MSIC N80 : SECURITY AND INVESTIGATION ACTIVITIES 2024

KEMENTERIAN SUMBER MANUSIA

OCCUPATIONAL FRAMEWORK

MSIC N80
SECTION N : ADMINISTRATIVE AND SUPPORT SERVICE ACTIVITIES
DIVISION 80 : SECURITY AND INVESTIGATION ACTIVITIES

Jabatan Pembangunan Kemahiran
Kementerian Sumber Manusia, Malaysia

Department of Skills Development
Ministry of Human Resources, Malaysia

OCCUPATIONAL FRAMEWORK

SECTION N: ADMINISTRATIVE AND SUPPORT SERVICE ACTIVITIES

DIVISION 80: SECURITY AND INVESTIGATION ACTIVITIES

First Printing 2024

Published in Malaysia by Department of Skills Development (DSD)

Level 7-8, Block D4, Complex D
Federal Government Administrative Centre
62530 Putrajaya, Malaysia
http://www.dsd.gov.my

Printed by
UPUM Resources Sdn. Bhd. (989963-D)
Aras 6, Kompleks Pengurusan Penyelidikan dan Inovasi,
Universiti Malaya, Wilayah Persekutuan Kuala Lumpur,
50603 Kuala Lumpur.
Tel: +603 7967 3556

Perpustakaan Negara Malaysia Cataloguing-in Publication Data

Occupational Framework
N80 – Security and Investigation Activities

ISBN 978-967-2393-31-3

TABLE OF CONTENT

CHAPTER V: DISCUSSION AND CONCLUSION

ABSTRACT

The escalating severity of safety concerns within the industrial sector underscores the imperative for the exploration conducted in this study. The primary goal of this research is to formulate an Occupational Framework (OF) tailored to N80. This comprehensive framework will encompass three distinct groups: private security activities, security systems service activities, and investigation activities. The research encompasses a diverse range of methodologies, including the application of the Design and Developmental Research (DDR) approach, meticulous document analysis, engrossing Focus Group Discussions (FGD), the strategic employment of the Fuzzy-Delphi method and active involvement from key players in the industrial domain through interview sessions. The DDR approach establishes the research's foundation, while the FGD sessions are designed to elicit qualitative insights into job domains and titles. The FGD sessions are divided into two distinct segments. The initial session centers on the identification of occupational structures (OS) and the corresponding responsibilities (OR). Subsequently, the second session focuses on developing occupational descriptions for high-demand roles. An exhaustive overview of the sector is furnished, elucidating its definition, scope, prevailing local dynamics, and industry trajectories. Close collaboration with industry luminaries and stakeholders guarantees that the OF accurately mirrors the sector's competency prerequisites. The first FGD, held on 19 and 20 August 2023, convened 10 experts hailing from the N80 industry. This session yielded delineation of fifteen domains encompassing N80 security and investigation activities, spanning all three N80 sector groups—group 801 private security activities, group 802 security systems service activities, and group 803 investigation activities. A total of 44 distinct job titles were identified across eight hierarchical levels, each aligned with the Malaysia Occupational Skills Qualification Framework (MOSQF) level descriptors. While some levels encompass multiple job titles, this stems from the overlap in duties and responsibilities, albeit with distinct applications. Although diverse in titles, these roles are unified under a single job title, considering the similarity in tasks. The job titles span from the pinnacle at level 8, denoted as Operation Director, to the base at level 1, titled Assistant Security Officer. The forthcoming OF is poised to serve as a foundational reference for the formulation of the National Occupational Skills Standard (NOSS) document. Furthermore, it will drive curriculum development across educational providers, spanning universities and training institutes alike.

ABSTRAK

Ketegasan yang meningkat berkaitan dengan kebimbangan keselamatan dalam sektor industri menekankan keperluan bagi penyelidikan yang dijalankan dalam kajian ini. Matlamat utama penyelidikan ini adalah untuk merumuskan Kerangka Pekerjaan (OF) yang disesuaikan untuk N80. Kerangka menyeluruh ini akan merangkumi tiga kumpulan yang berbeza: aktiviti keselamatan swasta, aktiviti perkhidmatan sistem keselamatan, dan aktiviti penyiasatan. Penyelidikan ini meliputi pelbagai metodologi, termasuk aplikasi pendekatan Penyelidikan Reka Bentuk dan Pembangunan (DDR), analisis dokumen yang teliti, Perbincangan Kumpulan Fokus yang menarik, penggunaan strategik kaedah Fuzzy-Delphi, dan penglibatan aktif dari pemain utama dalam domain industri melalui sesi temu ramah. Pendekatan DDR membentuk asas penyelidikan, manakala sesi FGD direka untuk mendapatkan pandangan kualitatif ke dalam domain dan jawatan kerja. Sesi FGD ini dibahagikan kepada dua bahagian yang berbeza. Sesi awal memberi tumpuan kepada pengenalan struktur pekerjaan (OS) dan tanggungjawab yang berkaitan (OR). Seterusnya, sesi kedua memberi tumpuan kepada pembangunan huraian pekerjaan untuk peranan permintaan tinggi. Satu tinjauan menyeluruh mengenai sektor diberikan, menjelaskan definisinya, ruang lingkupnya, dinamik tempatan yang dominan, dan trend industri. Kerjasama rapat dengan tokoh industri dan pihak berkepentingan menjamin bahawa OF mencerminkan dengan tepat keperluan kompetensi sektor. FGD pertama, diadakan pada 19 dan 20 Ogos 2023, menghimpunkan 10 pakar dari industri N80. Sesi ini menghasilkan penjelasan lima belas domain yang merangkumi aktiviti keselamatan dan penyiasatan N80, merentasi tiga kumpulan sektor N80—kumpulan 801 aktiviti keselamatan swasta, kumpulan 802 aktiviti perkhidmatan sistem keselamatan, dan kumpulan 803 aktiviti penyiasatan. Sejumlah 44 tajuk kerja yang berbeza dikenal pasti merentasi lapan tahap hierarki, setiap satu diselaraskan dengan penerangan tahap Kerangka Kelayakan Kemahiran Pekerjaan Malaysia (MOSQF). Walaupun beberapa tahap merangkumi beberapa tajuk kerja, ini disebabkan oleh tugas dan tanggungjawab yang tumpang tindih, walaupun dengan aplikasi yang berbeza. Walaupun berbeza dalam tajuk, peranan ini bersatu di bawah satu tajuk kerja tunggal, mengambil kira persamaan dalam tugas. Tajuk kerja merentasi dari tahap tertinggi pada tahap 8, yang dikenali sebagai Pengarah Operasi, kepada asas pada tahap 1, yang diberi tajuk Pegawai Keselamatan Pembantu. OF yang akan datang dijangka berfungsi sebagai rujukan asas untuk penyediaan dokumen Standard Kemahiran Pekerjaan Kebangsaan (NOSS). Tambahan pula, ia akan mendorong pembangunan kurikulum di institusi pendidikan, termasuk universiti dan institut Latihan.

LIST OF TABLES

LIST OF FIGURES

ABBREVIATION

Abbreviation	Definition
ABF	Australian Border Force
ACIC	Australian Criminal Intelligence Commission
AFP	Australian Federal Police
AG	Armed Guarding
AI	Artificial Intelligence
AM	Alarm Monitoring
APMM	Agensi Penguatkuasaan Maritim Malaysia
AR	Augmented Reality
ASIO	Australian Security Intelligence Organisation
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSTRAC	Australian Transaction Reports and Analysis Centre
AVSEC	Aviation Security
Bakamla	Indonesian Maritime Security Agency
BNPT	National Counter Terrorism Agency
BR1M	*Bantuan Rakyat 1Malaysia*
BSSN	National Cyber and Crypto Agency
BYOD	Bring Your Own Device
CAC	Cybersecurity Administration of China
CCTV	Closed-circuit Television
CISA	Cybersecurity and Infrastructure Security Agency
CM	Cash Management
CNB	Central Narcotics Bureau
CP	Close Protection

CRI	Cybersecurity Readiness Index
CSA	Cybersecurity Agency of Singapore
CV	Curriculum Vitae
CYOD	Choose Your Own Device
DDR	Design and Development Research
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
EEZ	Malaysia's Exclusive Economic Zone
FBI	Federal Bureau of Investigation
FDM	Fuzzy Delphi Method
FGD	Focus Group Discussion
GDP	Gross Domestic Product
GRI	Global Reporting Initiative
GS	Guarding Services
GCHQ	Government Communications Headquarters
HAZWMA	Hazardous Substances and Solid Waste Management Agency
HMRC	His Majesty’s Revenue & Customs
ICA	Immigration and Checkpoints Authority
ICT	Information and Communication Technologies
IoT	Internet of Things
IR4.0	Industrial Revolution
ISD	Internal Security Department
ISF	Internal Security Force
ISO	International Organization for Standardization
ILB	Industry Lead Body
JPK	*Jabatan Pembangunan Kemahiran*

JD	Job Description
K9	K9 Services
KDN	*Kementerian Dalam Negeri*
KPK	Indonesian Corruption Eradication Commission
MAF	Malaysian Armed Forces
MI5	Security Services
MI6	Secret Intelligence Service
MACC	Malaysian Anti-Corruption Commission
MAHB	Malaysia Airports Holdings Berhad
MASCO	Malaysia Standard Classification of Occupational
MC-R	Meta Cloud-Redirection
MIOSHA	Malaysian Occupational Safety and Health Association
MMEA	Malaysian Maritime Enforcement Agency
MOI	Ministry of Interior
MOHA	The Ministry of Home Affairs
MOHR	Ministry of Human Resources
MOSQF	Malaysia Occupational Skills Qualification Framework
MOT	Ministry of Transport Malaysia
MPS	Ministry of Public Security
MSIA	Malaysian Security Industry Association
MSIC	Malaysia Standard Industrial Classification
MSS	Ministry of State Security
MyCERT	Malaysian Computer Emergency Response Team
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NEP	New Economic Policy

NEM	New Economic Model
NOSS	National Occupational Skills Standard
OF	Occupational Framework
OR	Occupational Responsibilities
OS	Occupational Structure
OSH	Occupational Safety and Health
PAP	People's Armed Police
PDRM	*Polis Diraja Malaysia*
PIKM	*Persatuan Industri Keselamatan Malaysia*
PMSC	Private Maritime Security Companies
POLRI	Indonesian National Police
PSMB	*Pembangunan Sumber Manusia* Berhad
RMCD	Royal Malaysia Customs Department
RMN	Royal Malaysian Navy
RMP	Royal Malaysia Police
SIA	Security Industry Authority
SDGs	Sustainable Development Goals
SLA	Service Level Agreements
SME	Small Medium Enterprise
SCDF	Singapore Civil Defense Force
SPRM	*Suruhanjaya Pencegahan Rasuah Malaysia*
SPF	Singapore Police Force
SSB	State Security Bureau
SUHAKAM	Human Rights Commission of Malaysia
UNDP	United Nations Development Programme
USMS	U.S Marshals Services

GLOSSARY

Occupational Framework	A structured outline or plan tailored specifically for the N80 sector, outlining various job categories, roles, and responsibilities.
Private Security Activities	Engagements or tasks related to security concerns within privately-owned entities or sectors
Security Systems Service Activities	Tasks or services related to the installation, maintenance, or management of security systems within different sectors
Investigation Activities	Activities involving inquiries, fact-finding, or research typically related to security concerns or specific incidents.
Occupational Structures	The organizational layout or arrangement of job roles within a specific sector or framework
Responsibilities	Duties or tasks associated with specific job roles or positions
National Occupational Skills Standard (NOSS)	A document detailing the standard skills required for various occupations nationally
Malaysia Occupational Skills Qualification Framework	A framework used to classify and assess skills, qualifications, and job roles within Malaysia
Stakeholders	Individuals or groups with vested interests or involvement in a particular industry or sector
Industry Luminaries	Respected or influential figures within the industry known for their expertise and contributions

CHAPTER I

INTRODUCTION

1.1 Study Background

The Occupational Framework (OF), also known as *Kerangka Pekerjaan* in Malay, is a system used to classify types of jobs based on tasks, responsibilities, and other related criteria associated with those jobs. The OF helps provide a clearer understanding of various types of work and the relationships between these jobs within an organization or industry. The main purpose of the OF is to organize and group jobs into broader categories, enabling companies or organizations to assess and comprehend tasks across different job types, identify skills, education, and training requirements for each job type, compare salaries or wages among similar jobs, develop clear career paths, facilitate career mobility within the organization, and effectively plan human resource needs.

Typically, the OF consists of categories or classes of jobs that have similar or related tasks and responsibilities. Each job category in the OF is assigned a unique label or code for easy identification and reporting. For instance, within an organization, the OF might include job categories such as "Project Manager," "Data Analyst," "Human Resources Specialist," and others. In addition to aiding human resource management within organizations, the OF can also be used for macro-level labor market analysis, assisting government policy formulation in the labor field, and facilitating the exchange of job-related information across industries or countries. In some cases, the OF may be established by government authorities or specific industry bodies to ensure consistency and uniformity in job classification and understanding of the roles of these jobs within society and the economy.

1.2 Problem Statement

Problems related to OF requirements in the field of security and investigation in Malaysia involve challenges and changes that arise as a result of the industrial revolution and increasingly sophisticated technology. The industrial revolution led to the introduction of new technologies such as artificial intelligence, big data analysis, and automation. Security and investigation professionals in Malaysia need to master this technology to ensure they are able to manage, analyze, and deal with security threats and criminal incidents more effectively (Fuad, 2022). In today's rapidly evolving security landscape, security and investigation professionals in Malaysia need to master cutting-edge technology solutions to ensure they are

able to manage, analyze, and deal with security threats and criminal incidents more effectively. For instance, the use of advanced video analytics and facial recognition software can greatly enhance surveillance capabilities, enabling security personnel to swiftly identify and respond to potential threats in crowded public spaces, such as airports or shopping malls. Embracing modern cybersecurity tools and techniques is equally crucial, as they empower investigators to track and trace cybercriminals who may attempt to breach sensitive government or corporate networks. By staying abreast of technological advancements and integrating them into their practices, security and investigation experts can significantly bolster their ability to safeguard both public and private interests in an increasingly digitized world. With the advancement of technology, cyber threats and cybercrimes are increasing in Malaysia. Security investigators need to meet these new challenges with renewed cyber skills and the latest technology to protect sensitive information and respond to cyber threats quickly and efficiently.

OF in the form of artificial intelligence (AI) enables data analysis and security forecasting more accurately and quickly. However, the use of this technology also requires a skilled workforce in operating and administering this artificial intelligence system, as well as providing appropriate training for its use. The use of advanced technology in the field of security and investigation has implications for individual privacy. Problems related to data security and privacy protection may arise, and OF should ensure compliance with data security laws and regulations and the ethical use of such technology. With the introduction of new technologies, the need for continuous training and development of human resources in the field of security and investigation is increasingly important. This involves providing regular training and courses to ensure staff involved in security and investigations have relevant and up-to-date skills.

In the face of the industrial revolution and OF's needs in the field of security and investigation, Malaysia needs to undertake efforts to ensure that professionals in this field are equipped with the skills, technology, and knowledge required to deal with current challenges and threats effectively and efficiently. Improvement and adaptation to the latest technology will ensure the effectiveness of security and investigation in this country in the face of an increasingly complex and high-tech world.

In 1993, several countries, including the United States, Canada, France, Germany, the United Kingdom, and the Netherlands, collaborated to develop the "Common Criteria for Information Technology Security Evaluation". This initiative was adopted as the first international standard for assessing the security of information technology. The International Organization for Standardization (ISO) recognized and endorsed the Common Criteria. The

Common Criteria is composed of three main parts. First, it includes the basic criteria for evaluating the security of information systems and provides general assessment models. Second, it outlines security technical requirements that systems and equipment must meet. Finally, it encompasses security certification requirements, which include both technical and non-technical aspects. These requirements cover development processes and engineering processes, ensuring that security considerations are incorporated throughout the system's lifecycle. This means that it focuses more on management and process-oriented aspects of information security rather than providing detailed technical specifications and assessment methodologies (Hu et al., 2019).

To achieve the desired outcomes of local security and investigation and enhance the overall quality of security services, a collaborative effort involving government entities, industry stakeholders, and businesses is crucial. The collective focus must be redirected towards specific goals, including improving compliance-enforcement licensing practices and elevating the standards of accredited security services. This endeavor requires the active involvement of several key entities. Firstly, the government, represented by the Ministry of Home Affairs (MOHA) or *Kementerian Dalam Negeri (KDN)*, plays a vital role in providing the necessary regulatory framework and support. They are responsible for creating policies and guidelines that promote the employment of local security guards and ensure their qualifications, skills, and competence align with industry requirements. Secondly, the *Jabatan Pembangunan Kemahiran (JPK)* of the Ministry of Human Resources (MOHR) is responsible for developing the skills of local security guards. They play a crucial role in training programs, certification, and establishing competency standards to enhance the capabilities of the security workforce. Lastly, industry and business stakeholders, represented by the proposed Security Industry Lead Body (ILB), which is the *Persatuan Industri Keselamatan Malaysia (PIKM)*, need to actively participate in shaping the security industry. The ILB acts as a central authority responsible for setting industry standards, promoting best practices, and ensuring the overall quality of security services. Through the collaborative efforts of these entities, a comprehensive and effective approach can be established to address the challenges and elevate the standards of the security and investigation in Malaysian industry, ultimately benefiting both the security and the clients they serve.

Stakeholders required an extensive knowledge, skills, and regulations in security due to limited awareness, evolving nature of security, limited of training and expertise, fragmented or inconsistent regulations, limited resources, and resource constraints. To address these gaps, efforts should be made to enhance awareness, provide training and education programs,

streamline regulations, and ensure access to resources. Collaboration between stakeholders, industry professionals, and regulatory bodies can help close these knowledge and skill gaps and strengthen security practices (Samonas et al., 2020).

Definition of security and investigation is not properly defined in Malaysia. This is due to the factor of vague definition, limited scope, and citations. The indefinite of these definitions can result in ambiguity, making it challenging to precisely determine the roles and responsibilities of different agencies and stakeholders involved in security and investigation. Developing more detailed and precise definitions can help clarify these roles and facilitate better coordination among various entities. The limited scope of the definitions may not fully encompass the breadth of security and investigation activities in Malaysia. For instance, they may not adequately address emerging threats or areas like cybersecurity, which have become increasingly critical in the digital age. Expanding the scope to include these aspects is essential to reflect the current security landscape accurately. The definitions could benefit from referencing specific laws, regulations, and authoritative sources within the Malaysian legal framework. Citations provide a legal basis for these definitions and help ensure that they are aligned with the relevant legislation governing security and investigation practices in the country. Acknowledging recent developments and trends in security and investigation is crucial. These fields are continuously evolving and keeping pace with emerging threats and technological advancements is essential. By incorporating discussions of recent developments, the definitions can remain relevant and adaptable to changing circumstances.

Governments frequently collaborate with the private sector to enhance security and investigation capabilities, emphasizing information sharing as a crucial element. Through the exchange of relevant data and intelligence, both entities develop a comprehensive understanding of emerging threats, vulnerabilities, and evolving risk landscapes, aiding in early threat detection, rapid incident response, and the formulation of effective countermeasures. This collaboration is particularly vital in combating sophisticated cyber threats, leveraging the valuable insights of private sector organizations. Joint initiatives, such as task forces and research programs, harness the combined strengths and resources of government agencies and private companies, enhancing overall security measures and fostering a coordinated approach to risk mitigation. The pragmatic strategy of resource-sharing addresses the significant demands of security and investigation activities, allowing governments to leverage private sector expertise and technologies, while private entities benefit from government support. This collaborative synergy contributes to a more robust and resilient security infrastructure,

safeguarding critical assets and interests and advancing the overarching goal of maintaining national and global security.

In summary, while previous research has focused on the linguistic ambiguity of the content of a security policy (Buthelezi et al., 2016), as well as the perceptions of stakeholders regarding the effectiveness of the form of a security policy (Goel & Chengalur-Smith, 2010), there is very limited research on what stakeholders think of a security policy. The extent to which different stakeholders absorb the content of a security policy ultimately feeds into the iterative process of security policy development and maintenance (Goel & Chengalur-Smith, 2010). To this end, our paper heeds to the broader call of Cram et al. (2017) for research that examines the adjustments of security policy. Since stakeholder perceptions of a security policy are dynamic, we demonstrate how capturing the perceptions of stakeholders in regard to security policies through the use of the repertory grid technique can help organizations adjust their security policies to underscore key rules and/or clarify contentious issues.

1.3 Objective of Study

The objective of this research is to develop the Occupational Framework for the N80 which contains:

Phase 1:

a. To identify the needs of the current and future needs of the industry based on previous studies.

Phase 2:

a. To identify the job areas, job titles and job classifications according to the definitions and levels of Malaysian Occupational Skills Qualification Framework in N80
b. To identify the responsibilities and job descriptions for each job title.
c. To identify the critical job and the Job Description for N80 related to current developments in the industry
d. To analyse the competency needed to address the demand and supply of the security industry in Malaysia

Phase 3:

a. To document and validate the security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0.

1.4 N80 Study Scope

The research scope was referred from MSIC 2008 version 1.0. The details are explained below:

GROUP 801 (Private Security Activities)

Inclusion

Guards and patrols Services, picking up and delivering Money, receipts or other valuable items, Armoured Car Services, Bodyguard Services, Polygraph Services and security guard services

Exclusion

Public order and safety activities

GROUP 802 (Security Systems Service Activities)

Inclusion

Activity of selling, monitoring or remote monitoring of electronic security alarm system including maintenance Activity of selling, installing, repairing, rebuilding and adjusting mechanical or electronic locking devices, safe and security vaults

Exclusion

Installing of security system Selling security system, mechanical or electronic locking devices, sales, and security vaults, without monitoring installation, or maintenance services. Security consultants public order or safety activities providing key duplication services

GROUP 803 (Investigation Activities)

Inclusion

Activities of all private investigation, independent of the type of client or propose of investigation

1.5 Significance of Study for N80

1.5.1 Skills and Competencies Identification

An OF study helps identify the specific skills, competencies, and qualifications required for different job roles within a particular industry or profession. This information is invaluable for individuals planning their careers and for employers seeking to hire qualified candidates. Furthermore, an OF study not only defines the baseline skills but also highlights the evolving

and emerging competencies essential for staying relevant in a rapidly changing job market. This adaptability is crucial for individuals who wish to future-proof their careers and for employers aiming to maintain a competitive edge by attracting talent capable of addressing the industry's evolving challenges. As industries continue to innovate and transform, these studies serve as dynamic roadmaps that guide lifelong learning and skill development, benefiting both personal career trajectories and the long-term sustainability of businesses and sectors alike.

