affect our business, financial condition and financial performance.

Further, if any customer which is publicly known to use our services is the subject of a successful publicised cyber attack, some of our other existing customers may seek to replace our services with those provided by our competitors. In certain circumstances, due to the inherent vulnerabilities in the pre-existing IT environment of our customers such as software flaws which result in a Denial of Service condition or misconfiguration of network devices, our vulnerability assessment and penetration testing services may trigger unintended adverse effects such as disruptions and/or interruptions to our customer's operations. As at the LPD, there has not been any incident whereby our vulnerability assessment and penetration testing services has triggered unintended adverse effects on our customer's operations. Any real or perceived defects, errors or negligence in the provision of our services, or any failure of our recommended preventive actions in detecting or preventing a cybersecurity threat, could result in our customers delaying or withholding payment to us or electing not to renew their service agreements with us or to further engage us for our services. We may be subject to regulatory inquiries in cases where the relevant customer operates in a regulated industry such as the financial services industry, or liability claims for negligence or breach of our service agreements such as for failure to comply with service levels stipulated or delay in delivery of services. We are unable to quantify the maximum liabilities to which we may be exposed as certain contracts require us to indemnify our customers for and against all claims in respect of damage to any person or property due to any default or negligence on our part. Having to address and alleviate any of these issues may require significant expenditure by us and result in interruptions to our operations, which in turn, could adversely affect our business, financial condition and financial performance.

4. RISK FACTORS (cont'd)

4.1.3 **Our reputation may be harmed if the security of confidential information or personal information of our customers is breached or otherwise subject to unauthorised access or disclosure**

In the course of performing our services and with the consent of our customers, we will have access to confidential information of our customers including information on our customers' operations, IT policies and IT systems. As at the LPD, as far as we are aware, none of our customers have experienced any data leakage, loss of data or security breaches to its IT infrastructure following and as a result of the provision of our services.

Our Group has established stringent policies and protocols, which are designed to protect the security, integrity and confidentiality of the information that we handle and/or store. These stringent policies and protocols include installation of firewall systems, enforcement of authentication and user access restriction at workstations through the use of password protection on devices and access cards and/or biometrics scanning to access areas in the office, regular examination of security logs and installation of closed-circuit cameras within our office. We have installed security appliances to constantly monitor all outbound and inbound traffic of our office network, with alerts being raised to the relevant personnel via a fail-safe network in the event that the availability of our office network is affected. We also impose strict confidentiality obligations on all our employees and any contravention will result in disciplinary action, dismissal and/or court proceedings.

We have also established policy and security protocols for remote working arrangements such as the use of virtual private networks (VPNs) to connect to our internal network. In addition, we store our files in encrypted containers which can only be decrypted using a password. We also utilise certain tools and applications to monitor the activities and data usage by our employees.

As at the LPD, we have not experienced any security breaches to our systems and information to date, whether arising from internal sources (such as technical malfunctions, employee error or misconduct) or external sources (such as malware, hacking, espionage and cyber intrusion). However, despite our stringent efforts, there is no guarantee that inadvertent disclosure (which may arise from software bugs or other technical malfunctions, employee error or misconduct, or other factors) or unauthorised disclosure or loss of personal or confidential information will not occur or that third parties will not gain unauthorised access to such information.

As with any businesses with IT infrastructures, we may potentially encounter external security threats such as direct attacks from external elements such as malware, hacking, espionage and cyber intrusion. Any data leakage, loss of data or security breaches to our IT infrastructures, whether actual or perceived, could adversely affect market perception of our services and negatively affect our reputation. Consequently, our relationships with existing customers may be damaged and/or we may fail to acquire new customers. In addition, if any such incident is in relation to the leakage or loss of confidential information of our customers, it could expose us to significant liability if we are subject to litigation or other action resulting in monetary damages and legal fees. As a result, our revenue could decline and/or we may incur additional costs in defending any claims which could adversely affect our business, financial condition and financial performance.

4. RISK FACTORS (cont'd)

4.1.4 Our business is dependent on the achievement and/or maintenance of certain certifications or standards and partnerships

Our technical teams, which undertake and implement our cybersecurity projects, hold various internationally recognised cybersecurity related certifications which include but are not limited to those held by the Group (such as PCI Security Standards Council Approved Scanning Vendor company and PCI Security Standards Council Qualified Security Assessor company) and those held personally by members of our technical team (such as PECB Certified ISO/IEC 27001 Lead Auditor and Mile2 Certified Penetration Testing Engineer, PCI Security Standards Council Approved Scanning Vendor employee and PCI Security Standards Council Qualified Security Assessor). Our PCI ASV status allows us to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS while our PCI QSA status qualifies us to validate an entity's adherence to PCI DSS. For further details on the certifications required for each business segments, please refer to **Sections 6.3.2 and 6.16** of this Prospectus.

In addition, certain customers, some of which are regulators or government bodies, may require our services to comply with certain privacy and security regulations, or other certifications and standards.

Further, we have established a partnership with Mile2, an IT security company based in USA, for our training business. We are also authorised by PECB, ISACA and CSA to conduct training and examinations in Malaysia. In order to maintain our status as authorised trainers and examiners, our Group and/or our employees are required to comply with certain standards and/or obligations under the relevant partnership agreements. For instance, many of these certifications and standards require us to undergo annual audits for renewal to ensure that we continue to maintain and implement the best practices required by the relevant certification authority and also to successfully complete the accreditation process and/or certification program implemented by the relevant partner. In order to maintain our certifications and the certifications of our technical team, we had incurred approximately RM150,000 to RM181,000 for the certifications held by our Group and approximately RM32,000 to RM102,000 for the certifications held by individual members of our technical team for the FYEs 2018, 2019, 2020 and 2021. If our Group and/or our employees are late in achieving or if we fail to achieve or maintain compliance with these certifications and standards, we may be disqualified from selling certain of our services to our customers such as audit and certification on our customer's compliance with PCI DSS. In addition, we need to maintain our certifications and/or partnerships in order to conduct trainings and examinations offered by the relevant partners such as PECB, ISACA and CSA. As at the LPD, our Group and our employees have not encountered any difficulty in renewing the certifications and standards held or any circumstances which have restricted us from selling or offering our services to customers due to failure to maintain any certifications or standards. As we prioritise continuous training and certification of the technical employees within our workforce, there is limited reliance or dependency risk on any particular individual within our technical teams for any certifications or compliance with any certification and/or partnership standards. In addition, if our competitors achieve similar standards and certifications, we may lose our competitive advantage. Either of the foregoing events could harm our business, financial condition and financial performance.

4. RISK FACTORS (cont'd)

4.1.5 If our services fail to help our customers achieve and maintain compliance with regulations and/or industry standards, our business, financial condition and financial performance could be harmed

Apart from our cyber risk prevention segment, we generate a significant portion of our revenue from our cyber risk management and compliance segment, which involves the provision of cybersecurity advisory and compliance services as well as certifications. Revenue from this segment accounted for approximately 46.39%, 37.89%, 36.30% and 28.83% of our total revenue for the past 4 FYEs 2018, 2019, 2020 and 2021 respectively. Under this segment, we offer cybersecurity advisory and compliance services to help our customers comply with regulations or directives, implement industry best practices on information security management, identify any compliance gaps across their organisations, audit on compliance with industry standards as well as develop programs and processes that can ensure compliance with regulations, directives and/or industry standards in the future. For instance, a number of our customers engage our services to assist them to comply with the information security standards developed and maintained by the PCI Security Standards Council which apply to any organisation that processes, stores or transmits cardholder data and/or sensitive authentication data.

The foregoing industry cybersecurity standards and other regulatory requirements imposed by industry regulators may affect our customers' requirements and demand for, our professional services. Governments and industry organisations, such as the PCI Security Standards Council, may also adopt new laws, regulations or requirements, or make changes to existing laws or regulations, that could impact the demand for, or value of, our services. As such, we are required stay abreast of the latest developments, both in technology and the relevant laws and industry standards and as part of our efforts to do so, we ensure that our technical personnel undergo continuous training and development so that we are able to adapt our services accordingly. If we are unable to adapt our services to changing legal and regulatory standards or other requirements in a timely manner, or if our cybersecurity advisory services fail to assist with, or expedite, our customers' cybersecurity prevention and compliance efforts, our customers may lose confidence in our services.

In addition, if laws, regulations or standards related to data security, vulnerability management and other IT security and compliance requirements are relaxed or the penalties for non-compliances are amended to be less onerous, our customers may deprioritise government and industry best practice cybersecurity compliance as they may consider such compliance to be less critical to their businesses. In any of these circumstances, our customers may be less willing to use our services and our business, financial condition and financial performance could be harmed.

4.1.6 We are dependent on customers within the financial services and telecommunications and media industries

Although we are not dependent on any particular customer, we are however dependent on customers within the financial services and telecommunications and media industries as these customers operate in a regulated industry with strict cybersecurity and data protection policies in place. This group of customers (i.e. from the financial services and telecommunications and media industries) in aggregate accounted for approximately 72.76%, 66.63%, 67.29% and 55.03% of our total revenue for the past 4 FYEs 2018, 2019, 2020 and 2021 respectively, further details of which are set out as follows:-

4. RISK FACTORS (cont'd)

	Audited							
	FYE 31 December							
	2018		2019		2020		2021	
	(RM'000)	(%)	(RM'000)	(%)	(RM'000)	(%)	(RM'000)	(%)
Financial services	7,099	40.83	7,633	37.12	11,023	53.38	14,435	51.07
Telecommunications and media	5,551	31.93	6,069	29.51	2,873	13.91	1,118	3.96
Total	12,650	72.76	13,702	66.63	13,896	67.29	15,553	55.03

Any material change in the financial services and/or the telecommunications and media industries such as changes to the regulations governing or relevant to such industries, could adversely affect our business, financial condition and financial performance. Expenditure on technology and cybersecurity by such customers may reduce based on changes in economic conditions and other factors, such as decisions to reduce or restructure technology spending in an attempt to improve profitability. Further, in the event of the introduction of any new or amendments to regulatory requirements in relation to cybersecurity by the relevant regulators of the financial services and/or the telecommunications and media industries, we may be required to adapt our service offerings to meet such requirements and failure to do so at all or in a timely manner could adversely affect our business and financial performance.

Whilst our Group will continue in our efforts to diversify our customer base to mitigate the risk of over-reliance on a single customer or a single industry, any mergers or consolidations of financial institutions or telecommunications and media institutions could potentially reduce our current and potential customer base. Notwithstanding our reliance on these industries, we will strive to enhance our technical capabilities by keeping abreast with the latest cybersecurity and regulatory developments in order to maintain our competitive edge and position so that we may diversify our customer base to other industries. As the digitalisation of businesses is on the rise, we are of the view that going forward, more industries will require cybersecurity services to ensure business continuity and/or for compliance purposes. Nevertheless, in the interim, any changes in the financial services and/or telecommunications and media industries could cause the market for our services to decline and as a result, our business, financial condition and financial performance could be harmed.

4.1.7 We are dependent on our ability to secure new purchase orders and/or contracts, maintain and renew contracts with our customers

Our vulnerability assessment and penetration testing services and our other cybersecurity services are offered on a one-off basis or a regular basis, depending on the requirements of our customers.

There is no assurance that our customers will renew their service agreements with us after the expiration of their terms or that our customers will continue engaging our services and if renewed, any subsequent service agreements awarded or engagements by our existing customers, will be on terms not less favourable to us. It should also be noted that our customers may choose not to renew their service agreements or issue new purchase orders or our customers may reduce or limit the scope of services requested due to certain factors, including dissatisfaction with our prices or service levels compared to our competitors, reductions in our customer's budgets and spending levels. Generally, the main barriers to entry into the cybersecurity market is the need to have access to a team of qualified and experienced cybersecurity professionals as well as the achievement of professional accreditations by the potential new entrant(s) to the cybersecurity market. Further, in order to secure contracts from certain customers such as from the financial services industry, an established track record in the cybersecurity market would typically be required.

4. RISK FACTORS (cont'd)

Additionally, many of our customers, including certain major customers, have the right to terminate their agreements or engagements with us for convenience and for other reasons by giving advanced written notice under the agreement, with the period of advanced written notice, depending on the nature of services, ranging from 7 to 90 days. As at the LPD, we have not encountered any termination by our customers of any service agreements and/or purchase orders prior to the expiry of term of the agreement or purchase order or prior to the completion of the services to be provided.

In addition, notwithstanding that there is no regulatory requirement to do so, certain customers of ours from the financial services industry (including some of our major customers as set out in **Section 6.12** of this Prospectus) have internal risk management policies/practice which require them to alternate their service providers (including those providing cybersecurity services) after its internal prescribed period of time (which on average is 1 to 3 years) for their annual penetration testing as required under the Bank Negara Malaysia's policy document on Risk Management in Technology). Pursuant to the Risk Management in Technology policy document, a financial institution is required to engage suitably accredited penetration testers and service providers to conduct annual intelligence-led penetration tests on its internal and external network infrastructure as well as critical systems including web, mobile and all external-facing applications.

Accordingly, due to such internal policy/practice, certain customers may not be able to retain our services for their annual penetration testing exercise after such internal prescribed period and may only re-appoint us after they have engaged the services of other service provider. Nevertheless, such customers may continue to engage us for our other services and/or to conduct ad hoc penetration testing services. Notwithstanding that certain of our customers have such internal policies/practice, there has been no material financial impact on our Group's financial performance to-date.

In any of the above circumstances, our revenue may decline which could adversely affect our business, financial condition and financial performance.

4.1.8 Our business is subject to the risk of claims by our customers

We provide a hack-proof warranty for up to six months for certain projects for our vulnerability assessment and penetration testing services on the test scopes performed based on project size. In the event of a successful cyber attack stemming from our negligence, we shall rectify the shortcomings and provide support and assistance to the customer utilising our own resources and at our own cost. As at the LPD, we have not received any such claims from our customers. However, there is no guarantee that there will be no claims against us in the future.

We are also covered by a professional indemnity insurance policy that protects our legal liability due to professional negligence for damages up to approximately RM8 million. While we typically seek to limit our exposure to damages through the terms of our contracts, liability limitation provisions as set out in the contracts may not be enforceable under some circumstances or may not fully or effectively protect us from customer claims and related liabilities and costs. Furthermore, it should be noted that even claims that are ultimately unsuccessful could require us to incur costs in connection with litigation and divert our management's time and other resources. Any claims, regardless of whether ultimately successful or unsuccessful, could harm the reputation of our business.

4. RISK FACTORS (cont'd)

4.1.9 **We are unable to assess the full extent of the potential impact of the ongoing COVID-19 pandemic which, if uncontrolled and/or prolonged, can have a significant adverse impact on our Group**

On 11 March 2020, the World Health Organisation declared a global pandemic known as COVID-19. The pandemic has affected many countries globally with many still trying to control the spread of the disease. Although several vaccines have been developed and introduced to the market since the end of 2020, many countries are still facing challenges in their respective vaccine administration and as such, there is still a major risk with continuous spikes in COVID-19 cases creating economic uncertainties globally.

Malaysia, like many other countries globally, has put in place various measures to control the spread of the disease. The Malaysian Government has since March 2020 imposed a number of MCOs with varying degrees of restrictions that has led to travel restrictions, border closure and many businesses either closed or operating under strict operational procedures.

Although Malaysia has transitioned to the “Endemic” phase on 1 April 2022, we are unable to assess the full extent of the potential impact of the COVID-19 pandemic as at the LPD particularly if it persists for an extended period of time or due to any insurgence of new COVID-19 variants. Potential negative impact may include a decline in our customer prospects and the slowdown of the businesses of our existing customers, which may result in the weakening demand for our services as our customers may reduce and/or deprioritise overall spending on IT and/or cybersecurity services to increase profitability or as a result of scaling down of their operations. On the other hand, the demand for our cybersecurity services may increase with the rising trend of remote working arrangements given the increased cybersecurity vulnerabilities arising from poor cybersecurity hygiene and the lack of security protocols on home and other non-office based networks. As at the LPD, we have not experienced any material decline in demand of our services by our customers notwithstanding the challenging economic conditions due to the COVID-19 pandemic and the demand for our cybersecurity services has since increased. As the vaccine rollout ramps up and the workforce gradually returns to their offices following the “Endemic” phase, any positive impact on our business may slow down subsequently or decline once the impact of the pandemic tapers down.

Whilst we have seen a reduction in certain of our Group’s operating expenses due to reduced business travel and the virtualisation or cancellation of employee events, if our employees fail to comply with the COVID-19 standard operating procedures implemented by our Group and/or the government, we could also potentially face the spread of COVID-19 amongst our employees. If any of our employees are to contract COVID-19, the impact from the restricted human resource capacity may cause a delay to the delivery of our services to our customers. This could lead to higher costs due to any delay in the provision of our services and as a result of cost incurred to sanitise any affected premises of ours and for testing close contact employees and this may have a material adverse effect on the business, financial condition and financial performance of our Group.

4.1.10 **We may not be able to successfully implement our future plans and business strategies to grow our business which could limit our growth prospects**

We intend to expand our operations in accordance with our future plans and business strategies set out in **Section 6.25** of this Prospectus. Whilst we believe that the business expansion strategies will be beneficial to the performance of our Group, the expected benefits may not materialise immediately or at all or may take a longer time to be realised and/or could reduce our profitability in the short term.

4. RISK FACTORS (cont'd)

There is also no assurance that we will be able to recruit or attract a sufficient number of skilled employees required to support our future plans and business strategies.

In addition, the implementation of our future plans and business strategies may also be influenced by various factors beyond our control, such as changes in economic conditions as well as the social and political environment in Malaysia and the countries which we have identified for our initial geographical expansion (i.e. Singapore, Vietnam and Cambodia) which may affect the commercial viability of such strategies and future plans. Hence, there is no assurance that we will be successful in executing our future plans and business strategies, nor can we assure that we will be able to anticipate all business, operational and industry risks arising from our future plans and business strategies.

4.2 Risks relating to the industry in which we operate**4.2.1 We operate in a highly competitive environment and competitive pressures are expected to increase in the future, which could adversely affect our business, financial conditions and financial performance**

The market that we operate in is highly competitive, fragmented and characterised by rapid changes in technology, heightening industry standards and best practices, changing customer requirements, increasingly sophisticated cyber attacks, and frequent introduction of new or improved products and/or services to combat cybersecurity threats. In 2022, it is estimated that there are around 400 cybersecurity players in Malaysia, both local and foreign. We expect this challenging business climate to continue.

Our overseas and local-based competitors may have greater financial, technical, marketing, sales and other resources, longer operating histories, better name recognition, better funding for R&D or product and/or service development, larger strategic acquisition budgets, more extensive international operations and/or a larger base of customers than we do. In addition, our competitors may have substantially broader and more diverse product and service offerings as well as routes to markets, which may potentially allow them to leverage on their relationships to expand on existing services to gain customers from our business through strategies such as cross-selling or bundling their product and service offerings in order to offer lower prices. Some of our competitors may have also acquired or could acquire similar businesses or establish cooperative relationships, that will potentially allow them to offer more comprehensive solutions through bundled packages that are more attractive to potential customers. Although we seek to differentiate ourselves from our competitors by leveraging on our competitive strengths set out in **Section 6.3** of this Prospectus, there is no assurance that we will be able to compete effectively with our competitors to secure projects from our existing and/or potential customers. According to the Industry Overview Report in **Section 7** of this Prospectus, some of the local cybersecurity market players which also offer vulnerability and/or penetration testing services include Across Verticals Sdn Bhd, AKATI Sekurity (M) Sdn Bhd, Ask Pentest Sdn Bhd whilst the foreign cybersecurity market players which offer such services include BAE Systems Applied Intelligence Malaysia Sdn Bhd, Cisco Systems (Malaysia) Sdn Bhd and Commisum Sdn Bhd.

We also face overseas and local competition from computer hardware and networking equipment manufacturers, operating system providers, telecommunication companies and other large diversified technology companies. Cybersecurity functionalities are increasingly being incorporated into products and services by vendors of computer hardware and operating system software either through internal development or through strategic alliance or acquisitions. Providers of telecommunications are also investing in cybersecurity functionality enhancement in the devices and services offered by them.

4. RISK FACTORS (cont'd)

Competitive pressures in the market or our failure to compete effectively may result in price reductions, reduced margins, loss of market share and inability to gain market share, and a decline in revenue, any one of which could seriously impact our business, financial condition and financial performance. In order to compete successfully, we must continue to develop our human capital, recruit more talent, expand or enhance our offerings as well as effectively adapt to changes in the technology and market conditions. We also intend to enhance our penetration testing and vulnerability assessment services by making such services more accessible to small and medium enterprises. If we are unable to compete successfully, our business, financial condition and financial performance could be adversely affected.

4.2.2 The lack of sophistication of the regulatory landscape and customer awareness on the evaluation criteria for selection of cybersecurity service providers in Malaysia

The regulatory landscape and the level of customer awareness in Malaysia on the evaluation criteria for selection of cybersecurity service providers lack sophistication compared to other developed nations. For example, the National Cyber Security Centre of the United Kingdom (NCSC) has implemented a scheme known as the IT Health Check Service (CHECK) under which only companies approved by the NCSC can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks. In contrast, there are currently no detailed local guidelines or regulatory standards for assessing the credibility and track record of cybersecurity players in the local cybersecurity market in Malaysia. As a result, customers are often left to their own devices to conduct due diligence on their cybersecurity service providers. Therefore, there is no assurance that we will be able to successfully differentiate ourselves in the local cybersecurity market and leverage on the cybersecurity accreditations held by our Group and employees, which could affect our business, financial condition and financial performance.

4.2.3 Our financial performance will suffer if we fail to anticipate changing customer requirements or industry and market developments, or we fail to adapt our business model to keep pace with the evolving cybersecurity threats from a variety of increasingly sophisticated cyber attacks

We must continue to address the challenges of ever changing customer requirements, rapid technological development, dynamic and evolving market trends such as the decline in the sales of personal computers, the rise of mobility and the use of devices with embedded connectivity functions, cloud-based solutions as well as the emergence of new cybersecurity threats. Moreover, some of our enterprise customers operate in environments that require them to adapt quickly to increasingly complex cybersecurity requirements such as those in the financial services industry.

We may be unable to keep abreast with the latest technologies and the ever evolving threats. We may also experience unanticipated delays in the offering of new solutions that would meet customer expectations. Any failure to anticipate, address or meet, thoroughly and quickly, the evolving requirements, demands and expectations of our customers, may harm our competitive position and could materially and adversely affect our business, financial condition and financial performance.

4. RISK FACTORS (cont'd)

The introduction of new products and services by our competitors, the evolution of new standards (formalised or otherwise) and market acceptance of products and services based on emerging or alternative technologies could each render some or all of our existing service offerings obsolete or less attractive to our customers. Modern cyber attackers are also skilled at adapting to new technologies and developing new methods of breaching customers' IT networks and infrastructures as exemplified by the increase in the frequency and complexity of ransomware attacks. Whilst we will continuously work to ensure that we are able to identify and assist our customers against the increased volume and complexity of the cybersecurity threats, there can be no assurance that we will be able to do so. If our service offerings are not viewed by our customers as necessary or effective in addressing their cybersecurity needs, then our revenues may not grow as quickly as expected or may decline, leading to an adverse impact on our business, financial condition and financial performance.

4.2.4 Fluctuating economic conditions may have an adverse effect on demand for our services

Our revenue depends to an extent on general economic conditions and the demand for our services in the cybersecurity market. Economic weakness, customer financial difficulties, and constrained spending on cybersecurity may result in a decrease in our revenue and earnings. Such factors could make it difficult to ascertain and accurately forecast our operating results and could negatively affect our ability to manage expenses.

In addition, the current COVID-19 pandemic may continue to put pressure on global economic conditions and overall spending on information security. If our customers are not convinced that our services should be an integral part of their overall approach to cybersecurity or if there is a general reduction in IT spending by our customers due to economic pressures, such events are likely to have an adverse impact on our business, financial performance and financial condition.

General economic weaknesses may also lead to payment delays, increase in bad debts, restructuring initiatives and associated expenses. Future or continued economic weakness, our failure and/or our customers' failure to recover from such weakness, could have a material adverse effect on demand for our services and consequently on our business, financial condition and financial performance.

4.2.5 Our business is dependent on the level of awareness of cybersecurity threats

Our business is substantially dependent on companies and governments recognising the severity of the risks relating to cyber attacks and that such attacks are not effectively prevented by legacy security solutions and IT infrastructure. Based on our market observation, the majority of spending on cybersecurity in Malaysia to date has been on threat protection products, such as network, endpoint and web security that are designed to stop threats from penetrating corporate networks including anti-virus software. Organisations that use these security products may believe that their existing security solutions and/or IT infrastructure are considered sufficient to safeguard the access to their sensitive business data. Premised on such notions, they may hence continue to deprioritise cybersecurity services such as ours and allocate their budget towards threat protection products and may not adopt our vulnerability assessment and penetration testing services in addition to, or in lieu of, such traditional products.

High visibility attacks on prominent companies, in particular, financial institutions have increased market awareness of the impact of advanced cyber attacks on operations and help to provide an impetus for companies and governments to devote their resources to protecting against cyber attacks, which includes engaging our vulnerability assessment and penetration testing services.

4. RISK FACTORS (cont'd)

If the number of cyber attacks were to decline, or companies or governments perceive that the general level of cyber attacks have declined, our ability to attract new customers and expand our offerings within existing customers could be materially and adversely affected. A reduction, whether actual or perceived, in the cybersecurity threat landscape could adversely affect our business, financial condition and financial performance.

4.2.6 Our business operations and the use of technology are subject to evolving legal requirements regarding privacy throughout the world

We currently operate our business in jurisdictions where we are subject to data protection or privacy laws and regulations, including but not limited to the Personal Data Protection Act 2010 in Malaysia, being our primary market. Certain services may involve the transmission of data between jurisdictions or the interception, storage, disclosure, transfer and examination of data in a manner that may subject their use to privacy and data protection laws and regulations in those jurisdictions in which our customers operate. While we are continuously evaluating the compliance of our existing services with the current relevant regulatory and security requirements, there can be no assurance that such requirements will not change or that we will not otherwise be subject to legal or regulatory actions. Any action taken against us for failure or perceived failure by us to comply with these laws and regulations, may result in damage to our reputation or adversely affect our ability to sell our services. Moreover, in the event of change to any of these laws and regulations, or in the event they are interpreted or applied in a manner that is inconsistent with the manner in which we operate our business and/or data maintenance practice, we may need to take the necessary remedial steps. This could in turn result in an adverse effect on our business, financial condition and financial performance.

4.3 Risks relating to investment in our Shares**4.3.1 There has been no prior market for our Shares**

Prior to our IPO, there has been no public market for our Shares. Hence, there is no assurance that upon Listing, an active market for our Shares will develop, or if developed, that such a market will be sustainable. There is no assurance as to the liquidity of any market that may develop for our Shares, the ability of holders to sell our Shares or the selling prices at which holders would be able to obtain our Shares.

There can be no assurance that the IPO Price will correspond to the price at which our Shares will trade on the ACE Market upon our Listing and that the market price of our Shares will not decline below the IPO Price.

4.3.2 Delay in or cancellation of our Listing

The occurrence of certain events, including the following, may cause a delay in, or cancellation of, our Listing:-

- (i) the Underwriter exercising its rights pursuant to the Underwriting Agreement to discharge itself from its obligations therein; or
- (ii) our inability to meet the minimum public spread requirement under the Listing Requirements of having at least 25% of the total number of our Shares for which our Listing is sought being in the hands of at least 200 public shareholders holding at least 100 Shares each at the point of our Listing.

4. RISK FACTORS (cont'd)

Where prior to the issuance and allotment of our Issue Shares:-

- (i) the SC issues a stop order pursuant to Section 245(1) of the CMSA, the Applications shall be deemed to be withdrawn and cancelled and our Company shall repay all monies paid in respect of the Applications for our Issue Shares within 14 days of the stop order, failing which the Company shall be liable to return such monies with interest at the rate of 10% per annum or at such other rate as may be specified by the SC pursuant to Section 245(7)(a) of the CMSA; or
- (ii) our Listing is aborted, investors will not receive any of our Issue Shares, all monies paid in respect of all applications for our Issue Shares will be refunded free of interest.

Where subsequent to the issuance and allotment of our Issue Shares:-

- (i) the SC issues a stop order pursuant to Section 245(1) of the CMSA, any issue of our Issue Shares shall be deemed to be void and all monies received from the applicants shall be forthwith repaid and if any such money is not repaid within 14 days of the date of service of the stop order, the Company shall be liable to return such monies with interest at the rate of 10% per annum or at such other rate as may be specified by the SC pursuant to Section 245(7)(b) of the CMSA; or
- (ii) our Listing is aborted other than pursuant to a stop order by the SC, a return of monies to our shareholders could only be achieved by way of cancellation of share capital as provided under the Act and its related rules. Such cancellation can be implemented by either:-
 - (aa) the sanction of our shareholders by special resolution in a general meeting, consent by our creditors (unless dispensation with such consent has been granted by the High Court of Malaya) and the confirmation of the High Court of Malaya, in which case there can be no assurance that such monies can be returned within a short period of time or at all under such circumstances; or
 - (bb) the sanction of our shareholders by special resolution in a general meeting supported by a solvency statement from our Directors.

4.3.3 Volatility of our Share price

The market price of our Shares may fluctuate as a result of variations in the liquidity of the market for our Shares, differences between our actual financial operating results and those expected by investors and analysts, changes in analysts' recommendations or projections, changes in general market conditions and broad market fluctuations.

The performance of Bursa Securities is also affected by external factors such as the performance of regional and world bourses, inflow or outflow of foreign funds, economic and political conditions of the country as well as the growth potential of various sectors of the economy. These factors invariably contribute to the volatility of trading volumes witnessed on Bursa Securities, thus adding risks to the market price of our Shares.

4. RISK FACTORS (cont'd)

4.3.4 The interest of our Promoters who control our Group may not be aligned with the interest of our shareholders

Our Promoters will collectively hold approximately 69.96% of our enlarged issued share capital upon Listing. As a result, our Promoters will be able to, in the foreseeable future, effectively control the business direction and management of our Group including the election of Directors, the timing and payment of dividends as well as having majority voting control over our Group and as such, will likely influence the outcome of matters requiring the vote of our shareholders, unless they are required to abstain from voting either by law and/or by the relevant guidelines or regulations. There can be no assurance that the interests of our Promoters will be aligned with those of our other shareholders.

4.4 Other risks

4.4.1 Forward-looking statements in this Prospectus are subject to uncertainties and contingencies

Certain statements or expectations or forecasts in this Prospectus are based on historical data which may not be reflective of future results. Forward-looking statements in this Prospectus are based on assumptions and subject to uncertainties and contingencies.

Although we believe that the expectations reflected in such forward-looking statements are reasonable at this time, we cannot assure you that such expectations will subsequently materialise.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

5. INFORMATION ON OUR GROUP

5.1 Our Company

Our Company (Registration No. 202001039091 (1395412-W)) was incorporated in Malaysia under the Act on 30 November 2020 as a public limited company under our present name for the purposes of facilitating the Pre-IPO Restructuring as set out in **Section 5.3** of this Prospectus and our Listing.

Our Company is an investment holding company. Through our subsidiaries and associate company, we provide independent professional cybersecurity services and are primarily involved in cybersecurity assessment, penetration testing, cyber risk management and compliance, and the provision of digital forensic and incident response services.

Further details on our Group's history and business activities are set out in **Sections 6.1** and **6.2** of this Prospectus, respectively.

5.2 Share capital

As at the LPD, our Company's issued share capital is RM22,300,000 comprising 364,605,000 Shares. The changes in our Company's issued share capital since incorporation up to the LPD are as follows:-

Date of allotment	No. of shares allotted	Nature of transaction	Consideration	Cumulative issued share capital	
				RM	No. of Shares
30-11-2020	1,000	Subscribers' shares (Loo Yuen Ling and Lee San Koon*)	Cash	1,000	1,000
30-08-2021	22,299,000	Allotment of Shares pursuant to the Acquisitions	Other than cash	22,300,000	22,300,000
06-09-2021	342,305,000	Bonus Issue	N/A	22,300,000	364,605,000

Note:-

* *The subscribers are nominee directors and shareholders assigned by the company secretary to facilitate the incorporation of the Company. The said nominee directors and shareholders are not persons connected to the Promoters. The subscriber shares were subsequently transferred to the Promoters on 6 September 2021.*

As at the LPD, we do not have any outstanding warrants, options, convertible securities or uncalled capital in respect of the Shares in our Company. In addition, there are no discounts, special terms or instalment payment terms applicable to the payment of consideration for the above allotments.

Upon completion of our IPO, our enlarged share capital will increase to RM67,997,500, comprising 456,000,000 Shares.

5. INFORMATION ON OUR GROUP (cont'd)**5.3 Pre-IPO Restructuring**

For the purposes of facilitating the Listing, we have undertaken an internal reorganisation exercise, which involved the following:-

(i) Acquisition of LE Global

On 30 August 2021, our Company had entered into a share sale and purchase agreement to acquire the entire issued share capital of LE Global comprising 1,500,000 ordinary shares for a purchase consideration of RM22,199,500, which was fully satisfied through the issuance of 22,199,500 new Shares at RM1.00 each to the vendors of LE Global in the following manner:-

Vendor	No. of LE Global shares	%	No. of Shares issued
Fong Choong Fook	1,200,000	80.0	17,759,600
Goh Soon Sei	300,000	20.0	4,439,900
Total	1,500,000	100.0	22,199,500

The purchase consideration was based on a “willing-buyer willing-seller” basis and the audited NA of LE Global group of companies as at 31 December 2020 of RM22,056,314. The acquisition of LE Global was completed on 30 August 2021.

(ii) Acquisition of LGMS Advanced Tech

On 30 August 2021, our Company had entered into a share sale and purchase agreement to acquire the entire issued share capital of LGMS Advanced Tech comprising 50,000 ordinary shares for a purchase consideration of RM98,500, which was fully satisfied through the issuance of 98,500 new Shares at RM1.00 each to the vendors of LGMS Advanced Tech as follows:-

Vendor	No. of LGMS Advanced Tech shares	%	No. of Shares issued
Fong Choong Fook	25,000	50.0	49,250
Goh Soon Sei	25,000	50.0	49,250
Total	50,000	100.0	98,500

The purchase consideration was based on a “willing-buyer willing-seller” basis and LGMS Advanced Tech’s audited NA as at 31 December 2020 of RM97,219. The acquisition of LGMS Advanced Tech was completed on 30 August 2021.

(iii) Acquisition of Credence Defender

On 30 August 2021, our Company had entered into a share sale and purchase agreement to acquire the entire issued share capital of Credence Defender comprising 100,000 ordinary shares for a purchase consideration of RM500, which was fully satisfied through the issuance of 500 new Shares at RM1.00 each to the vendors of Credence Defender in the following manner:-

5. INFORMATION ON OUR GROUP (cont'd)

Vendor	No. of Credence Defender shares	%	No. of Shares issued
Fong Choong Fook	50,000	50.0	250
Goh Soon Sei	50,000	50.0	250
Total	100,000	100.0	500

The purchase consideration was based on a “willing-buyer willing-seller” basis, Credence Defender’s audited net liabilities as at 31 December 2020 of RM11,370 and an agreed nominal sum between both parties in view of the said net liabilities position. The acquisition of Credence Defender was completed on 30 August 2021.

(iv) Acquisition of LGMS Academy

On 30 August 2021, our Company had entered into a share sale and purchase agreement to acquire the entire issued share capital of LGMS Academy comprising 100 ordinary shares for a purchase consideration of RM500, which was fully satisfied through the issuance of 500 new Shares at RM1.00 each to the vendor of LGMS Academy in the following manner:-

Vendor	No. of LGMS Academy shares	%	No. of Shares issued
Fong Choong Fook	100	100.0	500

The purchase consideration was based on a “willing-buyer willing-seller” basis, LGMS Academy’s audited net liabilities as at 31 December 2020 of RM3,686 and an agreed nominal sum between both parties in view of the said net liabilities position. The acquisition of LGMS Academy was completed on 30 August 2021.