1.5.2 Employer Benefits

Employers benefit from an OF study as it helps them identify the qualifications and competencies needed when hiring new employees. This reduces the risk of hiring individuals who may not have the necessary skills for the job. Moreover, the insights derived from an OF study extend beyond initial hiring decisions. Employers can leverage this valuable information to design targeted training and professional development programs for their existing workforce. By aligning these programs with the identified qualifications and competencies, companies can continuously upskill and reskill their employees, ensuring that their teams remain adaptable and capable of meeting evolving industry demands. This proactive approach to talent development not only enhances job satisfaction but also bolsters employee retention rates, ultimately contributing to a more stable and high-performing workforce.

1.5.3 Policy Development

Policymakers can use the study's findings to inform labour market policies and workforce development strategies. It provides valuable data on industry trends, needs, and potential areas for government intervention. Furthermore, the data generated by an Occupational Framework study serves as a robust foundation for evidence-based policymaking. Policymakers can leverage this comprehensive understanding of industry requirements to craft targeted initiatives that promote job growth, economic stability, and competitiveness. Whether through funding vocational education programs aligned with identified skill gaps or incentivizing industry-specific research and development, these policies can foster innovation and resilience within key sectors. Additionally, by closely monitoring the evolving trends and needs highlighted in the study, policymakers can enact timely interventions to address labour market challenges, ensuring that the workforce remains responsive to the ever-changing dynamics of the global economy.

1.5.4 Safety and Regulation

In professions where safety is paramount, the study helps establish safety standards and ensures that individuals in these roles are trained to maintain safety protocols, contributing to overall safety in the workplace. Moreover, the OF study plays a vital role in maintaining the highest safety standards within safety-critical professions. By meticulously defining the required safety competencies and qualifications, it acts as a cornerstone for regulatory bodies and industry associations to develop and enforce safety protocols. This not only safeguards the well-being of workers but also enhances public safety and confidence in industries such as healthcare, aviation, and nuclear energy. The study's emphasis on continuous training and certification within these roles ensures that safety professionals remain up-to-date with the latest advancements and best practices, reducing the likelihood of accidents and incidents that could have far-reaching consequences for both workers and the broader community.

1.6 Operational Definition

1.6.1 Private Security Activities

The activities within this group encompass a wide range of services dedicated to investigation, supervision, guarding, and safeguarding both individuals and property. This includes tasks such as providing personal security as bodyguards, conducting road patrols, safeguarding various types of premises such as buildings, offices, factories, and hotels, and engaging in specialized investigative work like fingerprint analysis, signature verification, and handwriting examination.

1.6.2 Security Systems Service Activities

For activities in monitoring electronic security alarm systems, which include burglar and fire alarms, as well as handling their installation and maintenance, these entities are responsible for installing, repairing, refurbishing, and fine-tuning mechanical or electronic locking mechanisms, safes, and security vaults, all in conjunction with subsequent monitoring and remote surveillance.

1.6.3 Investigation Activities

Security-related services encompass a wide spectrum of offerings, including investigation as well as the secure transportation of valuable items with dedicated personnel and specialized equipment to ensure their protection during transit. Additionally, these entities are involved in the operation of electronic security alarm systems, specializing in remote monitoring, while

often providing comprehensive services that encompass the sale, installation, and repair of such systems.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

A study of OF security and investigation activities based on the need for control and safety systems in the industry. Several previous studies have been gathered to obtain information about OF produced both domestically and internationally. Various reference sources supporting this study are discussed in this section.

2.1.1 Sustainable Development Goals (SDGs)

The United Nations Development Programme (UNDP) operates in approximately 170 countries and territories, with a primary mission to combat poverty, reduce inequalities, foster inclusion, and enhance resilience in order to enable sustained progress. As a principal development agency, UNDP plays a pivotal role in supporting countries in their pursuit of the SDGs, also known as the Global Goals. These goals serve as a universal call to action, encompassing poverty eradication, environmental protection, and the promotion of peace and prosperity for all.

One of the specific SDG 11 centres on Sustainable Cities and Communities. With over half of the world's population residing in urban areas and an anticipated two-thirds urbanization rate by 2050, it is imperative to fundamentally transform urban development practices. The rapid expansion of cities, especially in developing regions, has led to the emergence of mega-cities and an increase in slums. Achieving sustainability in cities necessitates the creation of job and business opportunities, affordable and secure housing, and the establishment of resilient societies and economies. This transformation involves investments in public transportation, the creation of green public spaces, and the enhancement of participatory and inclusive urban planning and management.

The concept of creating an environment for future generations in the context of *Pelan Induk Industri Malaysia* involves a visionary approach that seeks to harmonize economic growth with ecological responsibility. By emphasizing the importance of sustainability in industrial development, this plan recognizes that a thriving economy and a healthy environment are not mutually exclusive but are, in fact, interdependent. It envisions an industrial landscape where innovation and environmental stewardship go hand in hand, fostering a legacy of

prosperity and ecological resilience that can be passed down to our children and grandchildren. This holistic perspective acknowledges the critical role that industries play in shaping the future and underscores the responsibility to safeguard the planet for generations yet to come. The integration of *Pelan Induk Industri Malaysia* able to integrate environmental education and awareness programs into the industrial sector to ensure that workers and stakeholders understand the importance of sustainable practices and their role in preserving the environment for future generations. In addition, the involvement of local communities in decision-making processes related to industrial development, particularly in areas where new industrial projects are planned. It promotes social acceptance and can help address community concerns regarding environmental impacts. This initiative aligns with Environmental Sustainability Goal (ESG), which aims to enhance the quality of human life while minimizing undue pressure on the earth's supporting ecosystems. Monitoring and reporting in ESG are crucial aspects of ensuring accountability, transparency, and progress towards a more sustainable future. The implementation of regular monitoring and reporting mechanisms to assess the environmental performance of industries operating under the master plan. Transparency in reporting environmental data is crucial for accountability. Planning and reporting index required a comprehensive structure to ensure the transparency and sustainability of organization. For instance, Global Reporting Initiative (GRI) provides a widely accepted framework for sustainability reporting, emphasizing transparency, accountability, and stakeholder engagement. Additionally, Bursa Malaysia, as a stock exchange, may have specific reporting requirements related to sustainability and corporate responsibility.

Malaysia, situated in Southeast Asia, boasts a population of approximately 33.37 million. Security services, when aligned with a human rights-based approach, play a foundational role in promoting social and economic development and safeguarding sustainability endeavours. Only robust and legitimate institutions are capable of addressing and mitigating the evolving security challenges characterized by violence, crime, and terrorism, often exacerbated by weak governance, limited resilience, and the impacts of climate change. In this context, the concept of human security offers an integrated and multidimensional framework that advocates for a people-centric approach to security systems. UNDP is actively exploring methods to incorporate this approach into its programming efforts, focusing on the synergies between top-down and bottom-up strategies, facilitating support to both state and non-state security actors, and advancing inclusivity and local ownership in security initiatives.

The Global Programme uniquely combines rule of law, justice, security, and human rights within an overarching umbrella framework, focused on preventing and responding to crisis, conflict and fragility through quality programming, knowledge brokerage and thought leadership, and policy support. The Global Programme's Phase IV commenced in 2022 and is guided by and aligned to the UNDP Strategic Plan for 2022-2025. The programme promotes people-centred and human rights-based approaches to addressing the drivers and symptoms of inequality, exclusion, injustice and insecurity, and accelerating progress towards the 2030 Agenda for Sustainable Development.

Figure 2.1: SDG 16 (Peace, Justice and Strong Institutions) (https://www.un.org/)

SDG 16 places a strong emphasis on promoting peace, justice, and robust institutions. Sustainable development hinges on the foundation of peace, stability, the safeguarding of human rights, and the establishment of effective governance guided by the rule of law. However, our world is becoming increasingly fragmented. While some regions experience peace, security, and prosperity, others find themselves trapped in seemingly endless cycles of conflict and violence. This situation is not inevitable and demands our immediate attention. Armed violence and insecurity exert a devastating toll on a nation's development, hampering economic growth and often leading to grievances that persist for generations. Sexual violence, crime, exploitation, and torture thrive in regions plagued by conflict or a lack of adherence to the rule of law. It is imperative for countries to take measures to protect those who are most vulnerable. The SDGs aspire to substantially diminish all forms of violence, collaborating with governments and communities to bring an end to conflict and insecurity. Central to this endeavour is the promotion of the rule of law and human rights. Simultaneously, efforts must be made to reduce the illicit arms trade and empower developing nations to participate more actively in global governance institutions.

Within the Job Street portal, there are over 3,500 job opportunities closely related to security and investigation activities. Each of these job opportunities is offered by various companies. However, every job title offered has different qualifications based on each company's requirements. Therefore, the Department of Skills Development needs to provide an OF related to Security and Investigation activities for reference by employers to have clear guidelines for each offered job title.

2.1.2 Value Chain

The value chain in Security and Investigation activities is of utmost importance to the Malaysian government as it underpins national security, economic stability, and international relations. A robust security and investigation sector ensures the safety of the nation, instils confidence in businesses and investors, and promotes economic growth. It is essential for safeguarding the tourism industry, maintaining good diplomatic relations, upholding the rule of law, protecting data and privacy, managing disasters, combating terrorism, and securing borders. In essence, this value chain is the linchpin that supports the government's efforts to ensure the well-being of its citizens, foster economic prosperity, and maintain a secure and stable environment in an increasingly interconnected and complex world.

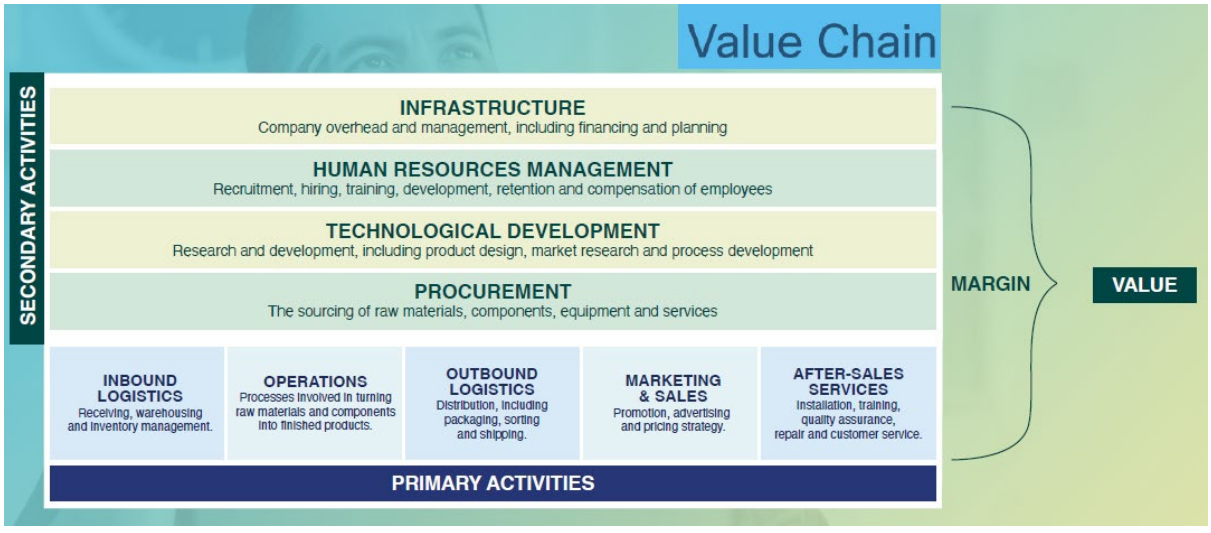

Figure 2.2: Value chain in Security and Investigation Activities

Within the framework of the value chain for security and investigation activities, Human Resource Management is a crucial aspect considered in the development of an occupational framework. This is done to ensure that job areas and job titles are specifically

tailored to focus on skill development. In simpler terms, Human Resource Management is an essential component in creating a structured plan that outlines the roles and responsibilities within the security and investigation sector. This framework helps ensure that the skills required for different job positions are well-defined and can be developed effectively. It plays a pivotal role in aligning the workforce with the specific needs and objectives of the security and investigation activities, ultimately contributing to their efficiency and effectiveness.

2.2 Scope Based on MSIC 2008

2.2.1 Private Security Activities (N801)

According to MSIC (2008), activities within the realm of private security include agencies providing one or more activities such as control and patrols, the handling and transportation of money, receipts or valuables with personnel and equipment to ensure protection during travel (e.g., armoured car services, personal guard services, polygraph services, fingerprinting services, and security guard services).

Personal guards, often known as executive protection specialists or bodyguards, are trained to provide physical security and ensure the safety of their clients. Their expertise extends beyond merely safeguarding clients; they are highly skilled in threat assessment, risk mitigation, and crisis management. These security professionals often undergo rigorous training in defensive tactics, emergency medical response, and advanced driving techniques. Whether accompanying clients during international travel, high-profile public appearances, or routine day-to-day activities, their presence offers more than just physical protection. They also act as a deterrent to potential threats, employing a combination of situational awareness and advanced security protocols to maintain a secure environment for their clients. Their commitment to safeguarding the well-being and reputation of their clients is unwavering, and they are prepared to respond swiftly and decisively in any situation that may compromise their clients' safety.

Before providing personal guard services, security firms conduct comprehensive risk assessments to identify potential threats and vulnerabilities. This assessment informs the development of a customized security plan tailored to the unique needs and circumstances of each client. These risk assessments often involve a thorough analysis of the client's daily routines, travel itineraries, and personal or professional associations that may pose security concerns. By carefully evaluating these factors, security experts can anticipate potential risks and devise strategies to mitigate them effectively. The resulting security plan encompasses a range of measures, such as route planning, secure transportation arrangements, communication

protocols, and contingency plans for various scenarios. This meticulous approach not only ensures that clients receive the highest level of protection but also allows for flexibility in adapting security measures to changing circumstances, guaranteeing that the client's safety always remains a top priority.

Each client's security needs are unique, and private security firms recognize the importance of personalized service. They work closely with clients to develop tailored security plans that address specific concerns and risks, taking into account factors like location, schedule, and personal preferences. This collaborative approach involves open communication between the security team and the client, allowing for the seamless integration of security measures into the client's lifestyle. For example, if a client frequently travels to regions with heightened security risks, the security plan may include travel advisories, secure transportation arrangements, and local contacts for immediate assistance. Additionally, the plan can be adjusted as circumstances change or as the client's needs evolve over time. This commitment to customization ensures that clients receive security solutions that align precisely with their requirements, allowing them to maintain their daily routines and activities with a heightened sense of security and confidence.

Personal guards may employ a range of security measures, including close protection, access control, and surveillance, to ensure the safety of the client. Close protection involves maintaining a close physical presence to deter potential threats and provide immediate assistance if necessary. Access control measures are implemented to restrict entry to designated areas, ensuring that only authorized individuals can approach the client. Surveillance techniques, both overt and covert, are utilized to monitor surroundings for potential risks or unusual activity. These security professionals are extensively trained in crisis response, including emergency medical care and evacuation procedures, enabling them to respond swiftly and effectively in case of emergencies or security breaches. Whether it's addressing medical emergencies, managing security threats, or executing quick evacuations, personal guards are equipped with the skills and knowledge to protect their clients with the utmost professionalism and competence. Their unwavering commitment to their clients' safety is a hallmark of their profession, providing peace of mind in even the most challenging situations.

Private security firms offering personal guard services must operate within the boundaries of local laws and regulations, and they place a paramount emphasis on legal compliance. Security personnel undergo comprehensive training to ensure they have a deep understanding of the legal requirements and ethical standards relevant to their services. This includes knowledge of laws related to the use of force, firearms regulations, privacy rights, and

relevant permits or licenses. Private security firms often collaborate closely with law enforcement agencies and legal experts to stay updated on evolving regulations and ensure their operations align with the latest legal standards. By adhering strictly to legal requirements, these firms not only protect their clients but also uphold the integrity and professionalism of their industry, fostering trust and confidence in their services within the legal framework. Clients can have peace of mind knowing that their protection is not only effective but also carried out with the highest regard for the law and ethical standards.

The primary goal of these security activities is to provide clients with peace of mind, knowing that their assets are under constant vigilance and protection throughout their journey. Private security firms understand that trust is paramount in their line of work, and they go to great lengths to establish and maintain it. They often engage in ongoing dialogue with their clients, keeping them informed about security measures, sharing real-time updates, and addressing any concerns promptly. Beyond safeguarding physical assets, these security professionals also prioritize the well-being and safety of those involved in the transportation process, whether it's employees, drivers, or passengers. By delivering a comprehensive security solution that goes beyond physical protection, these firms build strong and lasting relationships with their clients, reinforcing the assurance that their assets are in capable hands from start to finish. This level of dedication to service underscores the peace of mind clients experience when entrusting their valuable assets to transportation security experts.

2.2.2 Security System Service Activities (N802)

According to MSIC (2008), activities within Security System Service include (a) sales, monitoring, or remote-control supervision through security alarm systems (e.g., theft and fire alarms), including maintenance, and (b) sales, installation, repair, reconstruction, and alignment of mechanical or electronic locking devices, safes, and safety deposit boxes. Activities within the Security System Service sector encompass a wide range of functions. These activities not only include sales, monitoring, or remote-control supervision through security alarm systems but also extend to the installation and maintenance of security equipment. Sales professionals within the sector work closely with clients to assess their security needs, recommend appropriate solutions, and provide guidance on system options. Monitoring and remote-control supervision involve the continuous surveillance of security alarm systems, which may include intrusion detection, fire alarms, and CCTV systems, among others. Highly trained operators and technicians are responsible for monitoring these systems around the clock, ensuring rapid response to any alarms or incidents. Their vigilance and

immediate response capabilities are essential in minimizing risks and potential damages. Additionally, the integration of cutting-edge technology, such as artificial intelligence and data analytics, is becoming increasingly common in security system monitoring, further enhancing the efficiency and effectiveness of these services. Together, these activities play a vital role in safeguarding individuals and organizations, providing comprehensive security solutions that offer both proactive protection and rapid response when needed.

These activities ensure that security breaches or emergencies are promptly detected, and the appropriate response is initiated. Additionally, the installation and maintenance of security equipment are vital to keeping systems in optimal working condition, ensuring that they remain reliable and effective over time. Experienced technicians are responsible for the proper installation and configuration of security systems, ensuring that all components function seamlessly together. Beyond the initial installation, routine maintenance is critical to prevent system malfunctions and vulnerabilities. Maintenance tasks may include software updates, hardware inspections, and testing of alarm triggers to guarantee that the security system performs at its best. Regularly scheduled maintenance not only enhances the longevity of the equipment but also helps identify and rectify potential issues before they become major concerns. This proactive approach minimizes system downtime and maintains the integrity of security measures. Security service providers often offer service level agreements (SLAs) to ensure prompt response and resolution times for maintenance requests, thereby upholding the overall effectiveness of the security infrastructure. In this way, the installation and maintenance of security equipment serve as the backbone of reliable security systems, contributing to the safety and peace of mind of those they protect. This comprehensive range of services within the Security System Service sector plays a critical role in safeguarding people, property, and assets, providing peace of mind to individuals and organizations alike.

Activities within the Security System Service sector encompass a wide spectrum of services. In addition to sales, installation, repair, reconstruction, and alignment of mechanical or electronic locking devices, safes, and safety deposit boxes, these services often involve advanced security consultations and assessments. Security professionals assess the security needs of businesses, institutions, or individuals, providing expert advice on selecting the most suitable security solutions. This may include recommending access control systems, biometric authentication measures, or security system upgrades to enhance overall safety. The installation, repair, and maintenance of mechanical and electronic locking devices are essential for maintaining the integrity of physical security measures, such as door locks, vaults, and secure access points. Whether it's installing a high-security electronic access control system for

a corporate facility or repairing a home safe, these services are instrumental in protecting valuable assets and confidential information. The Security System Service sector's multifaceted approach ensures that clients receive tailored security solutions that encompass both traditional and cutting-edge technologies, offering comprehensive protection against potential threats.

2.2.3 Investigation Activities (N803)

According to MSIC (2008), investigation activities encompass a wide range of services, including private investigation activities that are open to all types of clients or investigative purposes. Private investigators play a crucial role in gathering information, uncovering facts, and conducting research on behalf of individuals, businesses, or legal entities. These professionals are adept at conducting thorough background checks, locating missing persons, and uncovering evidence for various purposes, including legal cases, due diligence in business transactions, or personal matters. Private investigation services can be tailored to address specific client's needs, offering a wide array of specialized services that cater to a diverse range of scenarios. For instance, private investigators can be instrumental in exposing insurance fraud by meticulously examining claims, conducting surveillance, and collecting evidence that can be crucial in legal proceedings. In marital or domestic cases, they play a vital role in conducting discreet surveillance to uncover potential infidelity or gather evidence for child custody disputes. Moreover, private investigators often collaborate with legal professionals, providing essential litigation support by gathering evidence, conducting witness interviews, and assisting in case preparation.

Whether it is safeguarding a company's interests by conducting corporate investigations, helping individuals navigate personal challenges such as locating missing family members, or assisting in complex legal matters like criminal defense investigations, private investigation services are known for their versatility and adaptability. These services cater to a wide spectrum of client needs and can extend to areas such as background checks, asset searches, due diligence investigations for business transactions, or even intellectual property protection. Private investigators are skilled at employing a combination of traditional investigative techniques and cutting-edge technology to provide clients with actionable insights and evidence. Their ability to offer personalized and precise assistance ensures that clients receive the support necessary to address their unique circumstances and concerns effectively. As trusted professionals with a deep understanding of legal and ethical standards, private investigators offer a valuable resource for individuals, businesses, and legal professionals seeking clarity, information, and resolution in a variety of situations.

These services operate within the boundaries of legal and ethical guidelines, adhering to strict codes of conduct and confidentiality to ensure the protection of clients' interests and privacy. Private investigators are typically licensed professionals who are well-versed in the laws and regulations governing their field. They prioritize ethical conduct and transparency, ensuring that their investigative methods are not only effective but also respectful of individuals' rights and privacy. Maintaining confidentiality is paramount, as they understand the sensitive nature of the information they handle. The versatility of private investigation activities makes them invaluable for a diverse range of clients seeking to uncover the truth or gather critical information for their unique purposes. Whether it is a concerned spouse looking for answers, a business owner safeguarding their assets, or an attorney building a strong case, private investigators provide an ethical, lawful, and discreet means to pursue truth and justice while upholding the highest standards of professionalism and integrity.

2.3 The Salary in Malaysia

Gross Domestic Product (GDP) by kind of economic activity at constant prices refers to a specific measure of a country's economic performance that provides a detailed breakdown of the value of goods and services produced within the country over a certain period. GDP is a comprehensive measure of a nation's overall economic activity. It represents the total value of all goods and services produced within the borders of a country over a specified period, typically a year. GDP is being analyzed and presented based on different sectors or types of economic activities. Economic activities are broadly categorized into sectors such as agriculture, manufacturing, construction, services, etc. Constant prices are an important aspect that adjusts the GDP for inflation or deflation. Constant prices are used to remove the effects of price changes over time, allowing for a more accurate assessment of real economic growth or contraction. It helps to isolate the changes in the physical volume of goods and services produced from the impact of changing prices. In this context, the data and figures are specific to Malaysia, and the analysis is focused on the economic activities within the borders of Malaysia.

GDP by kind of economic activity at constant prices in Malaysia between 2015 to 2022 was presented in Table 2.1. Data was presented according to the state. The GDP covered agriculture, mining and quarrying, manufacturing, construction, services and import duties sectors. The data indicates an increasement of constant prices starting from 2015 until 2019 in

every state and a decline in 2020. The decrease in constant prices in 2020 was caused by the impact of the rapidly spreading COVID19 infection during that year. However, constant prices have since risen again in 2021 and 2022.

Table 2.1: Gross Domestic Product by Kind of Economic Activity at Constant Prices in Malaysia (2015-2022)

State	Gross Domestic Product by Kind of Economic Activity							
	RM (Million)							
	2015	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Johor	110,002	116,682	123,561	130,586	134,226	128,074	131,303	142,056
Agriculture	15,610	15,030	16,170	16,246	16,403	16,857	16,980	17,304
Mining and Quarrying	476	569	656	711	813	658	587	631
Manufacturing	32,359	34,122	36,465	38,338	40,125	38,651	40,727	42,949
Construction	7,269	8,978	8,407	9,217	6,700	4,176	3,424	3,967
Services	53,058	56,266	59,999	64,402	68,577	66,406	68,316	75,672
Plus: Import Duties	1,230	1,717	1,864	1,672	1,609	1,327	1,269	1,533
Kedah	39,550	41,156	43,067	44,804	46,841	46,042	47,511	50,937
Agriculture	5,423	5,202	5,465	5,468	5,646	5,518	5,667	5,614
Mining and Quarrying	83	96	110	115	125	112	103	111
Manufacturing	11,427	11,934	12,449	12,827	13,430	13,619	14,465	15,633
Construction	863	998	928	1,009	1,090	1,113	1,019	1,206
Services	21,465	22,604	23,808	25,104	26,327	25,434	25,933	28,024
Plus: Import Duties	288	322	306	281	224	248	324	349
Kelantan	21,408	22,476	23,501	24,143	25,479	25,188	25,797	26,894
Agriculture	5,102	5,287	5,477	5,431	5,814	5,818	5,888	5,601
Mining and Quarrying	229	257	300	359	417	342	353	382
Manufacturing	1,147	1,172	1,278	1,281	1,300	1,234	1,260	1,299
Construction	445	575	521	324	383	396	401	480
Services	14,455	15,159	15,899	16,721	17,535	17,374	17,862	19,086
Plus: Import Duties	30	25	26	26	30	24	33	45
Melaka	36,077	37,713	40,830	42,376	43,583	41,030	41,900	45,488
Agriculture	4,141	4,312	4,625	4,567	4,433	4,584	4,556	4,526
Mining and Quarrying	44	53	57	62	68	59	55	60
Manufacturing	14,068	14,626	15,621	16,335	16,745	15,322	15,835	16,905
Construction	947	998	1,720	1,496	1,358	992	897	943
Services	16,811	17,655	18,613	19,731	20,918	19,970	20,497	22,988
Plus: Import Duties	66	68	194	185	62	104	59	67
Negeri Sembilan	40,186	41,771	43,816	45,694	48,034	46,336	47,783	50,840
Agriculture	3,235	3,056	3,321	3,323	3,557	3,319	3,306	3,287
Mining and Quarrying	165	198	217	224	236	200	186	201
Manufacturing	15,678	16,133	16,654	17,208	17,630	16,761	17,962	19,394
Construction	1,339	1,466	1,716	1,916	1,843	1,370	1,366	1,445
Services	18,951	19,976	20,916	22,126	24,037	23,822	24,352	26,195

State	Gross Domestic Product by Kind of Economic Activity							
	RM (Million)							
	2015	2016	2017	2018	2019	2020	2021	2022
Johor	110,002	116,682	123,561	130,586	134,226	128,074	131,303	142,056
Plus: Import Duties	817	942	992	897	731	864	610	318
Pahang	49,450	50,875	54,591	56,290	58,434	54,885	55,403	61,395
Agriculture	11,665	11,193	12,254	12,419	12,849	13,001	13,000	13,633
Mining and Quarrying	1,311	879	709	705	820	614	507	557
Manufacturing	10,417	10,820	11,531	12,194	12,767	12,246	12,990	13,745
Construction	2,105	2,726	3,231	2,399	1,727	1,352	1,603	1,586
Services	23,885	25,173	26,720	28,454	30,217	27,597	27,252	31,823
Plus: Import Duties	66	84	147	119	55	75	51	51
Pulau Pinang	78,146	82,493	86,768	91,234	94,645	92,691	99,111	112,126
Agriculture	2,084	1,988	2,034	1,969	2,068	2,049	2,002	2,069
Mining and Quarrying	124	135	144	156	171	139	130	140
Manufacturing	33,597	35,411	37,426	39,458	40,510	41,627	46,768	54,182
Construction	2,712	2,984	2,689	2,620	2,644	2,234	2,522	2,721
Services	38,917	41,167	43,458	46,120	48,645	45,979	47,064	52,371
Plus: Import Duties	712	808	1,017	910	606	663	625	643
Perak	63,176	65,958	69,337	73,031	75,993	74,264	76,923	80,213
Agriculture	10,352	10,151	10,942	10,994	11,312	11,430	11,798	11,338
Mining and Quarrying	354	414	438	461	505	432	402	438
Manufacturing	11,190	11,752	12,691	13,222	13,683	14,156	15,453	15,606
Construction	2,578	2,786	2,113	2,337	2,490	2,057	1,920	2,038
Services	38,628	40,762	43,028	45,911	47,971	46,137	47,314	50,742
Plus: Import Duties	73	93	124	107	32	51	35	52
Perlis	5,353	5,570	5,695	5,885	6,151	5,785	5,868	6,200
Agriculture	1,161	1,200	1,249	1,260	1,334	1,088	1,024	1,046
Mining and Quarrying	32	28	31	33	33	30	29	31
Manufacturing	458	449	459	466	470	444	468	489
Construction	193	212	121	147	167	151	151	153
Services	3,414	3,579	3,723	3,881	4,075	4,032	4,121	4,354
Plus: Import Duties	94	102	112	98	72	40	76	129
Selangor	268,825	281,839	302,186	323,215	345,008	326,805	343,983	384,871
Agriculture	4,076	3,872	4,319	4,535	4,709	4,721	4,954	4,874
Mining and Quarrying	499	643	692	737	859	755	708	777
Manufacturing	75,537	78,710	84,964	91,133	95,942	95,114	107,531	117,207
Construction	16,674	16,243	17,580	18,646	20,664	18,665	17,493	18,203
Services	163,967	173,870	186,018	200,324	214,348	200,127	205,213	233,125
Plus: Import Duties	8,072	8,501	8,613	7,841	8,487	7,423	8,084	10,686
Terengganu	31,124	32,133	33,979	34,838	36,001	33,994	35,238	37,309
Agriculture	2,765	2,681	2,921	2,847	3,016	2,903	2,753	2,623

State	Gross Domestic Product by Kind of Economic Activity							
	RM (Million)							
	2015	2016	2017	2018	2019	2020	2021	2022
Johor	110,002	116,682	123,561	130,586	134,226	128,074	131,303	142,056
Mining and Quarrying	146	159	174	183	201	176	178	192
Manufacturing	11,296	12,116	12,586	13,056	13,093	11,862	12,994	14,061
Construction	904	920	1,276	1,161	1,165	1,080	1,107	1,145
Services	15,965	16,207	16,916	17,527	18,509	17,943	18,190	19,280
Plus: Import Duties	49	50	105	64	16	31	16	8
Sabah	73,776	77,518	83,793	85,012	85,642	77,840	78,999	81,931
Agriculture	14,817	13,255	13,883	13,836	13,719	12,798	12,520	12,492
Mining and Quarrying	18,207	21,992	25,441	23,994	22,736	19,936	20,574	20,307
Manufacturing	6,266	6,037	6,362	6,514	6,472	6,042	5,931	5,780
Construction	2,446	2,357	2,322	2,918	3,099	2,197	2,370	2,517
Services	31,755	33,575	35,434	37,423	39,428	36,597	37,364	40,565
Plus: Import Duties	285	302	352	327	187	269	240	270
Sarawak	121,585	124,513	130,169	133,010	136,759	127,556	131,572	140,161
Agriculture	16,988	16,632	16,728	16,614	16,578	14,907	14,434	14,542
Mining and Quarrying	29,852	29,253	30,214	29,627	30,013	28,591	27,875	29,475
Manufacturing	32,128	33,567	34,811	35,579	36,613	33,428	37,122	39,207
Construction	3,843	3,633	4,355	4,402	4,476	4,082	4,497	4,676
Services	38,370	40,982	43,541	46,312	48,761	46,160	47,288	51,832
Plus: Import Duties	404	446	520	475	318	388	355	428
WP Kuala Lumpur	180,865	191,641	206,175	220,359	233,794	217,447	219,706	239,811
Agriculture	2	2	2	2	2	2	2	2
Mining and Quarrying	117	129	146	146	153	138	134	145
Manufacturing	5,641	5,795	5,871	5,868	6,119	5,733	5,978	6,297
Construction	12,915	14,509	16,406	17,446	18,470	13,589	11,974	12,215
Services	159,752	168,742	180,196	193,472	205,331	194,204	197,788	218,981
Plus: Import Duties	2,437	2,464	3,556	3,426	3,720	3,780	3,830	2,172
WP Labuan	5,999	6,412	6,790	7,245	7,623	7,613	7,650	7,954
Agriculture	118	114	119	126	133	115	117	121
Mining and Quarrying	-	-	-	-	-	-	-	-
Manufacturing	1,168	1,256	1,296	1,365	1,384	1,368	1,354	1,377
Construction	148	121	136	156	177	163	143	148
Services	4,490	4,844	5,093	5,481	5,898	5,910	5,997	6,274
Plus: Import Duties	74	77	147	118	32	58	39	34
Supra	51,420	50,562	46,512	46,044	45,738	40,698	41,896	42,754
Agriculture	-	-	-	-	-	-	-	-
Mining and Quarrying	51,420	50,562	46,512	46,044	45,738	40,698	41,896	42,754
Manufacturing	-	-	-	-	-	-	-	-
Construction	-	-	-	-	-	-	-	-
Services	-	-	-	-	-	-	-	-

State	Gross Domestic Product by Kind of Economic Activity							
	RM (Million)							
	2015	2016	2017	2018	2019	2020	2021	2022
Johor	110,002	116,682	123,561	130,586	134,226	128,074	131,303	142,056
Plus: Import Duties	-	-	-	-	-	-	-	-

Source: Department of Statistics Malaysia

The minimum salary in Malaysia can vary depending on factors such as the sector (private or government) and location. However, it is important to note that minimum wage regulations in Malaysia can change over time due to government policies and economic conditions. The government periodically reviews and adjusts the minimum wage to ensure that it remains fair and in line with the cost of living. Additionally, Malaysia's diverse economic landscape, with urban centers like Kuala Lumpur and rural areas, contributes to regional variations in minimum wage rates. The minimum wage serves as a baseline to protect the rights and livelihoods of workers, particularly those in lower-paying sectors. It reflects the government's commitment to ensuring that workers receive fair compensation for their labor, promoting economic stability, and improving the overall quality of life for Malaysians across the country. It's advisable for both employers and employees to stay updated on the latest minimum wage regulations to comply with current standards and ensure that workers are fairly compensated for their contributions to the Malaysian economy.

1. Private Sector: The minimum wage for employees in the private sector in Peninsular Malaysia was set at RM 1,500 per month since 1 July 2023. However, it may vary in different regions, industries and the relevant authorities for the latest rates. The government periodically reviews and adjusts the minimum wage to account for economic factors.

2. Government Sector: The minimum salary or wage for government employees in Malaysia was set at RM 1,500 per month since 1 July 2023. Civil service salary scales are typically structured with various grades and allowances, and these can change over time due to government policies and collective bargaining agreements. Therefore, specific salary information for government employees may not be statics.

2.4 Stakeholder

In Malaysia, the primary holders of security and investigation activities are several agencies and bodies that play a role in carrying out tasks related to law enforcement and security. There are some of the main agencies responsible for security and investigation activities in Malaysia. Governments frequently engage in collaboration with private sector entities to bolster their security and investigation capabilities, recognizing the mutual benefits of such partnerships. Information sharing stands out as a fundamental aspect of this collaboration. By exchanging relevant data and intelligence, both parties gain a more comprehensive understanding of emerging threats, vulnerabilities, and evolving risk landscapes. This sharing of information helps in early threat detection, rapid response to incidents, and the development of effective countermeasures. It is particularly crucial in combating sophisticated cyber threats, where private sector organizations often possess valuable insights into emerging cyber risks.

Joint initiatives are another key facet of government-private sector collaboration in the realm of security and investigation. These initiatives can take various forms, including the establishment of task forces, working groups, or joint research and development programs. By combining the strengths and resources of both government agencies and private companies, these initiatives enhance the overall effectiveness of security measures. Whether addressing cyber threats, terrorism, or other security challenges, joint efforts facilitate a more coordinated and unified approach to risk mitigation and incident response.

Resource-sharing is a pragmatic strategy employed in collaborative endeavors between governments and the private sector. Security and investigation activities often demand substantial resources, both in terms of technology and expertise. Governments can leverage the specialized skills and advanced technologies offered by private sector partners, while private entities benefit from government support and a shared framework for addressing security concerns. This synergy enables a more robust and resilient security infrastructure, ultimately safeguarding critical assets and interests. Through these collaborative mechanisms, the public and private sectors contribute synergistically to the overarching goal of maintaining national and global security. The main agencies responsible for security and investigation activities in Malaysia was presented in Table 2.2.

Table 2.2: The main agencies responsible for security and investigation activities in Malaysia

No.	Agencies	Roles, functions, and responsibilities
1.	Cyber Security Malaysia	Provide a broad range of cybersecurity innovation-led services, programmes, and initiatives to reduce vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace.
2.	Royal Malaysia Police (RMP)	Provide professional, quality, and integrity-driven police services towards public safety and security. RMP also responsible for the enforcement of law.
3.	Maritime	Enforcing the law and safeguarding lives and property at sea to ensure the well-being of the country's waters
4.	The Ministry of Home Affairs (MOHA)	Ensuring the safety and security of the nation and the well-being of the people are preserved
5.	The Malaysian Anti-Corruption Commission (MACC)	To eradicate corruption, abuse of power and malpractice in Malaysia. To concertedly and continuously strengthen integrity and enhance expertise through human resources development programmes.
6.	Ministry of Transport Malaysia (MOT)	Spearheading the transformation of an integrated efficient and safe transportation system driven by technology as a catalyst for national development. To formulate and implement land transport, logistics, maritime and aviation policies, law, services, safety and infrastructure projects.
7.	Aviation	MOT Role in Aviation sector is to develop an efficient, economical, and safe air transport system for passengers and cargo as well as to plan and implement infrastructural projects to meet the demands of the air transport. To plan and evaluate aviation policies, increase international air services network through air negotiation, plan and monitor implementation of airport development projects as well as coordinate civil aviation/air transport legal aspects.

2.4.1 Agency

2.4.1.1 Cyber Security Malaysia

Cyber Security Malaysia is the name of the national cybersecurity specialist agency in Malaysia. It is also known as Malaysian Computer Emergency Response Team (MyCERT). This organization is responsible for providing cybersecurity services, managing cyber threats and incidents, promoting cybersecurity awareness and education, and supporting the development of the country's cybersecurity industry. It plays a crucial role in enhancing the cybersecurity posture of Malaysia's government agencies, businesses, and the general public.
Cyber Security Malaysia serves as the central coordinating body for cybersecurity efforts across the country. It collaborates with various government ministries, law enforcement agencies, regulatory bodies, and industry stakeholders to ensure a holistic and unified approach to cybersecurity. This coordination is essential in addressing the evolving threat landscape and responding effectively to cyber incidents that may have cross-sector impacts.

Additionally, Cyber Security Malaysia's role as the central coordinating body extends beyond the borders of the nation. It actively participates in regional and international cybersecurity forums and organizations, forging partnerships with counterparts from around the world. This global engagement allows for the exchange of threat intelligence, best practices, and joint efforts to combat cyber threats on a broader scale, reflecting Malaysia's commitment to international cybersecurity cooperation.

The agency's collaborative efforts encompass the sharing of critical cybersecurity information and the development of joint strategies to counter cybercrime, cyber espionage, and cyberterrorism. By pooling resources and expertise with both national and international partners, Cyber Security Malaysia strengthens its ability to anticipate emerging threats and respond swiftly and effectively to protect the nation's digital infrastructure and assets.

Furthermore, the agency's coordination role extends to cybersecurity incident response exercises and simulations. It conducts drills and tabletop exercises involving various stakeholders, simulating cyber crisis scenarios. These exercises help enhance preparedness, communication, and coordination among different sectors, ensuring that Malaysia is better equipped to manage and mitigate cyber incidents, thereby safeguarding the nation's economic stability, public safety, and national security in an increasingly interconnected world.

In today's interconnected world, cyber threats often transcend national borders. Cyber Security Malaysia actively collaborates with international cybersecurity organizations,

agencies, and partners. This collaboration ensures the exchange of threat intelligence, best practices, and expertise, contributing to global efforts to combat cybercrime and protect critical infrastructure.

Moreover, Cyber Security Malaysia's international collaborations extend to participation in joint cybersecurity initiatives, conferences, and information-sharing platforms. By engaging with a global network of cybersecurity professionals and organizations, the agency gains access to a wealth of knowledge and resources. This allows for the adoption of innovative cybersecurity solutions and the implementation of cutting-edge practices that can be adapted to the unique challenges faced by Malaysia.

Through its active involvement in international cybersecurity dialogues, Cyber Security Malaysia contributes to the development of global cybersecurity norms and standards. It plays a role in shaping the international cybersecurity landscape, advocating for secure digital environments, and supporting international efforts to establish rules of engagement in cyberspace.

Furthermore, the agency's collaboration with international partners enhances Malaysia's cybersecurity resilience by providing timely and relevant threat intelligence. Cyber Security Malaysia is well-positioned to receive and disseminate information about emerging cyber threats, ensuring that the nation can proactively defend against evolving cybersecurity risks and vulnerabilities. Cyber Security Malaysia's engagement with international cybersecurity organizations and partners is instrumental in reinforcing the country's cybersecurity posture. This collaboration facilitates the exchange of knowledge and expertise, bolsters Malaysia's ability to combat cyber threats, and contributes to the global effort to create a safer and more secure digital environment for all nations.

2.4.1.2 Royal Malaysia Police (RMP)

Royal Malaysia Police (RMP) or also known as *Polis Diraja Malaysia (PDRM)* is a law enforcement agency in Malaysia that plays a crucial role in maintaining public safety, upholding the law, and addressing security issues within the country. RMP is the national police force of Malaysia and is one of the key agencies in the country's law enforcement system. The primary function of RMP is to maintain public order, prevent and address crimes, and provide protection to the community. They carry out tasks such as patrols, criminal investigations, inquiries, and the apprehension of individuals involved in criminal activities.

RMP is also responsible for managing road traffic, ensuring compliance with traffic laws, and safeguarding the safety of road users.

RMP is divided into various divisions and specialized units that focus on areas such as counterterrorism, narcotics, cybercrime, and serious crime investigations. Special task forces, including the general operations force, are trained to handle crisis situations and extraordinary circumstances. In addition to traditional law enforcement duties, RMP also engages in international cooperation with security agencies from other countries to address and mitigate cross-border crimes. RMP strives to maintain integrity, professionalism, and transparency in all their actions, and they continuously innovate by using the latest technology and methodologies to enhance the performance and effectiveness of their law enforcement operations. This organization plays a significant role in maintaining security and order in Malaysia, making it an essential aspect of the country's governance and safety framework.

2.4.1.3 Maritime

Maritime refers to the maritime areas and activities related to the sea in Malaysia. Malaysia is a maritime nation with coastlines stretching along the South China Sea and the Indian Ocean, providing access to major trade routes, and holding strategic importance in maritime security. The Ministry of Defence of Malaysia holds primary responsibility for maritime safety, and there are several agencies and bodies involved in safeguarding Malaysia's interests and security in the maritime region:

i. Malaysian Maritime Enforcement Agency (MMEA): MMEA is a government agency responsible for ensuring maritime safety in Malaysia. MMEA is tasked with conducting patrols, surveillance, and operations in Malaysian waters to protect against threats such as sea piracy, smuggling, fish theft, and other illicit maritime activities.
ii. Royal Malaysian Navy (RMN): The Malaysian Navy plays a vital role in safeguarding maritime security and national sovereignty at sea. RMN is involved in maritime and naval operations to maintain national security and enforce maritime law.
iii. Malaysian Maritime Customs: This agency is responsible for controlling the movement of goods and services in Malaysian waters and combating smuggling and violations of trade laws.
iv. Maritime Enforcement Agency (APM): APM is responsible for maintaining security and safety in Malaysia's Exclusive Economic Zone (EEZ) and planning and implementing maritime law enforcement activities.

v. Hazardous Substances and Solid Waste Management Agency (HAZWMA): This agency has a role in managing solid waste and hazardous chemicals in Malaysia's maritime area to reduce marine pollution.