(v) Bonus Issue

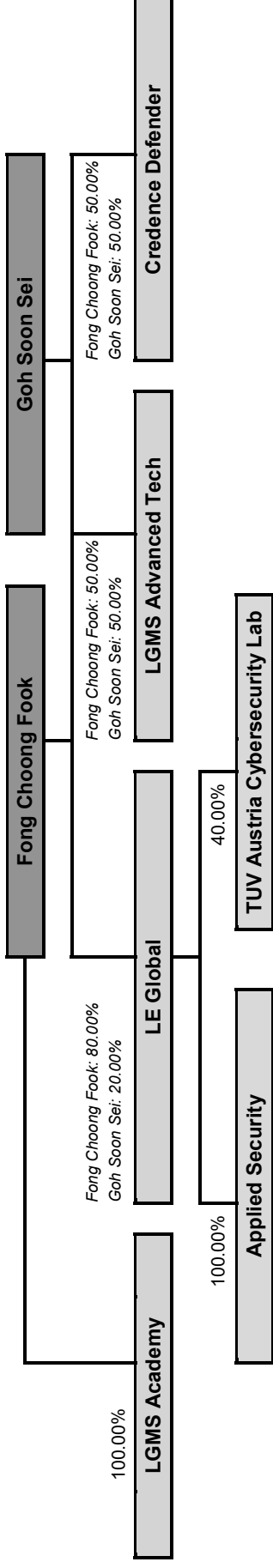
Following the Acquisitions, our Group had, on 6 September 2021, completed the Bonus Issue. The Bonus Issue was undertaken to enlarge the share capital base of the Company prior to the IPO. The share capital of the Company had been increased to RM22,300,000, comprising 364,605,000 LGMS Shares after the completion of the Bonus Issue.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

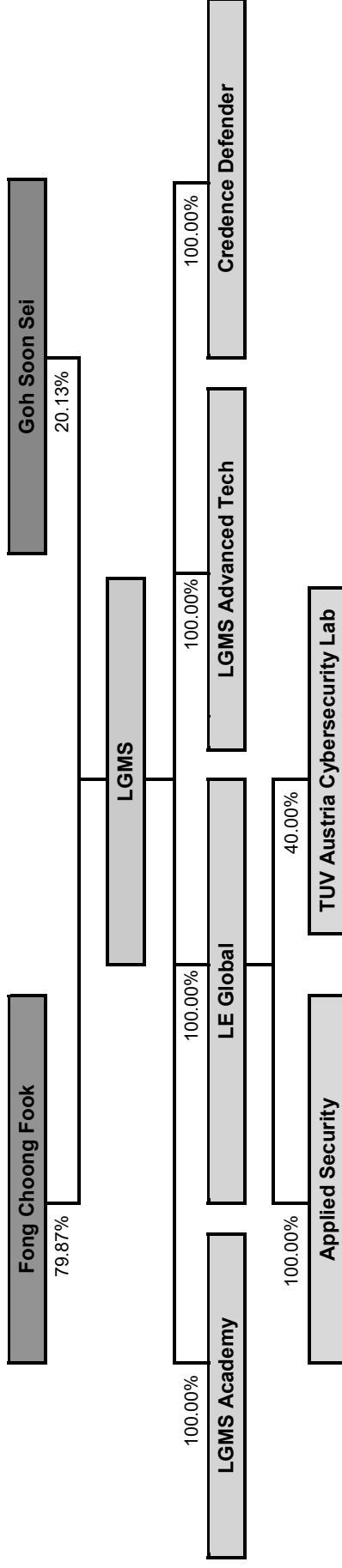
5. INFORMATION ON OUR GROUP (cont'd)

5.4 Our Group structure

Before the Pre-IPO Restructuring

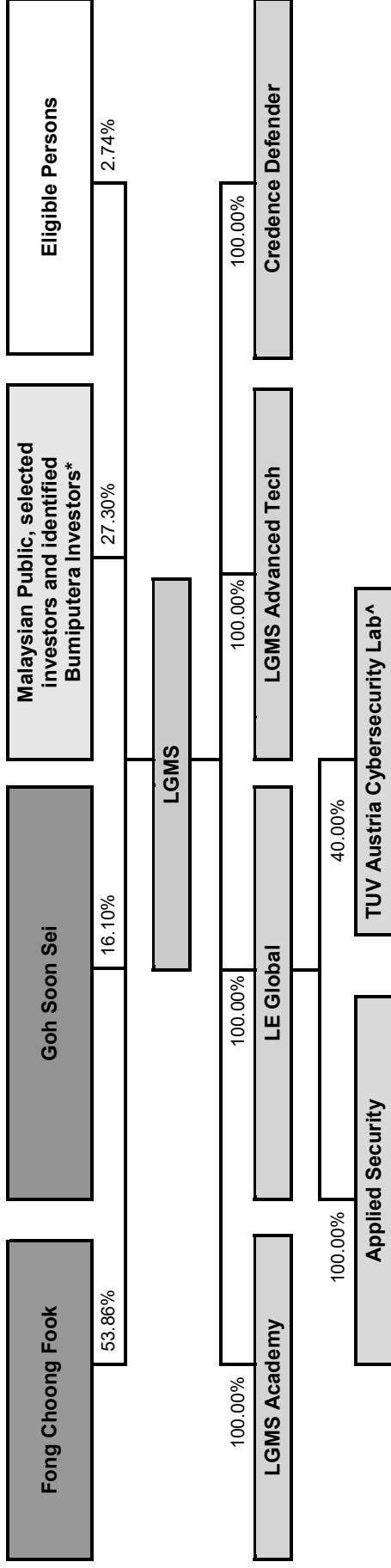


After the Pre-IPO Restructuring and as at the LPD



5. INFORMATION ON OUR GROUP (cont'd)

After the IPO



Notes:-

* Pursuant to the Public Issue and the Offer for Sale, further details of which are set out in Sections 3.3.1 and 3.3.2 of this Prospectus.

^ The remaining 60% equity interest is held by TÜV Trust I.T.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

5. INFORMATION ON OUR GROUP (cont'd)**5.5 Our subsidiaries and associate company**

The details of our subsidiaries and associate company as at the LPD are as follows:-

Name/Registration no.	Date/Place of incorporation	Principal place of business	Issued share capital (RM)	Effective equity interest (%)	Principal activities
Held by LGMS					
LE Global 200501018357 (700472-M)	17-06-2005 (Malaysia)	Malaysia	1,500,000	100.0	Provision of cybersecurity assessment, penetration testing, cyber risk management and compliance, and professional advice and recommendations to organisations on cybercrime and cybersecurity threats
LGMS Advanced Tech 201501042813 (1168134-M)	04-12-2015 (Malaysia)	Malaysia	50,000	100.0	Provision of IT security training and certification courses ⁽¹⁾
Credence Defender 201201037480 (1021962-T)	23-10-2012 (Malaysia)	Malaysia	100,000	100.0	Internet security services and general cybersecurity services such as vulnerability assessment
LGMS Academy 202001042702 (1399023-X)	23-12-2020 (Malaysia)	Malaysia	100	100.0	Dormant (<i>intended to undertake information security training activities</i>) ⁽¹⁾
Held by LE Global					
Applied Security 202001035047 (1391368-M)	30-10-2020 (Malaysia)	Malaysia	300,000	100.0	Provision of cybersecurity monitoring services
TUV Austria Cybersecurity Lab 201701002152 (1216302-X) (an associate of LE Global)	18-01-2017 (Malaysia)	Malaysia	10	40.0	Provision of technical testing and certification of IT related software and product

Note:-

- (1) We intend to consolidate and streamline all information security training businesses within our Group under LGMS Academy by the third quarter of 2022. LGMS Advanced Tech will focus on the IoT assessment services once its information security training business is transferred to LGMS Academy.

5. INFORMATION ON OUR GROUP (cont'd)**(i) Information on LE Global**

LE Global was incorporated on 17 June 2005 in Malaysia under the Companies Act 1965 as a private limited company under its present name. LE Global is principally involved in the provision of cybersecurity assessment, penetration testing, cyber risk management and compliance, and professional advice and recommendations to organisations on cybercrime and cybersecurity threats. The principal place of business of LE Global is at A-11-01, Empire Office Tower, Jalan SS 16/1, Subang Jaya, 47500 Selangor Darul Ehsan.

The issued share capital of LE Global is RM1,500,000 comprising 1,500,000 ordinary shares. Save as disclosed below, there has been no change in the issued share capital of LE Global since incorporation up to the LPD:-

Date of allotment	No. of shares allotted	Nature of transaction	Consideration	Cumulative issued share capital	
				RM	No. of Shares
17-06-2005	2	Subscribers' shares	Cash	2	2
07-01-2008	99,998	Allotment of shares	Cash	100,000	100,000
04-04-2011	400,000	Allotment of shares	Cash	500,000	500,000
12-07-2019	1,000,000	Allotment of shares	Cash	1,500,000	1,500,000

LE Global is our wholly-owned subsidiary. As at the LPD, LE Global only has a wholly-owned subsidiary, Applied Security and a 40.0%-owned associate company, TUV Austria Cybersecurity Lab.

As at the LPD, LE Global does not have any outstanding warrants, options, convertible securities and uncalled capital. In addition, there are no discounts, special terms or instalment payment terms applicable to the payment of the consideration for the allotments above.

(ii) Information on LGMS Advanced Tech

LGMS Advanced Tech was incorporated on 4 December 2015 in Malaysia under the Companies Act 1965 as a private limited company under the name of LGMS Group Sdn Bhd. On 8 September 2021, it assumed its present name. LGMS Advanced Tech is principally involved in the provision of IT security training and certification courses.

The principal place of business of LGMS Advanced Tech is at A-11-01, Empire Office Tower, Jalan SS 16/1, Subang Jaya, 47500 Selangor Darul Ehsan.

5. INFORMATION ON OUR GROUP (cont'd)

The issued share capital of LGMS Advanced Tech is RM50,000 comprising 50,000 ordinary shares. Save as disclosed below, there has been no change in the issued share capital of LGMS Advanced Tech since incorporation up to the LPD:-

Date of allotment	No. of shares allotted	Nature of transaction	Consideration	Cumulative issued share capital	
				RM	No. of Shares
4-12-2015	500,000	Subscribers' shares	Cash	500,000	500,000
15-08-2019	-	Reduction of share capital to return excess capital to the shareholders	-	50,000	50,000

LGMS Advanced Tech is our wholly-owned subsidiary. As at the LPD, LGMS Advanced Tech does not have any subsidiaries or associate companies.

As at the LPD, LGMS Advanced Tech does not have any outstanding warrants, options, convertible securities and uncalled capital. In addition, there are no discounts, special terms or instalment payment terms applicable to the payment of the consideration for the allotment.

(iii) Information on Credence Defender

Credence Defender was incorporated on 23 October 2012 in Malaysia under the Companies Act 1965 as a private limited company under its present name. Credence Defender is principally involved in the provision of internet security services and general cybersecurity services such as vulnerability assessment. The principal place of business of Credence Defender is at A-11-01, Empire Office Tower, Jalan SS 16/1, Subang Jaya, 47500 Selangor Darul Ehsan.

The issued share capital of Credence Defender is RM100,000 comprising 100,000 ordinary shares. Save as disclosed below, there has been no change in the issued share capital of Credence Defender since incorporation up to the LPD:-

Date of allotment	No. of shares allotted	Nature of transaction	Consideration	Cumulative issued share capital	
				RM	No. of Shares
23-10-2012	100,000	Subscribers' shares	Cash	100,000	100,000

Credence Defender is our wholly-owned subsidiary. As at the LPD, Credence Defender does not have any subsidiaries or associate companies.

As at the LPD, Credence Defender does not have any outstanding warrants, options, convertible securities and uncalled capital. In addition, there are no discounts, special terms or instalment payment terms applicable to the payment of the consideration for the allotment.

5. INFORMATION ON OUR GROUP (cont'd)**(iv) Information on LGMS Academy**

LGMS Academy was incorporated on 23 December 2020 in Malaysia under the Act as a private limited company under its present name. LGMS Academy is currently dormant and has been earmarked to undertake information security training activities (which is expected to commence by the third quarter of 2022). The principal place of business of LGMS Academy is at A-11-01, Empire Office Tower, Jalan SS 16/1, Subang Jaya, 47500 Selangor Darul Ehsan.

The issued share capital of LGMS Academy is RM100 comprising 100 ordinary shares. Save as disclosed below, there has been no change in the issued share capital of LGMS Academy since incorporation up to the LPD:-

Date of allotment	No. of shares allotted	Nature of transaction	Consideration	Cumulative issued share capital	
				RM	No. of Shares
23-12-2020	100	Subscribers' shares	Cash	100.00	100

LGMS Academy is our wholly-owned subsidiary. As at the LPD, LGMS Academy does not have any subsidiaries or associate companies.

As at the LPD, LGMS Academy does not have any outstanding warrants, options, convertible securities and uncalled capital. In addition, there are no discounts, special terms or instalment payment terms applicable to the payment of the consideration for the allotment.

(v) Information on Applied Security

Applied Security was incorporated on 30 October 2020 in Malaysia under the Act as a private limited company under its present name. Applied Security is principally involved in the provision of cybersecurity monitoring services. The principal place of business of Applied Security is at A-11-01, Empire Office Tower, Jalan SS 16/1, Subang Jaya, 47500 Selangor Darul Ehsan.

The issued share capital of Applied Security is RM300,000 comprising 300,000 ordinary shares. Save as disclosed below, there has been no change in the issued share capital of Applied Security since incorporation up to the LPD:-

Date of allotment	No. of shares allotted	Nature of transaction	Consideration	Cumulative issued share capital	
				RM	No. of Shares
30-10-2020	300,000	Subscribers' shares	Cash	300,000	300,000

Applied Security is a wholly-owned subsidiary of LE Global. As at the LPD, Applied Security does not have any subsidiaries or associate companies.

As at the LPD, Applied Security does not have any outstanding warrants, options, convertible securities and uncalled capital. In addition, there are no discounts, special terms or instalment payment terms applicable to the payment of the consideration for the allotment.

5. INFORMATION ON OUR GROUP (cont'd)**(vi) Information on TUV Austria Cybersecurity Lab**

TUV Austria Cybersecurity Lab was incorporated on 18 January 2017 in Malaysia under the Companies Act 1965 as a private limited company under the name of LGMS Infosec Lab Sdn Bhd and assumed its present name on 12 February 2020. TUV Austria Cybersecurity Lab is principally involved in the provision of technical testing and certification of IT related software and products. The principal place of business of TUV Austria Cybersecurity Lab is at A-11-01, Empire Office Tower, Jalan SS 16/1, Subang Jaya, 47500 Selangor Darul Ehsan.

The issued share capital of TUV Austria Cybersecurity Lab is RM10 comprising 10 ordinary shares. Save as disclosed below, there has been no change in the issued share capital of TUV Austria Cybersecurity Lab since incorporation up to the LPD:-

Date of allotment	No. of shares allotted	Nature of transaction	Consideration	Cumulative issued share capital	
				RM	No. of Shares
18-01-2017	10	Subscribers' shares	Cash	10	10

TUV Austria Cybersecurity Lab is a 40.0%-owned associate company of LE Global and the remaining 60.0% equity interest in TUV Austria Cybersecurity Lab is held by TÜV TRUST IT. TÜV TRUST IT was incorporated on 29 June 2009 in Cologne, Germany and is principally involved in, among others, the provision of services for companies and other institutions in all areas of control, planning, construction, implementation and operation of communication and information technology systems, in particular with regard to information security and quality. As at the LPD, the share capital of TÜV TRUST IT is EUR25,100 and it is wholly-owned by TÜV TRUST IT TÜV Austria GmbH. The directors of TÜV TRUST IT as at the LPD are Detlev Henze and Dirk Münchhausen.

As at the LPD, TUV Austria Cybersecurity Lab does not have any subsidiaries or associate companies.

As at the LPD, TUV Austria Cybersecurity Lab does not have any outstanding warrants, options, convertible securities and uncalled capital. In addition, there are no discounts, special terms or instalment payment terms applicable to the payment of the consideration for the allotment.

As at the LPD, neither our Company nor our subsidiaries or associate company is involved in any bankruptcy, receivership or similar proceedings.

5.6 Public take-overs

From the beginning of the FYE 31 December 2021 up to the LPD, there were no:-

- (i) public take-over offers by third parties in respect of our Shares; and
- (ii) public take-over offers by us in respect of other companies' shares.

5. INFORMATION ON OUR GROUP (cont'd)

5.7 Material investments and material divestitures

(i) Material investments

There have not been any material investments undertaken by our Group for the past 4 FYEs 2018, 2019, 2020 and 2021. As at the LPD, we also do not have any material investments in progress, within or outside Malaysia.

(ii) Material divestitures

Save as disclosed below, there have not been any material divestitures undertaken by our Group for the past 4 FYEs 2018, 2019, 2020 and 2021:-

- (a) LE Global had, on 4 February 2020, disposed of 60.0% equity interest of the total issued share capital of TUV Austria Cybersecurity Lab to TÜV TRUST IT for a total sale consideration of USD240,000 (equivalent to approximately RM0.97 million) following the establishment of a strategic partnership with TÜV TRUST IT. The sale consideration was calculated based on the agreed equity value for TUV Austria Cybersecurity Lab as at 25 October 2019, being the date of the share acquisition agreement, of USD400,000 (equivalent to approximately RM1.63 million), on the basis that TUV Austria Cybersecurity Lab does not and shall not have any liability as at the date of completion of the share acquisition agreement (including those related to tax). This sale resulted in a gain from disposal of approximately RM1.07 million by LE Global in the FYE 2020. Consequently, TUV Austria Cybersecurity Lab became an associate of LE Global.

As at the LPD, we do not have any material divestitures in progress, within or outside Malaysia.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

6. BUSINESS OVERVIEW

6.1 History and Background

The history of our Group began with the incorporation of LE Global on 17 June 2005 by our co-founders, Fong Choong Fook and Goh Soon Sei. Our founders have a combined working experience of more than 35 years in the cybersecurity market.

In the early years, LE Global was focused on information security training and formed an international partnership with Mile2 to set up and be the first Mile2 certified training and examination provider in Malaysia. Mile2 is an IT security company based in the USA which is involved in the provision of accredited education, training and cybersecurity certifications for information security professionals. Cybersecurity was still very new to Malaysia at that time, so this partnership with Mile2 allowed us to build our expertise and capabilities in this sector of the industry.

In 2009, LE Global became the first and only authorised PECB Trainer and Examiner in Malaysia. PECB is a certification body that provides education and certification under ISO/IEC 17024 for individuals in a wide range of disciplines.

In 2010, the management system of LE Global was assessed and certified to have conformed to the requirements of ISO/IEC 27001:2005 by DQS GmbH under the scope of the provision of information security services, including IT security risk consultancy, international standards compliance audit, training, penetration testing, computer crime investigation, IT security assessment and specialised IT security project implementation. LE Global was the first cybersecurity company in Malaysia to obtain the ISO/IEC 27001:2005 certification from DQS GmbH and later the updated ISO/IEC 27001:2013 certification from TÜV NORD (Malaysia) Sdn Bhd, enabling us to provide cybersecurity services to the financial services industry. As our business grew, we decided to move to our office located at Esplanade in Bukit Jalil, Selangor, in 2010.

In 2011, we made inroads into the e-payment industry after LE Global successfully became the first cybersecurity company in Malaysia to obtain the PCI Security Standards Council ASV status from PCI Security Standards Council. This status allows us to conduct security assessments for PCI DSS certification requirements. We had then relocated our office to Setiawalk in Puchong, Selangor. In 2013, LE Global became a Registered Training Provider with the Human Resources Development Fund, an agency under the Ministry of Human Resources Malaysia.

In 2014, LE Global became the first cybersecurity company in Malaysia to be a member of the CIS. CIS is a global community driven non-profit organisation that develops, validates and promotes timely best practice solutions that assist people, businesses, and governments to protect themselves against pervasive cyber threats.

In 2015, LGMS Advanced Tech was established to provide information security training to IT professionals in Malaysia and overseas. In 2016, LE Global became the first Malaysian cybersecurity company to collaborate with TÜV NORD Group, an international inspection, certification and testing organisation, through its subsidiary, TÜV NORD (Malaysia) Sdn Bhd, when it launched the TÜV-LGMS Secured Software Assurance programme. The TÜV NORD Group is a global technology group headquartered in Hanover, Germany, which offers its customers impartial, reliable and expert support in all matters concerning safety and security. The TÜV NORD Group has been active in the testing, inspection, certification, consulting, engineering and training market for over 150 years.

Under the programme, we conduct penetration testing and source code review on software applications and the resulting testing report is validated and certified by TÜV NORD (Malaysia) Sdn Bhd. In the same year, LE Global qualified as a QSA by the PCI Security Standards Council. A QSA company is an independent security organisation that has been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS.

6. BUSINESS OVERVIEW (cont'd)

In 2017, we established LGMS Infosec Lab Sdn Bhd (now known as TÜV Austria Cybersecurity Lab) to provide technical testing and analysis and other related IT services. A dedicated laboratory was also established to undertake the security testing of software. The laboratory of LGMS Infosec Lab Sdn Bhd had also been assessed and certified to have demonstrated its technical competence to operate in the field of software security testing in accordance with MS ISO/IEC 17025:2005 in the same year, allowing us to consistently deliver technically valid test results and allow us to provide certifications based on the Common Criteria standard.

LE Global also gained recognition from CREST, a not-for-profit accreditation and certification body representing the technical information security industry, after receiving a certificate of membership from the latter and becoming a full member organisation in the discipline of penetration testing. We were also the first cybersecurity company in Malaysia to gain such recognition for the discipline of penetration testing in 2017. In the same year, LE Global was awarded the 'Cyber Security Company of The Year' by CyberSecurity Malaysia in recognition of its innovativeness, commitment, industry/product/service leadership and sound business strategies. As our staff had by then grown to 35 persons, we relocated our office to Empire Office Tower in Subang, Selangor in the same year, occupying a total floor space of 14,748 sq ft.

In 2018, LE Global and ACE Accelerator Network Sdn Bhd formed a partnership to set up a cybersecurity hub in Malaysia – the Asia Cybersecurity Exchange to identify undiscovered cybersecurity talent and technology companies with growth potential. However, this collaboration was mutually ended in 2020 as the business focus of ACE Accelerator Network Sdn Bhd and LE Global had changed. In the same year, LE Global commenced its collaboration with Alibaba Cloud to help enterprises strengthen their security capabilities in a multi-cloud environment. Alibaba Cloud is the digital technology and intelligence backbone of Alibaba Group. LE Global was also named as one of the key IoT penetration testing vendors in the 2018 IDC Report titled 'Asia/Pacific IoT Security Landscape and Key Vendors' by IDC.

In 2019, LE Global became the first cybersecurity company in Malaysia to be a TÜV TRUST IT accredited tester. TÜV TRUST IT is a part of the TÜV Austria Group and is recognised in the field of information security and data protection as an objective, independent partner for consulting and certification services, with an international customer base from across a wide range of industries.

In July 2019, LE Global acquired the entire stake in LGMS Infosec Lab Sdn Bhd for a purchase consideration of RM3 from Fong Choong Fook (60% stake), Antonius Sommer (20% stake) and Teng Yung Chi (20% stake). The acquisition was part of the efforts to streamline and consolidate the information security services related businesses owned by Fong Choong Fook into our Group. In October 2019, LE Global agreed to dispose 60.0% of its equity interest of the total issued share capital of LGMS Infosec Lab Sdn Bhd to TÜV TRUST IT for a sale consideration of USD240,000 (equivalent to approximately RM0.97 million).

Consequently, following the completion of the transaction in February 2020, LGMS Infosec Lab Sdn Bhd became an associate of LE Global and was renamed TÜV Austria Cybersecurity Lab. TÜV Austria Cybersecurity Lab was accredited by CyberSecurity Malaysia as a Malaysian security evaluation facility (MySEF) for the Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme in 2020. The Common Criteria is an international standard for computer security certification. Since then, TÜV Austria Cybersecurity Lab has been undertaking Common Criteria certification projects involving international customers.

6. BUSINESS OVERVIEW (cont'd)

On 30 October 2020, Applied Security (now a wholly-owned subsidiary of LE Global) was established with LE Global and Ngiam See Chong holding a 52.0% and 48.0% stake in the company respectively. The 48.0% equity interest in Applied Security held by Ngiam See Chong was transferred to Fong Choong Fook on 15 December 2020, which in turn, was subsequently transferred to Chew Kia Sien on 24 February 2021. Chew Kia Sien disposed his 48.0% equity interest in Applied Security to LE Global on 9 June 2021. Ngiam See Chong and Chew Kia Sien, both of whom are not connected with our Promoters, divested their respective equity interest in Applied Security due to differences on the business direction of the company. Applied Security was established to provide cybersecurity monitoring services. During the same year, LGMS Academy was established by our Group with the aim to provide information security training to IT professionals in Malaysia and overseas. We intend to consolidate and streamline all information security training businesses within our Group under LGMS Academy by third quarter of 2022. LGMS Advanced Tech will focus on the IoT assessment services once its information security training business is transferred to LGMS Academy.

In July 2021, LE Global signed a Memorandum of Understanding (“**MoU**”) with Time dotCom Berhad to collaborate on a comprehensive cybersecurity management platform and services for critical infrastructure sectors. The MoU aims to better assist organisations of all sizes in increasing their cyber defence and cybersecurity awareness. In the same year, Alibaba Cloud announced a global partnership with LE Global whereby the integration of LE Global with Alibaba Cloud Marketplace will allow Alibaba Cloud's customers to gain access to LGMS' one-stop services to comply with PCI DSS. By leveraging on our collaboration with Alibaba Cloud and Time dotCom Berhad, we are able to expand our potential customer base by reaching out and offering our professional services to the customers of Alibaba Cloud and Time dotCom Berhad. As we have only recently started both collaborations in 2021, no revenue has been derived yet from the collaborations up to the LPD.

In April 2022, LE Global entered into a partnership with Celcom Mobile Sdn Bhd (“**Celcom**”) with the aim of LE Global offering vulnerability assessment services and cybersecurity rating reports to the business customers of Celcom. This partnership with Celcom allows Celcom to offer “value added” services to its business customers. The participating business customers of Celcom (“**Participating Organisations**”) will be able to enjoy a free 3-month summary report, whereby potential cybersecurity vulnerabilities of these Participating Organisations will be highlighted by way of ratings together with the possible cybersecurity risks and actionable recommendations will be provided to strengthen the security ecosystem of these Participating Organisations.

As at the LPD, we have grown into an established independent provider of professional cybersecurity services with a 90-person team with more than 16 years of operating track record.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

6. BUSINESS OVERVIEW (cont'd)

The key milestones for our Group are as follows:-

Year	Key milestones and achievements of our Group
2009	LE Global became the first and only authorised PECB Trainer and Examiner in Malaysia
2010	<ul style="list-style-type: none"> • LE Global's management system was assessed and certified to have conformed to the requirements of ISO/IEC 27001:2005 by DQS GmbH under the scope of the provision of information security services (including IT security risk consultancy, international standards compliance audit, training, penetration testing, computer crime investigation, IT security assessment and specialised IT security project implementation) • LE Global became the first cybersecurity company in Malaysia to obtain the ISO/IEC 27001:2005 from DQS GmbH, enabling us to provide cybersecurity services to the financial services industry
2011	LE Global became the first cybersecurity company in Malaysia to obtain the PCI Security Standards Council ASV status from PCI Security Standards Council
2014	LE Global became the first cybersecurity company in Malaysia to be a member of the CIS
2016	<ul style="list-style-type: none"> • LE Global collaborated with TÜV NORD (Malaysia) Sdn Bhd, a subsidiary of TÜV NORD Group, to launch the TÜV-LGMS Secured Software Assurance programme • LE Global qualified as QSA by the PCI Security Standards Council
2017	<ul style="list-style-type: none"> • LE Global became the first cybersecurity company in Malaysia to gain recognition from CREST, a not-for-profit accreditation and certification body representing the technical information security industry • LE Global was awarded the 'Cyber Security Company of The Year' by CyberSecurity Malaysia
2018	<ul style="list-style-type: none"> • LE Global commenced its collaboration with Alibaba Cloud to help enterprises strengthen their security capabilities in a multi-cloud environment • LE Global was recognised by IDC as one of the key IoT penetration testing vendors
2019	<ul style="list-style-type: none"> • LE Global became the first cybersecurity company in Malaysia to be a TÜV TRUST IT accredited tester • LE Global established a strategic partnership with TÜV TRUST IT via TUV Austria Cybersecurity Lab in which we have a 40% stake
2020	TUV Austria Cybersecurity Lab was accredited by CyberSecurity Malaysia as a Malaysian Security Evaluation Facility (MySEF) for the Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme
2021	Alibaba Cloud announced a global partnership with LE Global whereby the integration of LE Global with Alibaba Cloud Marketplace will allow Alibaba Cloud's customers to gain access to LGMS' one-stop services to comply with the PCI DSS
2022	LE Global entered into a partnership with Celcom to provide business customers of Celcom with vulnerability assessment services and cybersecurity rating reports

6. BUSINESS OVERVIEW (cont'd)

6.2 Description of our business

We are an independent provider of professional cybersecurity services, primarily involved in cybersecurity assessment and penetration testing, cyber risk management and compliance, and the provision of digital forensics and incident response services. The advancement of technologies and the widespread use of the Internet over multiple platforms and growth in cloud infrastructures, data centres and smartphones have led to an increase in the need and demand for cybersecurity protection. A snapshot of our business model is as follows:-

Business segment	Cyber risk prevention services	Cyber risk management and compliance services	Cyber threat and incident response services
Business activities	<p>Provision of services in pre-empting cyber attacks through:-</p> <p>Assessment</p> <p>(a) vulnerability assessment and penetration testing to identify vulnerabilities and cyber threats and prescribing the relevant recommendations and actions to be taken ("Assessment");</p> <p>Training</p> <p>(b) training for information security and IT professionals (who are typically employees of our Group's customers that are involved in the financial services sector[#]) on the relevant information security training courses; and</p> <p>Risk scoring</p> <p>(c) cybersecurity risk scoring and monitoring services[®] to assist our Group's customers in identifying the cybersecurity risks across its internet facing assets.</p>	<p>Provision of cybersecurity advisory and compliance services, which includes:-</p> <p>Compliance</p> <p>(a) identification and audit of any compliance gaps across their respective organisations to ensure compliances with the relevant regulations and directives, and the implementation of industry best practices for information security management as well as developing programmes and processes in compliance with regulations, directives and/or industry standards; and</p> <p>Certification</p> <p>(b) assess on the compliance with industry standards and certification services ("Certification services")</p>	<p>Provision of professional digital forensics services to assist our customers to understand the severity of cybersecurity threats and/or minimise its impact through:-</p> <p>Forensics & Incident Response</p> <p>(a) digital forensics and computer crime investigations;</p> <p>(b) cybersecurity incident response; and</p> <p>(c) compromise assessment.</p>
Revenue contribution*	57.36%	36.26%	6.38%
Our customers	Companies and businesses in the private sector as well as governmental and regulatory bodies		
Our industry coverage	Financial services [#] , telecommunications and media, technology companies and others (comprising manufacturing, logistics, hospitality, healthcare and retail)		

6. BUSINESS OVERVIEW (cont'd)

Notes:-

- # Includes financial institutions and insurance companies.
- @ We have introduced this new service under cyber risk prevention segment in the fourth quarter of 2020.
- ^ Computed based on the aggregate revenue contribution of the respective segments over the aggregate revenue of our Group for the past 4 FYEs 2018, 2019, 2020 and 2021.

Further details on our business segments are set out in **Sections 6.2.1, 6.2.2 and 6.2.3** of this Prospectus.

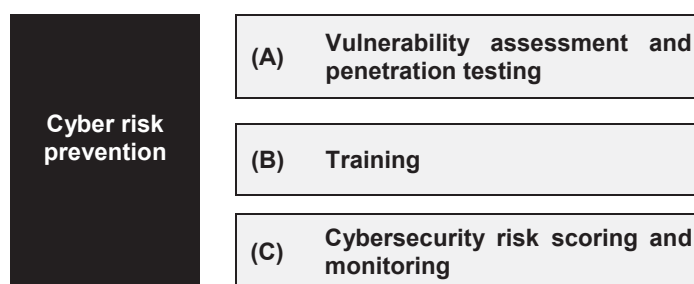
Our business is dependent on the performance of our customers' businesses. A good business performance can lead to higher budget and expenditure allocated by our customers for IT purpose including cybersecurity services and vice versa. We have a wide customer base as we count all entities and companies in the public and private sectors that utilise IT systems and/or the Internet as our potential customers. These include government bodies (comprising agencies and regulators) and companies that operate across a wide range of economic sectors such as financial services, telecommunications and media, technology companies, manufacturing, logistics, hospitality, healthcare and retail.

We provide our professional cybersecurity services predominantly in Malaysia. We also provide our services to overseas-based companies in countries within South East Asia (such as Singapore, Brunei, Cambodia, Indonesia, Thailand and Vietnam), Japan, Canada, Maldives, Netherlands, New Zealand, Australia, Saudi Arabia, France and the USA. Our cybersecurity team can carry out most of our service offerings remotely including for our overseas-based customers save for any works that require physical inspection such as physical security related assessment and computer crime investigation (that requires the physical presence of our technical personnel).

We do not represent any product brands. We do not actively sell cybersecurity hardware and software products. However, we may provide recommendations and/or assistance in procuring the required hardware and software products if such request is specifically made by our customers.

6.2.1 Cyber risk prevention

Our cyber risk prevention segment comprises the following services:-



6. BUSINESS OVERVIEW (cont'd)

(A) Vulnerability assessment and penetration testing

We offer vulnerability assessment and penetration testing to our customers with the aim of identifying vulnerabilities and cyber threats, and prescribing the relevant recommendations to fix the loopholes identified and actions to be taken by our customers (based on the recommendations) to address security weaknesses in their target information system. In order to maintain our independence, we do not assist our customers in implementing the recommendations. Typically, the implementation of our recommendations will be carried out by the internal IT department of our customers. External third parties or specialists such as system network integrators may be brought in by our customers to implement these recommendations in cases where the customer's internal IT department lacks the technical expertise, or if the maintenance of the customer's IT systems has been outsourced.

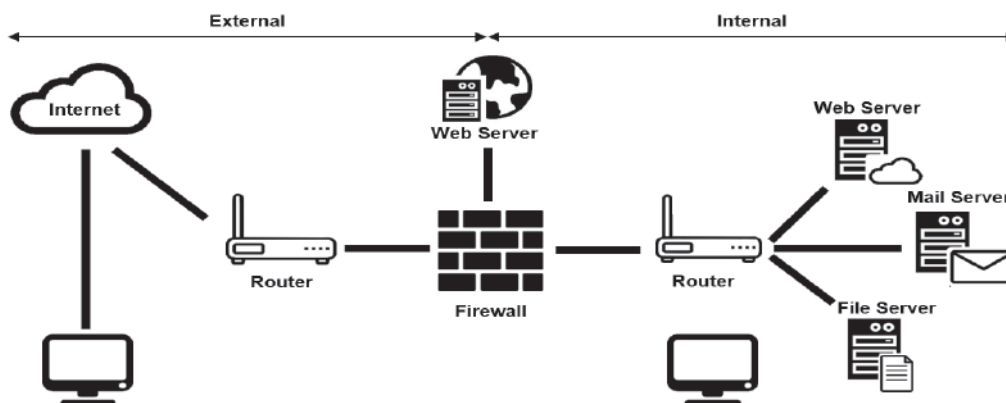
We rely heavily on the expertise of our technical personnel. Our technical personnel are also equipped with software tools (such as a vulnerability scanner to assess computers, networks and applications) when undertaking assessment and penetration testing projects.

We consider such assessment to be a critical part of information security protection strategies and is an area to be prioritised by businesses and organisations in view that digitalisation is getting more entrenched and technology is now widely used by enterprises, consumers and governments across different platforms, from conventional on-premise systems to cloud-based infrastructures. Vulnerability assessment and penetration testing can provide an early warning signal on whether a system can be attacked by cyber attackers by identifying weaknesses in the system that may cause negative impacts such as system shut down, data leakage and network disruption.

The vulnerability assessment and penetration testing services are typically performed in accordance with international standards such as OWASP and Open Source Security Testing Methodology Manual.

Our customers for this segment are from a wide range of end-user markets with a focus towards companies with mission-critical IT systems (i.e. systems that these companies are highly reliant on and any disruption or failure will have an adverse impact on its entire business and operations) namely, the financial services and telecommunications and media industries.

We conduct our vulnerability assessment and penetration testing services based on the following methodologies:-



[Picture courtesy of LGMS]

6. BUSINESS OVERVIEW (cont'd)

Testing environment	External scan	Internal scan
	Assessment on the outward presence (i.e. Internet facing and before the firewall) of our customers' information system/infrastructure, which include any perimeter devices, servers and applications that are accessible through the Internet	Assessment on the inward presence (i.e. beyond the firewall and the internal environment) of our customers' information system/infrastructure
Methodology	Black/Grey Box ("B/G Box")	White Box
	<ul style="list-style-type: none"> • The tester will mimic the actions of a malicious hacker at various skill levels (such as untrained individuals, mid-level hackers or elite hackers) and targets the information system (which includes computer systems or cloud platforms, fixed or wireless networks as well as web or mobile applications) • B/G Box assessment is conducted from the perspective of a hacker who is an outsider with no knowledge (Black Box), or an existing user (Grey Box) with limited access and knowledge of the inner workings of the target information system. The scope of testing under this method is considered limited as compared to White Box given the limited (Grey Box) or absence of knowledge (Black Box) of the inner workings of the target information system 	The tester is provided with full access (including log-in credentials and full authentication) to the target information system, which is the opposite spectrum from B/G Box methodology, where the tester has limited or no knowledge on the system

a) Vulnerability assessment

We conduct systematic review of security weaknesses in the target information system to:-

- (i) identify risks and vulnerabilities (including misconfigurations and policy non-compliance vulnerabilities that may not solely be resolved by patching or maintenance);
- (ii) evaluate the susceptibility of the target information system to known vulnerabilities;
- (iii) rank the level of severity of the vulnerabilities (based on priority, urgency and impact); and
- (iv) provide clear and actionable information on all identified vulnerabilities as well as recommend the corrective/remedial or mitigation actions to close the identified vulnerability gaps.

The key objective of undertaking the vulnerability assessment service is to create visibility to understand the security posture of networks, systems, applications and processes in order to establish a baseline security (minimum security controls to sufficiently safeguard against vulnerabilities) and reduce the security exposure of the information system of our customers from cyber attacks.

6. BUSINESS OVERVIEW (cont'd)

Our categories of vulnerability assessment services include but are not limited to the following:-

Key categories	Description
Network and server vulnerability assessment	Vulnerability assessment to determine the security vulnerabilities and security state of our customers' network environment, including public Internet protocol addresses, servers and connected devices linked to its network.
Configuration security assessment based on CIS database, host and network	We are able to undertake CIS configuration security assessment on our customers' databases, host and network devices based on the cybersecurity best practices supported by CIS Benchmarks.

b) Penetration testing

We perform authorised testing on computer systems or cloud platforms, wireless networks as well as web or mobile applications to identify security vulnerabilities which may be exploited by cyber attackers. It involves simulating an attempted breach into the target information system (such as front-end or back-end servers and application protocol interfaces) with the permission of its owner to identify, test and highlight vulnerabilities in the security posture (i.e. the overall state of cybersecurity readiness and hack proof) before they become critical liabilities. Penetration testing materially differs from vulnerability assessment as such testing involves active attempts to exploit security weaknesses in an operating environment and requires various levels of specific technical expertise, whilst vulnerability assessments may be automated via security scanning tools as this approach requires only minimal human interaction with the objective of identifying high level weaknesses.

Our Group, via our subsidiary, LE Global, is a full member organisation of CREST in the discipline of penetration testing ("**CREST Brand**") and LE Global was the first cybersecurity company in Malaysia to gain such recognition for the discipline of penetration testing. The CREST Brand is highly regarded in the IT security industry and is often recognised and associated with quality of service, technical cybersecurity expertise and know-how as well as competence in addressing the latest vulnerabilities and techniques used by real-life cyber attackers.

In undertaking our services, apart from adopting the standard penetration testing approaches and methodologies from OWASP and National Institute of Standards and Technology (such as Open Source Security Testing Methodology Manual), we will also take into consideration, amongst others, the business nature, business-related criticality, the level of risk tolerance of the relevant customer and overall industry practices.

The benefits of our penetration testing services are as follows:-

- (i) our customers will be able to test their information security controls, which were put in place for IT security purposes and to safeguard against cyber attacks;
- (ii) ensure compliance with industry standard(s) for IT security;
- (iii) expose the endpoints of the information system that are most susceptible to cyber attacks; and

6. BUSINESS OVERVIEW (cont'd)

- (iv) obtain the relevant recommendation and advice in terms of the prioritisation and remediation of the vulnerabilities.