Maritime safety is crucial for Malaysia as it encompasses various aspects such as trade, protection of marine resources, and sovereignty rights. Malaysia also seeks cooperation with neighboring countries and international parties to ensure safety and stability in the Southeast Asian maritime region.

2.4.1.4 The Ministry of Home Affairs (MOHA)

The Ministry of Home Affairs is one of the important ministries in the government of a country. Its primary focus is on maintaining security, public order, and law enforcement within the country. The ministry is responsible for planning, implementing, and overseeing policies and programs related to safety in various aspects. The ministry plays a pivotal role in ensuring public security and order in the country. This includes overseeing law enforcement, controlling criminal activities, and strategizing to address security threats. The ministry is responsible for overseeing law enforcement agencies such as the police and other security forces. They ensure the enforcement of laws and regulations and maintain the safety of the community.

The ministry engages in crime prevention efforts, including strategizing, implementing prevention initiatives, and developing programs to reduce crime rates. The ministry is involved in matters related to national security, including preventing internal and external threats and safeguarding the integrity of national borders. The ministry may also coordinate civil protection efforts during emergencies or disasters, including crisis management and humanitarian assistance operations. Some ministries of home affairs are also responsible for citizenship and immigration matters, including controlling the movement of immigrants, monitoring entry and exit, and overall immigration affairs. The ministry often engages in international security cooperation, collaborating with neighboring countries and global agencies to maintain regional and global security and order. The Ministry of Home Affairs is a crucial component of the government structure, ensuring the safety and tranquility of the society within the country and contributing to overall stability and development of the nation.

2.4.1.5 The Malaysian Anti-Corruption Commission (MACC)

The Malaysian Anti-Corruption Commission (MACC) or also known as *Suruhanjaya Pencegahan Rasuah Malaysia (SPRM)* is a government agency in Malaysia responsible for

combating and preventing corruption. It is an independent body that operates to ensure transparency, accountability, and integrity within various sectors of the Malaysian government and society. It serves several important purposes in Malaysia's efforts to combat corruption and promote good governance. The primary purpose of MACC is to prevent corruption in all sectors of Malaysian society. This involves raising awareness about the detrimental effects of corruption, educating the public and organizations about ethical behavior, and implementing strategies to minimize opportunities for corrupt practices. They investigate cases of corruption, bribery, and abuse of power. By conducting thorough and impartial investigations, the agency gathers evidence to build strong cases against individuals involved in corrupt activities. It then takes legal action to hold those individuals accountable.

MACC promotes a culture of integrity and ethical conduct within government agencies, private organizations, and society at large. It encourages individuals to uphold high standards of honesty and transparency in their actions and decisions. The agency provides protection and support to whistleblowers who expose corruption and provide information about corrupt activities. Whistleblower protection is crucial in encouraging individuals to come forward with information without fear of retaliation. By actively investigating and prosecuting corrupt practices, MACC helps to restore and enhance public trust in government institutions and public officials. This trust is essential for the effective functioning of a democratic society.

MACC monitors and verifies the asset declarations of public officials to ensure that their wealth is acquired through legal means. This helps to prevent and detect cases of illicit enrichment. The agency collaborates with international counterparts and anti-corruption organizations to share knowledge, best practices, and resources in the fight against corruption. This cooperation strengthens Malaysia's position in global efforts to combat corruption. MACC promotes accountability and transparency by investigating cases where public officials abuse their power for personal gain. This sends a message that those who engage in corrupt practices will face consequences. MACC contributes to the development and improvement of anti-corruption policies and legislation in Malaysia. It provides recommendations to enhance the legal framework for combating corruption effectively. The MACC plays a crucial role in promoting a clean and accountable society by preventing corruption, investigating cases, promoting integrity, and fostering a culture of transparency and honesty.

2.4.2 Association

Here are some of the main associations responsible for security and investigation activities in Malaysia.

Table 2.3: The main association responsible for security and investigation activities in Malaysia

No.	Association	Roles, functions, and responsibilities
1.	The Malaysian Occupational Safety and Health Association (MIOSHA)	To enhance and promote Occupational Safety and Health (OSH) in all workplaces and in all industries in support of the Government's policy on OSH
2.	Malaysia Security Industry Association (MSIA)	Disseminating accurate knowledge and information to members, enabling them to be responsible for compliance with standards, codes of good practice, and other regulations

2.4.2.1 The Malaysian Occupational Safety and Health Association (MIOSHA)

The Malaysian Occupational Safety and Health Practitioners Association (MIOSHA) is an organization that functions as a platform to promote occupational safety and health in Malaysia. The organization serves as a collective for individuals, organizations, and professionals interested in and engaged with the field of occupational safety and health. The primary focus of the Malaysian Occupational Safety and Health Association is to raise awareness about the importance of workplace safety and health across various industrial sectors in the country. MIOSHA strives to educate the public and stakeholders about best practices to ensure a safe and healthy working environment for employees.

MIOSHA's activities include providing training and courses related to occupational safety and health, organizing seminars, conferences, and workshops, as well as assisting in the development and assessment of workplace safety and health programs. The association also promotes compliance with existing occupational safety and health laws in Malaysia. Furthermore, the Malaysian Occupational Safety and Health Association also plays a role in fostering better relationships among employers, employees, and other stakeholders by providing guidance and support in implementing effective occupational safety and health practices. MIOSHA aims to achieve higher goals of occupational safety and health in Malaysia

through education, training, and awareness promotion among the worker community and stakeholders in this field.

2.4.2.2 Malaysia Security Industry Association (MSIA)

The Malaysian Security Industry Association (MSIA) or also known as *Persatuan Industri Keselamatan Malaysia (PIKM)* is a non-governmental organization registered with the Registrar of Societies Malaysia under the Societies Act 1966. This organization comprises security control companies registered and licensed by the MOHA. As of end December 2023, MSIA's membership encompasses 1147 security companies operating throughout the country.

The MSIA was established on 3 November 1980. Its inception was the result of a collaboration among a group of executive entrepreneurs in the security industry in Kuala Lumpur and Selangor who recognized the need to establish an entity that could protect and advocate for the interests of these industry players. During that period, in alignment with the implementation of the New Economic Policy, local labor began to find employment opportunities as security executives in private firms and industrial areas. Unfortunately, many of these executives did not receive proper treatment from their employers and worked under stressful and oppressive conditions. Most of the employers, who mainly consisted of investors and foreign traders, created various obstacles to hinder the mobility of local executives in advancing in their careers. Consequently, many left their positions and ventured into the security industry by forming security firms. Simultaneously, entrepreneurs from former police and military personnel who had recently entered the business arena, particularly in security services, also faced bitter challenges. They encountered fierce competition from experienced entrepreneurs, difficulties in obtaining capital and credit, and instances of sabotage, among other hurdles. However, the tribulations in the business world brought about a realization among these new entrepreneurs. With this awareness, meetings were arranged, and agreements were reached. MSIA was conceived as a platform for the protection and advocacy of the future of security industry entrepreneurs. The final decision to establish MSIA was reached following the first committee sponsor meeting with the MOHA, chaired by Tan Sri Osman S. Cassim. The committee sponsor members and pioneering figures who participated in the historic meeting on the morning of 8 February 1979, were Haji Noordin Truna (N.A.C.K Security), Encik Zainal Abidin Kinta (*Sistem Kawalan Sekutu*), Encik Haji Haron Haji Taib (Jaya Guard), Ahmad Tasir Ali (Raya Guard), and Encik Henry Ang Ann Poh (N.A.C.K Security).

With the establishment of MSIA, national security industry entrepreneurs moved forward with greater confidence and courage. Resources and efforts could be pooled more

effectively, needs and interests could be presented to the government, and challenges and issues could be collectively addressed. Starting in the Klang Valley, MSIA's membership has now expanded throughout the country. Likewise, the national security industry has progressed alongside the advancements in the service sector of Malaysia's economy. As stated in MSIA's Constitution, the objectives of the association are as follows:

1. To unite and consolidate all security companies into one national organization.
2. To establish understanding and cooperation among members and serve as a channel for the sharing of resources to advance the security industry.
3. To enhance the capabilities and professionalism of members in conducting security service businesses through various educational activities, training, information dissemination, and increased awareness of laws, regulations, guidelines, and industry ethics.
4. To represent members in negotiations with relevant authorities, consumers of security services, media, and the general public.

2.5 Law

The laws governing security and investigative activities in Malaysia involve several legislations that regulate the duties and responsibilities of law enforcement agencies and protect individual rights. Technology has become integral to modern law enforcement and investigation, particularly through the use of digital forensics tools that analyze electronic evidence, crucial in today's predominantly digital criminal landscape. This includes recovering data from devices, scrutinizing digital documents, and examining communication records, all contributing to comprehensive case-building. Furthermore, the escalating complexity of cybercrime has fostered increased collaboration between government agencies and private sector cybersecurity firms. This collaboration involves sharing threat intelligence, utilizing cutting-edge technologies, and enhancing collective capabilities to effectively detect, prevent, and respond to cyber threats. The partnership is mutually beneficial, with government agencies gaining access to private sector expertise and tools, and the private sector benefiting from regulatory support. This collaboration fortifies the cybersecurity posture, safeguarding critical infrastructure, protecting sensitive information, and ensuring digital system resilience against evolving cyber threats, highlighting its pivotal role in addressing contemporary cybercrime challenges. Some relevant legislations include:

1. Police Act 1967 (Act 344): The act provides for the organization, administration, and control of the police force in Malaysia. The act establishes the RMP as the national police force of Malaysia, responsible for maintaining public order and enforcing the law throughout the country.
2. Criminal Procedure Code (Act 593): The act relating to criminal procedure. The act focused on the investigation of crimes by the RMP, including powers and procedures for investigation.
3. Customs Act 1967 (Act 235): The act regulates the duties and powers of the Royal Malaysia Customs Department (RMCD) in controlling the movement of goods and enforcing customs laws.
4. Immigration Acts 1959/63 (Act 155): The act addresses immigration issues, including control of entry and exit, as well as enforcement of immigration laws.
5. Armed Forces Act 1972 (Act 77): The act governs the MAF defense duties, and involvement in security operations within the country.
6. Emergency (Public Order and Crime Prevention) Ordinance 1969: The ordinance specifies actions that authorities can take during emergencies or threats to national security.
7. Malaysian Anti-Corruption Commission Act 2009: The Malaysian laws which enacted to provide for the establishment of the MACC, to make further and better provisions for the prevention of corruption and for matters necessary thereto and connected therewith
8. Human Rights Commission of Malaysia Act 1999 (Act 97): The act establishes the Human Rights Commission of Malaysia (SUHAKAM) to protect and promote human rights in Malaysia.
9. Private Agency Act 1971 (Act 27): The act regulates private employment agencies and personnel recruitment activities in the country.
10. Malaysian Maritime Enforcement Agency Act 2004 (Act 633): The act responsible for safeguarding and enforcing laws within Malaysia's maritime jurisdiction, protecting its maritime interests, ensuring maritime security, and preventing various maritime offenses.
11. Industrial Relations Act 1967 (Act 177): The act responsible to protects the rights of employees in Malaysia, maintain a good relationship and fair dealings between employers, workers, and their trade union.
12. *Pembangunan Sumber Manusia* Berhad (PSMB) Act 2001 (Act 612): The act regulates matters related to compoundable offences under the PSMB Act and regulations. A

regulation to regulate matters related to registration of employers and payment of levy under the PSMB Act.

2.6 Government Agencies Policies and Initiatives

Malaysia's government policies and initiatives encompass a wide range of strategies, programs, and actions formulated and implemented by the government to achieve various socio-economic, political, and developmental objectives. These policies and initiatives are designed to address challenges, promote growth, enhance well-being, and contribute to the overall progress of the nation. Here are some key areas of Malaysia's government policies and initiatives. Malaysia has implemented various economic policies to stimulate growth, attract investments, and enhance economic competitiveness. The New Economic Policy (NEP) and subsequent iterations, such as the New Economic Model (NEM) and the Shared Prosperity Vision 2030, emphasize equitable economic distribution, poverty reduction, and sustainable development.

Malaysia's industrialization policies focus on developing high-value industries, such as electronics, manufacturing, and services. Initiatives like the National Industry 4.0 Policy and the Malaysia Digital Economy Blueprint aim to drive innovation, technology adoption, and digital transformation. The government places great emphasis on education and human capital development. Policies like the Malaysia Education Blueprint aim to enhance the quality of education at all levels, from primary to tertiary, to produce a skilled and knowledgeable workforce. Policies are in place to address regional disparities and promote balanced development between urban and rural areas. Initiatives like the Rural Transformation Programme and various rural development plans aim to improve infrastructure, access to basic services, and the overall quality of life in rural communities.

Malaysia is committed to environmental sustainability and conservation. Policies and initiatives include efforts to promote green technologies, address climate change, conserve biodiversity, and promote sustainable resource management. Social welfare policies focus on poverty eradication, social safety nets, and improving the overall well-being of Malaysians. Initiatives like the *Bantuan Rakyat 1Malaysia (BRIM)* and various healthcare programs aim to uplift vulnerable segments of society. Malaysia has embarked on large-scale infrastructure projects to improve connectivity, transportation, and urban development. Initiatives like the National Transport Policy and the East Coast Rail Link are examples of efforts to enhance the country's infrastructure. Malaysia's foreign policies and trade initiatives aim to strengthen diplomatic ties, foster international cooperation, and promote trade relations. Initiatives like

the Look East Policy and participation in regional organizations contribute to Malaysia's global engagement. Malaysia promotes its cultural heritage and tourism industry through initiatives like Visit Malaysia campaigns, which showcase the country's diverse cultural landscape and tourist attractions.

2.7 Industry and Market Study

In today's technological landscape, sensors play a critical role in various applications, including environmental monitoring, transportation, smart cities, healthcare, and more. Wearable medical devices equipped with sensors are particularly important for gathering comprehensive data related to our physical and mental health. The continuous generation of data by these sensors, often referred to as Big Data, poses challenges in terms of processing and analysis to extract valuable insights. Therefore, organizations require effective and secure architectures to handle and process Big Data in the integrated industry 4.0 environment. Manogaran et al. (2017) proposed a secure architecture for the Industrial Internet of Things (IoT) specifically designed for storing and processing scalable sensor data, with a focus on healthcare applications and proposed architecture, called Meta Cloud-Redirection (MC-R), incorporates a big data knowledge system that facilitates the collection and storage of sensor data generated by various sensor devices. In this system, medical devices equipped with sensors are attached to the human body to collect clinical measurements of patients. When the readings for parameters such as respiratory rate, heart rate, blood pressure, body temperature, and blood sugar exceed normal values, the devices send an alert message containing the clinical data to the doctor using a wireless network. Also, system utilizes a key management security mechanism to protect the big data within the industry 4.0 environment. This security mechanism ensures that the sensor data remains confidential and secure, preventing unauthorized access and maintaining data integrity.

Fuad's study (2022) discusses the importance of technology use in the security and investigation sector in Malaysia. The rapid development of technology has changed the landscape of crime incidents and security threats, and therefore, security and investigation professionals need to master this technology to be competitive and effective in their duties. This article breaks down some of the key technologies relevant to security and investigations and emphasizes the benefits and implications of using those technologies.

The industrial utilization of IoT technologies has gained significant popularity due to advancements in connectivity and automation. However, the rise of Industrial IoT has brought forth concerns regarding security vulnerabilities in industrial systems. These vulnerabilities,

previously less likely to be exploited in closed settings, have now become a major issue. One area of particular concern is the functional safety of industrial systems, which were not originally designed to protect against intentional malicious activities, but rather accidents and errors. However, Tomur et al. (2021) examines a generic IoT-based smart manufacturing use-case through the lens of both security and functional safety, recognizing their close correlation. The primary contribution of this study is the presentation of a taxonomy of threats that specifically target the critical safety function in industrial IoT applications. Moreover, based on this taxonomy, the research identifies potential attack scenarios that could have severe consequences for physical assets like manufacturing equipment, as well as human life and the availability of Industrial IoT applications. Finally, the paper proposes mitigation strategies for such attacks, primarily relying on industry standards and leveraging advanced security features offered by mobile communication technologies.

Furthermore, beyond practical studies addressing functional safety, academic literature also explores the conceptual relationship between security and safety. For instance, works such as Pan and Liu (2007), Novak and Treytl (2008), and Reichenbach et al. (2012) present formal methodologies for conducting combined risk analyses that address both safety hazards and security threats. These methodologies leverage shared features and resolve conflicts between safety and security considerations. However, none of these studies specifically delve into security attacks on functional safety.

One notable work that does consider security challenges with potential safety implications is the study by Singh, Kumar, and H¨otzel (2018) the authors focus on adapting IoT technology in underground mines to enhance safety and productivity through effective communication and data collection. The work provides a comprehensive overview of IoT security challenges specific to the underground mine use case and classifies them accordingly. It also presents a threat taxonomy. It is important to note that Singh, Kumar, and H¨otzel's (2018) taxonomy addresses security threats that impact safety functions in IoT-based smart manufacturing, while our taxonomy focuses on security threats impacting safety functions in the context of IoT-based smart manufacturing.

The current state of industrial manufacturing processes heavily relies on Information and Communication Technologies (ICT). This technological revolution has significantly impacted organizations, comparable to the transformative effects of mechanization and electricity in the first and second industrial revolutions. This advancement has led to the emergence of various trends, including cloud-based systems, the IoT, Big Data, Industry 4.0, Bring Your Own Device (BYOD), and Choose Your Own Device (CYOD). However, as with

any new technological solutions, there are inherent security vulnerabilities that can expose unexpected risks. As organizations increasingly depend on technology to gain a competitive edge, security concerns have become one of the most critical and challenging requirements for conducting successful business operations. Pereira et al. (2017) draw attention to the challenges posed by Industry 4.0, with a specific focus on security issues. By emphasizing the importance of security, the objective is to raise awareness about best practices and promote a security-conscious approach within the context of Industry 4.0.

The relationship between the private security industry and public institutions and agencies is intricate and not one-sided. While the industry provides assistance and acts as a substitute for the public sphere, it is also governed by it, although in an uneven and partial manner. Simultaneously, the industry reshapes the public sphere to pursue commercial advantages both domestically and internationally. Dorn and Levi (2007) delve into various aspects of cooperation and governance in European and broader contexts. The first aspect examined is private-public security cooperation, which involves the collaboration between private security entities and public agencies, also explores the regulation of the security market, focusing on the guarding sector. Additionally, it delves into the involvement of private security companies in corporate and military services on a global scale. Lastly, discussed how the private security industry contributes to the restructuring of states and legal relations, thereby shaping the overall landscape. Each of these considerations—private-public security cooperation, market regulation, global corporate and military services, and industry-driven restructuring of states and legal relations—raises distinct yet interconnected issues for analysis and all stakeholders involved. As well as concluded the boundaries between private and public security are not fixed, and private security demonstrates greater permeability than public security in their interactions with the public sphere. This dynamic between private and public security is both a historical and ongoing aspect of the public-private interface.

However, the private security industry now assumes a broad range of responsibilities that were traditionally the domain of the police. As the scope and nature of private security continue to evolve, regulations strive to keep pace with these changes. Among the European Union member states, Sweden stands out for having one of the most comprehensive frameworks governing the private security industry. Despite this, there are certain gaps, particularly concerning private security's involvement in criminal investigations, which, if left unaddressed, could potentially lead to a worrisome commodification of justice and a decline in trust towards the police. In this article, we delve into these issues through interviews conducted with various stakeholders. The insights garnered from these interviews reveal that the

underlying danger lies in situations where the police are compelled to decline investigations for various reasons. In such cases, both individuals and organizations have the opportunity to engage private security service providers to carry out the investigation. When presented with a solid foundation for prosecution, the police are thereby incentivized to proceed. Consequently, the discretionary power of the police to decide whether or not to initiate an investigation effectively becomes a commodity that can be bought and sold. Therefore, this article strongly advocates for a revision of the regulatory framework governing private security in Sweden (Stiernstedt, 2019).

Software security refers to the protection of the programs that are either bought from an outsider vendor or created in-house by users. It concerns with the methods used for controlling software used to run the operating system or utility software (Antoniou, 2018). The focus of software security is to proactively protect assets from attacks that will result in losses. Organizations that lack awareness of software security may suffer from cyberthreats which may affect the performance of the organizations and lead to losses. Hence, operating in the vulnerable cyber environment, it is crucial for organizations to be equipped with software security. Unlike most of the studies on software security that focus on addressing security at the beginning of the software process, built into the design, implementing it in the coding and verifying it during testing (Firesmith, 2012). This research aims to develop the capability of software security among end-users. The increasing development of IoT devices and the existence of sophisticated attackers have resulted in the emergence of cyber risks. Cyber risks refer to the operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems, and it can be classified according to the activity (e.g., criminal and noncriminal), the type of attack (e.g., malware, insider attack, spam, distributed denial of service), and the source (e.g., terrors, criminals, government) (Eling & Schnell, 2016). Therefore, workers working from home should have some knowledge about cyber privacy and cybersecurity, in which failing to do so may damage the reputation of the organization.

Studies on readiness often focus on the organizational use of ICT. Some works have explored readiness models that incorporate cloud security risk and readiness, such as the cybersecurity readiness index by Kiplimo (2018) and the e-readiness assessment model proposed by Gupta et al. (2015). Ferreira (2017) developed a readiness model specifically for cloud services customers, addressing various security areas like compliance, governance, and data protection. This model also helps identify potential risk factors associated with the use of

cloud computing. However, it is important to note that Ferreira's study primarily focuses on cloud services rather than information security as a whole.

Antoniou (2018) proposed a web-based model for computing the Cybersecurity Readiness Index (CRI) for hospitals. The model encompasses the four pillars of cybersecurity: people, process, policy, and technology. This study aims to assess a hospital's readiness to combat cyber-attacks, considering the vulnerability of healthcare organizations to such threats. While relevant to information security and cybersecurity, Antoniou's study is contextualized within the healthcare industry.

In another study, Gupta et al. (2015) put forward an e-readiness assessment model, defining e-readiness as the availability of physical infrastructure, bandwidth, reliability, affordable prices, access to information (software and information systems), availability of devices (hardware and network), alignment of ICT plans and policies with the organization's vision, security measures adopted by the organization, and human resources capable of using and managing ICT resources for e-governance implementation.

These studies demonstrate the various approaches taken to assess readiness in different contexts, such as cloud services, healthcare, and e-governance. They provide valuable insights into specific aspects of readiness and highlight the importance of considering factors like security, infrastructure, and human resources when evaluating an organization's readiness in utilizing ICT effectively.

2.8 Statistics on Administrative and Support Services

In the Economic Census conducted in 2016, data pertaining to administrative and support services for the reference year 2015 was analyzed. Administrative and support services encompass a range of sectors, including rental and leasing activities, employment services, travel agency, tour operator, and reservation service activities, security and investigation activities, services related to buildings and landscape maintenance, as well as office administrative and other business support activities. The total value of gross output generated by these services amounted to RM27.1 billion in 2015, reflecting an impressive annual growth rate of 11.6 percent when compared to the figures from 2010, as depicted in Exhibit 3. The sector that experienced the most substantial increase in gross output value was travel agency, tour operator, and reservation service activities, which witnessed an impressive growth of RM4.7 billion at an annual rate of 9.0 percent. Following closely were security and investigation activities, with an increase of RM2.3 billion, representing a remarkable growth rate of 17.5 percent, and rental and leasing activities, which expanded by RM2.2 billion,

marking a robust growth rate of 19.5 percent. In 2015, the highest value of gross output was contributed by travel agency, tour operator, and reservation service activities, totaling RM13.4 billion, commanding a substantial share of 49.4 percent in the overall landscape. This was trailed by security and investigation activities, which accounted for RM4.1 billion or 15.2 percent of the total, and rental and leasing activities, contributing RM3.7 billion, equivalent to 13.6 percent of the aggregate gross output.

In 2015, the value added by these services amounted to RM10.5 billion, a notable increase from the RM5.5 billion recorded in 2010. The annual growth rate during the period from 2010 to 2015 stood at a robust 13.8 percent. Among these services, security and investigation activities demonstrated the most significant rise in value added, expanding by RM1.4 billion, equating to an impressive annual growth rate of 18.6 percent. Following closely were rental and leasing activities, which saw an increase of RM1.2 billion, marking a substantial growth rate of 18.0 percent, and travel agency, tour operator, and reservation service activities, which experienced an increment of RM0.9 billion, translating to a growth rate of 9.3 percent.

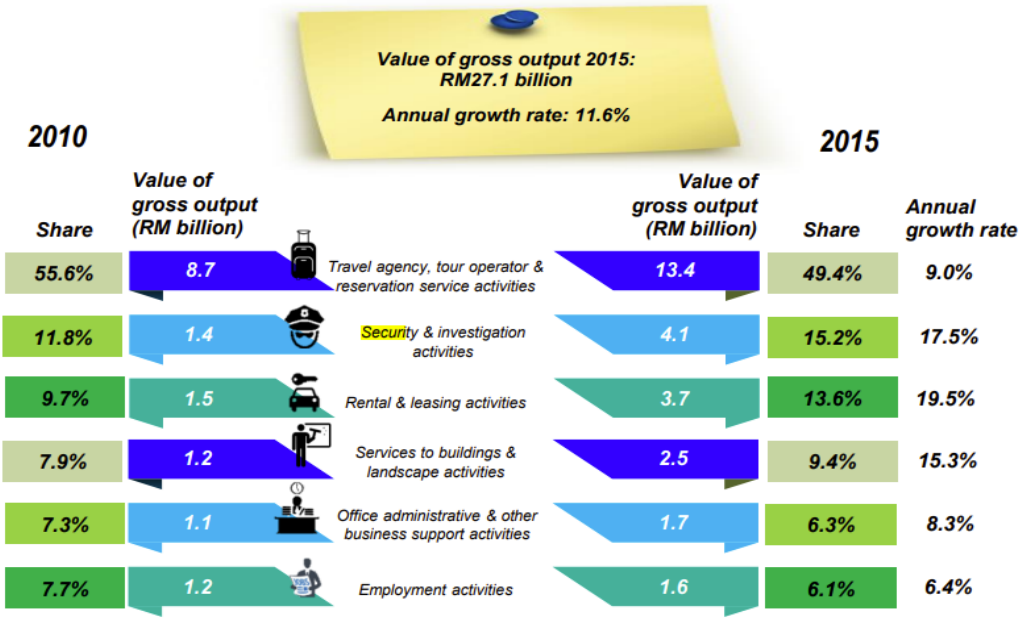

Figure 2.3: Value of gross output of administrative and support services by activities, 2010 and 2015 (https://newss.statistics.gov.my/)

The composition of value added closely mirrored that of the gross output, with travel agency, tour operator, and reservation service activities contributing the highest value at RM2.7

billion, representing a significant share of 25.5 percent, as demonstrated in Exhibit 4. This was followed by security and investigation activities, contributing RM2.4 billion, equivalent to 22.9 percent of the total, and rental and leasing activities, contributing RM2.2 billion, making up 20.8 percent of the overall value added.

In 2015, the total expenditure on salaries and wages amounted to RM3,967.4 million, marking a significant increase from the RM1,879.0 million reported in 2010. This growth represented an annual rate of 16.1 percent. Among the various sectors, security and investigation activities registered the most substantial surge in salaries and wages, with an increase of RM687.8 million and an annual growth rate of 19.0 percent. Following closely were travel agency, tour operator, and reservation service activities, which saw a rise of RM405.5 million, reflecting a growth rate of 13.0 percent, and rental and leasing activities, with an increment of RM342.8 million, indicating an impressive growth rate of 25.1 percent.

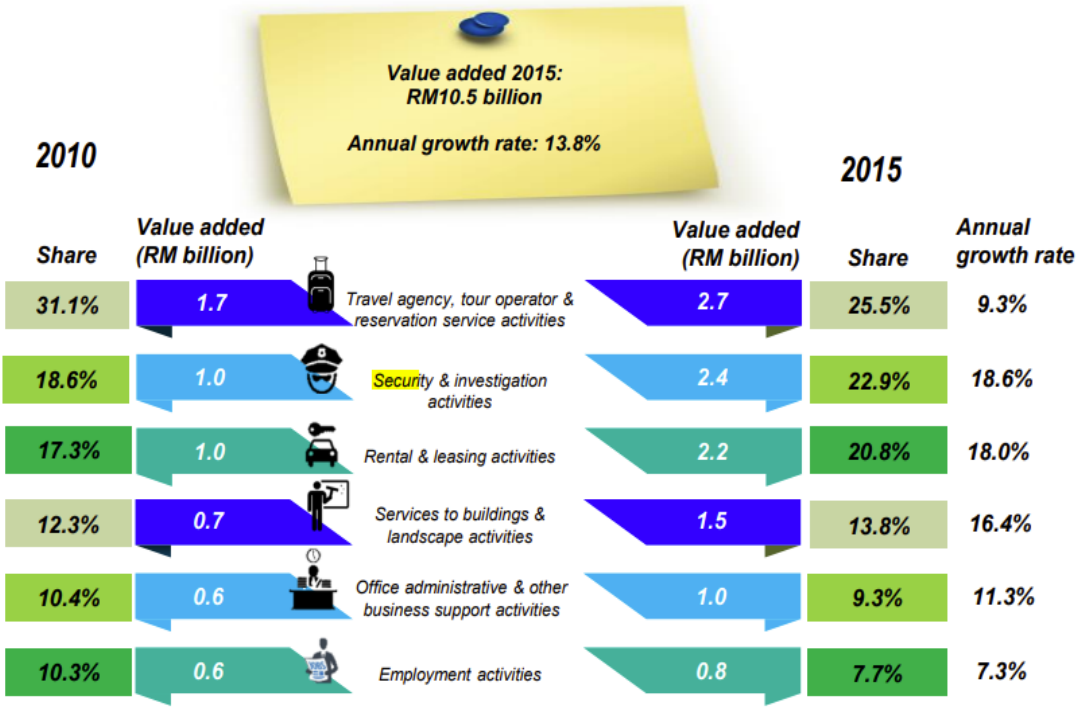

Figure 2.4: Value added of Administrative and Support Services by Activities, 2010 and 2015 (https://newss.statistics.gov.my/)

Comparing the figures to those from 2010, security and investigation activities continued to maintain the highest level of salaries and wages paid, totaling RM1,184.9 million, and accounting for a significant share of 29.9 percent. Subsequently, travel agency, tour operator, and reservation service activities reported salaries and wages amounting to RM887.6

million, representing 22.4 percent of the total, and services related to building and landscape activities with RM595.7 million, contributing 15.0 percent of the overall expenditure in this category.

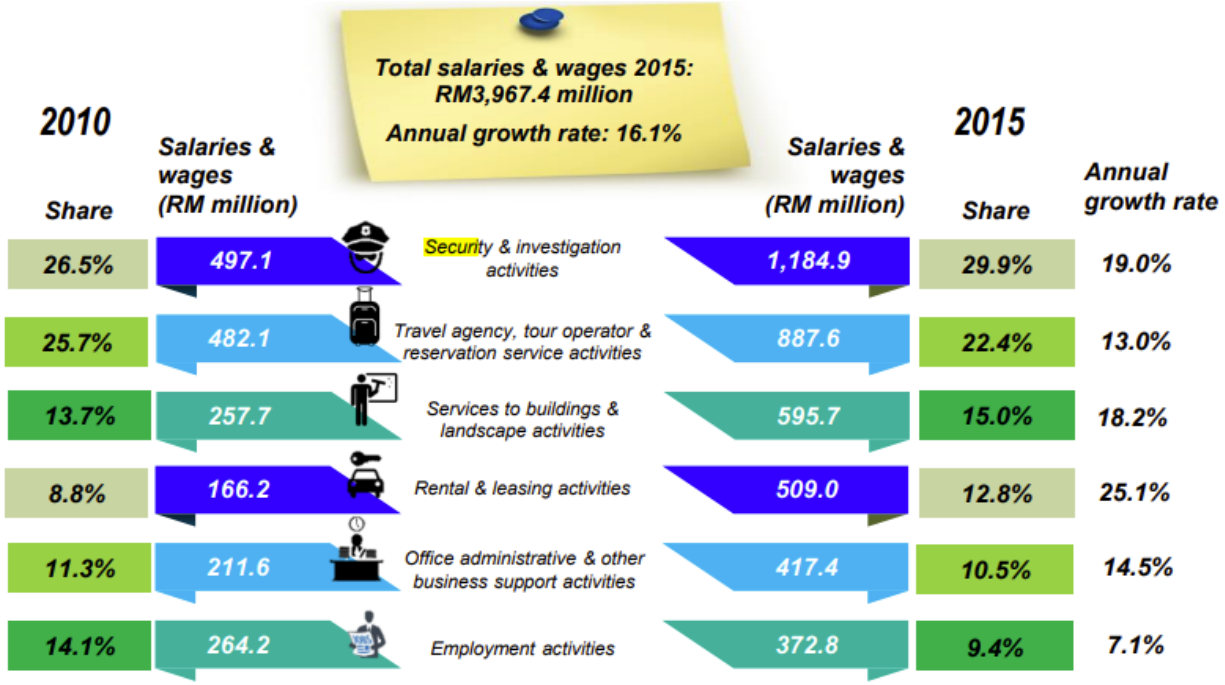

Figure 2.5: Salary and Wedges of Administrative Support Services by Activities, 2010 and 2015 (https://newss.statistics.gov.my/)

In the domain of administrative and support services, the average monthly salary stood at RM2,027, displaying a commendable annual growth rate of 6.9 percent, as depicted in Figure 5. Among the various subsectors within this domain, individuals engaged in rental and leasing activities earned the highest average monthly salary, which amounted to RM2,618. Following closely, the second-highest average monthly salary was reported in the field of office administrative and other business support activities, with an amount of RM2,593. This was trailed by travel agency, tour operator, and reservation service activities, where individuals earned an average monthly salary of RM2,581.

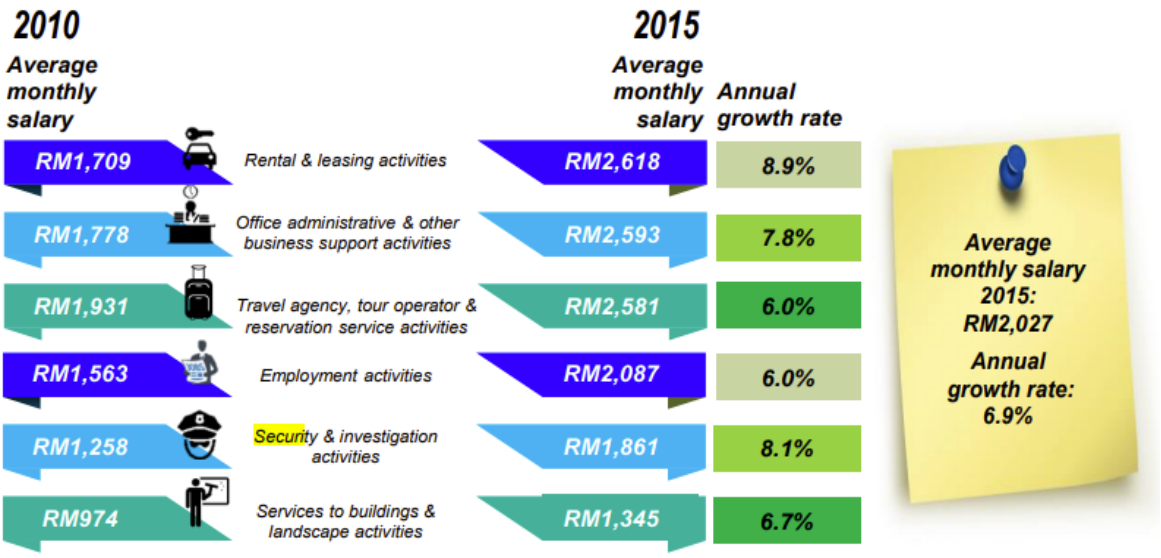

Figure 2.6: Average Montly Salary Administrative and Support Services by Activities, 2010 and 2015 (https://newss.statistics.gov.my/)

2.9 The Existing NOSS Areas Related to MSIC 2008

The National Occupational Skills Standards (NOSS) is a standard system used in Malaysia to identify, measure, and validate job skills across various industries. NOSS is developed by the *Jabatan Pembangunan Kemahiran (JPK)* and constitutes a set of standards that depict the competency levels and skills required for workers in specific fields. NOSS often correlates with the Malaysia Standard Industrial Classification (MSIC) 2008 and MSIC 2000, as MSIC is a classification code used to group economic activities into categories and sub-categories. When formulating NOSS for a specific job field, the relevant categories and sub-categories may refer to the MSIC 2008 and MSIC 2000 codes. Here are some examples of existing NOSS areas related to MSIC 2008 codes in Malaysia:

Table 2.4: NOSS areas related to MSIC 2008

No	NOSS Area	Program Code	MSIC 2008 Code
1	Security Services Operation	DS-010-2:2013	80100 - Private security activities
2	Security Services Supervision	DS-010-3:2013	80100 - Private security activities
3	Security Operation Management	DS-010-4:2013	80100 - Private security activities
4	Security Operation Management	DS-010-5:2013	80100 - Private security activities
5	Seaport Security Surveillance	DS-012-3:2015	80100 - Private security activities
6	Seaport Security Control	DS-012-4:2015	80100 - Private security activities
7	Seaport Security Management	DS-012-5:2015	80100 - Private security activities
8	Electronic Security System Installation & Maintenance	DS-050-3:2013	80200 - Security systems service activities
9	Security Senior Technician (Design)	EE-110-3	80200 – Security systems service activities
10	ICT System Security Technologist	IT-090-5	80200 - Security systems service activities
11	Telecommunications System and Network Security Technical Operation	J619-002-4:2021	80200 - Security systems service activities
12	Telecommunications System and Network Security Technical Operation Management	J619-002-5:2021	80200 - Security systems service activities
13	Cyber Security Penetration Testing & Assessment	J620-001-5:2019	80200 - Security systems service activities
14	Security Assistant	SS-010-1	80100 - Private security activities
15	Dog Unit Security Supervisor (K9)	SS-030-3	80100 - Private security activities
16	Investigation Detectives	SS-060-3	80300 - Investigation and detective activities

2.10 The Comparison of Jobs Between Malaysia and Selected Countries

Malaysia's industrial revolution (IR) has been characterised by extensive State control guaranteeing a high level of managerial prerogative within the workplace, minimal overt conflict and very little bargaining power for labour. These arrangements were an integral component of the package to attract investors when Malaysia's industrialization strategy focused on low-cost, export-oriented industries. Since then, however, Malaysia has adopted the goal of developed country status by 2020 and embarked on a higher value-added, more capital-intensive industrialization strategy. The security and investigation industry in Malaysia has been growing progressively in recent years, driven by government initiatives, Malaysia's strategic location, and reputation as a safe and secure destination for businesses and tourists. The industry is experiencing various technological disruptions, including the increasing use of advanced technologies such as AI, facial recognition, and cybersecurity. While the industry faces challenges such as increasing competition and the need to stay updated with emerging technologies and industry trends, the future outlook remains positive, with expected growth in the security and investigation services industry, diverse industries, and the ongoing digital transformation of the industry. As the industry continues to evolve, security and investigation firms need to stay informed and adapt to emerging trends and technologies to remain competitive in the market (Javaida et al., 2022). However, comparing job related to the security aspects between Malaysia and other countries involves considering factors such as the job market, industries, economic conditions, and security. Most of the security and investigation sector regulation is quite old and had placed focus on information security and cybersecurity more than the stakeholder's skill and knowledge about security. There is a general comparison of job aspects between Malaysia and other countries related to security and investigation industry.

The security and investigation sector in Malaysia is crucial for maintaining law and order, ensuring public safety, and combating criminal activities. Key aspects of the sector include the RMP which is responsible for maintaining peace, preventing and investigating crimes, and enforcing laws throughout the country. Malaysia actively engages in counterterrorism efforts, managing immigration policies, border control, and addressing human trafficking and smuggling. Cybersecurity is recognized as a vital aspect of Malaysia's security, with agencies like Cyber Security Malaysia addressing cyber threats and providing cybersecurity education. Intelligence and surveillance are also significant aspects of Malaysia's security sector, with the Special Branch of the RMP gathering intelligence related to terrorism, organized crime, and subversive activities. Private security companies provide services such

as manned guarding, surveillance systems, event security, and executive protection. Forensic investigations are essential in criminal investigations, with the Malaysian National DNA Databank enhancing the effectiveness of forensic investigations. The Malaysian Anti-Corruption Commission (MACC) is responsible for combating corruption in public and private sectors, investigating cases, educating the public, and promoting transparency and accountability in governance (Ismail et al., 2010).

The security and investigation sector in the United States is complex and involves various government agencies, law enforcement bodies, and private security companies. Key aspects include federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Marshals Service (USMS), and Secret Service, the Department of Homeland Security (DHS), state and local law enforcement, counterterrorism efforts, cybersecurity, intelligence community, private security industry, and forensic investigations. Federal law enforcement agencies maintain national security and combat various forms of crime, while the DHS protects the country from threats such as terrorism, border security, cyber threats, and natural disasters. State and local law enforcement agencies maintain law and order within their jurisdictions, while local law enforcement agencies play a crucial role in community policing and crime prevention. The US has established several agencies and initiatives to protect critical infrastructure and combat cyber threats, such as the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI's Cyber Division. The intelligence community comprises multiple agencies, gathering intelligence, analyzing threats, and providing critical information to policymakers and law enforcement agencies. The private security industry in the US is vast and diverse, offering services such as physical security, event security, executive protection, and security consulting. Forensic science and forensic investigations are essential in the U.S. criminal justice system, with federal, state, and local law enforcement agencies having forensic laboratories and teams of experts (Castrillón Rias & Guerra Molina, 2016).

The UK's security and investigation sector comprises government agencies, law enforcement bodies, and private security companies. The country has a devolved policing system, with separate forces for England and Wales, Scotland, and Northern Ireland. Key security and intelligence agencies include Security Services (MI5), Secret Intelligence Service (MI6), Government Communications Headquarters (GCHQ), and National Crime Agency (NCA), which focus on counterterrorism, counterintelligence, cybersecurity, and tackling serious organized crime. The UK has actively participated in counterterrorism efforts,

preventing terrorist attacks, investigating terrorist networks, and prosecuting individuals involved in terrorism-related activities. The UK Border Force is responsible for securing the UK border, preventing illegal immigration, and combating cross-border criminal activities. The National Cyber Security Centre (NCSC) provides advice, guidance, and incident response to protect critical infrastructure and enhance cybersecurity across the country. Law enforcement agencies have dedicated cybercrime units to investigate digital crimes. The private security industry is regulated by the Security Industry Authority (SIA), offering a range of services, including manned guarding, CCTV surveillance, event security, and close protection. Forensic science plays a crucial role in criminal investigations in the UK, with the Forensic Science Regulator overseeing the quality and standards of forensic science providers. The NCA leads the fight against serious and organized crime, focusing on drug trafficking, human trafficking, cybercrime, money laundering, and firearms offenses, working in collaboration with other law enforcement agencies and international partners (Stahl et al., 2012).

Indonesia's security and investigation sector includes government agencies, law enforcement bodies, and private security companies. The Indonesian National Police (POLRI) is the primary law enforcement agency responsible for maintaining public order, preventing and investigating crimes, and ensuring security. It consists of specialized units like the criminal investigation unit, traffic police, counterterrorism unit, and special detachment 88 for counterterrorism operations. The State Intelligence Agency Indonesia gathers intelligence and advises the government on security matters. Indonesia has been combating terrorism for years, with the National Counterterrorism Agency (BNPT) coordinating and enhancing efforts. The Indonesian Maritime Security Agency (Bakamla) maintains border security, maritime surveillance, and preventing illegal activities in Indonesia's territorial waters. The National Cyber and Crypto Agency (BSSN) oversees cybersecurity and encryption-related matters, while the Directorate General of Immigration manages immigration policies, border control, and immigration-related investigations. Private security companies provide services such as manned guarding, surveillance systems, event security, and executive protection. The Indonesian Corruption Eradication Commission (KPK) investigates corruption cases, prosecutes offenders, and promotes transparency and accountability in governance. Forensic science plays a crucial role in criminal investigations in Indonesia, with the POLRI operating forensic laboratories and employing forensic experts (Gill & Wilson, 2013).