We offer consulting and testing services that support compliance with various TÜV TRUST IT Security Assurance programmes. The compliance programmes are certified by TÜV TRUST IT. Our services offered under this programme are set out below:-

- (i) TÜV TRUST IT: Trusted Web Application Certifications;
- (ii) TÜV TRUST IT: Trusted Mobile App Certifications;
- (iii) TÜV TRUST IT: Trusted IoT Device Certifications;
- (iv) TÜV TRUST IT: Trusted Cloud Security Certifications;
- (v) TÜV TRUST IT: Trusted Secured Infrastructure Certification; and
- (vi) TÜV TRUST IT: Trusted Industrial IT Security Certification.

Under this programme, we conduct various assessments, testing, and validation that meet the requirements and certification guidelines set forth by TÜV TRUST IT. These services have become an integral part of the software development cycle for financial services customers in the European region.

The categories of penetration testing services offered by our Group include but are not limited to the following:-

Key categories	Descriptions
Web application and web services penetration testing	<ul style="list-style-type: none"> • We conduct our web application penetration testing based on technology and business logic (i.e. how data may be altered, created, shown and stored), and adhere to industry standards such as the OWASP Top 10 methodology (which regularly highlights security matters related to web application security particularly on the prevailing 10 most critical risks).
Mobile application penetration testing	<ul style="list-style-type: none"> • We conduct our mobile application penetration testing to identify configuration, development and deployment flaws of our customers' mobile applications from the latest mobile application security threats based on the Mobile OWASP Top 10 methodology.
Wireless access point security assessment	<ul style="list-style-type: none"> • We conduct our wireless access point security assessment to identify any gaps in the wireless security controls of wireless infrastructure. For existing wireless network users, we can enhance the existing environment to maximise radio frequency coverage while minimising channel interference.

6. BUSINESS OVERVIEW (cont'd)

Key categories	Descriptions								
<p>Social engineering with physical and logical attack</p>	<ul style="list-style-type: none"> • We conduct such assessment via social engineering based on the following methods:- <ul style="list-style-type: none"> (a) physical attack - intentional actions based on physical means to physical assets (such as hardware and infrastructure), such as attempting to gain access to restricted premises; or (b) logical attack - activities such as phishing, fake Wi-Fi access points, and/or scam calls, which are performed via virtual means on logical assets such as emails or personnel contact. • Social engineering is an act of using human interactions/human psychology to obtain or compromise information relating to the organisation or its information systems) and some of the examples are as follows:- <table border="1" data-bbox="687 786 1358 1128"> <thead> <tr> <th data-bbox="695 795 823 808">Types</th> <th data-bbox="831 795 1350 808">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="695 819 823 954">Phishing</td> <td data-bbox="831 819 1350 954">Using deceptive digital communication (such as email, telephone or text message) by posing as a trustworthy institution to lure the recipient of the digital communication into disclosing sensitive data such as usernames, passwords and credit card details</td> </tr> <tr> <td data-bbox="695 965 823 1043">Malware</td> <td data-bbox="831 965 1350 1043">A malicious software that is intentionally designed to harm or exploit any programmable devices, systems or networks</td> </tr> <tr> <td data-bbox="695 1055 823 1128">Tailgating</td> <td data-bbox="831 1055 1350 1128">Seeking entry to a restricted area that lacks the proper authentication by following behind or deceiving an authenticated person to gain physical access</td> </tr> </tbody> </table> 	Types	Description	Phishing	Using deceptive digital communication (such as email, telephone or text message) by posing as a trustworthy institution to lure the recipient of the digital communication into disclosing sensitive data such as usernames, passwords and credit card details	Malware	A malicious software that is intentionally designed to harm or exploit any programmable devices, systems or networks	Tailgating	Seeking entry to a restricted area that lacks the proper authentication by following behind or deceiving an authenticated person to gain physical access
Types	Description								
Phishing	Using deceptive digital communication (such as email, telephone or text message) by posing as a trustworthy institution to lure the recipient of the digital communication into disclosing sensitive data such as usernames, passwords and credit card details								
Malware	A malicious software that is intentionally designed to harm or exploit any programmable devices, systems or networks								
Tailgating	Seeking entry to a restricted area that lacks the proper authentication by following behind or deceiving an authenticated person to gain physical access								
<p>Intelligence-led penetration testing</p>	<ul style="list-style-type: none"> • We conduct our intelligence-led penetration testing to provide assurance on resilience to cyber attacks based on emerging and evolving threat scenarios such as malware/ransomware attacks, cyber intrusion, leaked credentials and phishing. • This penetration testing closely mimics the hacking tactics, techniques and procedures (“TTPs”) of sophisticated and persistent cyber attackers intending to compromise critical target information systems with the aim of reflecting extreme but plausible cyber attack scenarios. • Our intelligence-led penetration testing also assists our customers to comply with BNM’s Risk Management in Technology (a policy document which came into effect on 1 January 2020). The said BNM policy document requires the following financial institutions in Malaysia to conduct annual intelligence-led penetration tests on its internal and external network infrastructure as well as critical systems including web, mobile and all external-facing applications:- <ul style="list-style-type: none"> (a) licensed banks; (b) licensed investment banks; (c) licensed Islamic banks; (d) licensed insurers including professional reinsurers; (e) licensed takaful operators including professional retakaful operators; (f) prescribed development financial institutions; (g) approved issuers of electronic money; and (h) operators of a designated payment system. 								

6. BUSINESS OVERVIEW (cont'd)

Key categories	Descriptions
<p>Network and server penetration testing</p>	<ul style="list-style-type: none"> • We conduct our network and server penetration testing to assess the vulnerabilities of the network and servers from the angle of a malicious employee (insider) across different levels of access authority, or as a visitor. • We test the security of all the elements of the network that can be attacked from the outside (such as Internet protocol addresses and servers) as well as from the inside (such as servers and network devices).
<p>Cyber drill and blue team exercise simulation</p>	<ul style="list-style-type: none"> • Cyber drill refers to an exercise that tests all elements of an effective cyber attack or cyber threat detection and response strategy with an assigned team of defensive security professionals tasked to maintain the internal network defences against such cyber attacks and threats (referred as the blue team in the cybersecurity industry). • Our cyber drill and blue team exercise simulation allows an organisation to experience first-hand handling of real-life cyber attacks and cyber threats that have been simulated without running the risk of incurring actual damages. This will also increase the familiarity and preparedness of our customers' IT executives in facing a real-life cybersecurity crisis, in addition to identifying key gaps in the existing cybersecurity policies, standards and processes.
<p>Source code security review</p>	<ul style="list-style-type: none"> • We offer source code security review services to audit the source code for an application with the aim to verify and ensure proper security controls are in place and the application has been developed to be 'self-defending' in its given environment. • This service is deemed as an effective avenue to detect vulnerabilities that may not be identified during the process of penetration testing. Some of these application vulnerabilities may be introduced by the application developer either knowingly or unknowingly, such as application 'Backdoors' (methods that allow the bypassing of the usual security or authentication measures to gain access to an application or a computer). • We will assign our source code security reviewers to identify the blind spots, which some automated tools may not be able to uncover, and all our source code security review reports fully meet the compliance requirements of PCI DSS, Monetary Authority of Singapore Technology Risk Management Guidelines and Association of Banks in Singapore Cloud Computing Implementation Guide which are applicable to Singaporean financial institutions and their service providers.

6. BUSINESS OVERVIEW (cont'd)

Key categories	Descriptions
<p>Red team engagement</p>	<ul style="list-style-type: none"> • We offer red team engagement to conduct red teaming, an activity involving the assignment of a group of offensive cybersecurity experts to enact cyber attack scenarios on our customers' digital infrastructure (such as network, routers and applications) and physical infrastructure (such as data centres, offices and warehouses) as well as people (such as staff and third-party contractors) to evaluate the information security defence and security posture as well as how well the organisation would fare in the face of an actual cyber attack. <p>The scope of red teaming activities can be customised in accordance with the budget allocations and requirements of our customers.</p>
<p>IoT device security assessment</p>	<ul style="list-style-type: none"> • We conduct IoT device security assessment to protect our customers from the latest IoT device security threats. • We assess and identify common and complex security vulnerabilities which may be residing within the entire IoT ecosystem or in IoT devices (i.e. non-standard computing devices which are Internet-enabled, and have the ability to receive and transmit data).
<p>SST security assessment</p>	<ul style="list-style-type: none"> • The SST can be categorised into:- <ol style="list-style-type: none"> a) cash SSTs, which are computer terminals provided by banking institutions such as automated teller machines, cash deposit machines and cash recycler machines; and b) non-cash SSTs, which are computer terminals that provide non-cash transactions such as desktops, laptops, cheque deposit machines and tablets. <p>Our SST security assessments allow the owners of SSTs to review, update and ensure that sufficient logical and physical safeguards are implemented for their SSTs against the backdrop of an evolving threat landscape.</p>

Our vulnerability assessment and penetration testing services are offered on a one-off basis or a regular basis (which ranges from a quarterly basis to an annual basis) or multiple ad hoc engagements within a year, depending on the requirements of our customers. However, as the threat of cybersecurity incidents are continuously evolving, the need for vulnerability assessment and penetration testing are rarely kept to a one-time effort only. The need to keep an ongoing vigilance on our customers' information system to assist in uncovering any new vulnerabilities and prevent the exploitation of such vulnerabilities often result in our service agreements being renewed on a yearly basis. During the service period, we will perform assessments at various intervals throughout the year to ensure that updates of security patches or new components used do not inadvertently expose customers to cyber attacks.

After the completion of the vulnerability assessment or penetration testing service, our customers are entitled to our support services which include remediation advisory and guidance via email and/or phone support based on the agreed terms in the contract. Upon completion, we will re-visit our deliverables with the customers to address any remaining security gaps.

6. BUSINESS OVERVIEW (cont'd)

(B) Training

We have been providing training to information security and IT professionals since 2005 with a diverse line-up of relevant information security training courses. Our information security training courses are offered on a stand-alone basis or can be packaged together with our other cybersecurity services as a more comprehensive offering. These courses are also sometimes offered on a complimentary basis for projects involving other cybersecurity services of a certain size and scope.

Our partnership with Mile2, an IT security company based in the USA, allows us to provide accredited education, training and cybersecurity certifications for information security professionals. In addition, we are equipped as an authorised PECB Trainer and Examiner in Malaysia. PECB is a certification body that provides education and certification under ISO/IEC 17024 for individuals on a wide range of disciplines.

We are also an authorised trainer and examiner for CSA and ISACA accredited education and training since 2018. CSA is an organisation dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment, while ISACA is a global association that provides IT professionals with knowledge, credentials, training and community in audit, governance, risk, privacy and cybersecurity.

As at the LPD, we have collaborated, trained and/or certified more than 2,000 individuals. Some of the information security courses which we currently offer are as follows:-

Courses	Targeted Participants	Some of the key learning objectives
PCI DSS 3.2.1 Training Workshop	<ul style="list-style-type: none"> • Merchants • Payment service providers • IT service providers • Financial institutions 	<ul style="list-style-type: none"> • Introduce the importance of PCI DSS 3.2.1 compliance and share how businesses can maintain this compliance • Introduce best practices to be adopted by businesses
ISACA's Cybersecurity Nexus Cyber Security Fundamentals Certificate	<ul style="list-style-type: none"> • Information security professionals • IT professionals 	<ul style="list-style-type: none"> • Identify the key components of cybersecurity network architecture • Distinguish system and application security threats and vulnerabilities • Describe different classes of cyber attacks • Analyse threats and risks within the context of the cybersecurity architecture • Appraise cybersecurity incidents to apply an appropriate response
CSA Certificate of Cloud Security Knowledge	<ul style="list-style-type: none"> • Auditors seeking to perform and lead CSA Security, Trust & Assurance Registry programme audits • Project Managers or consultants seeking to master the CSA Security, Trust & Assurance Registry programme requirements • Information security professionals • IT professionals 	<ul style="list-style-type: none"> • Demonstrate technical knowledge, skills and abilities in developing a comprehensive cloud security programme relative to internationally accepted standards • Protect against threats with qualified professionals who have the expertise to competently design, build and maintain a secure cloud business environment • Ensure use of universal language, circumventing ambiguity with industry-accepted cloud security terms and practice

6. BUSINESS OVERVIEW (cont'd)

Courses	Targeted Participants	Some of the key learning objectives
PECB Certified ISO/IEC 27001:2013 Foundation	<ul style="list-style-type: none"> • Individuals involved in Information Security Management • Individuals seeking to gain knowledge about the main processes of information security management system (ISMS) • Individuals interested in pursuing a career in Information Security Management 	<ul style="list-style-type: none"> • Understand the elements and operations of an ISMS • Acknowledge the correlation between ISO/IEC 27001, ISO/IEC 27002 and other cybersecurity related standards and regulatory frameworks • Understand the approaches, standards, methods and techniques used for implementation and management of ISMS
PECB Certified ISO/IEC 27001:2013 Lead Implementer	<ul style="list-style-type: none"> • Managers and consultants involved in Information Security Management • Expert advisors seeking to master the implementation of an ISMS • Individuals responsible for maintaining conformance with ISMS requirements • ISMS team members 	<ul style="list-style-type: none"> • Acknowledge the correlation between ISO/IEC 27001, ISO/IEC 27002 and other cybersecurity related standards and regulatory frameworks • Master the concepts, approaches, methods and techniques used for the implementation and effective management of an ISMS • Learn how to interpret the ISO/IEC 27001 requirements in the specific context of an organisation • Learn how to support an organisation to effectively plan, implement, manage, monitor and maintain an ISMS • Acquire the expertise to advise an organisation in implementing ISMS best practices
PECB Certified ISO/IEC 27001:2013 Lead Auditor	<ul style="list-style-type: none"> • Auditors seeking to perform and lead ISMS certification audits • Managers or consultants seeking to master an ISMS audit process • Individuals responsible for maintaining conformance with ISMS requirements • Technical experts seeking to prepare for an ISMS audit • Expert advisors in Information Security Management 	<ul style="list-style-type: none"> • Understand the operations of an ISMS based on ISO/IEC 27001 • Acknowledge the correlation between ISO/IEC 27001, ISO/IEC 27002 and other cybersecurity related standards and regulatory frameworks • Understand an auditor's role to plan, lead and follow-up on a management system audit in accordance with ISO 19011 • Learn how to lead an audit and audit team • Learn how to interpret the requirements of ISO/IEC 27001 in the context of an ISMS audit • Acquire the competencies of an auditor to plan an audit, lead an audit, draft reports and follow-up on an audit in compliance with ISO 19011
Mile2 Certified Penetration Testing Engineer	<ul style="list-style-type: none"> • Information security professionals 	<ul style="list-style-type: none"> • Perform intensive hands-on lab activities based on a real world penetration testing model
Mile2 Certified Digital Forensics Examiner	<ul style="list-style-type: none"> • Cybercrime and fraud investigators 	<ul style="list-style-type: none"> • Gain knowledge on electronic discovery and advanced investigation techniques • Learn to use forensically sound investigative techniques

6. BUSINESS OVERVIEW (cont'd)

(C) Cybersecurity risk scoring and monitoring

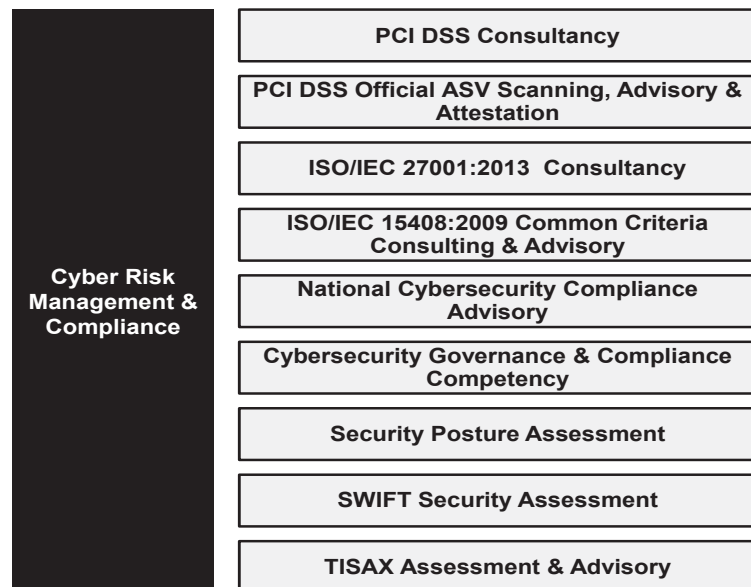
We are able to swiftly provide cybersecurity scores on an organisation’s cybersecurity risk to assist organisations in easily identifying and solving cybersecurity risks across their externally facing digital footprint. Our reports will provide ratings that take into the consideration Domain Name System (DNS) security, network security, endpoint security and information leakage, amongst others. As part of our internal policy, we require our technical personnel to be certified in the corresponding area of engagement when undertaking cybersecurity risk scoring and monitoring notwithstanding that there is no formal requirement to do so.

6.2.2 Cyber risk management and compliance

Our cyber risk management and compliance segment involve the provision of cybersecurity advisory and compliance services as well as certifications. We offer cybersecurity advisory and compliance services to assist our customers in complying with regulations and directives, implementing industry best practices on information security management, identify any compliance gaps across their respective organisations, audit on compliance with industry standards as well as develop programmes and processes that can assist with compliance with regulations, directives and/or industry standards in the future.

With our consultancy services, our customers are able to establish a comprehensive suite of cybersecurity governance framework that meets industry standards, in which our customers will have the option to invite a certification body to provide independent assurance on the effectiveness of cybersecurity controls implemented across the company. Such certification bodies include TÜV Austria and TÜV NORD Group amongst others depending on the type of framework involved. We are not a distributor of any cybersecurity products and solutions, and we also do not proactively sell or recommend any hardware and software products. However, we may, from time to time, and as and when requested by our customers, recommend and/or assist in procuring the required hardware and software products.

Our cyber risk management and compliance can be segmented into the following 9 areas:-



6. BUSINESS OVERVIEW (cont'd)

Type	Description
PCI DSS consultancy	<ul style="list-style-type: none"> Any organisation that accepts, processes and/or stores payment cards must comply with PCI DSS. This is particularly important as electronic payments have increasingly displaced the use of cash and cheque as the mode of payment of choice. We provide PCI DSS consultancy to assist our customers in complying with the PCI DSS requirements, a standard that applies to any organisation that processes, stores or transmits cardholder data and/or sensitive authentication data.
PCI DSS official ASV scanning, advisory and attestation	<ul style="list-style-type: none"> LE Global is a PCI ASV that is qualified by the PCI Security Standards Council to perform external network and system scans as required by the PCI DSS. As at the LPD, there are only 93 PCI ASVs in the world. Our PCI DSS ASV scanning is a fully managed service that does not require installation, configuration or maintenance. As such, our scanning service is considered to offer a more cost-effective service to our customers as the scanning is carried out by our own PCI experts with our own scanning solutions.
ISO/IEC 27001:2013 consultancy	<ul style="list-style-type: none"> ISO/IEC 27001:2013 is an internationally recognised information security management system (ISMS) standard. Our implementation methodology has assisted organisations in achieving and maintaining their certifications. We also offer pre-audit and internal audit as well as ISO/IEC 27001:2013 gap analysis to our customers.
ISO/IEC 15408:2009 Common Criteria consulting and advisory	<ul style="list-style-type: none"> Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408:2009) or 'Common Criteria' in short, is an internationally recognised standard for computer security certification. We provide guidance to our customers in the preparation and documentation of identified security properties of their information security products to be evaluated. Our associate company, TUV Austria Cybersecurity Lab, is a Common Criteria licensed laboratory that can undertake the formal evaluation of an information security product against claim(s) on its security attributes and also recommend Common Criteria certification to our national certification body if it passes the evaluation. The Common Criteria is recognised by all the signatories of the Common Criteria Recognition Arrangement, namely Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Republic of Korea, Singapore, Spain, Sweden, Turkey, USA, Austria, Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Indonesia, Israel, Pakistan, Poland, Qatar, Slovak Republic and the UK.
National cybersecurity compliance advisory	<ul style="list-style-type: none"> We assist our customers in meeting the following national cybersecurity regulatory and compliance requirements for the following:- <ul style="list-style-type: none"> (i) BNM's Risk Management in Technology Independent External Party Declaration Assessment <p>We can act as an independent external service provider as required in BNM's policy document for Risk Management in Technology ("BNM RMIT Policy") to provide assurance that the financial institution involved has addressed the technology risks and security controls associated with e-banking and Internet insurance.</p>

6. BUSINESS OVERVIEW (cont'd)

Type	Description
	<p>We provide compliance assurance for network resiliency and risk assessment as well as data centre resilience and risk assessment as required under the BNM RMIT Policy, where:-</p> <ul style="list-style-type: none"> (a) A network resilience and risk assessment is required to be conducted at least once every 3 years or whenever there is a material change in the network design, whichever is earlier; whilst; (b) A data centre resilience and risk assessment is to be conducted at least once every 3 years or whenever there is a material change in the data centre infrastructure, whichever is earlier to determine the current status of data centre resilience and to identify potential significant risks. <p>(ii) Monetary Authority of Singapore's Technology Risk Management Guideline</p> <p>The Monetary Authority of Singapore's Technology Risk Management Guideline requires threat and vulnerability risk assessment to be conducted whenever there is a significant change in the threat landscape or when there is a material change in the data centre's environment.</p> <p>We provide such threat and vulnerability risk assessment to identify the potential vulnerabilities and weaknesses of the data centre as well as the protection that should be established to safeguard it against physical and environmental threats.</p> <p>We also provide threat and vulnerability risk assessment through TUV Austria Cybersecurity Lab, with the certification issued by TÜV TRUST IT.</p> <ul style="list-style-type: none"> • We provide this service to banking and financial institutions, insurance and takaful companies, reinsurance and retakaful companies, approved issuers of electronic money and operators of a designated payment system.
<p>Cybersecurity governance and compliance competency</p>	<ul style="list-style-type: none"> • We assist our customers in meeting the following cybersecurity framework and compliance requirements:- <p>(i) Cyber Security Risk and Maturity Assessment</p> <p>The Cyber Security Risk and Maturity Assessment framework focuses on the critical cybersecurity aspects of the industry standards and frameworks to provide a score for the following focus areas:-</p> <ul style="list-style-type: none"> (a) asset management; (b) cybersecurity risk management; (c) incident response management; (d) operational security; (e) access control; (f) business continuity management; (g) regulatory compliance; and (h) human resources security.

6. BUSINESS OVERVIEW (cont'd)

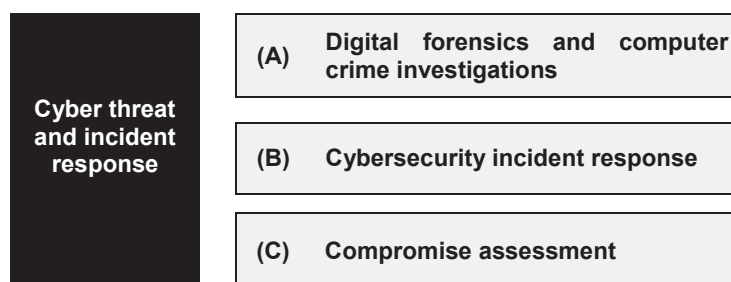
Type	Description
	<p>(ii) Unified Compliance Framework Consultancy</p> <p>Given that some organisations may be required to comply with multiple standards, regulations and guidelines, our service will assist our customers in consolidating and managing their compliance requirements under a single Unified Compliance Framework. Through the Unified Compliance Framework, our customers stand to benefit from more effective control, reduced compliance efforts, identification of compliance risks and increased visibility on the prevailing state of compliance at all times.</p> <p>(iii) COBIT gap analysis and advisory</p> <p>We can perform COBIT gap analysis and advisory to assist our customers in bridging critical gaps between control requirements, technical issues and business risks. COBIT is a framework for IT governance and management that is created by ISACA to ensure control, quality and reliability of the information system(s) of an organisation.</p> <p>(iv) Data security advisory</p> <p>Our Group provides advisory services on the protection of critical data assets. We assist organisations in minimising the risk of unintentional disclosure of sensitive data, effectively protecting data and privacy as well as achieving compliance with industry standards and laws and regulations.</p> <p>We are able to assist organisations in understanding their business-critical data (whose leakage, theft or exploitation would cause a significant impact on an entire business including business reputation), identifying its weaknesses and developing organisation-wide data protection and privacy strategies, processes and solutions.</p>
Security posture assessment	<ul style="list-style-type: none"> • Our security posture assessment services provide our customers with a realistic report consisting of an independent expert appraisal of the current cybersecurity issues that cover weaknesses, risks and loopholes within their organisations.
SWIFT security assessment	<ul style="list-style-type: none"> • Our Group is an official SWIFT approved CSP assessment provider. • SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services that support more than 11,000 financial institutions around the world and have systemic importance for the global economy whilst CSP is established by SWIFT to actively support its customers in the fight against cyber attacks by improving information sharing throughout the financial sector community, enhancing SWIFT-related tools for its customers and providing a set of cybersecurity controls which assists users to strengthen endpoint security and combat cyber fraud. • All SWIFT users have to attest to their level of compliance with a set of mandatory controls as described in the Customers Security Controls Framework ("CSCF"), which are prioritised to set realistic near-term goals for a noticeable increase in security posture and lower risk. We can also undertake vulnerability assessment and penetration testing for all related SWIFT applications and interfaces.

6. BUSINESS OVERVIEW (cont'd)

Type	Description
	<ul style="list-style-type: none"> With the release of the updated CSCF v2020 by SWIFT which sets a security baseline for all SWIFT users as part of its CSP, it is mandated that attestations will be required to be independently assessed by qualified assessors in accordance with the Community Standard Assessment for better accuracy of the attestations. <p>We can also act as an independent SWIFT CSP consultant in providing guidance, recommendations and/or validation of the controls deployed by our customers.</p>
TISAX assessment and advisory	<ul style="list-style-type: none"> TISAX is an assessment and exchange mechanism that was established by the German Association of the Automotive Industry (VDA) to support cross-company recognition of information security assessments in the automotive industry. We have the capabilities to conduct TISAX assessments based on the requested level 2 (random plausibility checks by telephone) or level 3 (on-site inspection).

6.2.3 Cyber threat and incident response

Our cyber threat and incident response segment involves the provision of professional digital forensics and incident response services. This segment consists of 3 sub-segments namely digital forensics and computer crime investigations, cybersecurity incident response as well as compromise assessment.



All cyber threat and incident response services offered by us are subject to strict compliance with the applicable federal, state and local laws and regulations. We have certified cybersecurity experts (with GIAC Certified Forensic Examiner and ACFE Certified Fraud Examiner) that can act as an expert witness.

(A) Digital forensics and computer crime investigations

There are 2 key areas to our digital forensics and computer crime investigations as follows:-

(i) Digital forensics

We offer digital forensics investigations and also provide litigation support by acting as expert witnesses. Digital forensics encompasses the recovery and investigation of materials found in digital devices, often concerning computer crime. Digital forensics is not only used to assist in cybercrime investigations but also to search and attempt to recover data that are not recoverable through normal means. Our digital forensics services include but are not limited to the following:-

6. BUSINESS OVERVIEW (cont'd)

- (a) computer fraud and crime investigation;
- (b) digital artifact forensics;
- (c) data recovery;
- (d) mobile device forensics;
- (e) cloud forensics;
- (f) litigation support and consulting; and
- (g) expert witness testimony.

Our professional digital forensics analysts are experienced in handling digital evidence and producing digital forensics reports that are admissible in court. We are equipped with the state-of-the-art software and hardware (which include commercialised digital forensics investigation analysis equipment). We can offer a wide range of digital forensics services on digital equipment/devices (such as computers, smartphones and servers) to individuals, legal firms, organisations (of any types and any sizes) and government agencies. Our digital forensics and computer crime investigation engagements are tailored to meet the specific needs of our customers.

(ii) Digital forensics readiness

Digital forensics readiness can be described as an organisation's capability in collecting, preserving and analysing digital evidence. The objective of digital forensics readiness is to maximise the potential usage of digital evidence while minimising the cost and time required for an investigation. In other words, it is the condition of being prepared in such a way that digital evidence is appropriately acquired before an incident so that it can be readily available when the need arises without interrupting business operations.

We assist our customers in the implementation of digital forensics readiness by:-

- a) identifying and assessing risk areas within the organisation and actions to be taken to avoid and minimise the impact of the identified risks; and
- b) conducting a comprehensive review and analysis of the organisation's existing security posture covering implemented technical controls, policies, procedures and employee skillsets.

(B) Cybersecurity incident response

As more corporations and businesses become dependent on computers in their daily business operations, cybersecurity incidents (such as malware and digital fraud) can occur in different aspects of a business resulting in the negative impact of different magnitudes ranging from minimal to critical. Responding to a cybersecurity incident is the key to ensuring that the resulting negative impact is confined to an acceptable level. Our trained cybersecurity experts are at all times (24 hours a day) ready to be deployed on-site to assist to act as the first responder for cybersecurity incident(s) on short notice (less than an hour response time for email and phone support, or physical presence in less than 2 hours during a declared cybersecurity incident within Klang Valley only). We can provide digital forensics and computer crime investigation engagements that are highly tailored to meet the specific needs of our customers, if required.

(C) Compromise assessment

We are able to conduct a compromise assessment for our customers to determine whether their system or network has been compromised. Activities that may indicate that a network or system has been compromised include but are not limited to the following:-

6. BUSINESS OVERVIEW (cont'd)

- (i) suspicious lateral movements in the network;
- (ii) escalation of user privileges;
- (iii) abnormal amount of network traffic;
- (iv) anti-virus configuration being tampered; and
- (v) unusual files and/or folders in protected directories.

6.3 Competitive strengths

6.3.1 Established track record and industry-wide recognitions

Our Group has been providing professional cybersecurity services since 2005, and we have been recognised by CyberSecurity Malaysia, IDC and other industry bodies (including accreditation and certification bodies) for our services as well as our contribution to the cybersecurity market. LE Global was awarded the 'Cyber Security Company of The Year' in 2017 by CyberSecurity Malaysia in recognition of its innovativeness, commitment, industry/product/service leadership and sound business strategies. LE Global was also named as one of the key IoT penetration testing vendors in the 2018 IDC Report titled 'Asia/Pacific IoT Security Landscape and Key Vendors' by IDC, a global provider of market intelligence, advisory services, and events for the IT, telecommunications, and consumer technology markets.

We believe that we have made a significant contribution to the growth of the local cybersecurity market through our pioneering efforts by being the first local cybersecurity company in Malaysia to achieve the following:-

- (i) 1st to be a member of the CIS;
- (ii) 1st to obtain the ISO/IEC 27001:2005 certification from DQS GmbH;
- (iii) 1st to obtain the ISO/IEC 27001:2013 certification from TÜV NORD (Malaysia) Sdn Bhd;
- (iv) 1st to obtain the PCI Security Standards Council ASV status;
- (v) 1st full member organisation of CREST in the discipline of penetration testing;
- (vi) 1st Mile2 certified training and examination provider;
- (vii) 1st authorised PECB Trainer and Examiner; and
- (viii) 1st to be a TÜV TRUST IT accredited tester.

In addition, as at the LPD, we are one of the only 93 PCI ASVs in the world. LE Global is the only PCI-certified ASV in Malaysia. As at the LPD, there are 389 PCI QSA companies globally. Any financial institutions, merchants, retailers, e-wallet service providers, call centres and data centres that need to meet full compliance with PCI DSS requirements are required to engage an officially appointed PCI ASV annually. This shows that we belong to only a small group of organisations in the world that have successfully met all PCI Security Standards Council requirements to perform PCI data security scanning. We believe that our achievements and continuous efforts will stand us in good stead, raise our profile and further enhance our reputation in the cybersecurity market. As at the LPD, LE Global is an active member of the following cybersecurity-related international certification bodies/communities:-

- (i) CIS;
- (ii) CREST;
- (iii) CSA;
- (iv) ISACA;
- (v) PCI Security Standards Council; and
- (vi) PECB.

6. BUSINESS OVERVIEW (cont'd)

We gain various benefits from the above mentioned memberships which include but are not limited to gaining access to members-only bulletins, software and/or training materials, which allow us to keep abreast with the latest developments in the cybersecurity market. We also benefit from being included in members directory listing of these certification bodies / communities from a branding and marketing perspective.

6.3.2 Experienced senior management team with certified cybersecurity expertise

Our Group is spearheaded by our founders, our Executive Chairman, Fong Choong Fook and Executive Director, Goh Soon Sei, who are both veteran cybersecurity experts, and have participated in the cybersecurity market for more than 20 years and 15 years respectively. Other members of our senior management team, which consist of our Chief Operating Officer, Gilbert Chu and our Senior Director, Professional Services, Fow Chee Kang, both have more than 10 years of working experience in the cybersecurity market. Our senior management team have been instrumental towards growing and sustaining our competitiveness in the cybersecurity market. Our technical team is also a key asset of our Group. As at the LPD, we have 2 PCI QSA certified employees and 3 PCI ASV certified employees in our team. The growth of our business is highly dependent on the size and expertise of our technical team. With more qualified and experienced technical personnel, we are able to take up more projects and projects that are more complex. Please refer to **Section 6.10** of this Prospectus for further details on the number of technical personnel (computer engineers and programmers) employed by our Group as at 31 December 2018, 2019, 2020 and 2021 and as at the LPD.

Our team holds the following key internationally recognised cybersecurity related certifications (at the individual level), which are highly regarded in the cybersecurity market:-

Certification(s)	Our business segment(s)		
	Cyber risk prevention Services	Cyber risk management and compliance services	Cyber threat and incident response services
• Certificate of Cloud Security Knowledge (CCSK) V4 from CSA	✓	✓	
• ISACA Certified Information Security Manager (CISM)	✓	✓	
• ISACA Certified Information Systems Auditor (CISA)	✓	✓	
• Offensive Security Certified Professional (OSCP)	✓	✓	
• Offensive Security Certified Expert (OSCE)	✓	✓	
• Offensive Security Experienced Penetration Tester (OSEP)	✓	✓	
• PCI Security Standards Council QSA (PCI QSA)		✓	
• PCI Security Standards Council ASV (PCI ASV)	✓	✓	
• (ISC) ² Certified Information Systems Security Professional (CISSP)	✓	✓	✓
• IRCA Information Security Management Systems Auditor	✓	✓	
• ACFE Certified Fraud Examiner (CFE)			✓
• PECB Certified ISO/IEC 27001 Senior Lead Auditor	✓	✓	
• PECB Certified ISO/IEC 27032 Senior Lead Cybersecurity Manager	✓	✓	

6. BUSINESS OVERVIEW (cont'd)

Certification(s)	Our business segment(s)		
	Cyber risk prevention Services	Cyber risk management and compliance services	Cyber threat and incident response services
• PECB Certified ISO/IEC 27001 Lead Implementer	✓	✓	
• PECB Certified ISO/IEC 27001 Senior Lead Implementer	✓	✓	
• PECB Certified ISO/IEC 27001 Lead Auditor	✓	✓	
• PECB Certified Trainer	✓	✓	
• Cellebrite Certified Logical Operator (CCLO)			✓
• Cellebrite Certified Physical Analyst (CCPA)			✓
• Malaysia Common Criteria Scheme Foundation Evaluator		✓	

The abovementioned list of certifications is a full list of key certifications held by our team as at the LPD. These internationally recognised cybersecurity related certifications can provide comfort and assurance to our customers on our ability and the technical capabilities of our team in undertaking cybersecurity related works. This allows us to be in a better position to secure projects, receive invitations for project tenders from potential customers and collaborate with strategic partners (such as the joint venture with TÜV Austria Group) that can drive business growth. Please refer to **Sections 8.1.3** and **8.4.2** of this Prospectus for further details of the credentials of our Promoters and members of our key senior management team.

6.3.3 Strategic partnership with TÜV Austria Group

In 2019, we established a joint venture with TÜV TRUST IT via TUV Austria Cybersecurity Lab in which we have a 40% stake. The strategic partnership allows us to leverage on the established TÜV methodologies and branding in the business of providing testing and certification services, focusing on Common Criteria certification projects involving international customers. Under the Common Criteria certification process (which is project based), TUV Austria Cybersecurity Lab will:-

- (a) assist its customers to conduct testing on the newly developed IT products (which require Common Criteria certification prior to product launch); and
- (b) issue the certification recommendation upon satisfactory assessment and successful completion of the testing process.

The typical duration of such process ranges from 3 months to 12 months.

TÜV TRUST IT is a part of the TÜV Austria Group and is recognised in the field of information security and data protection as an objective, independent partner for consulting and certification services with an international customer base from across a wide range of industries. This collaboration was a key milestone for our Group. As part of the joint venture, our role is to provide the workforce for performing technical testing and analysis and other related IT services as well as the marketing and technical support to the business in the overseas markets. Given that TÜV TRUST IT's established market presence in Europe, the strategic collaboration with LGMS through TUV Austria Cybersecurity Lab allows TÜV TRUST IT to have a presence in Asia and provides both parties with the platform to tap into the cybersecurity opportunities relating to Common Criteria certification services given that Malaysia is strategically located at the heart of South-East Asia.

6. BUSINESS OVERVIEW (cont'd)

The TÜV Austria Group's commitment to forming a joint venture with us has elevated our standing amongst our global peers. We are proud to be able to have a highly esteemed and trusted certification body as our strategic partner in the provision of technical testing and analysis and other related IT services. We believe that we can continue to work and grow together in the area of cybersecurity testing through TUV Austria Cybersecurity Lab's MS ISO/IEC 17025:2005 certified laboratory.

Since the formation of the strategic partnership, we have undertaken certification related projects in the overseas markets such as Cambodia, Indonesia, Singapore, Thailand and Vietnam. For example, we were involved in the Common Criteria certification for a major customer based in Singapore for its web portal, which was completed in 2021.

6.3.4 A diversified customer base and long-term customer relationships assist to drive customer retention, broaden revenue stream and maximise recurring income opportunities

With more than 15 years of operating history, we have an established local and international customer base across a broad range of industries. Our customers include major local banks and insurance companies, multinational companies and government agencies, some of whom have decade-long relationships with us and are recurring or repeat customers that believe in our professional cybersecurity services. For the past 4 financial years under review, we have serviced more than 400 customers across various end-user industries. A diversified customer base helps us to mitigate the risk of over-reliance on a single customer or a single industry.

6.3.5 An independent provider of professional cybersecurity services

We are an independent provider of professional cybersecurity services, primarily involved in cybersecurity assessment and penetration testing, cyber risk management and compliance and the provision of digital forensics and incident response services by providing professional advice and recommendations to organisations on cybercrime and cybersecurity threats. We consider ourselves as an independent provider of professional cybersecurity services as we do not represent any product brands and do not carry any quota as distributors to sell products. We take an impartial approach in all our service offerings. We are not a distributor of any cybersecurity products and solutions, and we also do not proactively sell or recommend any hardware and software products as our priority is on the services that we provide. We may, from time to time and as and when requested by our customers, recommend and/or procure the required hardware and software products. We believe that our impartiality contributes to building our customers' trust and confidence in the integrity of our services.

We offer a wide range of vulnerability assessment and penetration testing services to our customers, using industry best practices as well as internationally recognised and accepted methodologies and cybersecurity tools. Our team of certified cybersecurity experts is ready to support our customers in identifying and remediating the vulnerabilities in their IT systems and combating cyber threats, and complying with regulatory requirements and industry standards on information security, including PCI DSS.

We are committed to educating and increasing awareness of cybersecurity. We provide accredited education, training and cybersecurity certifications to information security and IT professionals. We have also provided consultation and trained multiple government agencies and multinational customers on information system security, enterprise risk matrix design, policy review, policy implementation assurance, penetration testing, technical configuration evaluation, security procedures and disaster recovery/business continuity planning.

We also assist our customers to investigate cybersecurity incidents and undertake the necessary digital forensics and compromise assessment works. Our cybersecurity experts have also been called to be 'expert witnesses' to study, assess, evaluate and testify in a court of law.

6. BUSINESS OVERVIEW (cont'd)

6.4 Impact of COVID-19 on our Group

COVID-19 was officially declared a health pandemic by the Director General of the World Health Organisation on 11 March 2020. Throughout 2020 and 2021, several phases of the Movement Control Order (“MCO”) were implemented in the country to curb the spread of the COVID-19 pandemic with varying levels of restrictions.

The COVID-19 pandemic had impacted our business operations in the following manner:-

- (a) our mode of engagement with our customers had increasingly revolve around remote engagements (i.e. calls and virtual meetings) rather than physical meetings; and
- (b) we have implemented relevant processes to ensure strict adherence to the health and safety protocols with the objective to safeguard the health and well-being of our employees and customers as well as comply with regulatory requirements.

Other potential negative impact may include a decline in our customer prospects and the slowdown of the businesses of our existing customers, which may result in a material decline in demand for our services as our customers may reduce and/or deprioritise overall spending on IT and/or cybersecurity services to increase profitability or as a result of scaling down of their operations. We have experienced a marginal decrease in our revenue from the local market of approximately RM0.92 million or 5.30% due to the lower number and slowdown of the implementation of cybersecurity projects in FYE 2020 in view of the COVID-19 pandemic (which led to the decrease in the total customers serviced during the financial year from 192 customers in 2019 to 165 customers in 2020).

Save as disclosed above, we have not experienced other negative impacts. On the other hand, the demand for our cybersecurity services may increase with the rising trend of remote working arrangements following the MCO.

Although Malaysia has transitioned to the “Endemic” phase on 1 April 2022, we are unable to assess the full extent of the potential impact of the COVID-19 pandemic as at the LPD particularly if it persists for an extended period of time or due to any resurgence of new COVID-19 variants. Further, as at the LPD, we have not experienced any material decline in demand for our services by our customers notwithstanding the challenging economic conditions due to the COVID-19 pandemic. As the vaccine rollout ramps up and the workforce gradually returns to their offices following the “Endemic” phase, any positive impact on our business may slow down subsequently or decline once the impact of the pandemic tapers down.

Whilst we have seen a reduction in certain of our Group’s operating expenses due to reduced business travel and the virtualisation or cancellation of employee events, if our employees fail to comply with the COVID-19 standard operating procedures implemented by our Group and/or the government, we could also potentially face the spread of COVID-19 amongst our employees. If any of our employees are to contract COVID-19, the impact from the restricted human resource capacity may cause a delay to the delivery of our services to our customers. This could lead to higher costs and may have a material adverse effect on the business, financial condition and financial performance of our Group.

During the pandemic period, we have implemented the following activities and protocols (which are only applicable to our operations at our premise and projects undertaken locally) to ensure the health and well-being of our employees and customers as well as comply with regulatory requirements:-

6. BUSINESS OVERVIEW (cont'd)

a) Disease prevention and restriction protocol

We have established a protocol at workplace to monitor and prevent the spread of the COVID-19. This protocol is documented in our health and safety manual.

b) Health screening and reporting

We have allocated 2 non-contact infrared thermometers at each entrance to our workplace. The body temperature reading of each person entering the workplace is performed and recorded by the assigned personnel at the entrance. The person entering the workplace would be required to 'check-in' via the MySejahtera mobile application. The assigned personnel will also be on alert for any symptom(s) of cough, sore throat and breathing difficulty. Any person with a body temperature of 37.5 degrees Celsius and above or who shows any above mentioned symptoms will be referred to the nearest clinic. The affected person will not be allowed to enter the workplace.

c) Eradication and decontamination of premise

Cleaning and sanitising of workplace are conducted at least twice a day throughout the common areas such as meeting rooms and toilets. We also conduct disinfection of the entire workplace before the start of a shift or operations. Besides that, hand sanitisers are also placed at various areas around the workplace including the entrances and common areas.

d) Social distancing and health safety procedures for our employees

We have adopted social distancing at workplace with each workstation being placed at least 1 metre from one another. Our employees are required to wear a face mask in common areas.

e) Ethics in the general area of the premise

We have allocated multiple break sessions on a staggered basis between all our employees. Our pantry is also stocked with packaged food and packet drinks limiting employees from going out to have their meals.

f) Social distancing and health safety procedures for customers

We have adopted social distancing measures at our meeting rooms. The seating is placed at least 1 metre from one another. Each person is also required to wear a face mask in the meeting room. The number of people allowed in the meeting room is also restricted to less than 5 persons at a time depending on the size of the meeting room involved.

g) Work from home arrangement

We have further adopted a flexible work arrangement which allows our employees to work from home to the extent possible. We have also made substantial modifications to employee travel policies, and cancelled or shifted selected marketing and other corporate events to virtual-only formats.

h) Emergency response

We have also created a working committee headed by Gilbert Chu to handle any emergency cases involving COVID-19 infection(s) or investigation(s). We will bear all the expenses incurred for the required COVID-19 testing on our employees and other close contact persons within the same workplace, the treatment of our employees who have contracted COVID-19 as well as the cost of disinfection of the workplace.

6. BUSINESS OVERVIEW (cont'd)

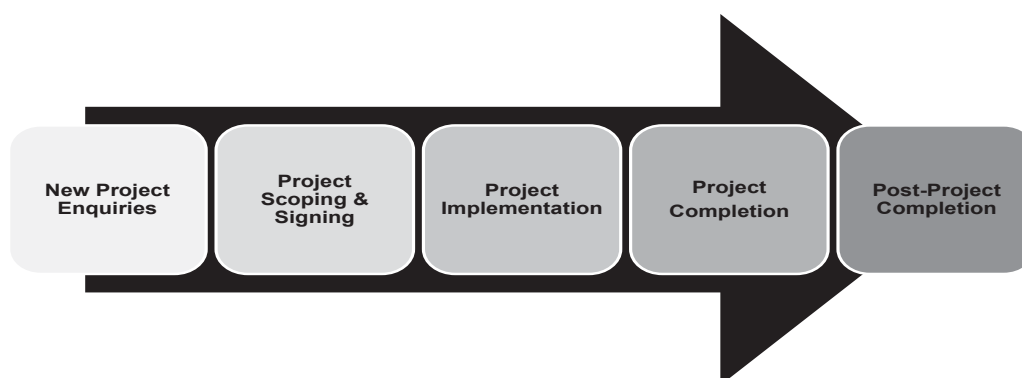
As at the LPD, the estimated compliance cost incurred by our Group arising from complying with the protocols mentioned above (in respect of our operations in our office premise) is RM28,000.

We closely monitor the development of the pandemic through the various levels of lockdown measures imposed in Malaysia and the jurisdictions in which our customers operate. As we have adopted flexible working arrangements (by allowing work-from-home arrangement subject to active communications with superiors) even prior to the COVID-19 pandemic, our business operations have not been adversely impacted as our employees are able to operate at full capacity and just as effectively, work from home (remotely). As for overseas engagements, we have been able to work remotely despite the travel restrictions. We have been able to enjoy savings on operational expenses of around RM98,000 and RM37,400 for FYE 2020 and FYE 2021 respectively due to reduced spending on business travels. The reduction in spending on business travels did not materially impacted our overseas revenue in the FYEs 2020 and 2021 as we were able to secure new purchase orders and/or contracts from our overseas customers as well as undertake the cybersecurity projects remotely without the need to travel overseas. Although Malaysia has transitioned to “Endemic” phase on 1 April 2022 (with the upliftment of all restrictions limiting business operating hours and number of employees in a workplace based on vaccination coverage), our management has opted to adopt a rotational work from home arrangements at this juncture. By continuing such work arrangements at this juncture, we do not expect any further closures or restrictions to impact our business operations in the event of any resurgence of new COVID-19 variants resulting in reintroduction of such restrictions and closures.

As at the LPD, we have 19 reported cases of our employees of our Group having contracted COVID-19. The affected employees contracted the virus outside the office and have already recovered from the virus.

6.5 Operational process and facilities

The operational processes which are applicable to all types of services offered by our Group, involve 5 stages starting from new project enquiries and ending with the post-project completion stage as follows:-



6. BUSINESS OVERVIEW (cont'd)

Stage 1: New project enquiries

We have a dedicated business development team consisting of 6 personnel that will follow up on incoming enquiries from potential customers through emails, our corporate website, walk-ins or phone calls. We have also been invited from time to time to participate in project tenders. Our Group also gains new projects through incoming leads (of potential customers) who have responded to our various marketing and sales activities and/or channels such as advertisements, our corporate website, media blitz, social media platforms, events (such as webinars or seminars) as well as referrals from our existing customers.

Stage 2: Project scoping and signing

Upon receiving an enquiry for a potential new project, we will initiate and engage with the potential customers to understand and determine the project or training requirements which include but are not limited to the scope of work, pricing, timeline and potential project risk associated with the engagement. Once the salient terms of the project or scope of training are agreed upon, a purchase order (for small-scale projects and training or ad hoc requests for particular services) will be issued by the customers or in certain circumstances, a formal contract (for large-scale projects or requests for multiple services which include training services) will be prepared and signed by both parties. A mobilisation fee will also be billed and collected depending on the type of engagement involved. The mobilisation fee is an upfront fee of a certain percentage of the project value (subject to negotiation) which is paid by the customer for us to begin our work.

Stage 3: Project implementation

The project team would meet with our customers regularly throughout the entire duration of the project implementation stage to monitor the progress of the project as well as to identify and rectify any project issue(s). The respective scope of works will be carried out as per project engagement. An interim report may be prepared and submitted to the customers depending on the type of engagement involved. Quality assurance activities such as verification and report review will be undertaken, where applicable. We may also conduct a presentation during one of the meetings with the customer. Depending on the salient terms of the contract, interim payment(s) may be billed and collected upon successfully achieving the agreed milestone(s). The duration of the project implementation is generally between 3 months and 12 months. For our training services, we will conduct the required training according to the proposed schedule.

Stage 4: Project completion

A final report (which may include executive summary, technical details, security risk rating and prioritisation of findings and/or comprehensive remediation guidance recommendation for future improvement) will be prepared and given to the customer. A final presentation will also be conducted with the customers if required. The final payment will be subsequently billed and collected. The project is officially completed once the final project sign-off is obtained or the final payment is made by the customer. As for our training services, we will issue a certificate of attendance to the training attendees upon the completion of the training.

Stage 5: Post-project completion

After the project completion, our customers are entitled to our support services which include remediation advisory and guidance via email and/or phone support based on the agreed terms in the contract. Upon completion, we will re-visit our deliverables with the customers to address any remaining security gaps. In the case of vulnerability assessment related projects, we also provide complimentary post-assessment services for our customers on a one-off basis. For our training services, we will conduct a post-training assessment to get feedbacks from our training attendees.

6. BUSINESS OVERVIEW (cont'd)**6.6 Technology used**

Our Group utilises and leverages on software technology to operate and execute specific tasks on the computer or other technological devices. We use both open source and commercially off-the-shelf software. We are equipped with specialised hardware which includes commercialised digital forensics investigation analysis equipment and forensic software tools used for forensic assignments. We have developed our own software tool, LGMS Reporter, to undertake analysis and reporting works involving the consolidation of results (details on vulnerabilities detected) from multiple scanning tools used, analysis of the results as well as generation of the reports on the findings made. Our LGMS Reporter holds a Common Criteria (EAL 2) certificate which indicates that a consistent process is established to maintain the security of the tool used and its data. Our LGMS Reporter was developed in 2009 and as at the LPD, it is a proprietary software of our Group and it is intended for internal use only. We have also developed the PCI DSS Compliance Wizard to help organisations achieve compliance, and facilitate management of assessments and documentations related to PCI DSS compliance in a single platform.

6.7 Our business segments and markets**6.7.1 Revenue by customer base**

The breakdown of our revenue by customer base is as follows:-

	Audited							
	FYE 31 December							
	2018		2019		2020		2021	
	(RM'000)	(%)	(RM'000)	(%)	(RM'000)	(%)	(RM'000)	(%)
Financial services	7,099	40.83	7,633	37.12	11,023	53.38	14,435	51.07
Telecommunications and media	5,551	31.93	6,069	29.51	2,873	13.91	1,118	3.96
Technology	2,144	12.33	3,750	18.24	4,182	20.25	6,216	21.99
Industrial, manufacturing and automotive	717	4.12	492	2.39	809	3.92	910	3.22
Consumer and retail	503	2.89	354	1.72	279	1.35	338	1.20
Hospitality and leisure	421	2.42	511	2.49	247	1.20	173	0.61
Aviation and logistics	190	1.10	242	1.18	702	3.40	2,189	7.75
Others*	762	4.38	1,512	7.35	534	2.59	2,883	10.20
Total revenue	17,387	100.00	20,563	100.00	20,649	100.00	28,262	100.00

Note:-

* Mainly includes utility service providers, government, healthcare and education which are not major contributors to our Group's revenue.

Commentary on past performance**FYE 2018 to FYE 2019**

We recorded total revenue of approximately RM20.56 million in the FYE 2019 (FYE 2018: RM17.39 million), representing an increase of approximately RM3.17 million or 18.23%.

6. BUSINESS OVERVIEW (cont'd)

The increase in revenue was attributed to the following:-

(i) higher revenue generated from our Assessment services in FYE 2019 of approximately RM3.07 million or 36.16% which was derived from the overall higher revenue generated from both Malaysia and overseas market, which mainly driven by the following:-

(a) the increase from the telecommunications and media industry of approximately RM1.97 million or 160.16% from RM1.23 million in FYE 2018 to RM3.20 million in FYE 2019; and

(b) the increase from the technology industry of approximately RM0.87 million or 85.29% from RM1.02 million in FYE 2018 to RM1.89 million in FYE 2019,

which were to a certain extent offset by the decrease from the industrial, manufacturing and automotive industries.

(ii) higher revenue generated from Certification services in FYE 2019 of approximately RM1.72 million or 66.67% which was derived from the overall higher revenue generated from both Malaysia and overseas market due to the increase in the number of projects secured during the FYE 2019 and mainly driven by the following industries:-

(a) the increase from the technology industry of approximately RM0.72 million or 138.46% from RM0.52 million in FYE 2018 to RM1.24 million in FYE 2019;

(b) the increase from the financial services industry of approximately RM0.63 million or 94.03% from RM0.67 million in FYE 2018 to RM1.30 million in FYE 2019; and

(c) the increase from the telecommunications and media industry of approximately RM0.45 million or 59.21% from RM0.76 million in FYE 2018 to RM1.21 million in FYE 2019,

which were to a certain extent offset by the decrease from other industries, in particular, consumer and retail, industrial and manufacturing as well as logistics.

FYE 2019 to FYE 2020

We recorded total revenue of approximately RM20.65 million in the FYE 2020 which was relatively consistent with the total revenue recorded in the previous financial year (FYE 2019: RM20.56 million).

Our total revenue in the FYE 2020 was mainly contributed by our customers from the financial services, technology and the telecommunications and media industries, which contributed to 53.38%, 20.25% and 13.91% to our total revenue in the FYE 2020 respectively.

The revenue generated from the financial services, technology and the telecommunications and media industries in the FYE 2020 was primarily due to the increase in demand for our Assessment services and Compliance services and the subsequent upward revision in our advisory fees.

FYE 2020 to FYE 2021

We recorded total revenue of approximately RM28.26 million in the FYE 2021 (FYE 2020: RM20.65 million), representing an increase of approximately RM7.61 million or 36.85%.

6. BUSINESS OVERVIEW (cont'd)

The increase in revenue was mainly attributed to the following:-

- (i) higher revenue generated from our Assessment services in the FYE 2021 of approximately RM3.96 million or 32.62% which was derived from the overall higher revenue generated from both Malaysia and overseas market;
- (ii) higher revenue generated from Forensics & Incident Response services in the FYE 2021 of approximately RM2.73 million or 354.55% which was mainly derived from the higher revenue generated from Malaysian market as a result of a high number of compromise assessment projects undertaken in the FYE 2021. This was driven by the increase in demand for such services from the financial services, technology and other industries (comprising mainly professional service providers); and
- (iii) higher revenue generated from Certification services in the FYE 2021 of approximately RM0.86 million or 22.69% which was derived from the overall higher revenue generated from Malaysia market due to the increase in the number of projects secured during the FYE 2021.

For further information on past performance of LGMS, please refer to **Section 11.3.2(i)** of this Prospectus.

6.7.2 Revenue by geographical location

The breakdown of our revenue by geographical location is as follows:-

	Audited							
	FYE 31 December							
	2018		2019		2020		2021	
	(RM'000)	(%)	(RM'000)	(%)	(RM'000)	(%)	(RM'000)	(%)
Malaysia	16,106	92.63	17,271	83.99	16,356	79.21	22,259	78.76
Overseas markets								
• Singapore	309	1.78	1,872	9.11	2,425	11.74	3,274	11.58
• Other ASEAN countries [^]	280	1.61	786	3.82	1,128	5.46	954	3.38
• Asia countries and region [#] (excluding ASEAN)	620	3.57	459	2.23	637	3.09	1,325	4.69
• Others [*]	72	0.41	175	0.85	103	0.50	450	1.59
Subtotal	1,281	7.37	3,292	16.01	4,293	20.79	6,003	21.24
Total revenue	17,387	100.00	20,563	100.00	20,649	100.00	28,262	100.00

Notes:-

[^] Including Cambodia, Indonesia, Thailand, Vietnam and Myanmar.

[#] Including India, Taiwan, Japan and Hong Kong.

^{*} Including Canada, Netherlands, Maldives, Australia, Saudi Arabia, France, USA, Turkey and Belgium as well as Vanuatu.

Our revenue for the past 4 FYEs 2018, 2019, 2020 and 2021 was mainly derived from Malaysia (being the primary market in which our Group operates).

The revenue contribution from our overseas markets accounted for approximately 7.37%, 16.01%, 20.79% and 21.24% of our total revenue in past 4 FYEs 2018, 2019, 2020 and 2021 respectively.

6. BUSINESS OVERVIEW (cont'd)

Revenue from our overseas markets grew from RM1.28 million for the FYE 2018 to RM6.00 million for the FYE 2021, representing a 3 year of CAGR of approximately 67.36%. Singapore was the largest contributor, which accounted for approximately 56.87%, 56.49% and 54.54% of our total overseas revenue for the past 3 FYEs 2019, 2020 and 2021 respectively. Revenue from the Singapore market for the past 4 FYEs 2018, 2019, 2020 and 2021 was mainly derived from our Assessment and Certification services, which amounted to approximately RM0.29 million, RM1.78 million, RM2.39 million and RM3.23 million respectively.

Our overseas revenue (apart from Singapore) was largely contributed by Cambodia, Indonesia and Thailand, all of which collectively accounted for approximately 15.93%, 23.42%, 26.28% and 12.62% of our total overseas revenue for the past 4 FYEs 2018, 2019, 2020 and 2021 respectively, where Assessment and Certification services were the primary revenue contributors.

For further information on revenue by geographical location, please refer to **Section 11.3.2(i)(b)** of this Prospectus.

6.7.3 Revenue by business segments

Our revenue by business segments is illustrated in the table below:-

	FYE 2018		FYE 2019		FYE 2020		FYE 2021	
	(RM'000)	(%)	(RM'000)	(%)	(RM'000)	(%)	(RM'000)	(%)
Cyber risk prevention								
- Assessment	8,490	48.83	11,560	56.22	12,139	58.79	16,103	56.98
- Training	239	1.37	532	2.59	241	1.17	249	0.88
- Cybersecurity risk scoring and monitoring	-	-	-	-	-	-	268	0.95
Subtotal	8,729	50.20	12,092	58.81	12,380	59.96	16,620	58.81
Cyber risk management and compliance								
- Certification	2,576	14.82	4,298	20.90	3,788	18.34	4,654	16.47
- Compliance	1,855	10.67	1,726	8.39	2,408	11.66	1,857	6.57
- Sale of Third Party Products*	3,634	20.90	1,768	8.60	1,301	6.30	1,636	5.79
Subtotal	8,065	46.39	7,792	37.89	7,497	36.30	8,147	28.83
Cyber threat and incident response								
- Forensics & Incident Response	593	3.41	679	3.30	772	3.74	3,495	12.36
Total revenue	17,387	100.00	20,563	100.00	20,649	100.00	28,262	100.00

Note:-

* Part of the project requirements, which primarily relates to the sale of third party software licenses.

Cyber risk prevention segment

Our revenue from the cyber risk prevention segment was derived from the provision of Assessment services and Training.

6. BUSINESS OVERVIEW (cont'd)

The growth in our revenue for the cyber risk prevention segment was mainly attributable to the increase in revenue arising from our Assessment services, which was predominantly driven by the increase in customers for the past 2 FYEs 2018 and 2019 and the subsequent revision in our advisory fees in the FYE 2020. We experienced a significant growth in revenue arising from our Assessment services in FYE 2021. This was mainly due to the increase in the demand for our Assessment services from our new customers primarily operating in the technology and financial services industries. The Assessment services was also the largest revenue contributor to our Group for the past 4 FYEs 2018, 2019, 2020 and 2021, and accounted for 48.83%, 56.22%, 58.79% and 56.98% of our total revenue respectively.

This was mainly due to the increasing demand and market awareness for such services in view of the legal and regulatory compliance requirements on information and data security which regulates our customers operating in industry with strict cybersecurity and data protection policies/practices in place (i.e. financial services, telecommunications and media).

During the past 4 FYEs 2018, 2019, 2020 and 2021, our Assessment services was primarily provided to customers operating in technology, financial services and telecommunications and media industries⁽¹⁾.

Cyber risk management and compliance segment

Our revenue from the cyber risk management and compliance segment was derived from the provision of Compliance and Certification services.

The growth in our revenue for the cyber risk management and compliance segment was mainly attributable to the increase in revenue arising from our Certification services primarily provided to the technology, financial services and telecommunications and media industries⁽¹⁾. Certification services was the second largest revenue contributor to our Group for the past 4 FYEs 2018, 2019, 2020 and 2021 which accounted for 14.82%, 20.90%, 18.34% and 16.47% of our total revenue respectively.

Cyber threat and incident response segment

Our revenue from the cyber threat and incident response segment was derived solely from provision of Forensics & Incident Response.

The growth in our revenue for the cyber threat and incident response segment was mainly due to our management's response to breaches in cybersecurity infrastructure and our marketing efforts in developing this segment of the business. The revenue from our Forensics and Incident Response services was the third largest revenue contributor to our Group for the FYE 2021, accounting for 12.36% of our total revenue. This was mainly due to the high number of compromise assessment projects undertaken by our customers operating in the financial services, technology and the other industries (comprising mainly professional service providers) in the FYE 2021.

Note:-

(1) Based on the industry sector classification as set out in revenue segmentation by our customer base set out in **Section 6.7.1** above.

For further information on revenue by business segment, please refer to **Section 11.3.2(i)(a)** of this Prospectus.

6. BUSINESS OVERVIEW (cont'd)

6.8 Marketing and sales activities

Our Group is cognizant of the importance of having continuous activities to market our professional cybersecurity services. As at the LPD, we have a marketing team consisting of 4 personnel reporting to our Chief Operating Officer, that is tasked with developing marketing strategies and spearheading our marketing drive to increase the sales of our professional cybersecurity services, build our “LGMS” brand, and expand our customer base. Our marketing team also designs, creates and/or manages our brochures, corporate website, social media presence and corporate videos. We have another dedicated 6-person business development team that will follow up on all sales leads from potential customers through emails, our corporate website, walk-ins or phone calls and build relationships with our existing customers.

We have also been invited from time to time to participate in project tenders. Our Group also gains new projects through incoming leads (of potential customers) who have responded to our various marketing and sales activities and/or channels such as advertisements, our corporate website, media blitz, social media platforms, events (such as webinars or seminars) as well as referrals from our existing customers.

We utilise various marketing channels to reach out to targeted customers when promoting our professional cybersecurity services and driving our brand building efforts. Our Group has been conducting promotional activities through the use of both offline and online mediums to gain better visibility for our Group and our ‘LGMS’ brand. We intend to increase our revenue stream and drive our competitiveness through the following marketing strategies:-

(i) Active participation in conferences, webinars and media interviews

Our Executive Chairman, Fong Choong Fook is a regular speaker at conferences (such as CYDES 2021 organised by Majlis Keselamatan Negara and Agensi Keselamatan Siber Negara, Malaysia Tech Month 2021 organised by the Ministry of Communications and Multimedia Malaysia and Malaysia Digital Economy Corporation (MDEC) Sdn Bhd as well as Alibaba Cloud Summit 2021 organised by Alibaba Cloud) and webinars (such as The National Tech Association of Malaysia (“PIKOM”) Webinar Series Cybersecurity Chapter Webinar Series organised by PIKOM, Fortify Your Enterprise Security With Advanced Penetration Testing organised by Alibaba Cloud and Digital Week 2021: Southeast Asia organised by W.Media). He has also been frequently interviewed or asked for his expert opinions on cybersecurity matters for inclusion in local and/or international based national television programmes (such as 8TV, Bernama TV and TV2), radio broadcasts, print media, websites or online platforms including social media.

(ii) Organising events for targeted audience

We have been organising both physical and online events such as seminars to increase brand awareness and educate the public (including the business communities, government entities, educational institutions and social bodies) on cyber threats and the importance of implementing cybersecurity measures. Our key targeted audience includes C-Suite Executives who are in the position to make strategic and major decisions regarding a company’s cybersecurity policy and budget. In the past, we have organised webinars which were attended by members or students of the Federation of Malaysian Manufacturers, Asia Banking School, MIA, MICPA, PIKOM, Asia School of Business and Securities Industry Development Corporation.

6. BUSINESS OVERVIEW (cont'd)

(iii) Collaboration with Alibaba Cloud, Time dotCom Berhad and Celcom

By leveraging on our collaborations with Alibaba Cloud, Time dotCom Berhad and Celcom, we are able to expand our potential customer base by reaching out and offering our professional services to all the customers of Alibaba Cloud, Time dotCom Berhad and Celcom. Alibaba Cloud is a company involved in cloud computing and artificial intelligence, providing services to enterprises, developers, and governments organisations around the world whilst TIME dotCom Berhad and Celcom are telecommunication providers that offer a full range of telecommunications solutions including domestic and global connectivity, data centre, cloud computing and managed service solutions.

(iv) Online marketing strategy push

Our online marketing strategy also involves search engine optimisation that drives unpaid traffic (which is derived from various searches such as image and video searches, news search and academic search instead of paying to the search engine providers).

We regularly review and update the content of our corporate website to ensure that it is search engine friendly and hence, allowing potential customers to reach us.

(v) Regular updates on corporate website and social media

Besides that, we also actively update on our professional cybersecurity services online via our dedicated corporate websites, <https://lgms.global> and social media such as Facebook, Twitter, LinkedIn and Instagram. This allows us to target a large pool of netizens and promote our direct engagement with them.

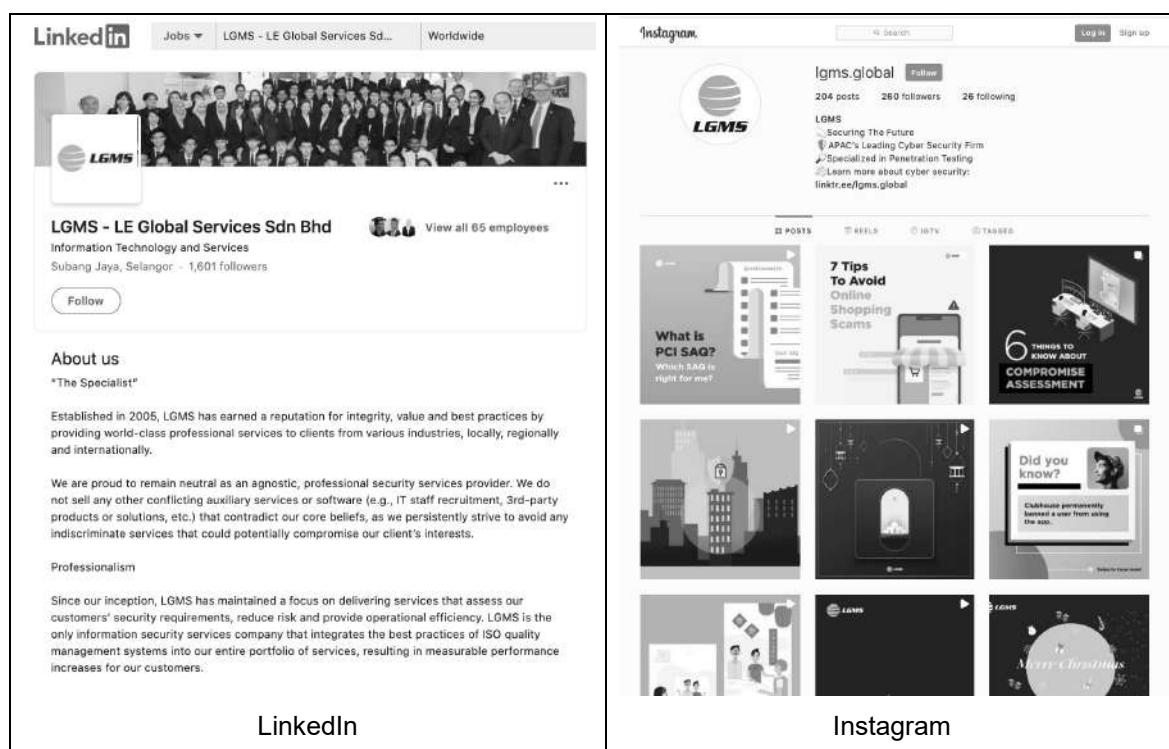


Facebook



Twitter

6. BUSINESS OVERVIEW (cont'd)



[Pictures courtesy of LGMS]

6.9 Seasonality

Our Group's business is not subject to any cyclical and seasonal trend.

6.10 Employees

As at the LPD, our Group has a total workforce of 90 employees, all of whom are permanent. As at the LPD, all our employees are Malaysian. We have not faced any shortages of employees for the past 4 FYEs 2018, 2019, 2020 and 2021 and up to the LPD which had resulted in a material disruption to our business operations.

Our Group pays social insurance for our employees, including medical, personal accident and work injury insurance in compliance with applicable local laws and regulations. None of our employees belongs to any trade unions, and there has been no industrial dispute since we commenced operations.

A summary of our Group's total workforce according to job functions as at 31 December of 2018, 2019, 2020 and 2021 as well as at the LPD is as follows:-

Categories	Number of employees				
	As at 31 December				As at the LPD
	2018	2019	2020	2021	
Management	4	4	5	5	5
Computer engineers and programmers	32	40	52	54	62
Business development and marketing	4	5	9	9	10
Commercial administration	8	7	7	6	6
Human resources, accounts and administration	1	4	6	7	7
Total number of employees	49	60	79	81	90

6. BUSINESS OVERVIEW (cont'd)

Our Group has put in place a management succession plan as a means of promoting business continuity. This includes:-

- (i) identifying promising internal candidates for grooming and training to further develop their competencies and skills to fill leadership positions within our organisation; and
- (ii) encouraging our middle management to take on more responsibilities beyond their existing roles in order to accelerate their learning curve and equip them with the required knowledge and competencies to succeed in more senior positions in the future.

6.11 Insurance

We have purchased insurance policies to cover a variety of risks that are relevant to our business needs and operations and which are customary in our industry, such as professional indemnity and general liability insurance for our operations. These insurance policies have specifications and insured limits that we believe are appropriate taking into consideration our risk levels and potential exposure to losses.

As at the LPD, LE Global maintains the following insurance policies which are material to our business operations:-

- (i) **professional indemnity policy** (with sum insured of RM8,360,000) that provides indemnity against liability at law for compensation and claimant's costs and expenses arising from any claim or claims made against the insured resulting from any civil liability incurred in connection with the profession services but not in respect of any such claim or claims resulting from any act, error or omission occurring or committed prior to the retroactive date;
- (ii) **employer's liability policy** (with sum insured of RM4,500,000) for any person under a contract of service or apprenticeship with the insured who sustain bodily injury by accident or disease caused during the period of insurance and arising out of and in the course of his/her employment by the insured in the business;
- (iii) **comprehensive general liability policy** (with sum insured of RM4,200,000) for any 1 claim and RM8,400,000 for aggregate of claims any one period of insurance) that provides indemnity against those sums which the insured shall become legally liable to pay as damages in respect of bodily injury or property damage occurring within the geographical limits during the policy period as a result of an occurrence happening in connection with the insured's business; and
- (iv) **fidelity guarantee policy** (with sum insured of RM4,000,000) for all such direct pecuniary loss as the insured shall sustain by an act of fraud or dishonesty committed by its employee(s).

As at the LPD, we have not made any claims under the above insurance policies to date.

6. BUSINESS OVERVIEW (cont'd)

6.12 Major customers

The table below lists the top 5 customers of our Group for the past 4 FYEs 2018, 2019, 2020 and 2021:-

Top 5 customers [^]	Description	Type of services provided by our Group	Country	FYE 31 December						Length of relationship as at 31 December 2021 (years)		
				2018		2019		2020			2021	
				RM'000	%	RM'000	%	RM'000	%		RM'000	%
Customer A	A financial institution and a subsidiary of a company listed on the Main Market of Bursa Securities.	Mainly Assessment and digital forensics services	Malaysia	1,331	7.65	561*	2.73*	3,874	18.76	3,998	14.15	10
Customer B	A security and consultancy services provider and a subsidiary of a Singapore government-linked company.	Mainly Assessment and Certification services	Singapore	-*	-*	765	3.72	1,184	5.74	1,729	6.12	3
Customer C	A postal services provider which is listed on the Main Market of Bursa Securities.	Mainly Assessment and Certification services	Malaysia	-*	-*	-*	-*	489*	2.37*	1,365	4.83	2
Customer D	A financial institution and a subsidiary of a company listed on the Main Market of Bursa Securities.	Mainly Assessment and digital forensics services	Malaysia	-*	-*	104*	0.51*	104*	0.50*	1,234	4.37	3
Customer E	A financial institution which is listed on the Main Market of Bursa Securities.	Mainly Assessment, compliance and digital forensics services	Malaysia	1,209	6.95	1,342	6.52	1,068	5.17	1,163	4.11	11
Customer F	A financial institution which is listed on the Main Market of Bursa Securities.	Mainly Assessment and compliance services	Malaysia	521	3.00	715	3.48	1,022	4.95	1,058*	3.74*	7

6. BUSINESS OVERVIEW (cont'd)

Top 5 customers [^]	Description	Type of services provided by our Group	Country	FYE 31 December						Length of relationship as at 31 December 2021 (years)		
				2018		2019		2020			2021	
				RM'000	%	RM'000	%	RM'000	%		RM'000	%
Customer G	A financial institution which is listed on the Main Market of Bursa Securities.	Mainly Assessment, Certification and compliance services	Malaysia	667	3.84	939	4.57	493*	2.39*	207*	0.73*	10
Customer H	A telecommunication and related services provider and a subsidiary of a company listed on the Main Market of Bursa Securities.	Mainly Assessment and Certification services	Malaysia	5,015	28.84	4,650	22.61	1,987	9.62	26*	0.09*	10
Total				8,743	50.28	8,411	40.90	9,135	44.24	9,489	33.58	
Total revenue				17,387	100.00	20,563	100.00	20,649	100.00	28,262	100.00	

Notes:-

[^] The names of our Top 5 customers have not been disclosed to safeguard the competitive position of our Group and our major customers in the market in which we and/or our major customers operate. Further, we had sought consent from the abovementioned customers for disclosure of the information required pursuant to the IPO but such consent for the above disclosures were not granted.

* The customer was not a top 5 customer of our Group in the respective FYE.

Our services are primarily carried out on a project-to-project basis. As such, the composition of our top 5 customers changes from year-to-year. We are not dependent on any particular customer given the following:-

- (i) our Group does not typically enter into long term contracts (of more than 1 year) with its customers as the duration and scope of engagement change from time to time in tandem with the rapidly changing nature of the IT environment; and
- (ii) our customer base is diversified across various industries, including financial services, telecommunications and media, manufacturing, hospitality and logistics. For the past 4 FYEs 2018, 2019, 2020 and 2021, we have serviced more than 400 customers across various end-user industries.