Singapore's security and investigation sector is well-developed, involving government agencies, law enforcement bodies, and private security companies. Key aspects include the Singapore Police Force (SPF), Internal Security Department (ISD), Immigration and

Checkpoints Authority (ICA), Singapore Civil Defense Force (SCDF), Cybersecurity Agency of Singapore (CSA), Central Narcotics Bureau (CNB), private security industry (manned guarding, access control, event security, and security consultation), forensic science, financial investigation, and counterterrorism efforts. The SPF is responsible for maintaining law and order, preventing and investigating crimes, and ensuring public safety. The ICA manages immigration policies, border control, and customs enforcement, while the SCDF is responsible for firefighting, rescue operations, and emergency medical services. The CSA coordinates cybersecurity efforts, while the Central Narcotics Bureau combats drug-related offenses. Singapore's private security industry is regulated by the Police Licensing and Regulatory Department (Nalla et al., 2015).

The security and investigation sector in China is complex and involves various government agencies, law enforcement bodies, and intelligence organizations. Key aspects include the Ministry of Public Security (MPS), State Security Ministry (MSS), People's Armed Police (PAP), Cybersecurity Administration of China (CAC), and the Ministry of State Security (MSS). The MPS is responsible for maintaining public order, preventing crimes, and ensuring internal security. The MSS focuses on intelligence gathering, counterintelligence operations, and safeguarding national security. The PAP is responsible for maintaining public security, handling riots and protests, protecting key government installations, and supporting local law enforcement agencies. The CAC oversees cybersecurity efforts, while the MSS is responsible for foreign intelligence gathering, counterintelligence, and national security. Public security intelligence units operate within the MPS, focusing on domestic security issues. Forensic science plays a crucial role in criminal investigations in China, with the MPS operating forensic laboratories. China has implemented strict measures to combat terrorism, with counterterrorism units established within the MPS and the PAP. The private security industry in China is growing, providing services like manned guarding, event security, and asset protection, regulated by local public security authorities (Tanner, 2002).

The security and investigation sector in England comprises various government agencies, law enforcement bodies, intelligence organizations, and private security companies. Key aspects of the sector include police forces, the NCA MI5, MI6, GCHQ, Serious Fraud Office, His Majesty's Revenue and Customs (HMRC), and private security industry. Police forces operate at various levels, while the NCA focuses on combating serious and organized crime. MI5 is responsible for domestic intelligence, MI6 for foreign intelligence, and GCHQ for signals intelligence. The Serious Fraud Office investigates and prosecutes complex fraud cases, while HMRC enforces tax laws and investigates financial crimes. The private security

industry in England offers services such as manned guarding, event security, surveillance, and asset protection, under the regulation of the Security Industry Authority (SIA). Forensic science is crucial in criminal investigations in England, with organizations like police forces and forensic laboratories conducting forensic analysis, autopsies, and expert testimony in court (England & Center, 2009).

Qatar's security and investigation sector is well-developed, involving government agencies, law enforcement bodies, intelligence organizations, and private security companies. Key aspects include the Ministry of Interior (MOI), State Security Bureau (SSB), Public Prosecution, Internal Security Force (ISF), Cybercrime Investigation Unit, Private Security Industry, Forensic Investigations, and Counterterrorism Efforts. The MOI oversees various departments and entities involved in security, while the SSB safeguards national security, counters terrorism, and protects Qatar's interests. The Public Prosecution is responsible for investigating and prosecuting criminal cases, while the ISF is paramilitary and plays a crucial role in counterterrorism operations and public order. The MOI also establishes a specialized unit for cybercrimes, ensuring cybersecurity and raising awareness about online safety. The private security industry in Qatar is well-regulated, with private security companies providing services such as manned guarding, access control, event security, and security consultation. Forensic science plays a vital role in criminal investigations, with the MOI operating forensic laboratories to analyse evidence and provide expert services. Qatar actively participates in international counterterrorism efforts, collaborating with regional and international partners, sharing intelligence, and taking action against individuals and organizations involved in terrorist activities (Mehreza & Bakria, 2019).

The security and investigation sector in Australia is well-developed, involving government agencies, law enforcement bodies, intelligence organizations, and private security companies. Key aspects of the sector include the Australian Federal Police (AFP), Australian Security Intelligence Organisation (ASIO), Australian Border Force (ABF), State and Territory Police, Australian Criminal Intelligence Commission (ACIC), Australian Transaction Reports and Analysis Centre (AUSTRAC), private security industry, forensic investigations, and counterterrorism efforts. The AFP is responsible for enforcing federal laws, investigating crimes, and maintaining national security. ASIO is responsible for domestic intelligence, while the Border Force manages borders and immigration and customs enforcement. Each state and territory have its own police force responsible for maintaining law and order, preventing crimes, and ensuring public safety. The ACIC collaborates with law enforcement agencies to target organized crime, drug trafficking, money laundering, and other serious offenses.

AUSTRAC is responsible for combating money laundering, terrorism financing, and other financial crimes (Prenzler & Sarre, 2012).

2.11 The Relationship between Industry and Industrial Revolution

In OF, there are several elements of the industrial revolution that can influence how work is conducted. These elements are encompassed within the Fourth Industrial Revolution, which represents the latest stage in industrial revolution. The elements of the industrial revolution that are relevant to OF was explained independently in the next sub section.

2.11.1 Artificial Intelligence (AI)

AI is a technology that enables computers and other systems to perform tasks that typically require human intelligence. In the realm of work, AI impacts automated processes, data analysis, and information management. Jobs involving routine tasks or large data collection can be automated with AI, reducing human workload and enhancing efficiency.

2.11.2 Big Data

The industrial revolution leads to the generation of big data, referring to a vast and complex amount of data produced through digital activities and human interactions. This data is analysed and used for improved decision-making, such as in strategic planning, market analysis, and operations management within specific industries.

2.11.3 Internet of Things (IoT)

IoT involves a network of interconnected devices that can communicate and share data without human intervention. In the workplace, IoT enables remote monitoring, quality control, and environmental maintenance more efficiently. For example, the use of IoT sensors in manufacturing processes can enhance product quality and reduce maintenance costs.

2.11.4 Integrated Design

The industrial revolution introduces integrated design approaches that encompass interconnected processes and systems. In the field of work, integrated design allows collaboration across various job fields and facilitates the integration of cutting-edge technology into innovation and production processes.

2.11.5 Robotics and Automation

Robotics and automation technologies are increasingly dominating the workplace. The use of robots in manufacturing, shipping, and other industries helps enhance productivity and reduce work-related risks. Automation also leads to changes in the skill requirements of workers, necessitating adaptation to new technologies.

2.11.6 Augmented Reality (AR) and Mixed Reality (MR)

AR and MR provide enriched or blended reality experiences with the virtual world. In industries, these technologies are used for training and maintenance, allowing workers to perform tasks more accurately and efficiently.

The Fourth Industrial Revolution is reshaping the way work is conducted across various industries and is transforming many aspects of jobs. It is crucial for workers to take steps to enhance their skills and adapt to the latest technologies to ensure employability and success in this increasingly advanced industrial era.

2.12 Summary

Based on various collected and outlined reference sources, the need for the development of OF security and investigation aligns with the context of Malaysia. Other countries around the world have already developed such OF, albeit some have done so for quite some time. The development of OF in Malaysia has now become a necessity, given the increasing pace of industrial revolution, emphasizing the importance of safety and investigation across various sectors. Immediate actions need to be taken to control the situation and address safety issues, particularly within the industrial field.

CHAPTER III

METHODOLOGY

3.1 Introduction

Methodology combines desk research, field studies, expert insights, and stakeholder engagement to develop a comprehensive and contextually relevant framework for OF security and investigation in Malaysia. In this section, we will provide a more detailed description of the research design, sample, instruments, study procedure, and data analysis used in this study.

3.2 Research Design

The Design and Development Research (DDR) approach (Sahrir et al., 2012), is a systematic and iterative methodology used in educational research and instructional design. It involves the creation, implementation, and evaluation of innovative educational interventions, materials, or programs. DDR is a systematical research approach that focuses on understanding and interpreting social phenomena through non-numerical data, such as words, images, and narratives. It aims to explore and gain insights into the complexities, meanings, and contexts of human experiences, behaviors, and interactions.

DDR approach emphasize in-depth exploration, subjective interpretation, and the researcher's role in shaping the research process. This approach is particularly suited for investigating complex and contextually rich phenomena where numerical measurement may not capture the full depth and nuances of the subject matter. DDR approach is widely used in various disciplines, including sociology, anthropology, psychology, education, and healthcare. They are particularly valuable for exploring topics where little is known, investigating social and cultural contexts, and generating theories or hypotheses for further exploration. In this study, we will accomplish the first objective during the initial phase. Objectives 2, 3, 4, and 5 will be addressed in the second phase, while objective 6 scheduled for completion during the third phase.

Table. 3.1: Developmental Research (DDR)

Phase 1 The Analysis Phase	Phase 2 Development of the OF	Phase 3 Evaluation of the OF
Objective 1: To identify the needs of the current and future needs of the industry based on previous studies.	**Objective 2:** • To identify the job areas, job titles and job classifications according to the definitions and levels of Malaysia Occupational Skills Qualification Framework (MOSQF) in N80 • To identify the responsibilities and job descriptions for each job title. • To identify the critical job and the Job Description for N80 related to current developments in the industry • To analyze the competency needed to address the demand and supply of the industry in Malaysia	**Objective 3:** To document and validate the security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0.

3.3 Sample

The purposive sampling method was used to select respondents who are considered the most relevant or important to achieve the research objectives. The researcher actively selects respondents based on specific characteristics or criteria related to the study topic. In this study, a sample size of 23 respondents was chosen to participate. These 23 participants were carefully selected to ensure representation from three distinct areas: Private Security Activities Group (9 respondents), Security System Service Activities (7 respondents), and Investigation Activities (7 respondents).

3.4 Focus Group Discussion (FGD)

During the second phase of the study, two distinct research techniques were employed: Focus Group Discussion (FGD) and the Fuzzy Delphi technique. FGD is a qualitative research method used in social science and market research to gather information, insights, and opinions from a small group of participants about a specific topic or set of issues. FGD are typically conducted by a skilled moderator or facilitator who guides the discussion, encourages

participation, and probes for deeper insights. The detailed breakdown of the key aspects of FGD was explained independently in the next sub section.

3.4.1 Moderator/Facilitator: A skilled moderator or facilitator leads the discussion. Their role is crucial, as they are responsible for ensuring that the conversation stays focused, productive, and respectful. Moderators should have excellent interpersonal skills, be neutral, and maintain a balance in participation among the group members. They use a pre-determined set of questions or topics as a guide for the discussion.

3.4.2 Purpose and Objectives: FGD was conducted to explore participants' perceptions, attitudes, beliefs, and experiences related to a particular topic. The research objectives should be clearly defined before the discussion, and the FGD is designed to address these objectives.

3.4.3 Structured Discussion: FGD is semi-structured discussions. The moderator introduces topics, questions, or scenarios related to the research objectives. However, the conversation is allowed to flow naturally, with participants encouraged to express their thoughts and engage in open dialogue. The facilitator may probe for more in-depth responses and encourage participants to respond to each other.

3.4.4 Duration: FGD typically last one to two hours, depending on the complexity of the topic and the number of questions to be addressed. It's essential to strike a balance between gathering sufficient information and preventing participant fatigue.

3.4.5 Location and Setting: The researcher will decide on the location and setting for the research activities, taking into account the preferences and input of the experts involved. Given that the experts are geographically dispersed, their consent to convene for the FGD is highly valued. In cases where physical attendance is not feasible for any expert, the moderator will arrange for online communication to ensure their participation.

3.4.6 Recording and Documentation: FGD is often audio or video recorded to capture participants' responses accurately. Detailed notes are taken during the discussion, including non-verbal cues, participant interactions, and any noteworthy observations.

3.4.7 Data Analysis: After the FGD, the recorded data and notes are transcribed and analyzed. Researchers look for recurring themes, patterns, and insights that emerge from the discussion. The results are often used to inform decision-making, policy development, product development, or further research.

3.4.8 Confidentiality: Participants' identities and their specific responses are typically kept confidential to encourage open and honest discussion. Participants are usually assigned pseudonyms or identifiers to protect their privacy.

3.4.9 Sampling and Recruitment: Careful consideration is given to the recruitment of participants to ensure they represent the target population or share relevant characteristics. Sampling methods may vary depending on the research goals.

FGD is a valuable qualitative research tool for gaining in-depth insights into participants' perspectives and experiences related to a specific topic. They provide a platform for rich, interactive discussions and are commonly used in various fields, including market research, social sciences, healthcare, and more.

3.5 Site Visit and Interview

In instances where additional clarification is deemed necessary following a FGD, a combination of site visits and interview methods will be employed. The site visit to the agency associated with N80 is intended to provide firsthand exposure to industry practices. The subsequent interview sessions aim to meticulously resolve any ambiguities before advancing to the next stage of the study. A meticulously crafted semi-structured interview protocol will be adhered to, ensuring the validity of the obtained insights. Following the interviews, the collected findings will undergo thematic analysis, facilitated by NVIVO version 12 software, to prepare them for the subsequent phase of research.

3.5.1 Data Collection: This research conducted semi structured interview session through face-to-face, over the phone and site visit. The interviewer recorded participants' responses by using audio-recording and noted down.

3.5.2 Data Analysis: After data collection, researchers analyze the interview transcripts and notes by using thematic analysis method. This procedure of data analysis was guided by Braun

and Clarke's (2006) six phase of thematic analysis. The process includes (1) becoming familiar with the data, (2) generating code, (3) generation themes. (4) reviewing themes, (5) defining and naming themes, and (6) producing the report.

3.5.3 Ethical Considerations: Researchers must adhere to ethical guidelines when conducting interviews. This includes obtaining informed consent from participants, ensuring confidentiality, and addressing any potential harm or discomfort that may arise from discussing sensitive topics.

3.5.4 Reporting: The findings from interviews are typically presented in research reports, articles, or presentations. Researchers used quotes, anecdotes, and summaries to support their conclusions and provide context for their findings.

3.6 Fuzzy Delphi Method (FDM)

The Fuzzy Delphi Method (FDM) is an extension of the traditional Delphi Method, a structured forecasting and consensus-building technique used in various fields, including research, business, and decision-making. While the Delphi Method seeks to reach a consensus among a panel of experts, the FDM adds an element of fuzziness to account for uncertainty and ambiguity in the experts' judgments and predictions. By incorporating fuzzy logic, the FDM provides a more flexible and nuanced approach to capturing expert judgments and consensus in situations where precise numerical estimates may not be feasible or appropriate. It acknowledges and accommodates the inherent uncertainty and imprecision that often characterize complex real-world problems. The structure of the FDM includes:

Step 1:

In the initial phase, the first task involves determining the total number of experts participating in the study, which amounts to 23 experts distributed across three distinct groups

Step 2:

Following the determination of the expert groups, the next step is to establish a linguistic scale based on fuzzy triangle numbers. In this study, a choice was made to employ five fuzzy scales instead of 7 due to time constraints. Additionally, prior to implementing the fuzzy technique, a FGD was conducted to shape the research instrument.

Step 3:

The third step involves defining the threshold distance between numbers to establish the threshold value. This value is calculated using a specific threshold formula. The study sets a threshold value acceptance criterion of less than or equal to 0.2; values exceeding 0.2 are considered unacceptable.

Step 4:

To determine the agreement within the group, an item must reach a threshold value of at least 75% of the established threshold value (0.2). Items falling short of this criterion will be rejected.

Step 5:

The fifth step involves the calculation of an aggregate fuzzy evaluation by summing all the fuzzy numbers. This calculation aids in determining the priority ranking of items in the subsequent step.

Step 6:

The final step, known as "defuzzification", is the process through which the priority ranking of items for each variable or sub-variable is determined. This step helps establish the relative importance of each item within the study's framework.

3.7 Research Instrument

Developing an effective FGD, interview and Fuzzy Delphi protocol involves a systematic process to ensure that the process are well-structured, focused, and yield valuable insights. The first step is to clearly define the research objectives and goals of the study. This clarity helps in determining the scope of the methods and the specific areas to explore. Next, identify the key variables and themes relevant to the research. These could include topics, concepts, or phenomena central to the study's focus. Once these are established, formulate a set of open-ended questions that encourage participants to elaborate on their experiences, perspectives, and insights. These questions should flow logically and cover the identified variables comprehensively which are private security activities, security system service activities, and investigation and investigation activities. These variables derived from MSIC 2008 version 1.0. After drafting the initial protocol, it's crucial to review and refine the questions for clarity, relevance, and coherence. Piloting the protocol with a small sample of participants allows for adjustments based on feedback, ensuring that the FGD, interview and Fuzzy Delphi process is

well-structured and aligned with the research objectives. The finalized FGD, interview and Fuzzy Delphi protocol should include clear instructions for the interviewer, a warm introduction, the sequence of questions, prompts for follow-up, and a polite closing.

The protocol should be adaptable to various participants and contexts. Researchers must be prepared to improvise and probe deeper based on participants' responses to elicit rich and meaningful data. Flexibility in conducting the FGD, Interview and Fuzzy Delphi allows for the exploration of unexpected insights and nuances that might arise during the process. Additionally, conducting a pilot test with a diverse group of participants helps refine the protocol further and identify potential challenges or biases. A well-developed protocol serves as a roadmap for conducting structured and insightful research, ultimately contributing to the depth and quality of research outcomes.

3.8 Study Procedure

The first phase is the needs analysis phase. This phase is carried out by collecting literature studies and analyzing documents related to the requirements of OF development. The researcher gathers all this information and conducts a systematic review for the purpose of OF development.

The second phase is design and development. In this phase, the researcher involves 23 experts from selected stakeholders using the purposive sampling method. During this phase, a FGD is conducted to obtain suggestions and feedback from the experts involved in the development of OF for security and investigation activities. The strategic employment of the Fuzzy-Delphi method (Yusoff et al., 2021), and active involvement from key players in the industrial domain will be conducted to get the ultimate consensus. The DDR approach establishes the research's foundation, while the FGD sessions are designed to elicit qualitative insights into job domains and titles.

In contrast, the Fuzzy-Delphi method yields quantitative data concerning the sector's current landscape, encompassing the demand for skilled professionals, requisite skills, employment trends, emerging talents, positions pertinent to the Fourth Industrial Revolution, as well as the challenges and concerns hindering the sector's expansion. The FGD sessions are divided into two distinct segments. The initial session centers on the identification of occupational structures (OS) and the corresponding responsibilities (OR). Subsequently, the second session focuses on developing occupational descriptions for high-demand roles. An exhaustive overview of the sector is furnished, elucidating its definition, scope, prevailing local

dynamics, and industry trajectories. Close collaboration with industry luminaries and stakeholders guarantees that the OF accurately mirrors the sector's competency prerequisites.

The third phase is evaluation. In this phase, the researcher also involves 23 experts from stakeholders to assess the produced OF. Experts in this phase are also selected using the purposive sampling method to conduct session of interview.

Table 3.2: Summary of the research methods, analysis and outputs for achieving the objectives

Phase 1 **The Analysis Phase**	**Phase 2** **Development of the OF**		**Phase 3** **Evaluation of the OF**
Objective 1: To identify the needs of the current and future needs of the industry based on previous studies.	**Objective 2:** • To identify the job areas, job titles and job classifications according to the definitions and levels of Malaysia Occupational Skills Qualification Framework (MOSQF) in N80 • To identify the responsibilities and job descriptions for each job title. • To identify the critical job and the Job Description for N80 related to current developments in the industry • To analyze the competency needed to address the demand and supply of the industry in Malaysia	**Objective 3:** To document and validate the security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0.	**Objective 1:** To identify the needs of the current and future needs of the industry based on previous studies.
Method • Literature review • Document review • Relevant policies and acts • Existing NOSS • Other documents	**Method** • Focus Group Discussion (FGD) • Site Visit & Interviews	**Method** • Focus Group Discussion (FGD) – verification of OS and OR • Fuzzy Delphi Method – identify critical jobs and job descriptions	**Method** • Presentation at international conference • Interview with experts
Data analysis Content analysis	**Data analysis**	**Data analysis** Thematic analysis	**Data analysis** Thematic analysis

Phase 1 The Analysis Phase	Phase 2 Development of the OF		Phase 3 Evaluation of the OF
	Thematic analysis from FGD and interviews	Defuzzification to achieve consensus	
Output Information for Chapters 1, 2 and 3	**Output** Draft Occupational Structure (OS) & Occupational Responsibilities (OR)	**Output** Review & Refine OS and OR Brainstorming & Develop Occupational Descriptions (OD) Identify critical jobs titles	**Output** Update of OF for N80

3.9 Data Collection and Analysis

3.9.1 Phase 1: Need Analysis

The first phase involves analysis conducted using a systematic review approach, which entails gathering recent studies related to security and investigation, both domestically and internationally. A systematic review analysis is a research method used to systematically gather, assess, and synthesize existing research studies on a specific topic or research question. It aims to provide a comprehensive and unbiased overview of the available evidence on a particular subject. Systematic reviews are often used to inform evidence-based decision-making and policy development. Systematic review analyses are highly structured and rigorous, aiming to minimize bias and provide a reliable overview of the existing research. Document analysis is also conducted to examine previously developed OF. Document analysis is a research analysis that involves systematically examining and interpreting various types of documents to extract meaningful information, insights, or patterns. It is commonly used in qualitative research to gather data from existing textual, visual, or audiovisual sources. Document analysis can provide valuable insights into historical contexts, social dynamics, organizational processes, and more.