6. BUSINESS OVERVIEW (cont'd)

Although there is no dependency on any particular customer, we are however dependent on customers within the financial services and telecommunications and media industries (such as Customer A, D, E, F and G and Customer H respectively) as these customers operate in a regulated industry with strict cybersecurity and data protection policies in place. This group of customers (i.e. from the financial services and telecommunications and media industries) in aggregate accounted for approximately 72.76%, 66.63%, 67.29% and 55.03% of our total revenue for the past 4 FYEs 2018, 2019, 2020 and 2021 respectively. They are also repeat customers on yearly basis since their first engagement with our Group. Please refer to **Section 6.7.1** of this Prospectus for further details on the breakdown of our revenue by customer base for the past 4 FYEs 2018, 2019, 2020 and 2021. We have been informed by some of our major customers that they have internal risk management policy which necessitates the engagement with another different vendor after the internally prescribed period which on average, is 1 to 3 years. However, we have not experienced any discontinued engagement from any of our major customers due to their respective internal risk management policy for the past 4 FYEs 2018, 2019, 2020 and 2021. Only projects involving annual penetration testing services are likely to be affected by such internal policy. However, a customer may engage our services for other unaffected scopes of works such as ad hoc penetration testing services. We strive to maintain long-term business relationships with our customers by providing quality services that meet our customer's needs and requirements, which are key factors that may lead to its customers seeking out our services in the future. Whilst our Board foresee our continuing dependence on the financial services and telecommunications and media industries, we intend to leverage on our collaborations with Alibaba Cloud, TIME dotCom Berhad and Celcom to tap and penetrate into other industries. For further details on our marketing and sales activities involving our collaborations with Alibaba Cloud, TIME dotCom Berhad and Celcom, please refer to **Section 6.8** of this Prospectus.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

6. BUSINESS OVERVIEW (cont'd)

6.13 Major suppliers

We do not have any major suppliers as the type of products and/or services required for its cybersecurity projects may differ from each other depending on the technical requirements and complexity. As such, for illustration purposes, the table below sets out our suppliers that contributed more than 10% to the aggregated sum of the staff cost (technical department) and IT expenses (collectively referred to as the "Total Cost of Services")# for the past 4 FYEs 2018, 2019, 2020 and 2021:-

Supplier	Description	Types of products/ services supplied to our Group	Country	FYE 31 December						Length of relationship as at 31 December 2021 (years)		
				2018		2019		2020			2021	
				RM'000	(1)%	RM'000	(1)%	RM'000	(1)%		RM'000	(1)%
Titan Guard Solution Sdn Bhd	An information security consultant and service provider of managed network and security	Cybersecurity related software	Malaysia	-	-	-	-	840	14.71	26*	0.47*	1
Adaptive Netpoleon Malaysia Sdn Bhd	An IT professional services, consultancy services provider in all areas of application	Cybersecurity related software	Malaysia	947	23.69	749	13.83	63*	1.10*	81*	1.48*	6
Glocomp Systems (M) Sdn Bhd	An ICT solution provider	Cybersecurity related software	Malaysia	-	-	-	-	-	-	792	14.46	1
Total				947	23.69	749	13.83	840	14.71	792	14.46	
Total Cost of Services# (RM'000)				3,997	100.00	5,417	100.00	5,711	100.00	5,477	100.00	

Notes:-

(1) Computed based on the Total Cost of Services.

* Not applicable as the purchases from the respective supplier did not exceed more than 10% to the Total Cost of Services in the respective financial years.

As our income statement does not have a separate line item for cost of services, the aggregated sum of the employees benefits expense (technical department) and IT expenses has been adopted to estimate the Total Cost of Services.

6. BUSINESS OVERVIEW (cont'd)

6.14 Types, sources and availability of supplies

The following are the major types of IT expenses that we have purchased for our business operations for each of the past 4 financial years under review.

	FYE 31 December 2018		FYE 31 December 2019		FYE 31 December 2020		FYE 31 December 2021	
	RM'000	% of total purchases	RM'000	% of total purchases	RM'000	% of total purchases	RM'000	% of total purchases
Software expenses	1,434	84.30	1,742	84.85	1,233	69.00	1,231	58.23
Certification and assessment related fees	82	4.82	42	2.05	326	18.24	850	40.21
Training related expenses	185	10.88	269	13.10	228	12.76	33	1.56
Total	1,701	100.00	2,053	100.00	1,787	100.00	2,114	100.00

Our major types of supplies are software products and licenses sourced from software vendors, certification and assessment related fees paid to relevant certification bodies and training related expenses related to the training courses provided. The amount of our purchases for these supplies is dependent on the number and requirements of the secured contracts (including training programmes involved) in the particular year. During each of the past 4 financial years under review, we have not experienced any difficulties in sourcing supplies from third-party vendors and certification bodies, and these supplies are not subject to volatile price fluctuations. For further details on the IT expenses, please refer to **Section 11.3.2** of this Prospectus.

6.15 Major licenses and permits

Details of the approvals, major licenses and permits obtained by our Group for the operation of our business are set out as follows:-

1) LE Global

No.	Approving authority / issuer	Description of approval / license / permit	License / Reference no.	Date of issuance / validity	Major conditions imposed	Status of compliance
1.	Subang Jaya City Council	Business premise and advertising licence for A-11-01 Empire Tower Office, Jalan SS 16/1, 47500 Subang Jaya, Selangor	20191100546	Effective Date: 6 April 2022 Validity: Valid until 17 May 2023	None	Complied

6. BUSINESS OVERVIEW (cont'd)

No.	Approving authority / issuer	Description of approval / license / permit	License / Reference no.	Date of issuance / validity	Major conditions imposed	Status of compliance
2.	Subang Jaya City Council	Business premise and advertising licence for A-11-02A Empire Tower Office, Jalan SS 16/1, 47500 Subang Jaya, Selangor	20191100547	Effective Date: 6 April 2022 Validity: Valid until 17 May 2023	None	Complied

6.16 Certifications and qualifications

Details of the certifications and qualifications held by our Group for the operation of our business are set out as follows:-

No.	Certification Issuer / Partner	Approving authority / Issuer / Partner	Relevant Entity within our Group	Relevant business segment(s)	Scope	Validity Period
1.	ISO / IEC 27001:2013	TÜV NORD CERT GmbH	LE Global	<ul style="list-style-type: none"> Cyber risk prevention services Cyber management and compliance services Cyber threat and incident response services 	<p>LE Global applies a management system in line with ISO / IEC 27001:2013 for the following scope:-</p> <p>Provision of information security services, including IT security risk consultancy, international standards compliance audit, training, penetration testing, computer crime investigation, IT security assessment and specialised IT security project implementation</p>	19 January 2019 to 18 January 2022. A re-certification audit was conducted from 3 January 2022 to 6 January 2022 and is now pending the issuance of the renewed certificate. Based on our past experience, we expect the certificate to be renewed within 3 months from the completion of the re-certification audit.

6. BUSINESS OVERVIEW (cont'd)

No.	Certification	Approving authority / Issuer / Partner	Relevant Entity within our Group	Relevant business segment(s)	Scope	Validity Period
2.	ISO 9001:2015	TÜV NORD CERT GmbH	LE Global	<ul style="list-style-type: none"> Cyber risk prevention services Cyber risk management and compliance services Cyber threat and incident response services 	<p>LE Global applies a management system in line with ISO 9001:2015 for the following scope:-</p> <p>Provision of information security assessment including penetration test, web application assessment, mobile application assessment, source code review, network security assessment & host assessment</p>	24 February 2020 to 23 February 2023
3.	CREST Membership	CREST (International)	LE Global	<ul style="list-style-type: none"> Cyber risk prevention services 	<p>LE Global has successfully met the CREST requirements for membership and is a full member organisation for the following discipline:-</p> <p>Penetration testing operating in Asia</p>	1 April 2022 to 31 March 2023
4.	PECB Authorised Trainer and Examiner	PECB	LGMS Advanced Tech	<ul style="list-style-type: none"> Cyber risk prevention services 	<p>PECB appoints LGMS Advanced Tech as its non-exclusive reseller Asia Pacific to (i) organise and provide the training services (including the sale of the training materials), and (ii) promote the certification services (the conduct of certification examination sessions, correction of certification examinations and the issuance of certifications) to individuals who wish to obtain certification</p>	1 January 2020 to 31 December 2022

6. BUSINESS OVERVIEW (cont'd)

No.	Certification	Approving authority / Issuer / Partner	Relevant Entity within our Group	Relevant business segment(s)	Scope	Validity Period
5.	ISACA Training Provider and Channel Partner	ISACA	LE Global	<ul style="list-style-type: none"> Cyber risk prevention services 	<p>LE Global is authorised to act on a non-exclusive basis to (i) resell the ISACA's products (i.e. course kits and membership) to end users and enterprises located in Malaysia and (ii) conduct training programmes using an authorised trainer for attendees in Malaysia in respect of the following ISACA's certification or certificate programmes:-</p> <ul style="list-style-type: none"> (i) CISA (ii) CISM (iii) CRISC (iv) CGEIT (v) CDPSE (vi) Cybersecurity Fundamentals (vii) Cybersecurity Audit (viii) COBIT 	Renewed annually unless otherwise terminated
6.	Mile2 Authorized Training Center	Mile2	LE Global	<ul style="list-style-type: none"> Cyber risk prevention services 	<p>LE Global is authorised to jointly with Mile2 provide instructional classes via standard instructor-led training live-remote or computer based training in Information Technology in all course titles marketed by www.Mile2.com including but not limited to:-</p> <ul style="list-style-type: none"> (i) Certified Penetration Testing Engineer (ii) Certified Penetration Testing Consultant (iii) Certified Wireless Security Engineer (iv) Certified Digital Forensics Examiner (v) Certified Secure Coding Engineer (vi) Certified Secure Virtual Machine Engineer (vii) Certified Information Systems Security Officer 	Renewed annually unless otherwise terminated

6. BUSINESS OVERVIEW (cont'd)

No.	Certification	Approving authority / Issuer / Partner	Relevant Entity within our Group	Relevant business segment(s)	Scope	Validity Period
7.	Cloud Security Alliance Training Partner	CSA	LE Global	<ul style="list-style-type: none"> Cyber risk prevention services 	LE Global is granted a non-exclusive license to use, reproduce and display training courseware for the sole and exclusive purpose of conducting training classes with respect to the preparation of the Certificate of Cloud Security Knowledge (CCSK) examination	Renewed annually unless otherwise terminated
8.	PCI DSS Approved Scanning Vendor (ASV)	PCI Security Standards Council	LE Global	<ul style="list-style-type: none"> Cyber risk prevention services Cyber risk management and compliance services 	Qualified as an ASV. An ASV is an organisation with a set of security services and tools ("ASV scan solution") to conduct external vulnerability technical scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2. The scanning vendor's ASV scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC's List of Approved Scanning Vendors	22 July 2021 to 22 July 2022
9.	PCI DSS Qualified Security Assessor (QSA)	PCI SSC	LE Global	<ul style="list-style-type: none"> Cyber risk management and compliance services 	Qualified as a Qualified Security Assessor company, which are independent security organisations that have been qualified by PCI SSC to validate an entity's adherence to PCI DSS	17 March 2023
10.	ISO / IEC 17025:2005	Department of Standards Malaysia	TUV Austria Cybersecurity Lab	<ul style="list-style-type: none"> Cyber risk management and compliance services 	TUV Austria Cybersecurity Lab, Subang Jaya, Selangor, Malaysia has been granted accreditation in respect of software testing, subject to the terms and conditions governing the Skim Akreditasi Makmal Malaysia (SAMM), the Laboratory Accreditation Scheme of Malaysia Scope of testing: Software testing	27 November 2020 to 2 November 2023

6. BUSINESS OVERVIEW (cont'd)

The abovementioned certifications and qualifications are not automatically renewed. We are still able to operate even without the abovementioned certifications and qualifications save for the provision of audit and certification services in respect of PCI DSS, in respect of which we are required to maintain our PCI DSS ASV and/or PCI DSS QSA status. However, these certifications and qualifications bring a lot of value and recognitions to our Group, particularly in terms of providing us with the opportunities to penetrate into end-user markets with high IT security compliance requirements.

PCI ASV focuses on conducting external vulnerability technical scanning services which is one of the requirements in PCI DSS whilst PCI QSA focuses on processes, policies and practices. Both certifications allow us to provide services to all entities located all around the world (for PCI DSS ASV) and in Asia Pacific (for PCI DSS QSA) that store, process, or transmit cardholder data, in compliance with the PCI DSS requirements. Only authorised PCI ASVs and PCI QSAs recognised by PCI SSC are able to provide such services and as such, these credentials are essential to our Group. By having these certifications, we are able to serve a sizeable pool of potential customers such as financial institutions, merchants, retailers, e-wallet service providers, call centres and data centres, given the wide adoption of payment card systems. If such entities wish to meet full compliance with PCI DSS requirements, they are required to engage an officially appointed PCI ASV annually.


We typically commence and undertake the full preparation for the renewal of the abovementioned certifications and qualifications at least one month before the expiry of their respective validity. However, the timing of the required re-certification audit exercise is also dependent on the availability of the auditor involved. As at the LPD, we have not faced any difficulties in renewing the abovementioned certifications and qualifications.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

6. BUSINESS OVERVIEW (cont'd)

6.17 Material trademarks and other intellectual property rights

Save for the trademark registration below, our Group does not have any other trademarks registrations and intellectual property rights which are material to our Group:-

No.	Trademark	Issuing authority	Registered owner	Application or registration no. / class	Description	Validity Period
1.		Intellectual Property Corporation of Malaysia	LE Global	2017061279 / Class 42	Proprietor of the said trademark for a period of 10 years in respect of the following services:- Computer security consultancy; computer security services (testing and risk assessment of computer networks); data security consultancy; data security services (firewalls); Internet security consultancy; network security services (test and risk assessment of electronic networks); security risk assessment services relating to computer systems; all included in Class 42.	19 June 2017 to 19 June 2027

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

6. BUSINESS OVERVIEW (cont'd)

6.18 Material properties, machinery and equipment

6.18.1 Properties owned by our Group

A summary of the material properties owned by our Group as at the LPD are as follows:-

No.	Postal Address	Description of property/ Existing use/ Expiry of lease (if any)/ Category of land use (if any)	Purchase price (RM'000)	Beneficial owner	Land area/ Built-up area (sq ft)	Date of purchase/ Date of CCC	Encumbrance	Audited NBV as at 31 December 2021 (RM'000)
1.	C-3A-07, Level 3A, i-Tech Tower @ Shaftsbury Square, Jalan Impact, Cyber 6, 63000 Cyberjaya, Selangor	Office unit on 4 th floor/ Investment property ⁽¹⁾ / Freehold/ Building	625	LE Global	Not applicable/ 1,119	22 February 2011/ 29 April 2014	Charged to United Overseas Bank (Malaysia) Berhad ⁽²⁾	529
2.	C-3A-09, Level 3A, i-Tech Tower @ Shaftsbury Square, Jalan Impact, Cyber 6, 63000 Cyberjaya, Selangor	Office unit on 4 th floor/ Investment property ⁽¹⁾ / Freehold/ Building	355	LE Global	Not applicable/ 600	14 February 2011/ 29 April 2014	Charged to United Overseas Bank (Malaysia) Berhad ⁽²⁾	305

Notes:-

(1) These office units are currently rented out to third parties.

(2) Given that the term loans granted by United Overseas Bank (Malaysia) Berhad to LE Global have been fully settled, as at the LPD, LE Global and United Overseas Bank (Malaysia) Berhad are in the process of effecting the discharge of the charges over these properties.

We purchased both office units which are located in Cyberjaya with the initial intention of moving our operations there. However, both office units are not able to accommodate the prevailing scale of our operations by the time they were completed. As such, we decided to use both office units to generate rental income.

6. BUSINESS OVERVIEW (cont'd)

6.18.2 Properties rented by our Group

A summary of the material properties rented by our Group as at the LPD are as follows:-

No.	Postal Address	Landlord/ Tenant	Description/ Existing use	Floor area (sq ft)	Period of tenancy	Rental per annum (RM)
1.	A-11-01 Empire Office Tower, Jalan SS 16/1, 47500 Subang Jaya, Selangor Darul Ehsan.	Cheerful Effect Sdn Bhd/ LE Global (Sub-tenant: TUV Austria Cybersecurity Lab)	11 th floor office unit/ Office of LE Global and TUV Austria Cybersecurity Lab	8,828	1 December 2020 to 30 November 2023	RM291,324.00 for the 1 st year and RM333,698.40 for the 2 nd year and 3 rd year
2.	A-11-02A Empire Office Tower, Jalan SS 16/1, 47500 Subang Jaya, Selangor Darul Ehsan.	Cheerful Effect Sdn Bhd/ LE Global	11 th floor office unit/ Office of LE Global	5,920	1 June 2022 to 31 May 2023	RM223,776.00

As at the LPD, our Group is in compliance with the terms of the tenancy agreements in respect of the material properties rented above. In addition, as at the LPD, our Group has not received any notice of breach from the landlord or any notice of non-compliance with applicable laws and regulations from any regulatory authorities in relation to our use of the properties above which will have material adverse impact on our business operations.

6.18.3 Material machinery and equipment

Due to the nature of our operations, we do not utilise any key machinery and equipment in undertaking our cybersecurity services.

6. BUSINESS OVERVIEW (cont'd)

6.19 Governing laws and regulations

Save as disclosed below, there are no other key regulatory requirements governing our Group which are material to our business operation. However, the disclosure made below is not intended to be an exhaustive description of all laws and regulations to which our business is subject to (such as, among others, the Companies Act 2016, Employment Act 1955 and the Employees Provident Fund Act 1991):-

(i) Personal Data Protection Act 2010 (“PDPA”)

The PDPA governs the laws on the processing of personal data in commercial transactions to protect personal data of common interest and to ensure information security, network reliability and integrity. Any person or body corporate involved in the processing of personal data must comply with the Personal Data Protection Principles set out in the PDPA. The Personal Data Protection Standard 2015 prescribes the minimum requirement for data security in processing personal data. In processing personal data, we are also required to take steps and implement measures to protect the personal data from loss, misuse and modification and maintain the integrity of the personal data processed. The personal data processed should not be kept longer than is necessary for the fulfilment of the purpose for which it was collected.

Our Group is required to observe the requirements of the PDPA in the event any personal data is processed, such as the requirement to provide a privacy notice to the data subject which contains certain prescribed information (including the purpose of the processing of the data) and to obtain the data subject’s consent for the processing of his/her data. As at the LPD, we do not process or store any personal data on behalf of our customers as part of our services.

(ii) Local Government Act 1976 (“LGA”)

Under the Local Government Act 1976, local government authorities in West Malaysia have the power to issue any by-laws enforceable within its jurisdiction, including business, trade and advertisement licences. Most local or district councils have a (Licensing of) Trades, Businesses and Industries By-Laws which stipulate that no person shall carry on any trade, business or industry in any place or premise within the respective district council unless he is licensed. Each by-law applies within the boundaries of each local or district council. The local authorities may prescribe for breach of any by-law, a fine not exceeding RM2,000 or a term of imprisonment not exceeding 1 year, or both and in the case of a continuing offence, a sum not exceeding RM200 for each day during which such offence is continued after conviction.

Accordingly, we are required to obtain a business premise license for the premises occupied for our business operations and an advertising license for any signboard erected at such premise.

Whilst there are certain cybersecurity-related regulations and/or guidelines which govern certain groups of our customers (such as those in the financial services industry), the obligations to adhere to these regulations are on the relevant customers. For example, pursuant to the Risk Management in Technology policy document issued by BNM, a financial institution is required to engage suitably accredited penetration testers and service providers to conduct annual intelligence-led penetration tests on its internal and external network infrastructure as well as critical systems including web, mobile and all external-facing applications. It is the obligation of the financial institutions to ensure that the entities the financial institutions engage to perform such penetration tests are suitably accredited.

6. BUSINESS OVERVIEW (cont'd)

6.20 Dependency on contracts, agreements, documents or other arrangements

As at the LPD, we are not dependent on any contracts, agreements, documents or other arrangements for our business operations.

6.21 Productive capacity and extent of utilisation

Measures of productive capacity and extent of utilisation are not applicable to the provision of professional cybersecurity services by our Group.

6.22 Research and development

We do not have a dedicated R&D department that undertakes R&D activities. Notwithstanding this, all our cybersecurity experts are involved in R&D activities. Our Senior Director, Professional Services, Fow Chee Kang spearheads and coordinates all our R&D efforts. Our activities are aligned with our ultimate objectives to provide professional cybersecurity services which are independent, realistic and up to date to local, regional and international customers across a diverse range of industries and backgrounds. Our Group's R&D activities primarily revolve around efforts to identify and keep abreast with the latest cyber threats that are happening around the world; enhance and/or create techniques or methodologies that can be used to combat the latest cyber threats across traditional and new digital touchpoints and applications; deploying the latest cybersecurity related technologies as well as undergoing new or renewal of professional cybersecurity related certifications. We continue to accumulate a vast repository of real-world business security issues that are derived from the penetration tests conducted by us.

As at the LPD, we have successfully developed 2 software products, namely LGMS Reporter and PCI DSS Compliance Wizard. We seek to continually improve and upgrade our internally developed unique security assessment result system (for server vulnerability assessments and penetration testing), LGMS Reporter and our one-stop solution for PCI DSS compliance, PCI DSS Compliance Wizard. We are also leveraging on our established relationship and collaboration with TÜV Austria via TUV Austria Cybersecurity Lab by sharing threat intelligence, industry knowledge and expertise in the field of cybersecurity.

All the expenses incurred for our R&D activities are expensed off to the income statement when incurred instead of being capitalised as an intangible asset. There is no specific amount of budget that is allocated for R&D activities.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

6. BUSINESS OVERVIEW (cont'd)

6.23 Interruptions to business and operations

We have not experienced any other interruption that has a significant effect on our business during the past 12 months preceding the LPD. COVID-19 has not interrupted or caused a significant effect on our Group's business and operations. For details on the impact of COVID-19 on our business, please refer to **Section 6.4** of this Prospectus.

6.24 Environmental matters

As at the LPD, there are no environmental issues that may materially affect our Group's business or operations.

6.25 Future plans and business strategies

We intend to grow our business by leveraging on our competitive strengths and through the following future plans and business strategies:-

6.25.1 Purchasing an office in Klang Valley to cater to our growing customer base given that our Group secured new number of customers of 94, 85, 85 and 167 in the past 4 FYEs 2018, 2019, 2020 and 2021 respectively

We intend to purchase an office premise with a built-up area of at least 20,000 sq ft from the property market in Klang Valley to house our business operations, including our digital forensics and IoT labs. This will allow us to save on our rental expenses of up to RM557,000 annually. The new facilities will allow us to scale up our operations and accommodate a larger workforce to support our growing customer base as well as increasing our technical capacity (via the setting up of new labs at the new office). As at the LPD, we are still in the midst of identifying a suitable property that meets our operational requirements.

We intend to purchase our new office premise by the second half of 2022 by utilising the earmarked IPO proceeds of RM18.00 million. Please refer to **Section 3.6.1(i)** of this Prospectus for further details on the use of proceeds from the IPO for the purchase of our new office premise.

6.25.2 Scaling up our operations by expanding our capability and developing our human capital

We intend to scale up our operations to support our growing customer base and continue developing the right professionals for our business. As part of our growth strategy, we plan to hire at least an additional 70 technical personnel in the next 2 years. We do not foresee any major issues in the hiring of the additional 70 technical personnel amid the cybersecurity market in Malaysia is facing a shortage of skilled cybersecurity professionals. Although there is a critical shortage of skilled personnel as disclosed in **Section 5.1** of the Industry Overview Report (set out in **Section 7** of this Prospectus), we believe that we are in a better position to attract skilled cybersecurity professionals for our operations in view of our established brand and operating track record as well as our competitive remuneration packages. We are also embarking on a recruitment drive through various channels (such as vacancy postings on our corporate website and social media platforms), collaboration with local public and private universities, engaging recruitment agencies as well as undertaking a talent search through platforms such as JobStreet and LinkedIn. We regularly receive job applications to join our Group.

6. BUSINESS OVERVIEW (cont'd)

The indicative allocation of the additional 70 technical personnel for each of our business segment is as follows:-

- (i) 45 technical personnel under the cyber risk prevention segment;
- (ii) 15 technical personnel under the cyber risk management and compliance segment; and
- (iii) 10 technical personnel under the cyber threat and incidence response segment.

The above allocation is indicative as at this juncture and may subject to further changes depending on the workforce demand of the respective segment from time to time.

We will provide them with on-the-job training and continue to support them to obtain internationally recognised cybersecurity certifications such as (ISC)² Certified Information Systems Security Professional, ISACA Certified Information Security Manager, ISACA Certified Information Systems Auditor, CREST Registered Penetration Tester, Offensive Security Certified Professional, GIAC Certified Forensic Examiner, ACFE Certified Fraud Examiner, PCI Security Standards Council Approved Scanning Vendor, PCI Security Standards Council PCI Qualified Security Assessor, PECB Certified ISO/IEC 27001 Lead Implementer, PECB Certified ISO/IEC 27001 Lead Auditor, ISACA Certified in Risk and Information Systems Control, CSA Certificate of Cloud Security Knowledge V4, Certified Penetration Testing Specialist and Mile2 Certified Penetration Testing Engineer. These certifications can help them to provide better services to customers through continuous training and development.

We also intend to support the expansion of our workforce disclosed above with the purchase of new IT equipment, tools, and software forensic tools. We have earmarked a portion of the RM6.00 million from the IPO proceeds, towards such capital expenditure, further details of which are set out in **Section 3.6.1(iii)** of this Prospectus.

In addition, we intend to enhance our capability in undertaking digital forensics as well as IoT assessments and testing through the setting up of new labs at our new office premise as disclosed in **Section 6.25.1** above. This can help us to scale up our operations to take on more projects including undertaking multiple projects simultaneously.

In view of the above, we have earmarked RM6.50 million from the IPO proceeds to fund the expansion of our workforce, of which RM5.50 million will be utilised to fund the staff salaries of 70 new technical recruits for an estimated period of 12 months. Please refer to **Section 3.6.1(ii)** of this Prospectus for further details on the use of proceeds from the IPO for the expansion of our workforce.

6.25.3 Increasing our geographical footprint through the setting up of a local branch in Singapore, strategic tie-ups or joint ventures with local partners in Vietnam and Cambodia as well as potential strategic acquisitions, if such opportunity arises

We are embarking on an international expansion strategy and plan to have a localised direct presence in selected countries within the Southeast Asia region within the next 2 years. This is aimed to broaden our customer base, mitigate country-specific risk and allow us to ride on the potential growth in demand for cybersecurity services in the region. The countries identified for our initial international expansion are Singapore, Vietnam and Cambodia.

We intend to set up a branch office in Singapore to provide direct operational and sales support to our existing customers. We will also be pursuing potential tie-ups or joint-ventures with local partner(s) in Vietnam and Cambodia. The criteria that we will use in the selection of local partner(s) include:-

- (i) have internationally recognised cybersecurity certifications and/or memberships in cybersecurity-related bodies/communities;

6. BUSINESS OVERVIEW (cont'd)

- (ii) have a team of dedicated, experienced and skilled personnel with recognised cybersecurity certifications; and
- (iii) an existing local cybersecurity market player with an established track record servicing reputable corporations either in the private or public sector.

We also intend to embark on potential strategic acquisitions of companies within the local and regional cybersecurity market with the aim to potentially broaden our service offerings and customer base, as well as expand our market presence. As at the LPD, we have not identified any specific business for acquisition or tie-ups/joint ventures. Our Company will make the necessary announcements as required under the Listing Requirements as and when we have entered into any material agreement in relation to such strategic acquisitions and/or investments. In the event that shareholders' approval and/or regulatory approvals are required, such approvals will be sought by our Company.

We have earmarked a total of RM7.70 million from the IPO proceeds to fund our strategic expansion. Please refer to **Section 3.6.1(iv)** of this Prospectus for further details on the use of proceeds from the IPO for the strategic expansion plan of our Group.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

7. INDUSTRY OVERVIEW

PROTEGE ASSOCIATES SDN BHD (673767-H)
SUITE C-09-12, PLAZA MONT' KIARA
2 JALAN KIARA, MONT' KIARA
50480 KUALA LUMPUR, MALAYSIA
GEN +603 6201 9301 FAX +603 6201 7302
www.protege.com.my

Protégé
ASSOCIATES

BRAND | FINANCE | MARKET

The information in this Section 7 is based on market research conducted by Protégé Associates commissioned by LGMS Berhad for the purpose of the Listing.

Date: 27 April 2022

The Board of Directors
LGMS Berhad,
A-11-01, Empire Office Tower,
Jalan SS 16/1,
47500 Subang Jaya,
Selangor Darul Ehsan.

Dear Sirs,

Strategic Analysis of the Cybersecurity Market in Malaysia

Protégé Associates Sdn Bhd ("**Protégé Associates**") has prepared this 'Strategic Analysis of the Cybersecurity Market in Malaysia' for inclusion in the Prospectus of LGMS Berhad ("**LGMS**") in relation to the Listing.

Protégé Associates is an independent market research and business consulting company. Our market research reports provide an in-depth industry and business assessment for companies raising capital and funding in the financial markets; covering their respective market dynamics such as market size, key competitive landscape, demand and supply conditions, government regulations, market trends and the outlook of the market.

Mr. Seow Cheow Seng is the Managing Director of Protégé Associates. He has 22 years of experience in market research starting his career at Frost & Sullivan where he spent 7 years. He has been involved in a multitude of industries covering Agriculture, Automotive, Construction, Electronics, Healthcare, Energy, Information Technology ("**IT**"), Oil and Gas, etc. He has also provided his market research expertise to government agencies such as Malaysia Digital Economy Corporation Sdn Bhd, Malaysia Debt Ventures Berhad and Malaysia Technology Development Corporation Sdn Bhd.

We have prepared this report in an independent and objective manner and have taken adequate care to ensure the accuracy and completeness of the report. We believe that this report presents a true, balanced and fair view of the industry within the boundaries and limitations of secondary statistics, primary research and continued industry movements. Our research has been conducted to present a view of the overall industry and may not necessarily reflect the performance of individual companies in this industry. We are not responsible for the decisions and/ or actions of the readers of this report. This report should also not be considered as a recommendation to buy or not to buy the shares of any company or companies.

Thank you.

Yours sincerely,



SEOW CHEOW SENG
Managing Director

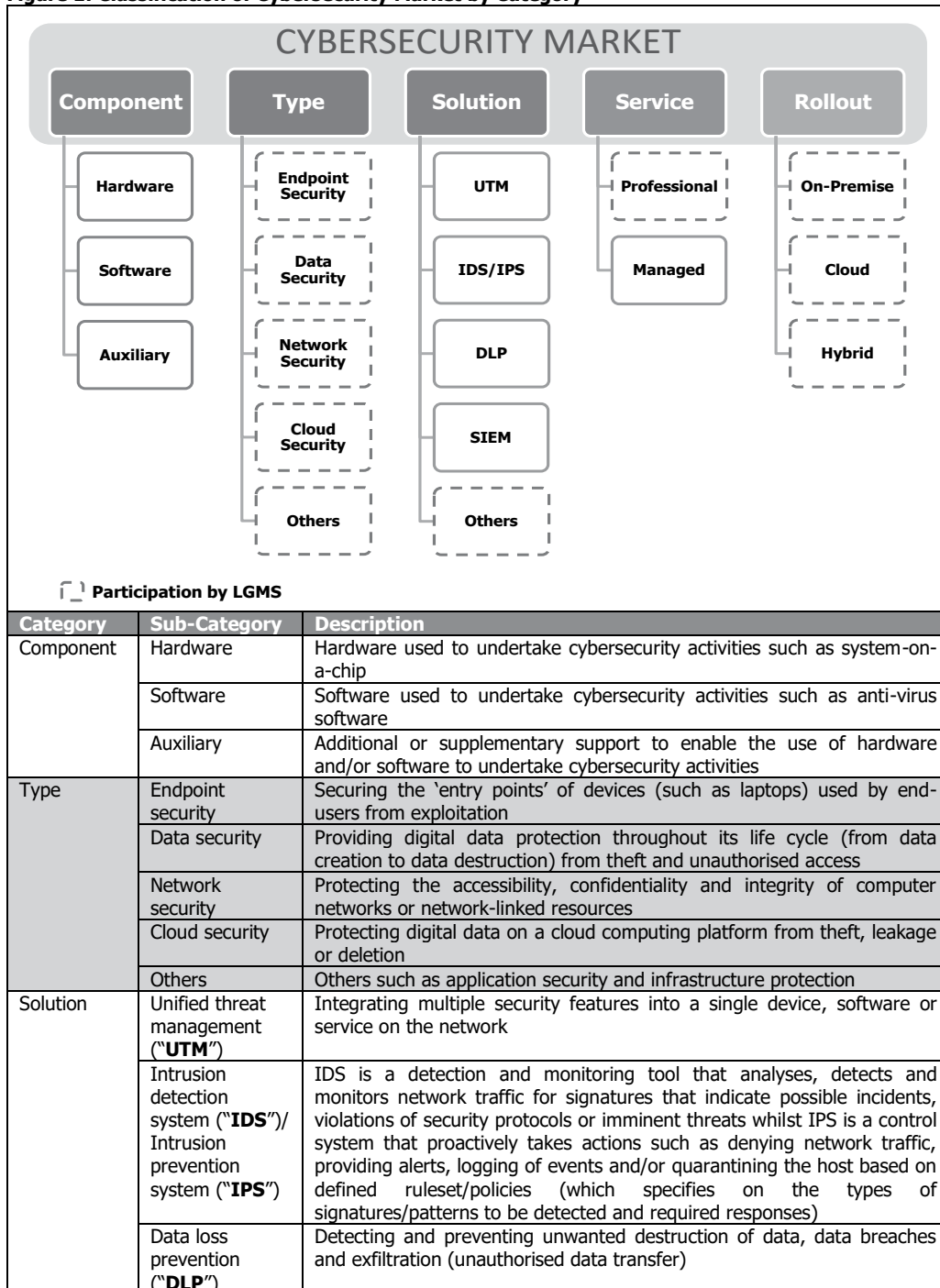
7. INDUSTRY OVERVIEW (Cont'd)



1.0 Introduction to Cybersecurity

Cybersecurity generally refers to components (hardware or software) used or action performed to safeguard a person, enterprise, organisation or country and their information systems and infrastructures against crimes and unauthorised access or attacks carried out using the Internet. The cybersecurity market is constantly evolving to address the ever-growing sophistication of cybercrime. The cybersecurity market covers key operational functions namely preventive, detective and corrective functions. These functions look to identify, protect, detect and provide the right response to the threat and can be classified based on 5 major categories namely component, type, solution, service and rollout.

Figure 1: Classification of Cybersecurity Market by Category



7. INDUSTRY OVERVIEW (Cont'd)



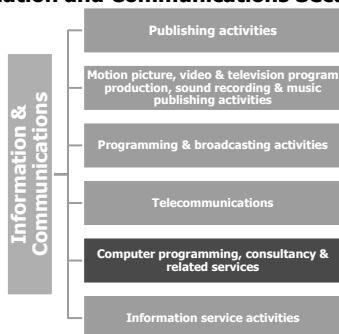
Category	Sub-Category	Description
	Security information and event management ("SIEM")	A single security management system, which is a combination of security information management and security event management, that offers real-time visibility of information management system, data consolidation from various logs or security sources, automatic security notifications for security issues and whether the security events are inter-related with one another
	Others	Others such as risk management and cybersecurity compliances and identity access management
Service	Professional	Short-term engagements that address specific challenges in respect of cybersecurity, which typically involve amongst others, analysing the existing state of information security through vulnerabilities assessment and penetration testing; assisting the customers in complying with information security related standards, laws and regulations; designing and establishing information security framework; conducting digital forensics and conducting information security training
	Managed	Performing the day-to-day management, maintenance and support of clients' information security needs on an on-going basis including on-boarding, vendor management, remote and on-site IT support and proactive network monitoring amongst others
Rollout	On-Premise	Conducting cybersecurity activities on-site at the client's premise
	Cloud	Conducting cybersecurity activities via the cloud computing platform
	Hybrid	A combination of both on-site and cloud deployments

Sources: LGMS and Protégé Associates

1.1 Segmentation in the Cybersecurity Market

In Malaysia, cybersecurity activities are categorised as part of the computer programming, consultancy and related services segment, which in turn, is one of the subset categories of activities under the information and communications sector as shown in Figure 2. The computer programming, consultancy and related services segment can be divided into 3 core activities as seen in Figure 3.

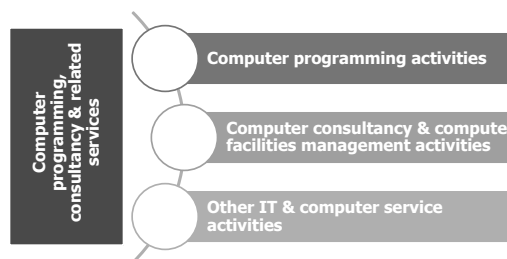
Figure 2: Categories of Activities under the Information and Communications Sector



■ Participation by the cybersecurity market

Source: Department of Statistics Malaysia ("DOSM") and Protégé Associates

Figure 3: The 3 Core Activities of the Computer Programming, Consultancy and Related Services Segment



Source: DOSM and Protégé Associates

1.2 End-User Markets of the Cybersecurity Market

As the digital economy continues to develop with digitalisation becoming more entrenched and widely used by consumers, enterprises and governments, the cybersecurity market has a wide range of end-user markets in both the private and public sectors. The advancement of the Internet of Things ("IoT") technology and the widespread use of the Internet over multiple platforms as well as growth in cloud infrastructures, data centres and smartphones have created new and rising demands for cybersecurity protection. Examples of the end-user market for cybersecurity include but are not limited to banking and finance, insurance, technology, telecommunications, consumer products, education, healthcare, manufacturing, retail, hospitality and leisure, automotive, aviation, logistics and transportation.

7. INDUSTRY OVERVIEW (Cont'd)



2.0 Overview of the Cybersecurity Landscape in the ASEAN Region

The Association of Southeast Asian Nations ("ASEAN") member states have been collectively taking additional steps to protect the region from cyber attacks particularly in the areas of cyber strategy, cyber operations-technology collaboration and cyber capacity building. All ASEAN member states have subscribed, in-principle, to the United Nations voluntary, non-binding norms of responsible state behaviour in cyber space. In the ASEAN region, cybersecurity efforts are expected to gain traction. Much progress has been made in policy coordination and incident response as one ASEAN since the adoption of the ASEAN Cybersecurity Cooperation Strategy. Against the backdrop of growing demand for digital goods and services, and digital disruption, the digital threat landscape is expected to expand as ASEAN economies thrive leading to potentially higher demand for all types of cybersecurity services in both public and private sectors. The market outlook remains positive for cybersecurity markets in the ASEAN region with market size (revenue) in ASEAN projected to expand from RM14.66 billion in 2021 to RM28.47 billion in 2026, registering a compound annual growth rate ("CAGR") of 14.2%.

Singapore has a competitive and developed cybersecurity market that provides services to both local and multinational businesses. The cybersecurity market in Singapore, which is already well established with ready infrastructures and skilled cybersecurity professionals, is projected to grow from RM5.42 billion in 2021 to RM9.14 billion in 2026, registering a CAGR of 11.0%. Rapid digitalisation of core business processes in businesses and public institutions have driven the growth of cybersecurity market in large markets such as Indonesia, the Philippines and Vietnam. However, the preparedness of other ASEAN member states such as Cambodia and Lao People's Democratic Republic to prevent cyber threats and manage cyber incidents are still at the infancy stage of development. The cybersecurity market in Cambodia is projected to expand from RM49.7 million in 2021 to RM193.5 million in 2026, registering a CAGR of 31.2%. In Vietnam, its growing economy is expected to spur further growth in its cybersecurity market, expanding the market size from RM811.8 million in 2021 to RM1.90 billion in 2026, registering a CAGR of 18.5%.