3.9.2 Phase 2: Design and Development

In the second phase, data is analyzed using Thematic analysis through FGD and Fuzzy Delphi technique, where the researcher identifies emerging themes from respondents' answers concerning aspects that can be incorporated into the OF. Thematic analysis is a qualitative research method used to identify, analyze, and report patterns (themes) within qualitative data. It involves systematically coding and categorizing textual or visual data in order to uncover underlying themes, patterns, or meanings. Thematic analysis allows researchers to gain insights into participants' perspectives, experiences, and interpretations.

The protocol for FGD 1 in general is as follows:

(1) The Opening and Introduction.

(a) Introduction to expert panel

(b) Introduction to the purpose and context of the study, the exclusion and inclusion criteria for the Groups N80: Private Security Activities (N801), Security Systems Service Activities (N802) and Investigation Activities (N803).

(2) The Development of the Occupational Framework. The discussion and contribution among panel members will be to obtain the occupational structure (OS) and job description (JD).

For objective 4 and 5, FGD 2 and the Fuzzy Delphi Method was conducted. In FGD 2, the protocol is to obtain the job-in demand for the skills, jobs' title and critical jobs.

a) **Skill Competence Needed:** The comprehensive skill set essential for industry workers to effectively fulfill their current and prospective roles, alongside factors influencing the potential skills gap among both recent graduates and existing employees.

b) **Job Demand Analysis:** Examination of job sectors or categories facing shortages or surpluses of workers, identifying critical job roles and factors contributing to the scarcity of labor.

c) **Emerging Skill Requirement**s: Anticipated upcoming skills crucial for industry advancement, including the reasons prompting the necessity for these specific skills.

d) **Industry Challenges:** Identifying prevalent issues or hurdles commonly faced within the industry.

The assessment, conducted through FGD 3, aimed to authenticate and affirm the OS findings, merging insights from the finding's dissemination meeting.

Fuzzy Delphi Method

The FDM was employed to ascertain agreement among experts when identifying crucial job roles. The Fuzzy Delphi Questionnaire, formulated based on expert interviews conducted before FGD 2, aimed to establish a consensus regarding the pivotal jobs within the industry.

The information gathered through the questionnaire underwent analysis using the Fuzzy Delphi's Triangular Fuzzy Number and a Defuzzification Process, as proposed by Ishikawa et al. (1993). The FDM allows for group decisions to be reached, with results and scores for each item organized hierarchically. In this study, the experts' responses, rated on a five-point Likert scale in the questionnaire, were transformed into Fuzzy numbers utilizing a five-point linguistic scale. The Triangular Fuzzy Number comprises three mean points (m1, m2, m3): representing the minimum, most plausible, and maximum values derived from a mean graph. The defuzzification process facilitates ranking the consensus. The triangular fuzzy numbers were employed to compute the evaluation value, and all data were tabulated to derive the average value (m1, m2, m3) (Kaufmann & Gupta, 1988). Subsequently, the formula was used to calculate the average distance between two fuzzy numbers:

$$d(\overline{m},\overline{n}) = \sqrt{\frac{1}{3}\left[(m_1 - n_1)^2 + (m_2 - n_2)^2 + (m_3 - n_3)^2\right]} \qquad (1)$$

d = threshold value

m1 = average of minimum value

m2 = average of average value

m3 = average of maximum value

n1 = fuzzy number (minimum)

n2 = fuzzy number (average)

n3 = fuzzy number (maximum)

The calculation of the distance between two fuzzy numbers along with the threshold value, denoted as 'd', is conducted to determine consensus. The criterion dictates that if d is equal to or less than 0.25, it signifies unanimous agreement among all panel members. When there are discrepancies in the results, a subsequent round becomes necessary (Kaufmann & Gupta, 1988). In this particular scenario, the calculated values of d are less than or equal to 0.25, and the consensus percentage exceeds 70%, meeting an acceptable criterion. The attainment of group consensus occurs when the consensus percentage reaches 70%. One of the merits of employing the FDM lies in its validity, which persists even when the number of participating experts is limited (Siraj & Ali, 2008).

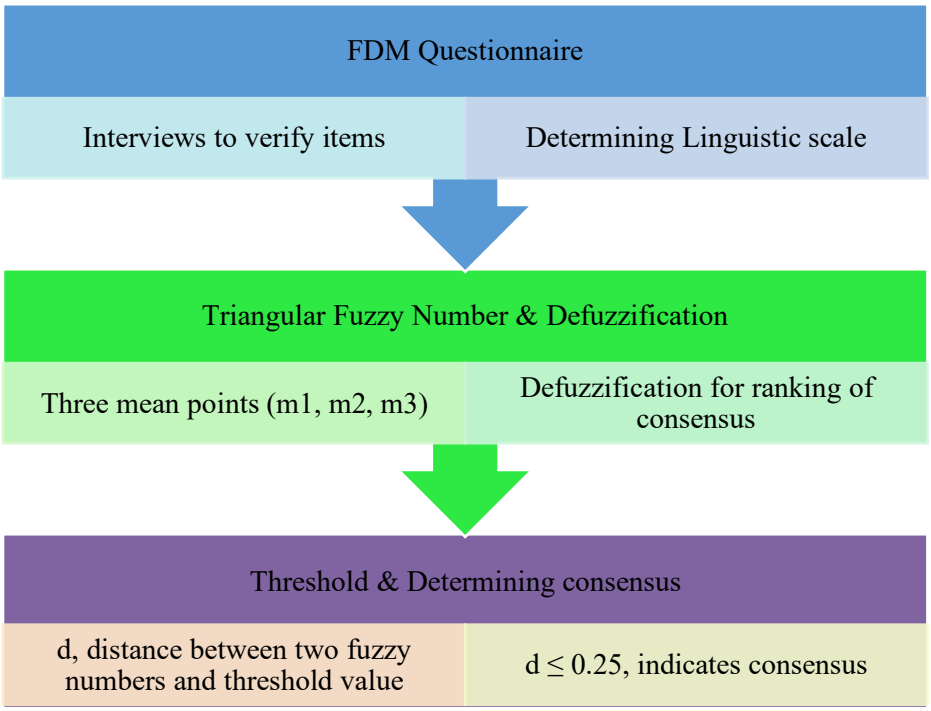

Figure 3.1: Data Analysis for the Fuzzy Delphi Method

3.9.3 Phase 3: Evaluation

The third phase also utilizes thematic analysis, derived from respondents' answers regarding their evaluation of the produced OF. Thematic analysis is widely used in various fields, including social sciences, psychology, healthcare, education, and more, to explore and understand complex qualitative data and uncover meaningful insights.

3.10 Analysis Data Phase

This section summarizes the data collection methods, sources of data, respondents, and data analysis method to answer the research objectives. The summary was presented independently in the next sub section according to the phase of study.

3.10.1 Phase 1: The Need Analysis

This section explained the process involved in phase one of the study to identify the current and future need of the security and investigation industry. The summarize of phase one was presented in Table 3.3

Table 3.3: The Analysis Phase

Objective	Data collection methods	Sources of data / Respondents	Data analysis method
a. To identify the needs of the current and future needs of the industry based on previous studies.	Literature Review and Document analysis	Documents such as: 1. National Skills Development Act 2006 (ACT 652) 2. Malaysia Standard Industrial Classification 2008 (MSIC 2008) 3. Economic Database Reports from the Department of Statistics Malaysia, other reports in the Occupation: MASCO, 12th Malaysia Plan, National Budget and Talent Corporation. 4. MOSQF (Malaysian Occupational Skills Qualification Framework) 5. Other related documents to the Security and Investigation Activities	Document analysis and comparative analysis

3.10.2 Phase 2: The Design and Development Phase

This section explained the process involved in phase two of the study to identify the definition of terms, job responsibilities, job description and analyze the demand and supply of Malaysian's security and investigation industry. The summarize of phase two was presented in Table 3.4.

Table 3.4: The Design and Development Phase

Objective	Data collection methods	Sources of data / Respondents	Data analysis method
b) To identify the job areas, job titles and job classifications according to the definitions and levels of Malaysia Occupational Skills Qualification Framework (MOSQF) in N80	There will be 2 FGD for developing the OF. 1. FDG involving experts from industry in a workshop. The need analysis from the first phase would be presented first as a point of discussion for the issues within the industry and to obtain the industry workforce position.	18 experts from security and investigation activities. The criteria of the experts are as follows: 1. Employed with registered companies under Companies Commission of Malaysia (Criteria: SME companies, multinational companies)	Thematic Analysis and comparative analysis.

Objective	Data collection methods	Sources of data / Respondents	Data analysis method
c) To identify the responsibilities and job descriptions for each job title d) To identify the critical job and the Job Description for N80 related to current developments in the industry e) To analyse the competency needed to address the demand and supply of the industry in Malaysia	2. The FGD would involve discussion on the occupational structure (OS), job description (JD), demand for the skills, jobs' title and critical jobs, assessment of curriculum and training programmes, accreditation and qualification based on industry needs suitable to MOSQ framework, potential workforce challenges, future outlook and strategic recommendations to be proposed. Structured interview protocol for the FGD would involve the future needs for the industry such as: 1. What is the occupational structure required (OS)? 2. What are the job descriptions (JD) for each job title? 3. How can the needs for the skills and competences in the industry be determined? 4. How can the job descriptions for jobs relevant to industry revolution? 5. What are the critical jobs for the industry?	2. A minimum of 5 years' experience in the Security and Investigation Activities. 3. **18 experts** from related to the Security and Investigation Activities	
	1. Site Visit and Interviews with experts at Security and Investigation Activities 2. Interview with expert in Security and Investigation Activities 3. Telephone interviews with experts on Armored Security and some related to different expertise.	See List of experts for site visit and interviews.	Thematic analysis

Focus Group Discussion 1

FGD 1 was conducted on 19 and 20 August 2023 at the Hotel Grand Dorsett, Putrajaya. Ten experts from industries related to N80 attended these two days sessions. The objectives of FGD 1 are to discuss and develop the occupational structure, determining the competencies in demand, emerging skills, job related to IR, and issues related for N80.

The initial OS for the three groups, Group N801: Private Security Activities, Group N802: Security Systems Service Activities and Group N803: Investigation Activities were successfully developed from the FGD 1. Nevertheless, additional engagement with experts from the stakeholder, through interviews were conducted to develop and confirm the initial OS. The details result and explanation of the OS are discussed in this section. The data collected during this stage is also used to develop the Fuzzy Delphi questionnaire used for the next stage of the study.

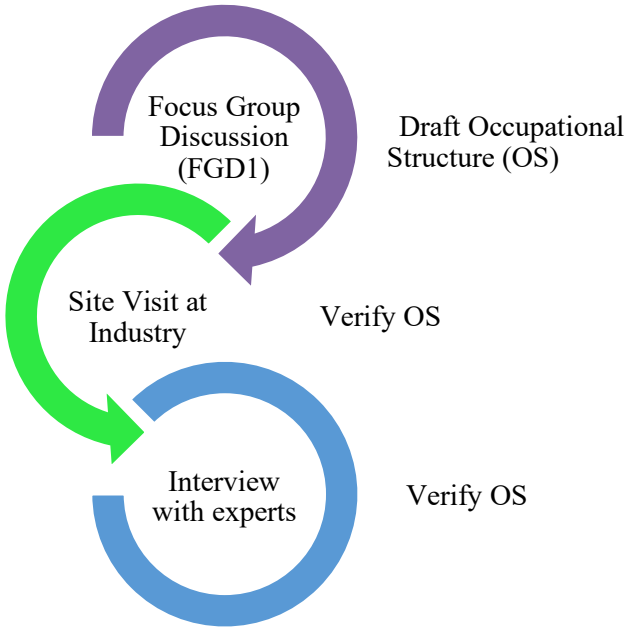

Figure 3.2: Developing the Occupational Structure

Interviews with experts identified from industry which are civil aviation authority of Malaysia, FL Group & Corporate Risk, Maritime Security (Tropical Quantum), Service Constancy System (SCS) and Malaysia Airports Holdings Berhad (MAHB). These experts are identified from the experts during the FGD. In addition to their experience and their willingness to commit, they would be selected on their innovative approach.

Figure 3.3: Composite photos of activities during FGD 1

Figure 3.4: Composite photos of activities during visit and interviews with experts

Focus Group Discussion 2

The second FGD (FGD 2) was conducted on 14 October 2023 at the Hotel Grand Dorsett, Putrajaya and 8 experts from industries related to N80 attended. The objectives of the FGD 2 are to finalize the developed OS and gather information on the jobs in demand and critical jobs,

competencies as well as confirm the job responsibilities and description for all related job titles in the N80. The findings and outcome of the FGD are discussed later in this section.

Figure 3.5 Developing the Occupational Responsibilities

Interviews with experts identified from industry which are civil aviation authority of Malaysia, FL Group & Corporate Risk, Maritime Security (Tropical Quantum), Service Constancy System (SCS) and MAHB. These experts are identified from the experts during the Focus Group Discussions especially development of OR.

Fuzzy Delphi Method

For this purpose, FDM was used to determine consensus among the experts on the critical jobs and competencies needed in the industry. A Fuzzy Delphi Questionnaire was designed from the Occupational Structure. The questionnaire was verified through interviews with two experts. The Fuzzy Delphi Questionnaire was distributed to 23 experts to determine consensus on the critical jobs and competencies.

The application of FDM has been used for forecasting and hence it is suitable for determining the critical jobs and competencies in B80 (Kaufmann & Gupta, 1988). Triangular fuzzy numbers are used in the analysis where aggregation of experts' opinions, defuzzification, and reaching a consensus is done (Ishikawa et al., 1993).

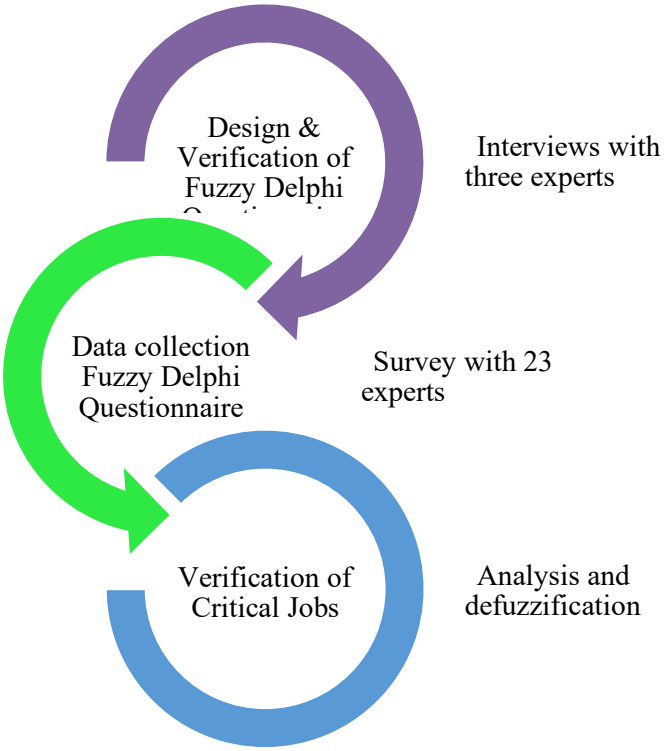

Figure 3.6: Process for Fuzzy Delphi Method

The level of consensus refers to percentages of expert agreement. When experts in a particular field or domain do not reach a collective agreement or consensus on a topic, and the percentage of their agreement falls below 70%, it is considered as low consensus. Consensus typically implies a general agreement among a group of experts or individuals on a specific issue or topic. This lack of consensus could arise due to various reasons such as differing opinions, insufficient evidence, conflicting interpretations of data, or varying methodologies used to arrive at conclusions. Generally, a higher level of consensus, often represented by a threshold like 70% or more, is sought to ensure a more solid and widely accepted understanding within the expert community.

Figure 3.7: Composite photos of activities during FGD 2

Figure 3.8: Composite photos of activities during visit and interviews with experts after FGD 2

3.10.3 Phase 3: The Evaluation Phase

This section explains the process involved in phase three of the study to validate the security and investigation activities industries. The summary of phase threes presented in Table 3.3.

Table 3.5: The evaluation phase

Objective	Data collection methods	Sources of data / Respondents	Data analysis
f) To document and validate the security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0.	a) Interview experts from industry to verify the structure and to obtain the industry workforce position. b) Presentation of findings at International Conference of Sustainability Education Development (ICSED 2023) on 25. & 26 October 2023.	23 experts from the Security and Investigation Activities industry. The criteria of the experts are as follows: 1. A minimum of 5 years' experience in the security and investigation activities. 2. Working and expertise in the field security and investigation activities industry.	Thematic Analysis

In Phase 3, the OF would be evaluated and validated. This involved interviews from 3 experts on the OS. These experts are professionals and managers in the industry. The verification of the final OF will be conducted. The interview will be to confirm the occupational structure, job descriptions and critical job titles as well as the competences in demand. The aim of this task is to gather further information to verify, support and add on to the data.

Presentation of findings at ICSED 2023 and received gold award category best paper. The attainment of the gold award in the best paper category focusing on security and investigation activities in ICSED 2023 was held on 25 and 26 October 2023, marks a remarkable recognition and validation of exceptional contributions within the realm of sustainable security practices. This recognition not only underscores the remarkable quality and significance of the research presented but also acknowledges its paramount role in shaping the discourse and implementation of sustainable security and investigative methodologies. Such an honor elevates the study to a distinguished status, affirming its pivotal impact in guiding future policies, strategies, and transformative approaches in the field of security and investigation. This accolade serves as a catalyst for advancing sustainable security practices globally, inspiring further innovative research and encouraging practitioners to adopt and implement sustainable approaches in ensuring safety and security while fostering broader sustainable development goals.

Figure 3.9: Certificate of Gold Award at ICSED 2023

3.11 Summary

In this study, the comprehensive exploration and validation of research outcomes were facilitated through the utilization of DDR approach, amalgamating divergent and convergent thinking for a holistic understanding of the subject matter. The strategic application of a purposive sampling method ensured the deliberate selection of participants based on their specialized expertise, effectively aligning with the study's targeted objectives. Moreover, the implementation of the Fuzzy Delphi technique played a pivotal role in navigating uncertain or ambiguous scenarios, enabling the systematic aggregation of expert opinions to reach consensus within the research domains. Additionally, meticulous data analysis techniques were employed, meticulously synthesizing both

qualitative and quantitative data through appropriate tools and software, ensuring the integrity and credibility of the research findings.

CHAPTER IV

FINDING

4.1 Introduction

Chapter 4 constitutes a comprehensive inquiry into the burgeoning demands and evolving landscape of the industry in Malaysia, leveraging insights gleaned from prior research. Central to this investigation is the meticulous identification of prevailing and future industry requisites, necessitating an exploration of job areas, titles, and classifications aligning with the NOSS within the N80 sector. Delving deeper, this chapter endeavors to delineate the specific job responsibilities and descriptions affiliated with each job title, thereby illuminating the granularity of roles within this occupational framework. Furthermore, an emphasis is placed on discerning critical roles and their job descriptions concerning contemporary industry advancements, providing a nuanced understanding of pivotal positions amidst the sector's evolution. Through a rigorous analysis of competencies requisite to address industry demands and supply dynamics, this chapter seeks to elucidate the skills and proficiencies crucial for industry sustainability and growth. Lastly, an evaluation, documentation, and validation of the security and investigation activities industries in Malaysia, as per the MSIC 2008 version 1.0, will be conducted, affording a validated perspective on the industry's landscape. By addressing these multifaceted dimensions, this chapter aims to contribute valuable insights to stakeholders, policymakers, and professionals seeking to navigate and fortify the industry's trajectory in Malaysia.

4.2 Profile Demography

The demographic profile of respondents presents a meticulously curated representation of expertise in various domains within the security and investigation activities realm, encompassing nine experts for Private Security Activities, seven experts for Security Systems Service Activities and seven experts for Investigation Activities. This deliberate selection ensures a comprehensive understanding of nuanced perspectives, specialized skills, and diverse experiences crucial for illuminating the intricacies within each specific sector of the broader industry landscape.

4.3 The Needs of the Current and Future Needs of the Industry

Objective 1(a): To identify the needs of the current and future needs of the industry based on previous studies.

Table 4.1 The needs of the current and future needs of the industry

Resources	Current Need	Future Need
Private Security Activities		
• At Organizational level, effort encompasses guidelines, frameworks and certification marred by issues and inhibitors (Teoh et al., 2018). • 5,480 general incidents classification statistics 2023 (MyCERT, 2023). • The Malaysian Government is steadfast in creating a safe living environment for its 30 million citizens (Ibrahim, 2016) • Upskill and upgrade the current private security guard industries (Wen et al, 2023).	• Knowledge and Skills • Responsibility • Budget allocation • Enforcement and resources • Technology	• Need technical skills talents workers to address the incidents
Security Systems Service Activities		
• A new system or platform has to be developed that encompasses new operational processes (Wen et al, 2023). • Kamaruzaman and Rashid (2023) develop a supervisory mobile application for the GEP security system. • Gannapathy et al., (2023) develop a Security Guard Patrolling, Monitoring and Reporting (eSmartGuard) system that able incorporates many unique and intelligent technologies such as NFC, GPS and IoT to records and save the patrolling data automatically on the cloud/server in real-time basis • Anwar et al., (2023) created a conceptual framework for PMSC in Malaysia so that the resulting SOP would be fully compatible with national and international maritime law and practices • Created a low-cost surveillance system that can capture video and identify movements in restricted areas such as user belongings and property.	• Need to develop new operational processes • Hardware system design • Community policing • Community security • Cloud technology	• Need for new technology IoT • Cloud Technology. • Supervisory mobile application • New framework • Faster connectivity

Resources	Current Need	Future Need
Investigation Activities		
• In Malaysia, gated and guarded communities are commonly known as a group of residents or communities (Adnan et al., (2023) • MOHA and the Malaysian NSC developed an SOP for Private Maritime Security Companies (PMSC) in Malaysia for local security companies to follow (Anwar et al., 2023) • In Malaysia, Section 130B (2) of the Penal Code (Act 574) defines terrorism as any act that is done with the intention of causing death or serious bodily injury to any person; or causing extensive destruction to a place or property; or causing serious disruption of any essential service, facility or system; or creating a public emergency (Othman, 2023)	• Creating a public urgency.	• Need for new framework • New act for investigation activity • Specific in a job scope and role related to investigation activities.