2.1 Overview of the Cybersecurity Landscape in Malaysia

In Malaysia, the continued presence of relatively high number of cybercrime remains alarming with a number of businesses opting against reporting their cybersecurity incidents with the aim of, amongst others, safeguarding their reputation and/or to avoid such incidents being made known to the general public. Based on statistics from the Royal Malaysian Police, cybercrime in Malaysia totalled 14,229 cases in 2020 as compared to 11,875 cases registered in 2019. Total combined losses from cybercrime in 2019 and 2020 amounted to RM911 million. Telecommunication fraud, e-commerce fraud (online purchase) and '419 scam' (Nigerian scam) are the main types of cybercrime cases in Malaysia. Meanwhile, statistics from Malaysia Computer Emergency Response Team ("MyCERT") revealed that there were 10,016 reported cybersecurity incidents in Malaysia for 2021 as compared to 10,790 reported cybersecurity incidents recorded in 2020. In 2021, the main types of cybersecurity incidents reported were fraud, intrusion, cyber harassment and malicious codes.

Figure 4: Reported Incidents Based on General Incident Classification, 2017-2021

Incident	2017	2018	2019	2020	2021
Content related	46	111	298	170	91
Cyber harassment	560	356	260	596	417
Denial of service	40	10	19	16	22
Fraud	3,821	5,123	7,774	7,593	7,098
Intrusion	2,011	1,160	1,359	1,444	1,410
Intrusion attempt	266	1,805	104	116	159
Malicious codes	814	1,700	738	593	648
Spam	344	342	129	145	102
Vulnerabilities report	60	92	91	117	69
Total	7,962	10,699	10,772	10,790	10,016

Source: MyCERT

Malaysia has also been a target for Advanced Persistent Threats ("APTs") in which an unauthorised user (individual, criminal enterprise, terrorist organisation or nation-state) gains access to a system or network for an extended period of time without triggering any detection. Many organisations that continue to operate legacy and unsupported systems (which does not support any updates on the latest security patches) are particularly susceptible to APTs. The increasing number of content related issues in Malaysian cyberspace such as fake news and misinformation is also another area for concern. The effects of content-related issues are deemed to be potentially more detrimental and damaging given the widespread of information and fast nature of the Internet as a medium of delivery. The local law enforcement agencies are also mindful of the threats of terrorism and violent extremism with various web services and social media being used as breeding grounds to entice new recruits, followers and supporters to their causes. Although efforts have been made to curb

7. INDUSTRY OVERVIEW (Cont'd)



such threats, the local enforcement agencies continue to face challenges due to the ease of developing a new forum or website for any agenda.

The Malaysian Government has acknowledged the critical shortage of skilled cybersecurity professionals and has outlined plans to address this issue. There are plans for the development of school curricula to include cybersecurity along with focus-based skills at the institutions of higher learning as well as training and skills development schemes for experts and non-experts in both public and private sectors. The Malaysian Government is also looking to enhance the existing Centre of Excellence which involves collaboration with local universities to fill the gap in the supply of local cybersecurity talents.

3.0 Market Size

Protégé Associates has provided the following historical and growth forecast of the cybersecurity market in Malaysia based on a combination of resources, including the data obtained from Malaysia Digital Economy Corporation (MDEC) Sdn Bhd, CyberSecurity Malaysia, Malaysian Communications and Multimedia Commission ("MCMC") and DOSM. Data has also been gathered from further secondary and primary research works conducted. Searches on private limited cybersecurity market players have also been conducted with the Companies Commission of Malaysia ("CCM") while financial information from public listed cybersecurity market players has been extracted from the website of Bursa Malaysia Securities Berhad to gather more information on their business performance. Primary research works have been conducted with stakeholders in the local cybersecurity market in order to gather their insights on the market. All the findings have been collated, analysed and/or computed to ascertain the outlook of the cybersecurity market in Malaysia.

Figure 5: Historical Size and Growth Forecast of the Cybersecurity Market in Malaysia, 2019-2026

Year	Size (Revenue) (RM million)	Annual Growth Rate (%)
2019	2,576.7	-
2020	2,924.6	13.5
2021	3,325.3	13.7
2022 ^f	3,780.1	13.7
2023 ^f	4,299.9	13.8
2024 ^f	4,893.3	13.8
2025 ^f	5,578.5	14.0
2026 ^f	6,359.5	14.0

CAGR (2022-2026) (base year of 2021): 13.9%

Note: ^f denotes forecast

Source: Protégé Associates

The cybersecurity market in Malaysia is at the growth stage of the industry life cycle. At this stage, the adoption rate for cybersecurity is expected to continue growing at a double-digit rate. Malaysia is already well regarded in terms of cybersecurity as it was ranked 5th globally (jointly with Russia Federation and United Arab Emirates) and ranked 2nd in the Asia Pacific region with score of 98.06 out of 100.00 in the Global Cybersecurity Index 2020 released by International Telecommunication Union ("ITU"). Malaysia achieved top scores in 3 of 5 categories used by ITU namely legal measures, capacity development and cooperative measures. The size (revenue) of the cybersecurity market in Malaysia expanded from RM2.92 billion in 2020 to RM3.33 billion in 2021. The local cybersecurity market received a lift as demand for digital services gained traction amid the lockdown measures imposed during the coronavirus disease ("COVID-19") pandemic period. The advent of new digital technologies such as 5th generation ("5G") and the emergence of various technology-led industries such as fintech (financial technology) are also expected to drive digital economy leading to potential rising demand for cybersecurity offerings. Moving forward, the local cybersecurity market in Malaysia is expected to keep expanding with the annual growth rate projected to hover around 13.7% to 14.0% during the forecast period from 2022 to 2026 as the local economy continues its digital transformation journey. The size (revenue) of the cybersecurity market in Malaysia is projected to reach RM6.36 billion in 2026, registering a CAGR of 13.9% for the forecast period.

4.0 Competitive Analysis

The cybersecurity market is fragmented with market players competing in various categories within the market ranging from cybersecurity product re-sellers to cybersecurity professional service providers. In 2022, it is estimated that there are around 400 cybersecurity market players in Malaysia. These cybersecurity market players are divided into foreign and local cybersecurity market players covering all categories in the cybersecurity market. Factors that influence the competitive positioning of each market player in the cybersecurity market in Malaysia include but are not limited to number of skilled cybersecurity professionals employed; domain expertise including access to cybersecurity technologies, technology differentiation and intellectual properties; pricing; quality of offerings; breadth of product or service portfolio and scope of solutions, distribution network (including global presence) and availability and responsiveness of customer support. However, the degree of relevancy of the competitive factor(s) involved is dependent amongst others,

7. INDUSTRY OVERVIEW (Cont'd)



end-user markets targeted, customers targeted, services and products involved and business strategies undertaken.

Foreign-owned cybersecurity market players are able to leverage on their respective parent company's technical expertise, significant scale, operating track record and global pool of manpower to gain competitive advantage. They strive for technological leadership and typically obtain or comply with various internationally recognised cybersecurity related standards and qualifications. However, the scope and scale of their operations are very much subject to the internal business strategy deployed by their respective parent companies. Their capabilities and offerings generally vary from one to another depending on the intended strategy including targeted product or service segment(s) as well as targeted end-users (consumers, enterprises or governments) or end-user markets. Examples of foreign cybersecurity market player include but are not limited to BAE Systems Applied Intelligence Malaysia Sdn Bhd ("**BAE Systems**"), Cisco Systems (Malaysia) Sdn Bhd ("**Cisco Systems**"), Commisum Sdn Bhd ("**Commisum**"), F-Secure Corporation (M) Sdn Bhd ("**F-Secure**"), and NTA Monitor (M) Sdn Bhd ("**NTA Monitor**").

Local cybersecurity market players are mainly home grown Malaysian companies who benefit from having vast local knowledge and established relationships within the information and communications technology ("**ICT**") landscape in Malaysia. Some of these local cybersecurity market players work on building strategic business relationships or partnership with foreign cybersecurity companies with the required technology to provide comprehensive solutions in meeting expanding information security needs. Local cybersecurity market players have also been gaining ground on their foreign counterparts in terms of technical competency and industry recognition by obtaining or complying with various internationally recognised cybersecurity related standards and qualifications. Meanwhile, others may pursue a more focused approach on products and services, and cater to the specific needs of local customers or their targeted end-users. Some of the known local cybersecurity market players include but are not limited to LGMS, Across Verticals Sdn Bhd ("**Across Verticals**") and AKATI Sekuriti (M) Sdn Bhd ("**AKATI**").

These local and foreign cybersecurity market players in Malaysia can also be grouped into various categories which include but are not limited to professional service providers (such as LGMS and Ask Pentest), ICT system integrators (such as HeiTech Padu Berhad and HLA Integrated Sdn Bhd), cybersecurity products suppliers or distributors (such as Tech Titan Distribution Sdn Bhd), data centre owners and/or operators (such as AIMS Data Centre Sdn Bhd and HDC Data Centre Sdn Bhd), consulting companies which also include the business advisory arms of accounting firms (such as Ernst & Young Consulting Sdn Bhd (formerly known as Ernst & Young Advisory Services Sdn Bhd) ("**Ernst & Young**") and KPMG Management & Risk Consulting Sdn Bhd ("**KPMG**") and universities (such as Multimedia University and Universiti Malaysia Sarawak) which offer cybersecurity products and/or services. Each cybersecurity market player may not be directly competing with one another as they may participate in one or more cybersecurity categories or sub-categories.

Key barriers to entry in the local cybersecurity market include the need to possess a team of cybersecurity professionals as well as technical competency and/or qualifications. Potential market entrants also need to be mindful of the need to have an established operating track record and meet higher capital requirement to grow the business.

4.1 Comparison between LGMS and Selected Cybersecurity Market Players

LGMS is an independent provider of cybersecurity professional services based in Malaysia with extensive experience and technical competency particularly in the areas of vulnerability assessment and penetration testing. As such, Protégé Associates has compiled a list of market players that are also participating in the cybersecurity professional services category within the Malaysian cybersecurity market through the offering of vulnerability assessment and/or penetrating testing services for comparison purpose. The selected cybersecurity market players have been further divided into 2 categories namely local and foreign cybersecurity market players.

Figure 6: Selected Cybersecurity Market Players for Comparison with LGMS

Market Player	Financial Year Ended ("FYE") ⁽¹⁾	Revenue (RM'000)	Profit after Tax (RM'000)	Profit after Tax Margin ⁽²⁾ (%)
Local Cybersecurity Market Players				
LGMS	31-12-2021	28,262	10,306	36.5
Across Verticals	30-06-2021	6,427	1,900	29.6
AKATI	31-12-2020	3,543	368	10.4
Ask Pentest Sdn Bhd	31-12-2020	3,960	395	10.0
Condition Zebra (M) Sdn Bhd	30-06-2021	2,714	343	12.6
Deloitte Business Advisory Sdn Bhd ⁽³⁾	31-05-2021 ⁽³⁾	45,390	-1,002	-2.2
e-Lock Corporation Sdn Bhd	31-01-2021	23,483	569	2.4

7. INDUSTRY OVERVIEW (Cont'd)

Market Player	Financial Year Ended ("FYE") ⁽¹⁾	Revenue (RM'000)	Profit after Tax (RM'000)	Profit after Tax Margin ⁽²⁾ (%)
Ernst & Young ⁽⁴⁾	31-12-2020	154,647	25,938	16.8
KPMG ⁽⁵⁾	31-12-2020	56,836	-1,762	-3.1
Netassist (M) Sdn Bhd	31-03-2021	4,152	217	5.2
Pricewaterhousecoopers Advisory Services Sdn Bhd ⁽⁶⁾	30-06-2021	64,760	18,597	28.7
SysArmy Sdn Bhd	31-03-2021	9,622	1,556	16.2
Foreign Cybersecurity Market Players*				
BAE Systems	31-12-2020	71,675	-414	-0.6
Cisco Systems ⁽⁷⁾	31-07-2021	110,240	2,794	2.5
Commissum	30-06-2020	1,647	172	10.4
F-Secure	31-12-2020	25,195	632	2.5
NTA Monitor	31-12-2020	1,500	266	17.7

Notes:

The above figures only provide an indication and are not considered directly comparable to LGMS as not all companies:

- (a) have the same FYE;
- (b) carry out activities which are completely similar to each other; and
- (c) operate in the same geographical area.

* Majority shares in company owned by foreigner(s)

⁽¹⁾ This represents the latest available financial information from CCM as at 28 March 2022 and the prospectus of LGMS;

⁽²⁾ Profit after Tax Margin = Profit after Tax / Revenue;

⁽³⁾ Deloitte Business Advisory Sdn Bhd (formerly known as Deloitte Risk Advisory Sdn Bhd) is principally involved in carrying on the business of consultants and advisers in the areas of IT, risk management and other corporate governance related services and to provide training courses related to these areas. As segmental financial information is not available from the results of the CCM search conducted on the company, the proportion of its revenue which was derived from cybersecurity activities cannot be determined. Following the change of Deloitte Business Advisory Sdn Bhd's financial year end from 31 December, the financial period covered in the table is for a period of 17 months from 1 January 2020 to 31 May 2021, and thereafter, the financial year of the company shall revert to 12 months ending 31 May, for each subsequent year;

⁽⁴⁾ Ernst & Young is principally involved in providing a suite of advisory and consultancy services involving business solutions, project management and shared support services. As segmental financial information is not available from the results of the CCM search conducted on the company, the proportion of its revenue which was derived from cybersecurity activities cannot be determined.

⁽⁵⁾ KPMG is principally involved in providing advisory services. As segmental financial information is not available from the results of the CCM search conducted on the company, the proportion of its revenue which was derived from cybersecurity activities cannot be determined;

⁽⁶⁾ Pricewaterhousecoopers Advisory Services Sdn Bhd is principally involved in providing advisory services. As segmental financial information is not available from the results of the CCM search conducted on the company, the proportion of its revenue which was derived from cybersecurity activities cannot be determined; and

⁽⁷⁾ Cisco Systems is principally involved in acting as a promoter of Cisco products (which includes networking hardware, software and other computer products). As segmental financial information is not available from the results of the CCM search conducted on the company, the proportion of its revenue which was derived from cybersecurity activities cannot be determined.

Sources: LGMS, CCM and Protégé Associates

4.2 Estimated Market Share of LGMS

For FYE 31 December 2021, LGMS generated revenue of RM28.26 million, equivalent to 0.8% share of the cybersecurity market in Malaysia of RM3.33 billion in 2021 which includes revenue contributions by local and foreign cybersecurity market players from all the 5 broad categories (namely component, type, solution, service and rollout) as depicted in Figure 1.

7. INDUSTRY OVERVIEW (Cont'd)

**5.0 Demand Conditions****Figure 7: Demand Conditions Affecting the Cybersecurity Market in Malaysia, 2022-2026**

Impact	Demand Conditions	Short-Term	Medium-Term	Long-Term
		2022-2023	2024-2025	2026
+	Digital transformation economy	High	High	High
+	A proliferation of digital touchpoints and applications	High	High	High
+	The need to uphold digital privacy	Medium	Medium	Medium
+	Encouraging broadband penetration rate	Medium	Medium	Medium
-	Lack of awareness on the importance of implementing best cybersecurity practices	Medium	Medium	Medium

Source: Protégé Associates

Digital transformation economy

As we continue to embrace the shift towards a more digital economy and closer to global connectivity via the Internet, data is increasingly being changed from analogue to digital form (through digitisation) while digital technologies (such as 5G, artificial intelligence, cloud computing, robotics, IoT and big data analytics) are increasingly being adopted to change business models or provide new revenue streams and value-producing opportunities (through digitalisation of business processes). These have led to the emergence of various technology-led industries such as fintech (financial technology), insurtech (insurance technology), medtech (medical technology), agritech (agriculture technology) and edutech (education technology). The digital economy has also spurred the rapid adoption of IT, including the Internet, in end-user markets (such as the transportation and agriculture sector) that traditionally were not heavy utilisers of the IT or Internet. The COVID-19 pandemic has also accelerated the usage of IT with e-commerce shopping, video conferencing and work from home following the need for physical distancing amid nationwide lockdown. Such online activities, due to their convenience, are expected to be the new normal post COVID-19 pandemic. With higher exposure to online activities, it is hence likely to elevate the urgent needs for products, solutions and/or services to protect against cyber attacks. It has also been noted that the utilisation of IT including the Internet has been increasing in end-user markets (such as healthcare and manufacturing sector) in line with the advent of the IoT, big data analytic and artificial intelligence. For example, in the healthcare end-user market, medical robotic technology and robot-assisted surgical procedures are now connected to computer systems and networks while patient records are digitised. Similar to the concept of traditional retail businesses requiring security, these developments in digital businesses will also likely spur the demand for cybersecurity offerings. Hence, accordingly, the local cybersecurity market has plenty of room to mitigate the risk of over-reliance on a single customer segment or end-user market and also stands to have more room for market size expansion.

A proliferation of digital touchpoints and applications

Cyber threats are no longer limited to the confines of computers as consumers are interacting online increasingly through multiple devices, platforms and networks, and leveraging technology in almost every aspect of their lives. This has hence led to a proliferation of digital touchpoints and applications. There is also a pronounced convergence of personal life and work stemming from remote working and increasing work from home arrangements. As consumers increasingly shift their daily activities online, they now face more potential cyber threats in view of the increase in points of vulnerability, risking their data, identity, privacy and other vital resources.

As for enterprises and governments, there has been an amplification in the number of workloads across endpoints as they embrace employee mobility, allowing employees to bring their own personal devices to work, work from home strategies and greater cloud adoption, all of which in turn, will potentially broaden the attack surface and dissolving network perimeter. As a result thereof, enterprises and governments are hence finding it increasingly challenging to monitor and safeguard all of their workloads and applications. The growing prevalence of cyber threats has heightened the awareness and importance of consumers, enterprises and governments in making security decisions on their converged digital lives which include the needs to purchase cybersecurity products and services. The local cybersecurity market which is in the business of information security is poised to ride on any increase in demand for its offerings.

The need to uphold digital privacy

Due to the digitalisation shift, businesses need to be mindful on the need to safeguard their customers' data to avoid running afoul of the Personal Data Protection Act 2010 ("PDPA") that can lead to substantial financial and reputational damage. The PDPA, which came into force in 2013, regulates the processing of personal data in commercial transactions and to provide for matters connected therewith. Practical steps need to be taken to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure as well as alteration or destruction. To this end, businesses are likely to be more inclined to

7. INDUSTRY OVERVIEW (Cont'd)



strengthen their IT networks and system infrastructures which bode well for the growth of the local cybersecurity market.

Encouraging broadband penetration rate

The penetration rate for broadband in Malaysia has been encouraging. There is a relatively high mobile-broadband penetration rate in Malaysia. From 2017 to 2020, the mobile-broadband penetration rate per 100 inhabitants in Malaysia stood at above 100% and remained so in the third quarter of 2021. (Note: A penetration rate over 100% can occur because of multiple subscriptions). The mobile-broadband penetration rate in Malaysia has been increasing since the third quarter of 2020 and is expected to return to the pre-pandemic level during the forecast period. This trend is expected to continue to rise during the forecast period as we continue to shift our daily activities online, in particular our banking activities and purchasing of goods and services online. In the third quarter of 2021, all the states in Malaysia registered more than 100% in mobile-broadband penetration rate per 100 inhabitants save for Sabah (90.6%), Wilayah Persekutuan Putrajaya (83.4%) and Wilayah Persekutuan Labuan (95.5%). Meanwhile, the penetration rate for fixed-broadband per 100 premises stood at 39.9% in the third quarter of 2021 as compared to 41.0% registered in the second quarter of 2021.

The cybersecurity market in Malaysia is hence a beneficiary of this trend given that its offerings can serve the need of online users seeking to manage information security and protect themselves against cyber attacks. The implementation of the national digital infrastructure plan known as Jalanan Digital Negara (including the future deployment of the 5G technology standard for broadband cellular networks) is also expected to further drive the usage of broadband. With a relatively high broadband penetration rate, this augurs well for the growth in the local cybersecurity market.

Figure 8: Broadband Penetration Rate in Malaysia, Quarter 4 2019-Quarter 3 2021

Year	Quarter	Fixed-Broadband Penetration Rate per 100 premises (%)	Mobile-Broadband Penetration Rate per 100 inhabitants (%)
2019	4	32.8	123.7
2020	1	33.8	118.5
	2	34.5	116.7
	3	35.6	117.4
	4	37.2	118.7
2021	1	39.0	120.1
	2	41.0	124.2
	3	39.9	127.4

Source: MCMC

Lack of awareness on the importance of implementing best cybersecurity practices

There is generally a lack of awareness among consumers, businesses, organisations and governments on the importance of implementing best cybersecurity practices. There is still a general reluctance or hesitation by the employees (including those at the senior management tier) to make investments towards the implementation of best cybersecurity practices which include buying anti-virus software or undertaking periodical vulnerability assessment on IT systems and networks. There are also organisations that continue to operate legacy and unsupported systems. Furthermore, the awareness and need to implement best cybersecurity practices are hindered by perceptions/views that such implementation is often deemed as an unnecessary additional cost to the businesses, organisations and governments. As such, this demand condition has a negative impact on the local cybersecurity market during the forecast period.

5.1 Supply Conditions

Figure 9: Supply Conditions Affecting the Cybersecurity Market in Malaysia, 2022-2026

Impact	Supply Conditions	Short-Term	Medium-Term	Long-Term
		2022-2023	2024-2025	2026
+	Continuing strong support from the Malaysian Government	High	High	High
-	Critical shortage of skilled cybersecurity professionals	High	High	Medium

Source: Protégé Associates

Continuing strong support from the Malaysian Government

Cybersecurity is recognised as a matter of national priority by the Malaysian Government. Since formulating the National Cyber Security Policy ("NCSP") in 2006, the Malaysian Government has been providing policy support and spearheading efforts to drive the growth in the local cybersecurity market. Such efforts by the Malaysian Government include establishing cybersecurity frameworks and enacting cybersecurity related laws,

7. INDUSTRY OVERVIEW (Cont'd)



forming government entities to handle cybersecurity matters, fostering close collaborations among stakeholders (such as government entities, law enforcement agencies, education institutions and business entities) and encouraging the adoption of international best practices on information security by pushing for the Malaysian Standard ("MS") International Organization for Standardization ("ISO")/International Electrotechnical Commission ("IEC") 27001 certification among Critical National Information Infrastructure ("CNII") agencies and organisations. In 2020, the Malaysian Government rolled out a medium-term action plan, Malaysia Cyber Security Strategy ("MCSS") with an allocation of RM1.8 billion to step up national cybersecurity preparedness. In Budget 2021, the Malaysian Government announced an allocation of RM27 million to CyberSecurity Malaysia in Budget 2021 to increase the country's cybersecurity. It also rolled out the Malaysia Digital Economy Blueprint in 2021 to bridge the digital divide among Malaysians. In Budget 2022, the Malaysian Government announced the implementation of the National Digital Identity project in 2022 to enhance connectivity between all kinds of transaction systems in order to ease and encourage safe digital transactions. The Malaysian Government is expected to remain committed in supporting the local cybersecurity market during the forecast period. This bodes well for the future growth of the cybersecurity market in Malaysia.

Critical shortage of skilled cybersecurity professionals

The local cybersecurity market faces a critical shortage of skilled cybersecurity professionals. The lack of awareness of the cybersecurity market has led to a lack of interest from the younger generations as they have little opportunity to learn about the industry and what the role of a cybersecurity professional entails. Given that cyber attacks are constantly evolving, cybersecurity professionals are also required to keep abreast with the latest trends and skill sets typically through conferences, classes and certifications; all of which require a considerable amount of time and money. As such, this supply condition has a negative impact on the local cybersecurity market during the forecast period.

6.0 Relevant Laws and Regulations Governing the Market

Cybersecurity was thrust into the spotlight in 2006 following the formulation of the NCSP by the Malaysian Government in recognition of the need to place cybersecurity as a national priority and to address the risks to the CNII. The sectors identified as CNII are banking and finance; emergency services; energy; government; health services; information and communications; agriculture and plantation; national defence and security; trade, industry and economy; transportation and water, which need to be protected to a level that commensurate with the risks faced. Their incapacity or destruction would have a devastating impact on national economic strength, image, security and defence, government capability to function as well as public health and safety.

In 2007, CyberSecurity Malaysia was officially launched. CyberSecurity Malaysia focuses on providing ICT security specialist services. In 2008, the Malaysian Government kick-started the National Cyber Crisis Exercise ("X-MAYA") to assess the readiness and preparedness of critical national infrastructure agencies against cyber attacks and to test the effectiveness of the procedures that have been developed under the National Cyber Crisis Management Plan. Since then, another 5 X-MAYAs had been organised with the latest X-MAYA (in 2017) being participated by more than 100 public and private agencies across the 10 CNIIs. In 2011, an executive directive, the National Security Council's Directive No. 24: Policy and Mechanism of the National Cyber Crisis Management ("Directive No. 24") was issued. It outlines the strategy that Malaysia will undertake for cyber crisis mitigation and response among Malaysia's CNII through public and private collaboration based on 6 principles. The 6 principles are (i) a national cyber crisis management structure; (ii) national cyber threat levels; (iii) Computer Emergency Response Team; (iv) cybersecurity protection mechanisms; (v) response, communication and coordination procedures; and (vi) readiness program.

In accordance with the requirements of the NCSP and Directive No. 24, NC4 was developed as a centre for dealing with cyber threats and crisis at the national level and ensuring coordination and cooperation between CNII agencies are enhanced for integrated management of cybersecurity in the country. It has the ability to assess the impact of cybersecurity threats to the country and determine the level of threat. The entire main cyber security-operating centre ("SOC") in Malaysia is linked to NC4. The SOC consists of Cyber Defence Operation Centre, CyberSecurity Malaysia SOC, Government Integrated Telecommunications Network SOC and MCMC Network Security Centre. In order to ensure that CNII agencies and organisations have the necessary information security protection in place, the Malaysian Government has taken steps to ensure their adoption and certification of the MS ISO/IEC 27001: Information Security Management System ("ISMS") standard and other related certifications. Such measure is also being prepared for other non-CNII sectors such as construction, education, manufacturing and retail.

In 2017, the national lead agency for cybersecurity matters, the National Cyber Security Agency ("NACSA") was officially established to secure and strengthen Malaysia's resilience in facing the threats of cyber attacks. NACSA is developing the National Cyber Security Awareness Master Plan to increase the level of cybersecurity awareness among Malaysian netizens through concerted and effective programs and initiatives. In 2020, the Malaysian Government had taken another significant step towards improving the country's cybersecurity

7. INDUSTRY OVERVIEW (Cont'd)



management with the launch of the MCSS that covers the period from 2020 to 2024. There are 5 strategic pillars outlined in the MCSS as guiding principles namely (i) effective governance and management; (ii) strengthening legislative framework and enforcement; (iii) catalysing world class innovation, technology, research and development (“R&D”) and industry; (iv) enhancing capacity and capability building, awareness and education; and (v) strengthening global collaboration. The successful execution of the strategies, action plans and programs under MCSS can put Malaysia on a stronger footing in the management of cybersecurity moving forward.

In Malaysia, there is a comprehensive set of cybersecurity related laws which can cater for the advent of digital age and the full scope of cybersecurity related issues.

Figure 10: Existing Laws for Cybercrime and Cybersecurity Issues in Malaysia

Laws		
Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001		
Capital Markets and Services Act 2007	Child Act 2001	Communications and Multimedia Act 1998
Computer Crimes Act 1997	Consumer Protection Act 1999	Copyright Act 1987
Criminal Procedure Code	Defamation Act 1957	Digital Signature Act 1997
Direct Sales and Anti-Pyramid Scheme Act 1993	Electronic Commerce Act 2006	Electronic Government Activities Act 2007
Evidence Act 1950	Film Censorship Act 2002	Financial Services Act 2013
Islamic Financial Services Act 2013	Mutual Assistance in Criminal Matters Act 2002	National Security Council Act 2016
Official Secrets Act 1972	Optical Discs Act 2000	Patents Act 1983
Penal Code	Personal Data Protection Act 2010	Prevention of Crime Act 1959
Prevention of Terrorism Act 2015	Security Offences (Special Measures) Act 2012	Sedition Act 1948
Sexual Offences Against Children Act 2017	Telemedicine Act 1997	Trademarks Act 2019

Source: National Security Council

7.0 Outlook and Prospects of the Cybersecurity Market in Malaysia

The outlook and prospects of the cybersecurity market in Malaysia are expected to be positive in view of the demand conditions set out in Section 5 above. The COVID-19 pandemic and subsequent lockdown measures imposed have accelerated the usage of the Internet and the adoption of digital medium which together lay a clear path for further potential demand for cybersecurity offerings. There are a lot of opportunities for the local cybersecurity market to expand its size.

Factors priming growth within the cybersecurity market include the continuing digital transformation of the economy and the proliferation of digital touch points and applications. Besides that, the need to uphold digital privacy and relatively high broadband penetration rate augur well for the growth in the local cybersecurity market. On the flip side, the lack of awareness on the importance of implementing best cybersecurity practices is expected to dampen the growth momentum in the local cybersecurity market.

On the supply side, the local cybersecurity market can expect to continue receiving strong support from the Malaysian Government. However, the cybersecurity market in Malaysia is expected to grapple with critical shortage of skilled cybersecurity professionals.

Moving forward, the local cybersecurity market is projected to grow at an annual double-digit growth rate throughout the forecast period from 2022 to 2026. The cybersecurity market in Malaysia is projected to grow from RM3.33 billion in 2021 to reach RM6.36 billion in 2026, registering a CAGR of 13.9% during this forecast period.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL

8.1 Promoters and substantial shareholders

8.1.1 Shareholdings in our Company

The table below sets out the direct and indirect shareholdings of our Promoters and substantial shareholders in our Company before and after our IPO:-

Promoters and substantial shareholders	Nationality	Before our IPO		After the Offer for Sale		After our IPO					
		Direct		Indirect		Direct		Indirect			
		No. of Shares ('000)	(¹)%	No. of Shares ('000)	(¹)%	No. of Shares ('000)	(¹)%	No. of Shares ('000)	(²)%		
Fong Choong Fook	Malaysian	291,200	79.87	245,600	67.36	(³)73,405	20.13	245,600	53.86	(³)73,405	16.10
Goh Soon Sei	Malaysian	73,405	20.13	73,405	20.13	(³)245,600	67.36	73,405	16.10	(³)245,600	53.86
Total		364,605	100.00	319,005	87.49			319,005	69.96		

Notes:-

- (1) Based on our issued share capital of 364,605,000 Shares after the Pre-IPO Restructuring but before the Public Issue.
- (2) Based on our enlarged issued share capital of 456,000,000 Shares upon Listing.
- (3) Deemed interested by virtue of his or her spouse's interest pursuant to Section 8 of the Act.

Our Promoters and substantial shareholders do not have different voting rights from any other shareholders of our Group.

Save for our Promoters and substantial shareholders, we are not aware of any other person who is able to, directly or indirectly, jointly or severally, exercise control over our Company. As at the LPD, there is no arrangement between our Company and the Promoters and our substantial shareholders, with any third party of which may result in a change in control of our Company.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.1.2 Changes in our Promoters' and substantial shareholders' shareholdings

Save for the issuance of our Shares to our Promoters and substantial shareholders pursuant to the Pre-IPO Restructuring as detailed in **Sections 5.2 and 5.3** of this Prospectus, there has been no change in the Promoters' and our substantial shareholders' shareholdings in our Company since the incorporation of our Company up to the LPD.

8.1.3 Profiles of our Promoters and substantial shareholders

The profiles of our Promoters and substantial shareholders are as follows:-

Fong Choong Fook

Fong Choong Fook, a Malaysian, aged 46, is our Promoter, substantial shareholder and Executive Chairman. He was appointed to our Board on 1 September 2021, and is a member of our Risk Management Committee. He is the co-founder of our Group and has been managing our business since its inception. He plays a pivotal role in the formulation of our business strategies, driving the growth of our Group.

He is an industry veteran in the field of cybersecurity with more than 20 years of working experience, primarily specialising in penetration testing, cybersecurity advisory and consulting as well as digital forensics. He was one of the co-founders and the first nomination chairman of (ISC)² Malaysia Chapter, a non-profit membership association focused on cybersecurity which formed part of (ISC)² and was approved by (ISC)² in 2014. (ISC)² is an international non-profit membership association that specialises in training and certifications for cybersecurity professionals. From 2004 to 2010, he was also appointed by (ISC)² to administer and proctor the CISSP and SSCP examinations in Malaysia and Indonesia.

He was awarded with the 2013 IDG ASEAN Chief Security Officer of the Year award from International Data Group, Inc., a global technology media, data and marketing services company, and the 2016 Cyber Security Professional of the Year award from CyberSecurity Malaysia, a national cybersecurity specialist agency under the purview of the Ministry of Communications and Multimedia Malaysia.

He is also a committee member of the National Tech Association of Malaysia (PIKOM) Cybersecurity Chapter since February 2018 and a member of the CREST (Asia) Advisory Group (an established international not-for-profit accreditation and certification body for technical information security market) since April 2018. He was the author of the "Certified Lead Forensic Examiner" (CLFE) courseware for the Professional Evaluation and Certification Board, USA ("**PECB**") in May 2015, and the training content is distributed worldwide by PECB for its training on computer crime investigations and digital forensics.

Fong Choong Fook graduated with a Bachelor of Information Technology in Information Systems from Charles Sturt University, Australia in October 1998. He has achieved numerous key professional certifications, which include, amongst others, the following:-

- (i) (ISC)² Certified Information Systems Security Professional (since April 2002);
- (ii) ISACA Certified Information Systems Auditor (since October 2004);
- (iii) IRCA Information Security Management Systems Provisional Auditor (since May 2005);
- (iv) ISACA COBIT Foundation Certificate (since January 2008);
- (v) ACFE Certified Fraud Examiner (since March 2010);
- (vi) ISACA Certified Information Security Manager (since April 2010);
- (vii) Certificate of Cloud Security Knowledge (CCSK) (since October 2010);

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

- (viii) Certified in Risk and Information Systems Control certification from ISACA (since January 2011);
- (ix) Certified PCI Security Standards Council Approved Scanning Vendor (since July 2013);
- (x) Cellebrite Certified Logical Operator (since July 2013);
- (xi) Cellebrite Certified Physical Analyst (since November 2013); and
- (xii) MyCC Scheme Foundation Evaluator (since April 2018).

He had also successfully completed the EnCase® v7 OnDemand Computer Forensics I course by Guidance Software in February 2013 and the Windows Forensic Analysis and GIAC Certified Forensic Examiner (GCFE) course by The SANS Institute in June 2014. The various key certifications demonstrate the technical skillsets obtained by Fong Choong Fook over the years which has provided him with the platform to steer our growth in the cybersecurity market and enabled him to provide comprehensive cybersecurity advisory services and broaden our scope of service offerings to our customers.

Upon his graduation in October 1998, he began his career in November 1998 with Infocus Sdn Bhd as a System Engineer and was primarily tasked to develop telecommunications-based applications. He subsequently joined RQ Net Sdn Bhd in March 1999 as a System Developer, where he played an integral part in pioneering and implementing a new web development tool named "Cold Fusion". In January 2000, he joined World.Net Services Ltd ("**World.Net**"), a subsidiary of Reliance Pacific Berhad ("**Reliance**") (now known as Avillion Berhad), as a Security Consultant and was mainly tasked to oversee the implementation of cybersecurity controls and systems for the entire Reliance group.

In January 2001, he joined Sun Microsystems Malaysia as an Information Security Consultant and was responsible in providing information security consulting and security penetration testing services. He subsequently left the company and joined British American Tobacco Global Service Delivery (Kuala Lumpur) Sdn Bhd ("**BAT GSD**") as an Information Security Manager in January 2004. BAT GSD is a company which provides IT shared services for British American Tobacco plc's businesses worldwide. During his tenure, he was primarily tasked with managing the information security of the company and British American Tobacco plc's global information security defence system.

Having built his experience and expertise in the IT and cybersecurity field, he saw the potential of the industry and subsequently decided to resign from BAT GSD and pursue the entrepreneurship path with Goh Soon Sei by setting up LE Global in 2005.

Goh Soon Sei

Goh Soon Sei, a Malaysian, aged 48, is our Promoter, substantial shareholder and Executive Director. She was appointed to our Board on 1 September 2021. She is the co-founder of LE Global and together with Fong Choong Fook, has been steering the business growth of our Group. She is primarily responsible for overseeing the cyber risk management and compliance segment of our Group.

She is an industry veteran in the IT field with more than 20 years of working experience, primarily specialising in information security governance, IT security risk assessment, PCI DSS compliance assessment and consultancy as well as the development and implementation of IT security framework, strategic plan and blueprint.

She graduated with a Bachelor of Science in Computer Science and Mathematics from Campbell University, USA (under a cooperative programme with Tunku Abdul Rahman College) in June 1998. She has achieved numerous key professional certifications, which include, amongst others, the following:-

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

- (i) IRCA Information Security Management Systems Lead Auditor (since November 2010);
- (ii) PCI Security Standards Council ASV (since July 2012);
- (iii) PECB Certified ISO/IEC 27001 Lead Auditor (since February 2013);
- (iv) PCI Security Standards Council Qualified Security Assessor (since March 2016);
- (v) PECB Certified ISO/IEC 27005 Provisional Risk Manager (since May 2018);
- (vi) PECB Certified ISO 9001 Provisional Auditor (since June 2018); and
- (vii) PECB Certified ISO/IEC 27001 Senior Lead Implementer (since November 2020).

In November 2004, she passed the Projects in Controlled Environments (PRINCE2) Practitioner Examination. This certification is an endorsement of Goh Soon Sei's project management capability in respect of projects in controlled environments.

Similar to Fong Choong Fook, the multitude of certifications coupled with the technical skillsets garnered over the years has enabled her to provide comprehensive cybersecurity advisory services and broaden our scope of service offerings to our customers.

She began her career in April 1998 as an Analyst Programmer in MBF Information Services Sdn Bhd and was responsible in providing IT support and maintenance, particularly as a database administrator. She subsequently left the company and worked as a Database Administrator in other companies including Biztone.com Sdn Bhd (from December 1999 to April 2000), Unisys (Malaysia) Sdn Bhd (MyKad project) (from July 2001 to June 2002), BAT GSD (from August 2002 to July 2007) and Neural Technologies Sdn Bhd (from June 2008 to March 2010). As a database administrator, she was involved in development environment activities, management and maintenance of local and regional production databases.

Having built her experience and expertise in the IT industry, she subsequently pursued the entrepreneurship path with Fong Choong Fook to establish LE Global in 2005.

8.1.4 Payments made to our Promoters and substantial shareholders

Save as disclosed below, there are no other amounts or benefits paid or intended to be paid or given to our Promoters and substantial shareholders within the 2 years preceding the date of this Prospectus:-

- (i) remuneration and material benefits in kind paid to Fong Choong Fook and Goh Soon Sei for the FYEs 31 December 2019, 2020 and 2021, and the subsequent period up to the LPD, are set out as follows:-

	Remuneration and material benefits-in-kind			
	FYE 31 December 2019	FYE 31 December 2020	FYE 31 December 2021	1 January 2022 to the LPD
	(RM'000)	(RM'000)	(RM'000)	(RM'000)
Fong Choong Fook	701	692	675	⁽¹⁾ 282
Goh Soon Sei	611	613	606	⁽²⁾ 252

Notes:-

- (1) The bonus in respect of the year 2021 amounting to approximately RM0.11 million was paid in March 2022.
- (2) The bonus in respect of the year 2021 amounting to approximately RM0.10 million was paid in March 2022.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

Further details on the remuneration and material benefits-in-kind are set out in **Section 8.6** of this Prospectus.

- (ii) declaration and payment of dividends to Fong Choong Fook and Goh Soon Sei within the 2 years preceding the date of this Prospectus, in the following manner:-

	Dividend declared		Dividend paid as at the LPD	
	Fong Choong Fook (RM'000)	Goh Soon Sei (RM'000)	Fong Choong Fook (RM'000)	Goh Soon Sei (RM'000)
FYE 31 December 2019	2,866	717	2,866	717
FYE 31 December 2020	4,400	1,100	⁽¹⁾ 4,335	1,100
FYE 31 December 2021	3,040	760	3,040	760

Note:-

- (1) An amount of RM65,145 was used to offset against amount due from director as at 31 December 2020.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.2 Directors

8.2.1 Shareholdings in our Company

The following table sets forth the direct and indirect shareholdings of each of our Directors before and after our IPO, assuming our Directors will subscribe for their respective entitlements under the Pink Form Allocation as set out in **Section 3.3.1(ii)** of this Prospectus in full:-

Director	Designation	Nationality	Before our IPO		After our IPO					
			Direct		Direct					
			No. of Shares ('000)	(1)%	No. of Shares ('000)	(1)%	No. of Shares ('000)	(2)%		
Fong Choong Fook	Executive Chairman	Malaysian	291,200	79.87	(3)73,405	20.13	245,600	53.86	(3)73,405	16.10
Goh Soon Sei	Executive Director	Malaysian	73,405	20.13	(3)291,200	79.87	73,405	16.10	(3)245,600	53.86
Chan Kam Chiew	Independent Non-Executive Director	Malaysian	-	-	-	-	250	0.05	-	-
Dr Teh Chee Ghee	Independent Non-Executive Director	Malaysian	-	-	-	-	250	0.05	-	-
Antonius Sommer	Independent Non-Executive Director	German	-	-	-	-	250	0.05	-	-
Ts. Lim Mei Shyan	Independent Non-Executive Director	Malaysian	-	-	-	-	200	0.04	-	-

Notes:-

- (1) Based on our issued share capital comprising 364,605,000 Shares after the Pre-IPO Restructuring but before the Public Issue.
- (2) Based on our enlarged issued share capital comprising 456,000,000 Shares upon Listing.
- (3) Deemed interested by virtue of his or her spouse's interest pursuant to Section 8 of the Act.

Notwithstanding the Pink Form Allocation reserved for our Directors, our Directors may subscribe for Issue Shares under the public balloting portion as set out in **Section 3.3.1(i)** of this Prospectus.

None of our Directors represents any corporate shareholder on our Board.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.2.2 Profiles of our Directors

The profiles of our Directors (save for Fong Choong Fook and Goh Soon Sei as set out in **Section 8.1.3** of this Prospectus) are as follows:-

Chan Kam Chiew

Independent Non-Executive Director

Chan Kam Chiew, a Malaysian, aged 57, is our Independent Non-Executive Director. He was appointed to our Board on 21 September 2021. He is also the Chairman of our Audit Committee and Nomination Committee and member of our Remuneration Committee and Risk Management Committee.

He holds a MICPA certification and has been a member of the MICPA (since April 1991), the MIA (since July 1993) and the Institute of Corporate Directors Malaysia (since February 2021).

He is an industry veteran in the field of audit and business advisory with more than 36 years of working experience. He had served on the Board of MASB for 2 terms from May 2012 to April 2018. He had also served as a member and chaired a few working groups of MASB. He was an examiner for the Regulatory and Financial Reporting Framework examination for the MICPA.

He started his career when he joined Peat Marwick (now known as KPMG) in Malaysia as Audit Assistant on December 1984. Between September 1991 and April 1993, he was seconded to KPMG in San Francisco, USA. Upon his return to KPMG Malaysia in April 1993, he was promoted to Audit Manager. In October 1998, he was admitted as a Partner of KPMG Malaysia and served until his retirement as a Senior Partner at the end of December 2020.

During his tenure, he was involved in the provision of audit and business advisory services to public listed companies and multinational corporations in various industries which include, amongst others, real estate investment trust, property development and construction, oil and gas, electronics and IT, as well as banking and financial services. In addition to statutory audits, he led and was involved in various assignments including International Financial Reporting Standards reviews, initial public offerings and reverse takeovers, local and cross-border mergers and acquisitions, financial due diligence reviews, provision of financial advisory services as well as review of policies and procedures.

In June 2021, he joined Can-One Berhad and Box-Pak (Malaysia) Berhad as the Group Finance Director responsible for overseeing the financial reporting and management of the companies. He was appointed as an Independent Non-Executive Director of Kerjaya Prospek Group Berhad in May 2021.

Dr Teh Chee Ghee

Independent Non-Executive Director

Dr Teh Chee Ghee, a Malaysian, aged 56, is our Independent Non-Executive Director. He was appointed to our Board on 21 September 2021. He is the Chairman of our Remuneration Committee and Risk Management Committee. He is also a member of our Audit Committee and Nomination Committee.

He holds a Doctor of Philosophy degree in Credit Management (since August 2010), a Master of Business Administration degree (since October 2001) and an Honours Degree in Accounting (since August 1990), all of which are from University of Malaya.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

He is a member of the MICPA (since January 1994) and sits on the Council of MICPA (from June 2002 to November 2006 and from June 2015 until present), a member of the Chartered Association of Certified Accountants (now known as Association of Chartered Certified Accountants) (since September 1996) and a member of the Malaysian Institute of Taxation (now known as Chartered Tax Institute of Malaysia) (since March 1994). He is also a member of the MIA since September 1993.

He started his career as an Associate Consultant with HRM Sdn Bhd (a firm under Hanafiah Raslan & Mohamad that merged with Arthur Andersen & Co in May 1990) in April 1990, where he assisted in providing corporate consultancy services. He was subsequently transferred to the audit and business advisory division of Arthur Andersen & Co in November 1990.

In February 1994, he joined CWS Washroom Services (M) Sdn Bhd ("**CWS**") (a company under CWS International AG) as Finance and Administration Manager and was primarily responsible for the finance and administrative functions of the company. Following the acquisition of CWS by Zuellig Group in March 1995, he was subsequently transferred and appointed as the Regional Finance Controller (Peninsular Malaysia) of Gold Coin Feedmills (Malaysia) Sdn Bhd (a company under the Zuellig Group) to oversee the overall finance and administrative functions for Peninsular Malaysia region.

In July 1996, he left Gold Coin Feedmills (Malaysia) Sdn Bhd and joined Engtex Sdn Bhd (a subsidiary of Engtex Group Berhad ("**Engtex**"), a company listed on the Main Market of Bursa Securities) as the Group Financial Controller in August 1996 until December 2003. He was also appointed as the Personal Assistant ("**PA**") to the Group Managing Director ("**GMD**") of Engtex Sdn Bhd from January 2000 to June 2002 and PA to GMD of Engtex group from July 2002 to May 2006 and was also the Company Secretary of Engtex between May 2001 and May 2006.

He subsequently joined TH Group Berhad as the PA to the GMD from June 2006 to October 2010. He was also appointed as the Acting Chief Operating Officer of Nilai Medical Centre (a hospital owned by TH Group Berhad) in February 2010. He resigned from TH Group Berhad in October 2010 and subsequently joined TSH Resources Berhad as the General Manager (Strategic Planning and Operations) where he remained until October 2012.

In October 2012, he left the corporate sector and joined Monash University Malaysia ("**Monash**") to pursue his career in academia as a Senior Lecturer in Department of Accounting and Finance in the School of Business. In Monash, he held various positions, which include the Deputy Director of Research of the School of Business, Monash from January 2013 to January 2014, the Deputy Director of Master of Business Administration Programme from July 2016 to February 2018, and the Deputy Director – Development and External Engagement of the Entrepreneurship and Innovation Hub from October 2017 to July 2019. In January 2022, he retired from Monash. He rejoined Engtex as the Chief Operating Officer of Engtex after his retirement from academia.

Whilst with Monash, he also took on the role of the Head of Research of the Socio-Economic Research Centre, operating under SERC Sdn Bhd, an independent think tank initiated by the Associated Chinese Chambers of Commerce and Industry of Malaysia under a retainer arrangement from January 2014 to February 2016.

He is the Independent Non-Executive Director of ACO Group Berhad (since August 2019), K. Seng Seng Corporation Berhad (since January 2021) and the Independent Non-Executive Chairman of Orgabio Holdings Berhad (since March 2021).

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

Antonius Sommer*Independent Non-Executive Director*

Antonius Sommer, a German citizen, aged 72, is our Independent Non-Executive Director. He was appointed to our Board on 21 September 2021, and is also a member of our Risk Management Committee. As he currently resides in Germany, Antonius Sommer will carry out his duties and roles as the Independent Non-Executive Director remotely via the virtual meetings with our Board and management.

He graduated with an “Ingenieur (grad.)” Maschinentechnik (equivalent to Bachelor of Science in Mechanical Engineering) in October 1976 and “Dipl.-Ing. Fertigungstechnik” (equivalent to Master of Science in Industrial Engineering) in February 1982, both of which are from University of Paderborn, Germany.

He is an IT security industry veteran with more than 40 years of working experience, primarily specialising in the technical inspection and certification industries in the fields of information security, information quality, data privacy and IT infrastructure. He was a member of the steering committee within Bitkom e.V. (German Federal Association for Information Technology, Telecommunication and New Media) (from June 2011 to March 2016) and a member of the advisory board of the foundation Data Protection, Stiftung Datenschutz in Germany (from November 2012 to March 2016).

He started his career with Rheinisch-Westfälischer Technischer Überwachungsverein e.V. in Germany as a Programmer in April 1977. He was responsible for the testing and development of the inspection and review software for nuclear power plants. In January 1981, he was subsequently assigned to manage the operations of decentralised computer systems of the company as well as system administration/programming. He was subsequently promoted to Head of Decentralised Computer Systems in April 1983 and was tasked with the supervision of the allocation of computing resources (hardware, software and network) to computer centres.

In December 1991, he was appointed as the Head of Staff Unit IT Security to supervise on IT security management and personnel. He was subsequently promoted to Head of Department of IT Security and was assigned to manage the entire IT security operations and personnel.

In April 1993, he joined RWTÜV Anlagentechnik GmbH in Germany. The IT Security department of the company was subsequently sold to TÜV Informationstechnik GmbH group (“TÜViT”). In March 1997, he was subsequently appointed as the General Manager for Marketing and Sales within TÜViT and was tasked to spearhead the company’s business development efforts. In March 1999, he was appointed as the Managing Director of the company and was responsible for managing its entire operations, including overseeing the IT Security, sales and marketing as well as the development of standards for certification of critical infrastructures (such as firewall installations and security of data centres).

During his tenure with TÜViT, he was also involved in setting up the German scheme for security labs according to the IT Security Evaluation Criteria and Common Criteria, Quid! (a data protection certification scheme) as well as the European Privacy Seal (for certification of products and IT based services with regard to data privacy). In addition, he was appointed as Chairman of the board of directors of TÜViT, Inc in USA (from March 1999 to December 2000) and member of the board of directors of TÜViT Japan K.K. (from 2008 to August 2011). He retired from TÜViT in March 2016.

He is also currently the Chairman of the advisory board of achelos, GmbH (a company involved in data protection and security) since August 2020.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

After his retirement, he is actively involved in undertaking management consulting works. He is supporting small and medium-sized enterprises within the IT security area on strategy development, market entry as well as mergers and acquisitions.

Ts. Lim Mei Shyan

Independent Non-Executive Director

Ts. Lim Mei Shyan, a Malaysian, aged 47, is our Independent Non-Executive Director. She was appointed to our Board on 21 September 2021, and is also a member of our Audit Committee, Nomination Committee, and Remuneration Committee.

She obtained her Bachelor of Science (Honours) in Mathematics from Universiti Kebangsaan Malaysia in June 1998 and Master of Science in Computing and Information Systems from University of Greenwich, United Kingdom in January 2000. She is a Professional Technologist registered and recognised by Malaysia Board of Technologists since July 2018.

She is an industry veteran in the education sector with more than 20 years of working experience. Her areas of expertise are cybersecurity and computer networking fields. She has subsequently obtained various key academic and professional certifications, which include, amongst others:-

- (i) Cisco Certified Academy Instructor (since November 2007);
- (ii) Mile2 Certified Penetration Testing Engineer (since December 2014);
- (iii) Cisco Certified CyberOps Associate (since September 2021);
- (iv) EC-Council Certified Ethical Hacker (from November 2016 to November 2019);
and
- (v) Security Operations Centre Incident Responder (from September 2018 to August 2021).

In April 1998, she started her career at INTI College Malaysia (now known as INTI International University) as a Lecturer. She left the college in August 1998 to pursue her postgraduate studies in United Kingdom. Upon her graduation, she returned to Malaysia and joined Tunku Abdul Rahman College (now known as Tunku Abdul Rahman University College) ("**TAR UC**") as a Lecturer in November 1999. At TAR UC, in addition to her duties as an academic staff, she was subsequently appointed to undertake the administrative positions as Course Tutor of the School of Arts and Science (from October 2001 to April 2005), Programme Supervisor of the School of Arts and Science (from May 2005 to January 2008), Head of the Computer Science Division of the School of Arts and Science (from January 2008 to September 2013), Deputy Dean of the Faculty of Computing and IT (from October 2013 to April 2017) and Dean of the Faculty of Computing and IT (from May 2017 to January 2021), where she was tasked and assigned to provide academic and administrative leadership in the Faculty of Computing and IT. She was promoted to the position of Principal Lecturer at TAR UC since August 2019.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.2.3 Involvement of our Directors in other businesses and corporations outside our Group

Save as disclosed below, none of our Directors has any directorships or principal business activities performed outside our Group for the past 5 years prior to the LPD:-

(i) Fong Choong Fook

Company	Principal business activities	Nature of relationship	Date of appointment as director	Date of cessation as director
<u>Past involvements:-</u> Ace Accelerator Sdn Bhd	Investment managers and to provide advisory, consultancy and related services in investment in all kinds of securities, properties and assets and in all rights and interests therein	Director. No equity interest in the company.	4 April 2018	11 September 2020
Nouveau Solution Sdn Bhd	Investment holding of companies involved in business management consultancy services, meeting, incentive, convention, exhibition (MICE) and other business support service activities. The company was dissolved on 22 November 2019	Director. No equity interest in the company.	27 June 2016	19 February 2019

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

(ii) Chan Kam Chiew

Company	Principal business activities	Nature of relationship	Date of appointment as director	Date of cessation as director
<u>Present involvements:-</u> Kerjaya Prospek Group Berhad (listed on the Main Market of Bursa Securities)	Investment holding of companies involved in the construction of high-end commercial and high-rise residential buildings, property development and manufacturing of lighting and kitchen solutions	Independent Non-Executive Director. No equity interest in the company.	12 May 2021	-
Biz Link Property Sdn Bhd	Property investment and development	Shareholder (Direct equity interest: 10.00%)	-	-
<u>Past involvements:-</u> Baig Hills Sdn Bhd	Investment holding of companies involved in property investment and development	Director Shareholder (Direct equity interest: 45.00%)	19 May 2014	29 February 2020
Jimbaran Holdings Sdn Bhd	Investment holding of companies involved in the provision of consultancy services. The company was dissolved on 31 March 2021	Director Shareholder (Direct equity interest: 51.00%)	9 June 2008	31 March 2021

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

(iii) Dr Teh Chee Ghee

Company	Principal business activities	Nature of relationship	Date of appointment as director	Date of cessation as director
<u>Present involvements:-</u>				
The Malaysian Institute of Certified Public Accountants	Professional accounting institute in Malaysia	Council Member	13 June 2015	-
ACO Group Berhad (listed on the ACE Market of Bursa Securities)	Investment holding of companies involved in the distribution of electrical products and accessories	Independent Non-Executive Director Shareholder (Direct equity interest: negligible)	5 August 2019	-
K. Seng Seng Corporation Berhad (listed on the Main Market of Bursa Securities)	Investment holding of companies involved in manufacturing stainless steel tubes and pipes	Independent Non-Executive Director. No equity interest in the company.	4 January 2021	-
Orgabio Holdings Berhad (en route for listing on the ACE Market of Bursa Securities)	Investment holding of companies involved in the provision of instant beverage premix manufacturing services to third party brand owners and manufacturing, sales and marketing of house brand instant beverage premixes	Independent Non-Executive Chairman. No equity interest in the company.	15 March 2021	-

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

Company	Principal business activities	Nature of relationship	Date of appointment as director	Date of cessation as director
<u>Past involvements:-</u> Engtex Group Berhad (listed on the Main Market of Bursa Securities)	Investment holding of companies involved in wholesale and distribution of pipes, valves and fittings; manufacturing and distribution of steel products, hospitality as well as property development.	Independent Non-Executive Chairman. No equity interest in the company.	20 January 2009	27 May 2021
Flexidynamic Holdings Berhad (listed on the ACE Market of Bursa Securities)	Investment holding of companies involved in the design, engineering, installation and commissioning of glove chlorination systems, as well as the design and installation of storage tanks and process tanks for the glove manufacturing industry.	Independent Non-Executive Chairman. No equity interest in the company.	9 June 2020	25 January 2021
Fiamma Holdings Berhad (listed on the Main Market of Bursa Securities)	Investment holding of companies involved in distribution of electrical home appliances, sanitaryware, kitchen, wardrobe system, medical devices and healthcare products, furniture and fittings as well as property development.	Independent Non-Executive Director. No equity interest in the company.	4 July 2001	28 December 2018
Parlo Berhad (listed on the ACE Market of Bursa Securities)	Investment holding of companies involved in provision of travel products and services for leisure travel, business travel, online travel booking and advertising services.	Independent Non-Executive Director. No equity interest in the company.	20 March 2015	30 May 2018

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

(iv) Antonius Sommer

Company	Principal business activities	Nature of relationship	Date of appointment as director	Date of cessation as director
<p><u>Present involvement:-</u> achelos GmbH</p>	Provider of embedded IT security solutions in Germany	Chairman of Advisory Board. No equity interest in the company.	25 August 2015	-
<p><u>Past involvement:-</u> TUV Informationstechnik GmbH</p>	A private technical inspection and testing company in the fields of information security, information quality, data privacy, IT infrastructure and certification	Executive Director. No equity interest in the company.	1 March 1999	31 March 2016

The involvements of our Directors mentioned above in other principal business activities outside of our Group will not affect their commitment and responsibilities to our Group in their respective roles as our Directors given that:-

- (a) their roles are substantially in the capacity as the Independent Non-Executive Director; and
- (b) they are not involved in the day-to-day operations of the respective companies.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.3 Board practice

8.3.1 Directorship

In accordance with our Constitution, our Directors shall have the power at any time and from time to time to appoint any person to be a Director either to fill a casual vacancy or as an additional Director, but so that the total number of Directors shall not at any time exceed the maximum number fixed by or in accordance with our Constitution which is 11 Directors.

Any person appointed as Director, either to fill a casual vacancy or as an addition to the existing Directors, shall hold office only until the next Annual General Meeting (“**AGM**”) and shall then be eligible for re-election but shall not be taken into account in determining the Directors who are to retire by rotation at that meeting.

Our Board has adopted the following responsibilities for effective discharge of its functions:-

- (i) to provide leadership and oversee the overall conduct of our Group’s businesses to ensure that our businesses are being properly managed;
- (ii) to review and adopt strategic plans for our Group and to ensure that such strategic plans and the risk, performance and sustainability thereon are effectively integrated and appropriately balanced;
- (iii) to review and adopt corporate governance best practices in relation to risk management, legal and compliance management and internal control systems to safeguard our Group’s reputation, and our employees and assets and to ensure compliance with applicable laws and regulations;
- (iv) to ensure that our Company has effective Board committees as required by the applicable laws, regulations, rules, directives and guidelines and as recommended by the Malaysian Code on Corporate Governance;
- (v) to review and approve our annual business plans, financial statements and annual reports;
- (vi) to monitor the relationship between our Group and our management, shareholders and stakeholders, and to develop and implement an investor relations programme or shareholders’ communications policy for our Group; and
- (vii) to appoint our Board committees, to delegate powers to such committees, to review the composition, performance and effectiveness of such committees, and to review the reports prepared by our Board committees and deliberate on the recommendations thereon.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

As at the LPD, the details of the date of expiration of the current term of office for each of our Directors and the period that each of our Directors has served in office are as follows:-

Name	Date of appointment as Director	Date of expiration of the current term of office ⁽¹⁾	Approximate no. of years in office
Fong Choong Fook	1 September 2021	Subject to retirement at AGM held in 2023	Less than 1 year
Goh Soon Sei	1 September 2021	Subject to retirement at AGM held in 2023	Less than 1 year
Chan Kam Chiew	21 September 2021	Subject to retirement at AGM held in 2024	Less than 1 year
Dr Teh Chee Ghee	21 September 2021	Subject to retirement at AGM held in 2024	Less than 1 year
Antonius Sommer	21 September 2021	Subject to retirement at AGM held in 2025	Less than 1 year
Ts. Lim Mei Shyan	21 September 2021	Subject to retirement at AGM held in 2025	Less than 1 year

Note:-

- (1) *Our Directors shall have the power at any time and from time to time to appoint any person to be a Director, either to fill a casual vacancy or as an addition to the existing Directors, but the total number of Directors shall not at any time exceed the number fixed in our Constitution. Any Director so appointed shall hold office only until the next following AGM and shall then be eligible for re-election but shall not be taken into account in determining the Directors who are to retire by rotation at that meeting. All our Directors retired from office in accordance with Article 18.9 of our Constitution and were re-elected at our first AGM held on 6 April 2022.*

In accordance with our Constitution, an election of Directors shall take place each year at the AGM of our Company. At the AGM in every subsequent year, 1/3 of our Directors for the time being, or, if their number is not three or multiple of three, then the number nearest to 1/3 shall retire from office and be eligible for re-election. This is provided always that all of our Directors shall retire from office once at least in each 3 years but shall be eligible for re-election. A retiring Director shall retain office until the close of the meeting at which he/she retires.

8.3.2 Audit Committee

Our Audit Committee was established by our Board on 21 September 2021. The composition of our Audit Committee is set out below:-

Name	Designation	Directorship
Chan Kam Chiew	Chairman	Independent Non-Executive Director
Dr Teh Chee Ghee	Member	Independent Non-Executive Director
Ts. Lim Mei Shyan	Member	Independent Non-Executive Director

The terms of reference of our Audit Committee, amongst others, include the following:-

- (i) to ensure openness, integrity and accountability in our Group's activities so as to safeguard the rights and interests of our shareholders;

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

- (ii) to review and approve our quarterly and annual financial statements for recommendation to our Board, focusing in particular on any changes in or implementation of major accounting policies and practices, significant and unusual events, significant adjustments arising from the audit, going concern assumption and compliance with accounting standards and other regulatory or legal requirements;
- (iii) to provide assistance to our Board in fulfilling its fiduciary responsibilities relating to corporate accounting and reporting practices;
- (iv) to improve our Group's business efficiency, the quality of accounting and audit function so as to strengthen the public's confidence in our reported results;
- (v) to maintain a direct line of communication between our Board and the external and internal auditors;
- (vi) to enhance the independence of our external and internal auditors;
- (vii) to create a climate of discipline and control, this will reduce the opportunity for fraud;
- (viii) to monitor and review matters relating to related party transactions entered into by our Group and any conflict of interests situations that may arise within our Group;
- (ix) to recommend to our Board the nomination and re-appointment of the external auditors, considering their independence, the adequacy of experience, audit fee and any issue regarding resignation or dismissal; and
- (x) to obtain advice from independent parties and other professionals, where necessary, in discharging their duties.

8.3.3 Remuneration Committee

Our Remuneration Committee was established by our Board on 21 September 2021. The composition of our Remuneration Committee is set out below:-

Name	Designation	Directorship
Dr Teh Chee Ghee	Chairman	Independent Non-Executive Director
Chan Kam Chiew	Member	Independent Non-Executive Director
Ts. Lim Mei Shyan	Member	Independent Non-Executive Director

The terms of reference of our Remuneration Committee, amongst others, include the following:-

- (i) to assist our Board in determining the remuneration of our executive directors and key senior management. In fulfilling this responsibility, our Remuneration Committee is to ensure that our executive directors and our key senior management:-
 - (a) are fairly rewarded for their individual contributions to overall performance;
 - (b) that the compensation is reasonable in light of our objectives; and
 - (c) that the compensation is similar to other companies.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

- (ii) to review and recommend on an annual basis, the performance of our Directors and our key senior management, and recommend to our Board specific adjustments in remuneration and/or reward payments to be passed at a general meeting;
- (iii) to establish our Executive Chairman's and Executive Director's goals, objectives and key performance indicators;
- (iv) to review our Executive Chairman's and Executive Director's performance against the goals, objectives and key performance indicators set; and
- (v) to ensure that the remuneration packages and benefits for Independent Non-Executive Directors do not conflict with their obligations to bring objective and independent judgement to our Board.

8.3.4 Nomination Committee

Our Nomination Committee was established by our Board on 21 September 2021. The composition of our Nomination Committee is set out below:-

Name	Designation	Directorship
Chan Kam Chiew	Chairman	Independent Non-Executive Director
Dr Teh Chee Ghee	Member	Independent Non-Executive Director
Ts. Lim Mei Shyan	Member	Independent Non-Executive Director

The terms of reference of our Nomination Committee, amongst others, include the following:-

- (i) to identify, assess and recommend to our Board, candidates for our board directorships, having regard to their expertise, experience, and other core competencies, potential conflict of interest, contribution and integrity which the Directors should bring to the Board;
- (ii) to recommend to our Board, a mixture of suitable, qualified and experienced candidates as Directors to fill the seats on our Board committees;
- (iii) to assess and evaluate, on an annual basis, or as required, the desirability of the overall composition of our Board and the balance amongst executive, non-executive and independent directors;
- (iv) to evaluate the effectiveness of our Board and Board committees (including its size and composition) and contributions of each individual Director;
- (v) to determine the independence of each Director annually and ensure that the independent Directors can bring independence and objective judgement to board deliberations;
- (vi) to review and ensure an appropriate framework and plan for our Board succession;
- (vii) to recommend Director(s) who are retiring (by casual vacancy and by rotation) for re-election at our AGM; and
- (viii) to ensure that our Directors receive appropriate induction programs and undergo continuous training to enhance their performance.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)**8.3.5 Risk Management Committee**

Our Risk Management Committee was established by our Board on 21 September 2021. The composition of our Risk Management Committee is set out below:-

Name	Designation	Directorship
Dr Teh Chee Ghee	Chairman	Independent Non-Executive Director
Chan Kam Chiew	Member	Independent Non-Executive Director
Antonius Sommer	Member	Independent Non-Executive Director
Fong Choong Fook	Member	Executive Chairman

The terms of reference of our Risk Management Committee, amongst others, include the following:-

- (i) to review the principal risks of our Group and recommend and ensure the implementation of an appropriate risk management framework and policies for our Group to mitigate/manage such risks;
- (ii) assess the quality, effectiveness and efficiency of our internal controls and advise our Board on setting appropriate policies on internal control;
- (iii) to review and deliberate on reports on significant risk findings and recommendations;
- (iv) to determine our level of risk tolerance and actively identify, assess and monitor key business risks to safeguard our shareholders' investments and our assets; and
- (v) to ensure that our Board conducts an annual review and periodic testing of our internal control and risk management.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.4 Key senior management

8.4.1 Shareholdings in our Company

The following table sets forth the direct and indirect shareholdings of each of our key senior management before and after our IPO, assuming our key senior management subscribe for their respective entitlements under the Pink Form Allocation as set out in **Section 3.3.1(ii)** of this Prospectus in full:-

Name	Designation	Nationality	Before our IPO		After our IPO			
			Direct		Direct		Indirect	
			No. of Shares ('000)	(1)%	No. of Shares ('000)	(2)%	No. of Shares ('000)	(2)%
Gilbert Chu Fow Chee Kang	Chief Operating Officer Senior Director, Professional Services	Malaysian Malaysian	-	-	1,800	0.39	-	-
			-	-	800	0.18	-	-
Lum Pui Yee	Financial Controller	Malaysian	-	-	400	0.09	-	-

Notes:-

- (1) Based on our issued share capital comprising 364,605,000 Shares after the Pre-IPO Restructuring but before the Public Issue.
- (2) Based on our enlarged issued share capital comprising 456,000,000 Shares upon Listing and assuming full subscription of the Issue Shares reserved under the Pink Form Allocations.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.4.2 Profiles of our key senior management

The profiles of our key senior management are as follows:-

Gilbert Chu
Chief Operating Officer

Gilbert Chu, a Malaysian, aged 36, is our Chief Operating Officer. He is responsible for managing our day-to-day operations, which includes overseeing the technical teams in charge of cyber risk prevention, cybersecurity management and compliance, and cyber threat and incident response. He has also been tasked to oversee the business development and marketing activities as well as the commercial team of our Group.

He is an experienced cybersecurity professional with more than 10 years of working experience in the IT security industry. His areas of expertise include information and cybersecurity risk assessment, consultation, implementation, assessment and training for ISO/IEC 27001, PCI DSS, PCI ASV as well as COBIT 5 consultation and assessment.

He graduated with First Class honours in Bachelor of Science in Business Information Systems from UCSI University in July 2010. He has achieved numerous key professional certifications, some of which include the following:-

- (i) Mile2 Certified Penetration Testing Engineer (since March 2012);
- (ii) ISACA Certified Information Security Manager (since September 2015);
- (iii) PCI Security Standards Council Qualified Security Assessor (since March 2016);
- (iv) PECB Certified ISO/IEC 27001 Lead Auditor (from March 2012 to March 2021) and Senior Lead Auditor (since March 2021);
- (v) PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager (from May 2017 to March 2021) and Senior Lead Cybersecurity Manager (since March 2021); and
- (vi) PECB Certified ISO 9001 Lead Auditor (since June 2018).

His experience and professional credentials as mentioned above have enabled him to provide comprehensive cybersecurity advisory services and technical support to our customers.

He started his career in April 2009 prior to his convocation in Genting Berhad as an IT Security Executive and was responsible for the execution of vulnerability assessment and penetration testing and IT security compliance programme for Genting Group. In November 2010, he left Genting Group and joined our Group as a Cybersecurity Engineer in December 2010.

He was promoted to Managing Consultant in September 2014 and Associate Director in September 2015. He assumed his current position in November 2016.

Fow Chee Kang
Senior Director, Professional Services

Fow Chee Kang, a Malaysian, aged 34, is our Senior Director for professional services. He is responsible to lead the technical teams in charge of cyber risk prevention and cyber threat and incident response. He is also tasked to supervise and implement the technological strategies and oversee the research and development activities of our Group.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

He is an experienced cybersecurity expert with more than 10 years of working experience in technical cybersecurity assessment and consultancy. His areas of expertise include network infrastructure and server penetration test, web application penetration test, wireless access point security assessment, mobile application hacking and computer crime forensics investigation.

He graduated with magna cum laude in Bachelor of Science in Internet Technology from Campbell University, USA (under a cooperative programme with Tunku Abdul Rahman College) in June 2010. He has achieved numerous key professional certifications, some of which include the following:-

- (i) Mile2 Certified Penetration Testing Engineer (since May 2012);
- (ii) PECB Certified ISO/IEC 27001 Provisional Auditor (since August 2014);
- (iii) Offensive Security Certified Professional (since June 2016);
- (iv) CREST Registered Penetration Tester (since April 2017 to April 2020*);
- (v) CREST Practitioner Security Analyst (since October 2017 to October 2020*);
- (vi) PECB Certified ISO/IEC 27005 Risk Manager (since December 2017); and
- (vii) CyberSecurity Malaysia MyCC Scheme Foundation Evaluator & Certifier (in April 2018).

Note:-

* *He was unable to renew the certifications as the examination centres were temporarily closed due to the lockdown measures and travelling restrictions imposed by the Malaysian and Singaporean governments during the COVID-19 pandemic. He is currently undergoing courses and examinations to renew these certifications by the third quarter of year 2022. The non-renewal of these certifications will not affect his ability to provide cybersecurity services.*

His experience and professional credentials as mentioned above have enabled him to provide comprehensive cybersecurity advisory services and technical support to our customers.

He started his career with our Group in May 2010 as a Cybersecurity Engineer. He was promoted to Managing Consultant in September 2014 and Associate Director in September 2015. He assumed his current position and role in November 2019.

Lum Pui Yee
Financial Controller

Lum Pui Yee, a Malaysian, aged 34, is our Financial Controller. She has more than 10 years of working experience in the field of auditing. She is responsible for overseeing our human resources activities and financial management related functions including financial reporting, treasury and financial corporate compliance, tax related matters and maintenance of internal controls.

She obtained a Bachelor of Arts with Honours in Accounting and Finance from the University of East London, United Kingdom in February 2010. She has been a member of the Certified Practising Accountants (“CPA”), Australia (since June 2017) and a member of the MIA (since January 2018).

In January 2011, she started her career in Messrs Baker Tilly Monteiro Heng PLT as an Audit Associate and was subsequently promoted to Semi Senior (in November 2011), Senior (in May 2012), Executive Senior (in June 2013), Assistant Manager (in June 2014) and Audit Manager (in December 2016). During her stint with the firm, she was involved in leading and managing a portfolio of clients in various industries and providing audit and assurance services to the clients. Her roles and responsibilities also include supervising and training audit junior and seniors.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

In August 2018, she joined RSM Chio Lim LLP in Singapore as an Audit Manager, where she was responsible for providing audit and assurance services primarily to healthcare companies and not-for-profit organisations. In November 2020, she decided to return to Malaysia and left RSM Chio Lim LLP to join LE Global. She assumed her current position in December 2020.

8.5 Key technical personnel

8.5.1 Shareholdings in our Company

The direct and indirect shareholdings of our key technical personnel in our Company are set out as follows:-

Fong Choong Fook

The direct and indirect shareholdings of Fong Choong Fook in our Company are set out in **Section 8.1.1** of this Prospectus.

Goh Soon Sei

The direct and indirect shareholdings of Goh Soon Sei in our Company are set out in **Section 8.1.1** of this Prospectus.

Gilbert Chu

The direct and indirect shareholdings of Gilbert Chu in our Company are set out in **Section 8.4.1** of this Prospectus.

Fow Chee Kang

The direct and indirect shareholdings of Fow Chee Kang in our Company are set out in **Section 8.4.1** of this Prospectus.

8.5.2 Profiles of our key technical personnel

The profiles of our key technical personnel are as follows:-

Fong Choong Fook

The profile of Fong Choong Fook is set out in **Section 8.1.3** of this Prospectus.

Goh Soon Sei

The profile of Goh Soon Sei is set out in **Section 8.1.3** of this Prospectus.

Gilbert Chu

The profile of Gilbert Chu is set out in **Section 8.4.2** of this Prospectus.

Fow Chee Kang

The profile of Fow Chee Kang is set out in **Section 8.4.2** of this Prospectus.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.6 Remuneration of Directors and key senior management

8.6.1 Directors

The aggregate remuneration and material benefits-in-kind (which includes contingent or deferred remuneration) paid or proposed to be paid to our Directors on a yearly basis for services rendered in all capacities to our Group for the FYE 31 December 2021 and FYE 31 December 2022 are as follows:-

(i) FYE 31 December 2021 (paid)

Director	Fixed and non-deferred remuneration			Variable and non-deferred remuneration		Total (RM'000)
	Director's Fee (RM'000)	Salary (RM'000)	Contributions to EPF and SOCSO (RM'000)	Bonus (RM'000)	Benefits-in-kind (RM'000)	
<u>Executive Directors</u>						
Fong Choong Fook	-	600	73	(1)112	2	787
Goh Soon Sei	-	540	66	(1)101	-	707
<u>Non-Executive Directors</u>						
Chan Kam Chiew	-	-	-	-	-	-
Dr Teh Chee Ghee	-	-	-	-	-	-
Antonius Sommer	-	-	-	-	-	-
Ts. Lim Mei Shyan	-	-	-	-	-	-

Note:-

(1) The bonuses in respect of the year 2021 was paid in March 2022.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

(ii) FYE 31 December 2022 (proposed)

Director	Fixed and non-deferred remuneration			Variable and non-deferred remuneration		Total		
	Director's Fee (RM'000)	Salary (RM'000)	Contributions to EPF and SOCSO (RM'000)	Bonus (RM'000)	Benefits-in-kind (RM'000)	Paid as at the LPD (RM'000)	Expected to be paid (RM'000)	Total (RM'000)
<u>Executive Directors</u>								
Fong Choong Fook	-	600	73	(1)-	2	170	505	675
Goh Soon Sei	-	540	66	(1)-	-	151	455	606
<u>Non-Executive Directors</u>								
Chan Kam Chiew	60	-	-	-	-	-	60	60
Dr Teh Chee Ghee	50	-	-	-	-	-	50	50
Antonius Sommer	45	-	-	-	-	-	45	45
Ts. Lim Mei Shyan	40	-	-	-	-	-	40	40

Note:-

(1) The bonuses for the FYE 2022, if any, will be determined at a later date based on the performance of the individual and our Group, and will be subject to recommendation by our Remuneration Committee and approval by our Board.

The remuneration of our Directors, which includes salaries, Directors' fees, bonus and such other allowances as well as other benefits-in-kind, must be considered and recommended by our Remuneration Committee and subsequently approved by our Board. Our Directors' fees must be further approved/endorsed by our shareholders at a general meeting.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.6.2 Key senior management

The aggregate remuneration and material benefits-in-kind paid and proposed to be paid to our key senior management for services rendered in all capacities to our Group are set out as follows:-

Key senior management	Remuneration band	
	FYE 31 December 2021 (RM'000)	⁽¹⁾ FYE 31 December 2022 (proposed) (RM'000)
Gilbert Chu	250-300	250-300
Fow Chee Kang	200-250	200-250
Lum Pui Yee	200-250	200-250

Note:-

(1) Excludes bonuses which will be paid to our key senior management on a discretionary basis.

The remuneration of our key senior management, which includes salaries, bonuses and allowances and other benefits (such as parking and mobile allowances), must be considered and recommended by our Remuneration Committee and subsequently approved by our Board.

8.7 Involvement of our key senior management and key technical personnel in other businesses and corporations outside our Group

Save as disclosed below, none of our key senior management and key technical personnel has any directorships or principal business activities performed outside our Group for the past 5 years prior to the LPD:-

(a) Gilbert Chu

Company	Principal business activities	Nature of relationship	Date of appointment as director	Date of cessation as director
<u>Present involvement:-</u>				
I-Spot Manufacturing Sdn Bhd	Investment holding of companies involved in dealing in premium gifts, souvenirs and the related accessories	<ul style="list-style-type: none"> • Director • Shareholder (Direct equity interest: 20.00%) 	3 September 2009	-
<u>Past involvement:-</u>				
Connect Tech Sdn Bhd	Provision of information and technology products and related services	Director. No equity interest in the company.	20 March 2018	18 August 2020

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

The involvements of our key senior management and key technical personnel mentioned above in other principal business activities outside of our Group will not affect his commitment and responsibilities to our Group in his roles as one of our key senior management and key technical personnel given that the day-to-day management and operations of the business is managed by the other shareholders and supported by an independent management team.

8.8 Declaration from our Promoters, Directors, key senior management and key technical personnel

As at the LPD, none of our Promoters, Directors, key senior management and key technical personnel is or has been involved in any of the following events (whether in or outside Malaysia):-

- (i) in the last 10 years, a petition under any bankruptcy or insolvency laws was filed (and not struck out) against such person or any partnership in which such person was a partner or any corporation of which such person was a director or member of key senior management;
- (ii) disqualified from acting as a director of any corporation, or from taking part directly or indirectly in the management of any corporation;
- (iii) in the last 10 years, charged or convicted in a criminal proceeding or is a named subject of a pending criminal proceeding;
- (iv) in the last 10 years, any judgment was entered against such person, or finding of fault, misrepresentation, dishonesty, incompetence or malpractice on such person's part, involving a breach of any law or regulatory requirement that relates to the capital market;
- (v) in the last 10 years, being the subject of any civil proceeding, involving an allegation of fraud, misrepresentation, dishonesty, incompetence or malpractice on such person's part that relates to the capital market;
- (vi) the subject of any order, judgment or ruling of any court, government, or regulatory authority or body temporarily enjoining such person from engaging in any type of business practice or activity;
- (vii) in the last 10 years, has been reprimanded or issued any warning by any regulatory authority, securities or derivatives exchange, professional body or government agency; and
- (viii) any unsatisfied judgment against such person.

8.9 Family relationships and/or associates

Save for Fong Choong Fook who is the spouse of Goh Soon Sei, there is no other family relationship and/or association between any of our Promoters, substantial shareholders, Directors, key senior management and key technical personnel as at the LPD.

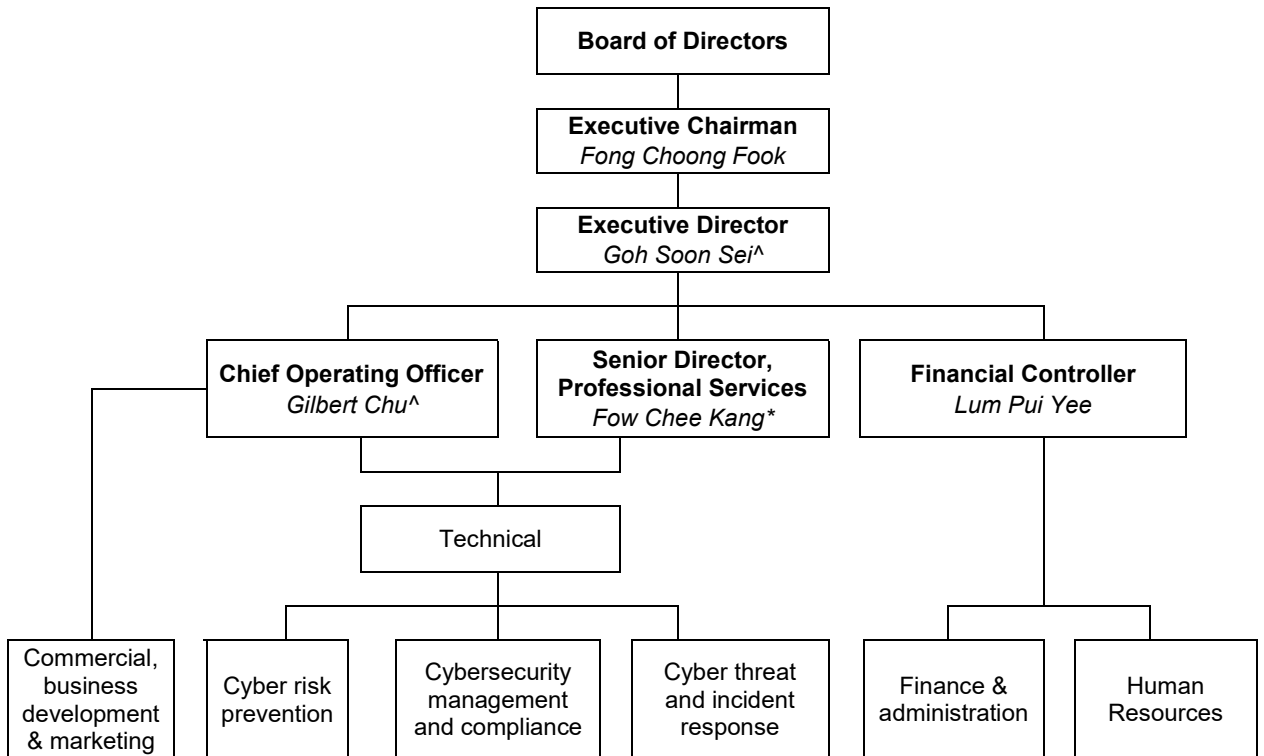
8.10 Service agreements

None of our Directors, key senior management or key technical personnel has any existing or proposed service agreement with our Group as at the LPD.

8. INFORMATION ON OUR PROMOTERS, SUBSTANTIAL SHAREHOLDERS, DIRECTORS, KEY SENIOR MANAGEMENT AND KEY TECHNICAL PERSONNEL (cont'd)

8.11 Management reporting structure

The management reporting structure of our Group is as follows:-



Notes:-

^ Goh Soon Sei and Gilbert Chu are responsible in overseeing the cybersecurity management and compliance segments of our Group.

* Fow Chee Kang is responsible to lead the technical teams in charge of cyber risk prevention and cyber threat and incident response only. He also oversees the research and development activities of our Group.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

9. RELATED PARTY TRANSACTIONS

9.1 Related party transactions

There are no existing and/or proposed related party transactions to be entered into by our Group which involve the interest, direct or indirect, of our Directors, substantial shareholders, and/or persons connected with them, for the past 4 FYEs 31 December 2018, 2019, 2020 and 2021 as well as the subsequent period up to the LPD.

Upon Listing, in the event our Group enters into any material related party transactions in accordance with the Listing Requirements, we will seek our shareholders' approval accordingly. However, if such related party transactions are deemed as recurrent related party transactions, we may then seek a general mandate from our shareholders to enter into these transactions without having to seek separate shareholders' approval each time our Group wishes to enter into such recurrent related party transactions during the validity period of the mandate.

In the event that there are any proposed related party transactions that require the prior approval of our shareholders, our Directors, substantial shareholders and/or persons connected with them, which have any interest, direct or indirect, in the transaction, will hence abstain from voting in respect of their direct and/or indirect shareholdings, if any. Such interested Directors and/or substantial shareholders will also undertake to ensure that the person(s) connected with them will abstain from voting on the resolution approving the proposed related party transaction at a general meeting of our Company.

In addition, our Audit Committee will, amongst others, review the terms of the related party transactions (if any) moving forward and report to our Board for further action to safeguard the interest of our Group and our minority shareholders, as well as to mitigate any potential conflict of interest situation. Further details on our monitoring and oversight practices in relation to related party transactions are set out in **Section 9.4** of this Prospectus.

9.2 Related party transactions that are unusual in their nature or conditions

Our Directors have confirmed that there are no transactions that are unusual in nature or conditions, involving goods, services, tangible or intangible assets, to which our Group was a party for the past 4 FYEs 31 December 2018, 2019, 2020 and 2021 as well as the subsequent period up to the LPD.

9.3 Outstanding loans and/or financial assistance (including guarantees of any kind) made to or for the benefit of related parties

9.3.1 Outstanding loans and/or financial assistance

Save as disclosed below, our Board has confirmed that there are no other outstanding loans and/or financial assistance that has been provided by our Group to or for the benefit of any related parties for the past 4 FYEs 31 December 2018, 2019, 2020 and 2021 as well as the subsequent period up to the LPD:-

Loan made to or for the benefit of related parties	Interested related party and nature of relationship	Nature of transaction and purpose	Outstanding amount as at 31 December				1 January 2022 up to the LPD
			2018	2019	2020	2021	
			(RM'000)	(RM'000)	(RM'000)	(RM'000)	(RM'000)
Advances made to Fong Choong Fook by LGMS	Fong Choong Fook is our Executive Chairman, substantial shareholder and Promoter	Advances	(1)268	(1)266	-	-	-

9. RELATED PARTY TRANSACTIONS (cont'd)**Note:-**

(1) *The said advances were fully paid as at the LPD.*

These advances were on an ad-hoc basis and are short term in nature and were for the said Director's personal investment purposes. As at the LPD, there are no outstanding advances made to our Directors. Moving forward, our Company will abstain from making such advances to our Directors.

9.3.2 Guarantees

Our Board has confirmed that there are no outstanding loans (including guarantees of any kind) and financial assistance that have been provided by our Group to or for the benefit of any related parties, for the past 4 FYEs 31 December 2018, 2019, 2020 and 2021 as well as the subsequent period up to the LPD.

Notwithstanding the above, our Executive Chairman and Promoter, Fong Choong Fook, had previously provided personal guarantees in respect of the hire purchase agreements financing the purchases of our Group's motor vehicles in the past 4 FYEs 31 December 2018, 2019, 2020 and 2021 as well as the subsequent period up to the LPD, details of which are set out in **Section 11.4.4** of this Prospectus. In respect thereof, our Company has undertaken to procure the withdrawal of the personal guarantees granted by Fong Choong Fook in connection with the above mentioned hire purchase agreements within 3 months from the date of the Listing, failing which, our Company shall ensure that the outstanding amounts under the said hire purchase agreements will be fully repaid and settled.

9.4 Monitoring and oversight of related party transactions**9.4.1 Audit Committee review**

Our Audit Committee review related party transactions and conflicts of interest situations that may arise within our Company or Group, including any transaction, procedures or course of conduct that raises questions of management integrity.

All reviews by our Audit Committee are reported to our Board for their further action. Where necessary, our Board will make the appropriate disclosure in our annual report with regard to any related party transaction (recurrent or one-off) entered into by us.

9.4.2 Our Group's policy on related party transactions

Related party transactions by their very nature, involve conflicts of interest between our Group and the related parties with whom our Group has entered into such transactions. It is the policy of our Group that all related party transactions in the course of business are carried out on an arm's length basis and on normal commercial terms which are not more favourable to the related parties than those generally available to third parties and these terms are not detrimental to the other shareholders of our Company who are not interested in the transaction.

In addition, we plan to adopt a comprehensive corporate governance framework that meets best practice principles to mitigate any potential conflict of interest situations and intend for the framework to be guided by the Listing Requirements and the Malaysian Code of Corporate Governance upon our Listing.

10. CONFLICT OF INTEREST

10.1 Interest in businesses which carry on similar trade as our Group or businesses of our customers or suppliers

As at the LPD, none of our Promoters, Directors or substantial shareholders has any interest, direct or indirect, in other businesses and corporations which are carrying on a similar trade as our Group or are customers or suppliers of our Group.

10.2 Declaration by advisers for our IPO**(i) Principal Adviser, Sponsor, Underwriter and Placement Agent**

UOBKH has given its confirmation that, as at the date of the Prospectus, there is no existing or potential conflict of interest in its capacity as the Principal Adviser, Sponsor, Underwriter and Placement Agent for our IPO.

(ii) Legal adviser

Rahmat Lim & Partners has given its confirmation that, as at the date of the Prospectus, there is no existing or potential conflict of interest in its capacity as the legal adviser for our IPO.

(iii) Auditors and reporting accountants

Baker Tilly Monteiro Heng PLT has given its confirmation that, as at the date of the Prospectus, there is no existing or potential conflict of interest in its capacity as the auditors and reporting accountants for our IPO.

(iv) Independent market researcher

Protégé has given its confirmation that, as at the date of the Prospectus, there is no existing or potential conflict of interest in its capacity as the IMR for our IPO.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

11. FINANCIAL INFORMATION

The historical financial information presented below for the past 4 FYE 31 December 2018 (“**FYE 2018**”), 31 December 2019 (“**FYE 2019**”), 31 December 2020 (“**FYE 2020**”) as well as 31 December 2021 (“**FYE 2021**”) have been extracted from the financial statements (“**Financial Statements**”) contained in the Accountants’ Report included in **Section 12** of this Prospectus. Our Financial Statements have been prepared in accordance with the MFRS and IFRS.

The following historical financial information should be read in conjunction with the management’s discussion and analysis of the financial condition and financial performance as set out in **Section 11.3** of this Prospectus and the Accountants’ Report as set out in **Section 12** of this Prospectus. There has been no audit qualification on our audited financial statements for the past 4 FYEs 2018, 2019, 2020 and 2021.

11.1 Historical statements of profit or loss and other comprehensive income

The following table sets out a summary of the audited financial information for the past 4 FYEs 2018, 2019, 2020 and 2021.

	Audited			
	FYE 2018	FYE 2019	FYE 2020	FYE 2021
	(RM'000)	(RM'000)	(RM'000)	(RM'000)
Revenue	17,387	20,563	20,649	28,262
Other income	523	526	1,725	361
Employee benefits expense	(4,912)	(6,143)	(6,195)	(8,335)
Information technology expenses	(1,701)	(2,053)	(1,787)	(2,114)
Depreciation expenses	(539)	(1,107)	(1,222)	(1,077)
Other operating expenses	(2,716)	(3,320)	(2,597)	(2,760)
Operating profit	8,042	8,466	10,573	14,337
Finance income	36	149	97	115
Finance costs	(60)	(174)	(168)	(132)
Share of results of associate, net of tax	-	-	109	(35)
PBT	8,018	8,441	10,611	14,285
Income tax expense	(2,027)	(2,112)	(2,537)	(3,980)
PAT	5,991	6,329	8,074	10,305
PAT attributable to:				
- Owners of the Company*	5,995	6,329	8,045	10,321
- Non-controlling interests	(4)	-	29	(16)
	5,991	6,329	8,074	10,305
EBITDA (RM'000) ⁽¹⁾	8,601	9,656	11,983	15,486
EBITDA margin (%) ⁽²⁾	49.47	46.96	58.03	54.79
Operating profit margin (%) ⁽³⁾	46.25	41.17	51.20	50.73
PBT margin (%) ⁽⁴⁾	46.11	41.05	51.39	50.54
PAT margin (%) ⁽⁵⁾	34.46	30.78	39.10	36.46
Effective tax rate (%)	25.28	25.02	23.91	27.86
No. of shares in issue after our IPO ('000)	456,000	456,000	456,000	456,000
Basic and diluted EPS (sen) ⁽⁶⁾	1.31	1.39	1.76	2.26

11. FINANCIAL INFORMATION (cont'd)**Notes:-**

* The Company had only completed the Acquisitions (which was part of the Pre-IPO Restructuring) on 30 August 2021.

(1) The table below sets out a reconciliation of our PBT to EBITDA:-

	Audited			
	FYE 2018	FYE 2019	FYE 2020	FYE 2021
	(RM'000)	(RM'000)	(RM'000)	(RM'000)
PBT	8,018	8,441	10,611	14,285
Adjusted for:-				
Finance costs	60	174	168	132
Interest income	(16)	(66)	(18)	(8)
Depreciation	539	1,107	1,222	1,077
EBITDA	8,601	9,656	11,983	15,486

(2) EBITDA margin is computed based on the EBITDA over revenue of our Group.

(3) Operating profit margin is computed based on the operating profit over revenue of our Group.

(4) PBT margin is computed based on the PBT over revenue of our Group.

(5) PAT margin is computed based on the PAT over revenue of our Group.

(6) Basic and diluted EPS is computed based on PAT attributable to the owners of our Company divided by the number of issued Shares of 456,000,000 after our IPO. There are no dilutive instruments as at the end of the respective financial years.

Historical statements of financial position

The following table sets out the audited statements of financial position for the past 4 FYEs 2018, 2019, 2020 and 2021.

	Audited			
	FYE 2018	FYE 2019	FYE 2020	FYE 2021
	(RM'000)	(RM'000)	(RM'000)	(RM'000)
ASSETS				
Non-current assets				
Property, plant and equipment	1,707	5,225	3,713	2,808
Investment properties	869	856	843	830
Investment in associate	-	-	109	74
Total non-current assets	2,576	6,081	4,665	3,712
Current assets				
Trade and other receivables	5,919	6,486	3,846	6,951
Other investments	1,519	3,036	3,115	4,361
Current tax assets	11	73	492	116
Cash and short term deposits	10,533	10,208	15,004	19,362
Total current assets	17,982	19,803	22,457	30,790
TOTAL ASSETS	20,558	25,884	27,122	34,502
Invested equity ⁽¹⁾	1,100	1,650	1,650	-
Share capital ⁽²⁾	-	-	1	22,300
Reorganisation reserve	-	-	-	⁽³⁾ (20,649)
Retained earnings	14,607	17,344	19,889	26,423
Non-controlling interests	(9)	-	173	-
TOTAL EQUITY / NA	15,698	18,994	21,713	28,074

11. FINANCIAL INFORMATION (cont'd)

	Audited			
	FYE 2018	FYE 2019	FYE 2020	FYE 2021
	(RM'000)	(RM'000)	(RM'000)	(RM'000)
Non-current liabilities				
Loans and borrowings	936	3,102	2,271	1,479
Contract liabilities	-	-	-	126
Deferred tax liabilities	137	82	69	9
Total non-current liabilities	1,073	3,184	2,340	1,614
Current liabilities				
Trade and other payables	2,868	2,887	2,253	2,737
Loans and borrowings	239	819	804	759
Contract liabilities	-	-	-	1,306
Current tax liabilities	680	#	12	12
Total current liabilities	3,787	3,706	3,069	4,814
TOTAL LIABILITIES	4,860	6,890	5,409	6,428
TOTAL EQUITY AND LIABILITIES	20,558	25,884	27,122	34,502

Notes:-

Denotes RM205.

- (1) For the purposes of combined statements of financial position, the invested equity as at the end of the respective FYE 2018, 2019 and 2020 represents the aggregate share capital of the combined entities constituting our Group prior to the Acquisitions in view that our current Group structure was only established on 30 August 2021.
- (2) Share capital represents the nominal value of the shares issued by LGMS Berhad.
- (3) Due to the completion of the Acquisitions (which was part of the Pre-IPO Restructuring) on 30 August 2021.

THE REST OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

11. FINANCIAL INFORMATION (cont'd)

11.2 Reporting Accountants' report on the compilation of the pro forma consolidated statement of financial position as at 31 December 2021



Baker Tilly Monteiro Heng PLT
201906000600 (LLP0019411-LCA)
Chartered Accountants (AF 0117)
Baker Tilly Tower
Level 10, Tower 1, Avenue 5
Bangsar South City
59200 Kuala Lumpur, Malaysia

T : +603 2297 1000
F : +603 2282 9980

info@bakertilly.my
www.bakertilly.my

22 April 2022

The Board of Directors
LGMS Berhad
A-11-01, Empire Office Tower
Jalan SS16/1
Subang Jaya
47500 Selangor

Dear Sirs,

LGMS BERHAD AND ITS SUBSIDIARIES

REPORTING ACCOUNTANTS' REPORT ON THE COMPILATION OF THE PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION AS AT 31 DECEMBER 2021 INCLUDED IN A PROSPECTUS

We have completed our assurance engagement to report on the compilation of the pro forma consolidated statement of financial position of LGMS Berhad ("LGMS" or "Company") and its subsidiaries, namely LE Global Services Sdn. Bhd., LGMS Advanced Tech Sdn. Bhd. (formerly known as LGMS Group Sdn. Bhd.), LGMS Academy Sdn. Bhd. and Credence Defender Sdn. Bhd. ("LGMS Group") for which the directors of LGMS are solely responsible. The pro forma consolidated statement of financial position consists of the pro forma consolidated statement of financial position as at 31 December 2021 together with the accompanying notes thereon, as set out in the accompanying statement, for which we have stamped for the purpose of identification. The applicable criteria on the basis of which the directors of LGMS have compiled the pro forma consolidated statement of financial position are as described in Note 2 to the pro forma consolidated statement of financial position and in accordance with the requirements of the *Prospectus Guidelines – Equity* issued by the Securities Commission Malaysia ("Prospectus Guidelines") ("Applicable Criteria").

The pro forma consolidated statement of financial position of LGMS Group has been compiled by the directors of LGMS, for illustrative purposes only, for inclusion in the prospectus of LGMS ("Prospectus") in connection with the listing of and quotation for the entire enlarged issued share capital of LGMS on the ACE Market of Bursa Malaysia Securities Berhad ("Listing"), after making certain assumptions and such adjustments to show the effects on the pro forma consolidated financial position of LGMS Group as at 31 December 2021 adjusted for the public issue and the utilisation of proceeds as described in Notes 1.2.2 and 3.2.1, respectively.

11. FINANCIAL INFORMATION (cont'd)**LGMS BERHAD AND ITS SUBSIDIARIES**

Reporting Accountants' Report on the Compilation of the
Pro Forma Consolidated Statement of Financial Position
as at 31 December 2021 Included in A Prospectus

As part of this process, information about LGMS Group's pro forma consolidated financial position has been extracted by the directors of LGMS from the audited financial statements of the LGMS Group.

The audited financial statements of the LGMS Group for the Financial Year Ended ("FYE") 31 December 2021 were reported by us to its members without any modifications.

Directors' Responsibility for the Pro Forma Consolidated Statement of Financial Position

The directors of LGMS are responsible for compiling the pro forma consolidated statement of financial position based on the Applicable Criteria.

Our Independence and Quality Control

We have complied with the independence and other ethical requirement of the *By-Laws (on Professional Ethics, Conduct and Practice)* issued by the Malaysian Institutes of Accountants and the International Ethics Standards Board for Accountants' *International Code of Ethics for Professional Accountants (including International Independence Standards)*, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our firm applies *International Standard on Quality Control 1 (ISQC 1), Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Reporting Accountants' Responsibilities

Our responsibility is to express an opinion, on whether the pro forma consolidated statement of financial position has been compiled, in all material respects, by the directors of LGMS based on the Applicable Criteria.

We conducted our engagement in accordance with *International Standard on Assurance Engagements (ISAE) 3420: Assurance Engagements to Report on the Compilation of Pro Forma Financial Information Included in a Prospectus*, issued by the International Auditing and Assurance Standards Board and adopted by the Malaysian Institute of Accountants. This standard requires that we plan and perform procedures to obtain reasonable assurance about whether the directors of LGMS have compiled, in all material respects, the pro forma consolidated statement of financial position based on the Applicable Criteria.

For the purpose of this engagement, we are not responsible for updating or reissuing any reports or opinions on any historical financial information used in compiling the pro forma consolidated statement of financial position, nor have we, in the course of this engagement, performed an audit or review of the financial information used in compiling the pro forma consolidated statement of financial position.

11. FINANCIAL INFORMATION (cont'd)**LGMS BERHAD AND ITS SUBSIDIARIES**

Reporting Accountants' Report on the Compilation of the
Pro Forma Consolidated Statement of Financial Position
as at 31 December 2021 Included in A Prospectus

Reporting Accountants' Responsibilities (Continued)

The purpose of the pro forma consolidated statement of financial position included in the Prospectus is solely to illustrate the impact of significant events or transactions on the unadjusted financial information of LGMS Group as if the events had occurred or the transaction had been undertaken at an earlier date selected for illustrative purposes only. Accordingly, we do not provide any assurance that the actual outcome of the events or transactions would have been as presented.

A reasonable assurance engagement to report on whether the pro forma consolidated statement of financial position has been compiled, in all material respects, based on the Applicable Criteria involves performing procedures to assess whether the Applicable Criteria used by the directors of LGMS in the compilation of the pro forma consolidated statement of financial position of LGMS Group provide a reasonable basis for presenting the significant effects directly attributable to Public Issue as described in Notes 1.2.2, to the pro forma consolidated statement of financial position, and to obtain sufficient appropriate evidence about whether:

- (a) The pro forma consolidated statement of financial position of LGMS Group has been properly prepared on the basis and assumptions set out in the accompanying notes to the pro forma consolidated statement of financial position, based on the audited financial statements of LGMS Group for the FYE 31 December 2021, and in a manner consistent with both the format of the financial statements and the accounting policies adopted by LGMS Group in the preparation of its audited financial statements for the FYE 31 December 2021; and
- (b) Each material adjustment made to the information used in the preparation of the pro forma consolidated statement of financial position is appropriate for the purpose of preparing the pro forma consolidated statement of financial position.

The procedures selected depend on our judgement, having regard to our understanding of the nature of LGMS Group, the events and transactions in respect of which the pro forma consolidated statement of financial position has been compiled, and other relevant engagement circumstances.

The engagement also involves evaluating the overall presentation of the pro forma consolidated statement of financial position.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

11. FINANCIAL INFORMATION (cont'd)



LGMS BERHAD AND ITS SUBSIDIARIES

Reporting Accountants' Report on the Compilation of the
Pro Forma Consolidated Statement of Financial Position
as at 31 December 2021 Included in A Prospectus

Our opinion

In our opinion:

- (a) the pro forma consolidated statement of financial position of LGMS Group has been properly prepared on the basis and assumptions set out in the accompanying notes to the pro forma consolidated statement of financial position, based on the audited financial statements of LGMS Group for the FYE 31 December 2021, and in a manner consistent with both the format of the financial statements and the accounting policies adopted by the LGMS Group in the preparation of its audited financial statements for the FYE 31 December 2021; and
- (b) each material adjustment made to the information used in the preparation of the pro forma consolidated statement of financial position of LGMS Group is appropriate for the purpose of preparing the pro forma consolidated statement of financial position.

Other matter

This report has been prepared for inclusion in the Prospectus in connection with the Listing. As such, this report should not be used, circulated, quoted or otherwise referred to in any document or used for any other purpose without our prior written consent. Neither the firm nor any member or employee of the firm undertakes responsibility arising in any way whatsoever to any party in respect of this report contrary to the aforesaid purpose.

Yours faithfully,

Handwritten signature of Robert Monteiro Heng in black ink.

Baker Tilly Monteiro Heng PLT
201906000600 (LLP0019411-LCA) & AF 0117
Chartered Accountants

Handwritten signature of Paul Tan Hong in black ink.

Paul Tan Hong
No. 03459/11/2023 J
Chartered Accountant

11. FINANCIAL INFORMATION (cont'd)

LGMS BERHAD AND ITS SUBSIDIARIES

PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION

1. INTRODUCTION

The pro forma consolidated statement of financial position of LGMS Berhad (“LGMS” or “Company”) and its subsidiaries (hereinafter collectively referred to as the “LGMS Group”) has been compiled by the directors of LGMS, for illustrative purposes only, for inclusion in the prospectus of LGMS in connection with the listing of and quotation for the entire enlarged issued share capital of LGMS on the ACE Market of Bursa Malaysia Securities Berhad (“Bursa Securities”) (“Listing”).

- 1.1 LGMS is undertaking a listing of and quotation for its entire enlarged issued share capital of RM67,997,500 comprising 456,000,000 new ordinary shares in LGMS on the ACE Market of Bursa Securities. The Listing comprises the following:

1.2 Listing Scheme

1.2.1 Offer for Sale

Offer for sale of 45,600,000 existing LGMS Shares at an indicative Offer Price of RM0.50 to be placed out to identified MITI approved Bumiputera investors.

1.2.2 Public Issue

The public issue of 91,395,000 new LGMS Shares at the initial public offering (“IPO”) price of RM0.50 per Share, representing approximately 20.04% of the enlarged number of shares of LGMS, to be allocated and allotted in the following manner:

- (i) 22,800,000 new Shares made available to the Malaysian public;
- (ii) 12,500,000 new Shares made available for application by the eligible directors and employees and persons who have contributed to the success of LGMS Group;
- (iii) 44,695,000 new Shares made available by way of private placement to selected investors; and
- (iv) 11,400,000 new Shares made available by way of private placement to identified MITI approved Bumiputera investors.

(Collectively hereinafter referred as “Public Issue”).

1.3 Listing

Admission to the official list and the listing of and quotation for the entire enlarged issued share capital of LGMS of RM67,997,500 comprising 456,000,000 Shares on the ACE Market of Bursa Securities.



11. FINANCIAL INFORMATION (cont'd)

LGMS BERHAD AND ITS SUBSIDIARIES

PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION

2. BASIS OF PREPARATION OF THE PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION (CONTINUED)

- 2.1 The pro forma consolidated statement of financial position has been prepared to illustrate the consolidated financial position of LGMS Group as at 31 December 2021, adjusted for the Public Issue and the utilisation of proceeds as described in Notes 1.2.2 and 3.2.1, respectively.
- 2.2 The audited financial statements of LGMS Group for the financial year under review were reported by the auditors to their respective members without any modifications.
- 2.3 The pro forma consolidated statement of financial position of LGMS Group have been prepared for illustrative purposes only and, such information may not, because of its nature, give a true picture of the actual financial position and the results of LGMS Group and does not purport to predict the future financial position and results of LGMS Group.
- 2.4 The pro forma consolidated statement of financial position of LGMS Group have been properly prepared on the basis set out in the accompanying notes to the consolidated statement of financial position based on the audited financial statements of LGMS Group for the FYE 31 December 2021, which have been prepared in accordance with the Malaysian Financial Reporting Standards and the International Financial Reporting Standards.



11. FINANCIAL INFORMATION (cont'd)**LGMS BERHAD AND ITS SUBSIDIARIES****3. PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION OF LGMS GROUP**

- 3.1 The pro forma consolidated statement of financial position of LGMS Group as set out below, for which the directors of LGMS are solely responsible, have been prepared for illustrative purposes only, to show the effects on the audited consolidated statement of financial position of LGMS Group as at 31 December 2021, had the Public Issue as described in Note 1.2.2 and the utilisation of proceeds as described in Note 3.2.1 been effected on that date, and should be read in conjunction with the notes accompanying thereto.

	Audited Statement of Financial Position as at 31 December 2021 RM'000	Pro Forma I After Offer for Sale RM'000	Pro Forma II After Pro Forma I and the Proposed Public Issue RM'000	Pro Forma III After Pro Forma II and the Proposed Utilisation of Proceeds RM'000
ASSETS				
Non-current assets				
Property, plant and equipment	2,808	2,808	2,808	2,808
Investment properties	830	830	830	830
Investment in associate	74	74	74	74
Total non-current assets	3,712	3,712	3,712	3,712
Current assets				
Trade and other receivables	6,951	6,951	6,951	6,951
Other investments	4,361	4,361	4,361	4,361
Current tax assets	116	116	116	116
Cash and short-term deposits	19,362	19,362	65,060	62,394
Total current assets	30,790	30,790	76,488	73,822
TOTAL ASSETS	34,502	34,502	80,200	77,534
EQUITY AND LIABILITIES				
Equity attributable to owners of the Company				
Share capital	22,300	22,300	67,998	66,364
Reorganisation reserve	(20,649)	(20,649)	(20,649)	(20,649)
Retained earnings	26,423	26,423	26,423	25,391
TOTAL EQUITY	28,074	28,074	73,772	71,106

Pro Forma Consolidated Statement of Financial Position



11. FINANCIAL INFORMATION (cont'd)**LGMS BERHAD AND ITS SUBSIDIARIES****3. PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION OF LGMS GROUP (CONTINUED)**

3.1 (Continued)

	Audited Statement of Financial Position as at 31 December 2021 RM'000	Pro Forma I After Offer for Sale RM'000	Pro Forma II After Pro Forma I and the Proposed Public Issue RM'000	Pro Forma III After Pro Forma II and the Proposed Utilisation of Proceeds RM'000
Non-current liabilities				
Loans and borrowings	1,479	1,479	1,479	1,479
Contract liabilities	126	126	126	126
Deferred tax liabilities	9	9	9	9
Total non-current liabilities	1,614	1,614	1,614	1,614
Current liabilities				
Trade and other payables	2,737	2,737	2,737	2,737
Loans and borrowings	759	759	759	759
Contract liabilities	1,306	1,306	1,306	1,306
Current tax liabilities	12	12	12	12
Total current liabilities	4,814	4,814	4,814	4,814
TOTAL LIABILITIES	6,428	6,428	6,428	6,428
TOTAL EQUITY AND LIABILITIES	34,502	34,502	80,200	77,534

Number of ordinary shares assumed to be in issue ('000)	364,605	364,605	456,000	456,000
---	---------	---------	---------	---------

NA [^] (RM'000)	28,074	28,074	73,772	71,106
NA per ordinary share (RM)	0.08	0.08	0.16	0.16
[^] attributable to owners of LGMS				

Pro Forma Consolidated Statement of Financial Position

11. FINANCIAL INFORMATION (cont'd)**LGMS BERHAD AND ITS SUBSIDIARIES****3. PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION OF LGMS GROUP (CONTINUED)**

3.2 Notes to the pro forma consolidated statement of financial position are as follows:

3.2.1 The proceeds from the Public Issue would be utilised in the following manner:

Purposes	RM'000	%	Estimated time frame for use (from the listing date)
Business expansion ⁽¹⁾	38,198	83.59	Within 12 to 24 months
Working capital	3,500	7.66	Within 12 months
Estimated listing expenses	4,000	8.75	Within 3 months
	<u>45,698</u>	<u>100.00</u>	

(1) As at the latest practicable date, the Company has yet to enter into any sales and purchase agreement in relation to the proceeds earmarked for purchase of office under business expansion. Accordingly, the utilisation of proceeds earmarked for capital expenditure are not reflected in the pro forma consolidated statement of financial position.

3.2.2 The pro forma consolidated statement of financial position should be read in conjunction with the notes below:

(a) Pro Forma I

Pro Forma I incorporates the effects of the adjustments for the Offer for Sale as described in Note 1.2.1.

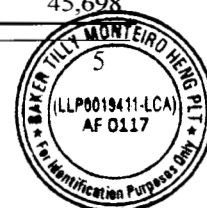
The Offer for Sale will not have an impact to the pro forma consolidated statement of financial position

(b) Pro Forma II

Pro Forma II incorporates the cumulative effects of Pro Forma I and the Public Issue as described in Note 1.2.2.

The Public Issue had the following impact on the audited consolidated statement of financial position of LGMS as at 31 December 2021:

	Increase	
	Effects on Total Assets RM'000	Effects on Equity RM'000
Cash and short-term deposits	45,698	-
Share capital	-	45,698
	<u>45,698</u>	<u>45,698</u>

Pro Forma Consolidated Statement of Financial Position

11. FINANCIAL INFORMATION (cont'd)**LGMS BERHAD AND ITS SUBSIDIARIES****3. PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION OF LGMS GROUP (CONTINUED)**

3.2 (Continued)

3.2.2 (Continued)

(c) Pro Forma III

Pro Forma III incorporates the cumulative effects of Pro Forma II and the utilisation of proceeds from the Public Issue.

The proceeds arising from the Public Issue earmarked for purchase of office under business expansion are not reflected in the pro forma consolidated statement of financial position as the Company has yet to enter into any sale and purchase agreement in relation to these capital expenditures.

As at 31 December 2021, out of the RM4.00 million, RM1.33 million had already been incurred and charged to the retained earnings account. As at the LPD, the entire amount incurred of RM1.33 million had been paid.

Out of the remaining estimated listing expense to be incurred of RM2.67 million, RM1.03 million will be charged to retained earnings account and RM1.63 million will be capitalized in the share capital account upon Listing as these are directly attributable expenses relating to the new issuance of shares.

The utilisation of proceeds will have the following impact on the pro forma consolidated statement of financial position of LGMS Group as at 31 December 2021:

	(Decrease)	
	Effects on Total Assets RM'000	Effects on Equity RM'000
Cash and short-term deposits	(2,666)	-
Share capital	-	(1,634)
Retained earnings	-	(1,032)
	(2,666)	(2,666)

11. FINANCIAL INFORMATION (cont'd)

LGMS BERHAD AND ITS SUBSIDIARIES

3. PRO FORMA CONSOLIDATED STATEMENT OF FINANCIAL POSITION OF LGMS GROUP (CONTINUED)

3.2 (Continued)

3.2.3 Movements in share capital and reserves are as follows:

	Share capital RM'000	Reorganisation reserve RM'000	Retained earnings RM'000
Audited statement of financial position of LGMS as at 31 December 2021	22,300	(20,649)	26,423
Arising from the Offer for Sale	-	-	-
Per Pro Forma I	22,300	(20,649)	26,423
Arising from the Public Issue	45,698	-	-
Per Pro Forma II	67,998	(20,649)	26,423
Arising from the utilisation of proceeds	(1,634)	-	(1,032)
Per Pro Forma III	66,364	(20,649)	25,391

3.2.4 Movements in cash and short-term deposits are as follows:

	RM'000
Audited statement of financial position of LGMS as at 31 December 2021	19,362
Arising from the Offer for Sale	-
Per Pro Forma I	19,362
Arising from the Public Issue	45,698
Per Pro Forma II	65,060
Arising from the Utilisation of Proceeds	(2,666)
Per Pro Forma III	62,394

Pro Forma Consolidated Statement of Financial Position



11. FINANCIAL INFORMATION (cont'd)

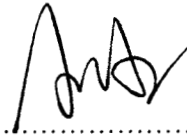
LGMS BERHAD AND ITS SUBSIDIARIES

APPROVAL BY BOARD OF DIRECTORS

Approved and adopted by the Board of Directors of LGMS Berhad in accordance with a resolution dated **22 APR 2022**



.....
Fong Choong Fook
Director



.....
Goh Soon Sei
Director