At the organizational level, the endeavor to establish comprehensive guidelines, frameworks, and certification processes aimed at enhancing operational standards and practices is hampered by several issues and inhibitors, as highlighted by Teoh et al. (2018). These challenges often include complexities arising from multifaceted structures within organizations, resistance to change from established norms, ambiguities in regulatory compliance, and resource constraints. The efforts to institute these measures face impediments such as lack of clarity in implementation strategies, insufficient buy-in from stakeholders, and the absence of cohesive frameworks adaptable to diverse organizational contexts. Despite the recognition of the importance of guidelines and certifications for fostering organizational excellence, these impediments underscore the need for a nuanced approach, addressing barriers to adoption and implementation, while simultaneously refining strategies to ensure effective integration of these frameworks into organizational practices.

The reported statistics of 5,480 incidents categorized under general classifications in the year 2023, as documented by Malaysia Computer Emergency Response Team (MyCERT), signify a comprehensive overview of the diverse array of incidents encountered within the digital landscape. These statistics likely encompass a range of cybersecurity events, encompassing various threats such as malware infections, phishing attacks, data breaches, and

other forms of cyber threats. Such meticulous classification and documentation of incidents by MyCERT underscore the significance of understanding the evolving cybersecurity landscape, allowing for a detailed analysis of trends, patterns, and vulnerabilities. These statistics serve as a valuable resource for stakeholders, policymakers, and cybersecurity professionals, aiding in the formulation of robust strategies, proactive measures, and targeted interventions to mitigate risks and enhance the resilience of digital infrastructures against emerging cyber threats.

The commitment of the Malaysian Government, as highlighted by Ibrahim (2016), remains unwavering in its dedication to establishing a secure and safe living environment for the approximately 30 million citizens of Malaysia. This steadfast commitment encompasses various initiatives, policies, and strategic measures aimed at ensuring public safety, fostering social stability, and safeguarding the well-being of the nation's populace. By prioritizing safety as a fundamental aspect of governance, the government seeks to address multifaceted challenges, including crime prevention, disaster management, and national security concerns. Such dedication underscores the government's proactive approach in deploying resources, collaborating with diverse stakeholders, and implementing comprehensive programs to create an environment where citizens can thrive, contributing to the nation's progress and development.

The imperative to upskill and elevate the standards within the private security guard industries, as emphasized by Wen et al. (2023), underscores a crucial need for advancements in training, expertise, and professional capabilities. This call for enhancement aims to address prevailing challenges and bridge existing gaps in the private security sector. By focusing on upskilling initiatives, the industry can empower security personnel with advanced training programs, cutting-edge technologies, and updated methodologies. This effort not only enhances the competency and effectiveness of security personnel but also elevates the industry's overall standards. By fostering continuous learning and development, such initiatives align with the evolving demands of security operations, ensuring a more proficient and capable workforce capable of tackling modern security threats effectively.

The necessity to devise a novel system or platform that incorporates innovative operational processes, as advocated by Wen et al. (2023), signifies a crucial requirement for adapting to evolving needs and technological advancements. These imperative underscores the importance of creating a comprehensive and efficient system that integrates modern technologies, streamlined procedures, and adaptable frameworks. Such a system is poised to optimize operations, enhance productivity, and address existing inefficiencies. By focusing on developing this new platform, organizations can harness the potential of cutting-edge tools and

methodologies, fostering agility and responsiveness in their operational workflows. This proactive approach aligns with the dynamic landscape of technological advancements, ensuring that businesses or entities can stay competitive, agile, and responsive to changing demands and market trends.

The collaboration between the MOHA and the NSC resulting in the development of a Standard Operating Procedure (SOP) for PMSC in Malaysia, as indicated by Anwar et al. (2023), represents a pivotal step towards ensuring standardized and regulated practices within the local security sector. This SOP serves as a guideline or framework outlining the specific protocols, procedures, and best practices that private maritime security companies are required to adhere to in the execution of their duties. By establishing such a comprehensive SOP, MOHA and the NSC aim to promote consistency, accountability, and professionalism among local security firms operating in the maritime domain. This concerted effort not only enhances the effectiveness of security measures but also reinforces compliance with legal and regulatory standards, ultimately contributing to bolstering maritime safety and security within Malaysian waters.

The necessity for a new OF within the domain of security and investigation activities indicates a critical need to adapt to evolving demands, technologies, and methodologies within this sector. Such a framework should encompass a comprehensive and updated structure that reflects the diverse facets of modern security and investigative practices. This call for a new OF emphasizes the urgency to redefine roles, competencies, and skill sets required in the field. It aims to address emerging challenges, technological advancements, and changing trends in security and investigation domains. By establishing a new occupational framework, stakeholders can better align training programs, job roles, and career pathways with current industry requirements, fostering a more capable and responsive workforce while ensuring the effective and efficient provision of security and investigative services.

Table 4.2 presented accessible eight aspects related to Security and Investigation Activities from eight different countries of Malaysia, US, UK, Indonesia, Singapore, China, Qatar and Australia. These eight aspects included (1) Law Enforcement Agencies, (2) Immigration and Border Control, (3) Intelligence and Surveillance, (4) Forensic Investigation, (5) Counterterrorism, (6) Cybersecurity, (7) Private Security Companies and (8) Anti-Corruption Effort/Police Force. There are three out of eight aspects are accessible for all eight countries, which are Counterterrorism, Immigration and Border Control and Private Security Companies. The rest of aspects are different and not applicable for certain countries according

to their own countries' regulation. The explanation of the eight aspects according to each country were discussed independently in next paragraph.

Table 4.2: Accessible eight aspects related to Security and Investigation Activities from different countries

Aspects	Malaysia	USA	UK	Indonesia	Singapore	China	Qatar	Australia
Law Enforcement Agencies	✓	✓	-	-	✓	✓	✓	-
Counterterrorism	✓	✓	✓	✓	✓	✓	✓	✓
Immigration and Border Control	✓	✓	✓	✓	✓	✓	✓	✓
Cybersecurity	✓	✓	✓	✓	✓	✓	✓	
Intelligence and Surveillance	✓	✓	✓	✓	-	✓	✓	✓
Private Security Companies	✓	✓	✓	✓	✓	✓	✓	✓
Forensic Investigations	✓	✓	✓	✓	✓		✓	✓
Anti-corruption Effort/Police force	✓	-	✓	✓	✓	✓	✓	✓

Sources: Wen et al. (2023) and Anwar et al. (2023)

In Malaysia, various resources and initiatives are accessible and employed by Law Enforcement Agencies, Counterterrorism units, Immigration and Border Control authorities, Cybersecurity teams, Intelligence and Surveillance departments, Private Security Companies, Forensic Investigation bodies, and Anti-Corruption Efforts within the Police Force. These entities utilize these available resources to address and manage a wide spectrum of security-related concerns, encompassing counterterrorism operations, border security, cyber threats, intelligence gathering, surveillance activities, private sector security services, forensic analysis, and the enforcement of anti-corruption measures within the national police force. This comprehensive framework and collaboration among different sectors aim to ensure a multifaceted approach to security and law enforcement in the country, addressing diverse threats and challenges across various domains effectively.

In the United States, a range of resources and tools is accessible and utilized by Law Enforcement Agencies, Counterterrorism units, Immigration and Border Control authorities, Cybersecurity entities, Intelligence and Surveillance departments, Private Security Companies, and Forensic Investigation units. These resources support the comprehensive management of diverse security-related concerns, including law enforcement operations, counterterrorism

measures, border security, cyber defense, intelligence gathering, surveillance activities, and forensic examinations. However, distinctly different from some other countries, there isn't a centralized national Anti-Corruption Efforts specifically focused within the realm of the Police Force. While various federal and state-level regulations, oversight bodies, and legal mechanisms exist to address corruption in different sectors, the absence of a specific Anti-Corruption effort directly tied to the police force as a distinct entity is a notable difference in the available resources for security-related concerns in the USA.

In the United Kingdom, a comprehensive array of resources and support is accessible for Counterterrorism units, Immigration and Border Control authorities, Cybersecurity initiatives, Intelligence and Surveillance agencies, Private Security Companies, Forensic Investigation units, and Anti-Corruption Efforts within the Police Force. However, notably distinct from certain other countries, the specific availability for Law Enforcement Agencies, as a separate and distinct entity, might not be as explicitly delineated. While law enforcement functions are carried out effectively through various agencies such as regional police forces and specialized units, the availability of dedicated resources specifically labeled for "Law Enforcement Agencies" might not be distinctly highlighted in comparison to the resources explicitly allocated for other security-related sectors. The emphasis is often placed on the broader law enforcement and security ecosystem encompassing various specialized functions and units rather than a singular focus on resources for Law Enforcement Agencies as an isolated category.

In Indonesia, a wide range of resources and assistance is accessible for Counterterrorism units, Immigration and Border Control authorities, Cybersecurity initiatives, Intelligence and Surveillance agencies, Private Security Companies, Forensic Investigation units, and the Anti-Corruption Efforts integrated within the Police Force. Nevertheless, unlike certain other nations, the explicit availability of resources exclusively dedicated to Law Enforcement Agencies might not be as clearly defined. Although law enforcement activities are effectively conducted through diverse entities like regional police forces and specialized units, the specific allocation of resources explicitly labeled for "Law Enforcement Agencies" may not receive distinct emphasis compared to resources designated for other security-related sectors. The focus typically centers on the broader spectrum of law enforcement and security functions, encompassing varied specialized units and operations, rather than exclusively highlighting resources earmarked for Law Enforcement Agencies as a distinct category.

In Singapore, a comprehensive range of resources and support is accessible for Law Enforcement Agencies, Counterterrorism units, Immigration and Border Control authorities, Cybersecurity measures, Private Security Companies, Forensic Investigations, and Anti-Corruption Efforts within the Police Force. However, notably distinctive from certain other sectors, the specific availability for Intelligence and Surveillance initiatives might not be as explicitly emphasized or delineated. While the country maintains a robust framework for various security-related functions and operations, resources tailored explicitly for Intelligence gathering and Surveillance activities might not be specifically highlighted compared to the resources allocated for other security sectors. The focus predominantly centers on the provision of resources and support across Law Enforcement Agencies and multiple security domains, yet the distinct spotlight on dedicated resources solely aimed at Intelligence and Surveillance is not as prominently highlighted in Singapore's security framework.

In China, a diverse spectrum of resources and support is accessible for Law Enforcement Agencies, Counterterrorism operations, Immigration and Border Control, Cybersecurity measures, Intelligence and Surveillance activities, Private Security Companies, and Anti-Corruption Efforts within the Police Force. However, notably distinct from some other facets, there might be relatively less explicit emphasis or resources specifically earmarked for Forensic Investigations. While the country boasts a robust infrastructure concerning various security-related domains, resources and efforts directed towards Forensic Investigations may not receive the same level of explicit allocation or dedicated focus within the overall security framework. The country's emphasis primarily centers on the provision of resources across a wide array of security sectors and functions, with less explicit focus on specific resources solely devoted to Forensic Investigations within the realm of security and law enforcement in China.

In Qatar, an extensive range of resources and support is accessible for Counterterrorism efforts, Immigration and Border Control, Cybersecurity measures, Forensic Investigations, Private Security Companies, and Anti-Corruption Efforts within the Police Force. However, notably distinct from certain other components, the specific availability and emphasis on resources designated for Law Enforcement Agencies, Intelligence, and Surveillance might not be as explicitly highlighted or allocated within the country's security framework. While Qatar demonstrates a robust infrastructure in various security-related domains, resources tailored exclusively for Law Enforcement Agencies and Intelligence and Surveillance sectors may not receive the same distinct focus or allocation compared to other sectors. The emphasis is primarily on resources addressing counterterrorism, border control, cybersecurity, forensics, private security, and anti-corruption efforts within Qatar's security apparatus, with relatively

less explicit delineation of resources specifically earmarked for traditional Law Enforcement Agencies, Intelligence operations, and Surveillance activities.

In Australia, a comprehensive array of resources and support is accessible for Counterterrorism operations, Immigration and Border Control, Intelligence and Surveillance activities, Forensic Investigations, Private Security Companies, and Anti-Corruption Efforts within the Police Force. However, distinctively different from certain other aspects, the specific availability and focused resources for Law Enforcement Agencies and Cybersecurity might not be as prominently highlighted or explicitly designated within the country's security framework. While Australia maintains a robust infrastructure in various security-related domains, resources specifically tailored for Law Enforcement Agencies and Cybersecurity might not receive the same degree of explicit emphasis or dedicated allocation compared to other sectors. The emphasis primarily centers on resources addressing counterterrorism, border control, intelligence, forensics, private security services, and anti-corruption endeavors within Australia's security landscape, with relatively less specific delineation of resources exclusively earmarked for traditional Law Enforcement Agencies and Cybersecurity initiatives.

4.4 The Job Areas, Job Titles and Job Classifications

Objective 2 (a): To identify the job areas, job titles and job classifications according to the definitions and levels of MOSQF in N80.

Table 4.3: Overall job areas and titles in N80 (security and investigation activities)

Occupational Structure (OS)	Total Identified Job Areas	Total Identified Job Titles	Total Job Titles Relevant to Industrial Revolution	Total Critical Job & Relevant to Industrial Revolution
N801 (Private Security Activities)	8	29	4	6
N802 (Security Systems Service Activities)	3	15	6	7
N803 (Investigation Activities)	1	6	0	2
TOTAL	**14**	**50**	**10**	**15**

The Occupational Structure (OS) delineates the collective arrangement of occupations within a society, delineated by skill level, economic function, or social hierarchy. In the context of groups N801, N802, and N803, the OS was crafted following FGD 1 and FGD 2 involving

a panel of experts from the N80 sector. Table 4.3 provides an overview of the total number of job titles within the N80 group. During these FGD sessions, 14 job areas were delineated, identifying a total of 50 job titles, including 10 deemed relevant to the industrial revolution and 15 critical and relevant to the industrial revolution in the security and investigation activities sector. The discussions encompassed critical roles necessitating specific skills, work methodologies, or technologies vital to the industry's functioning (TalentCorp, 2022).

Table 4.4: Private Security (N801) Activities Job Descriptions

801 (Private Security Activities)		
No	**Job Area**	**Description**
1	Guarding Services	Professional services provided by trained individual or security companies to protect people, organization and property.
2	Armed Guarding	Professional trained security that carry firearms or other weapons to provide protection and deter potential threats. (Security breaches, crime or violence)
3	Close Protection	Armed or unarmed bodyguards whose primary responsibility is to ensure the safety and security of an individual
4	Cash Management	Establish vault operations, perform armory operation, perform delivery operations of consignments company's vault or clients site.
5	K9 Service	Specialized services that involved trained dogs that is partnered with humans for a variety of purposes, including security, law enforcement, search and rescue, therapy and more.
6	Alarm Monitoring	Service that involves watching over security system, monitor incoming signals, verify alarms and respond appropriately.
7	Maritime Security	Service of the best practices to defend vessel against both internal and external threats.
8	Aviation Security	Safeguarding International Civil Aviation against Acts of Unlawful Interference

Table 4.5: Security Systems Service Activities (N802) Job Descriptions

802 (Security Systems Service Activities) – Security Surveillance		
No	**Job Area**	**Description**
1	Security System Analyst	Analyzing, strategizing, initiating and enhancing security measures for technological systems and solutions in security technology area
2	Security System Technologist	Installing, troubleshooting, constructing, and maintaining security systems and solution in security technology area
3	Security System Surveillance Operator	Monitor, operate, response, and maintain operational activity upkeep in security technology area.

Table 4.6: Investigation Activities (N803) Job Descriptions

803 (Investigation Activities)		
No	**Job Area**	**Description**
1	Surveillance Investigation	Involves monitoring and analyzing activities, often discreetly, to gather information and insights related to security, legal, or operational matters. Responsibilities include conducting field research, gathering evidence, maintaining detailed records, and collaborating with relevant stakeholders. This role may also involve using technology and tools to aid in data collection and analysis, as well as preparing comprehensive reports based on findings. Strong attention to detail, analytical skills, and the ability to work independently are essential for this position.

4.4.1 Private Security Activities (N801)

The study revealed eight distinct areas and twenty-nine job titles within the domain of private security activities (N801).

Table 4.7: Private Security Activities Job Areas

SECTION	N (Administrative Activities and Support Services)							
DIVISION	80 Security and Investigation Activities							
GROUP	801 (Private Security Activities)							
AREA / LEVEL	Guarding Services (GS)	Armed Guarding (AG)	Close Protection (CP)	Cash Management (CM)	K9 Service (K9)	Alarm Monitoring (AM)	Maritime Security	Aviation Security (Avsec) (Operation, Intelligent and investigation)
LEVEL 8	NJT	NJT	NJT	NJT	NJT	NJT	NJT	NJT
LEVEL 7	NJT	NJT	NJT	NJT	NJT	NJT	NJT	Avsec Senior Specialist
LEVEL 6	NJT	NJT	NJT	NJT	NJT	NJT	NJT	Avsec Specialist
LEVEL 5	GS Security Manager**	NJT	CP Manager**	NJT	NJT	NJT	Maritime Operation Manager***	Avsec Senior Executive
LEVEL 4	GS Security Executive**	NJT	CP Executive**	NJT	NJT	NJT	Maritime Control Center Supervisor**	Avsec Executive***
LEVEL 3	GS Security supervisor**	AG Supervisor*	CP Senior Bodyguard*	CM Supervisor	NJT	AM Supervisor***	Maritime Team Leader*	Avsec Senior Officer***
LEVEL 2	GS Security officer*	AG Security Officer*	CP Bodyguard*	CM Security Officer	K9 Security Officer*	AM Security Officer***	Maritime Unit Leader	Avsec Officer***
LEVEL 1	GS Assistant Security officer*	NJT	NJT	CM Assistant Security Officer	NJT	NJT	Ship Security Officer/ Operating Room Officer	Avsec Assistant*

These areas encompass Guarding Services/Security Operation Services, Armed Guarding, Close Protection, Cash Management/Cash in Transit/Value in Transit, K9 Service, Alarm Monitoring, Maritime Security, and Aviation Security. These classifications emerged from discussions facilitated by the FGD process with a panel. Each identified area is systematically divided into eight levels for a comprehensive breakdown. The subsequent sections provide detailed descriptions for each level within these areas.

The **Guarding Services** areas include positions such as GS Security Manager, GS Security Executive, GS Security supervisor, GS Security officer, and GS Assistant Security officer. The domain of Guarding Services encompasses a spectrum of crucial roles pivotal in ensuring comprehensive security measures. Within this field, positions span from the commanding GS Security Manager responsible for strategic planning and overseeing security protocols to the GS Security Executive managing the operational aspects and coordinating security functions. The GS Security Supervisor plays a critical role in the day-to-day supervision and implementation of security strategies, while the GS Security Officer executes these plans on the ground, ensuring vigilance and adherence to protocols. Complementing these roles, the GS Assistant Security Officer supports the team in various capacities, contributing to the smooth execution of security procedures. Together, these positions form an integrated framework, crucial in safeguarding assets, people, and premises, ensuring a robust and effective security infrastructure.

The **Armed Guarding** areas include AG Security Officer and AG Supervisor. The domain of Armed Guarding involves specialized roles dedicated to maintaining high-security standards. Within this sector, the roles of Security Officer and Supervisor are paramount. The AG Security Officer plays a pivotal role in armed security, utilizing extensive training and expertise to safeguard assets and individuals. Their responsibilities typically involve patrolling, monitoring, and implementing stringent security measures to ensure protection against potential threats. Meanwhile, the AG supervisor assumes a higher-tier position within Armed Guarding, holding greater responsibilities in strategizing and overseeing armed security operations. They often guide and supervise Security Officers, ensuring adherence to protocols, and may be involved in decision-making processes regarding security strategies.

The **Close Protection** areas include CP Bodyguard, CP Senior Bodyguard, CP Close Protection Executive and CP Close Protection Manager. The field of Close Protection

encompasses crucial roles focused on ensuring the safety and security of individuals in high-risk or sensitive environments. Within this domain, several key positions play vital roles. The role of a CP Bodyguard is fundamental in providing direct and immediate protection to individuals under their care. They are extensively trained in threat assessment, defensive tactics, and emergency response to mitigate risks and ensure the safety of their clients. Moving up the hierarchy, the CP Senior Bodyguard assumes a higher-level position within CP Close Protection. They possess advanced skills and experience in security operations, often leading a team of Bodyguards and orchestrating security plans to ensure comprehensive protection. CP Close Protection Executives play a pivotal role in strategizing and implementing security measures. They oversee the execution of protection plans, coordinate logistics, and liaise with clients to ensure their safety requirements are met effectively. At the upper echelon, the CP Close Protection Manager holds a leadership position, responsible for the overall management and coordination of Close Protection operations. They design security protocols, manage resources, and oversee the entire team, ensuring that security strategies are robust and aligned with the clients' needs.

The **Cash Management** areas include CM Assistant Security Officer, CM Security Officer and CM Supervisor. The primary focus of Assistant Security Officers, Security Officers, and Supervisors within Cash Management, Cash in Transit, and Value in Transit sectors revolves around safeguarding assets, particularly cash and valuables, during their transit or storage. CM Assistant Security Officers support the implementation of security protocols, aid in transportation security, and assist in training staff. CM Security Officers oversee the overall security operations, ensuring compliance with regulations, conducting risk assessments, and managing security systems to prevent breaches. CM Supervisors take charge of the entire cash management or transit operation, managing teams, implementing security plans, and evaluating security measures' effectiveness. Together, these roles work cohesively to maintain the highest standards of security, prevent potential risks, and respond promptly to security-related issues within the Cash in Transit and Value in Transit areas.

The **K9 Service** area is K9 Security Officer. In the K9 Service area, Security Officers play a pivotal role in managing and overseeing the deployment of specially trained canine units for security purposes. These K9 Security Officers are responsible for handling and coordinating K9 teams that are trained to detect explosives, drugs, or other prohibited substances. They ensure the proper care, training, and utilization of the canine units to maximize their

effectiveness in various security scenarios. Security Officers in the K9 Service area also collaborate closely with law enforcement agencies, security personnel, and handlers to execute security protocols, conduct searches, and provide a visible deterrent against potential threats. Additionally, they oversee the maintenance of K9 equipment, adherence to safety protocols, and the continuous training and development of both the K9 units and their handlers to ensure peak performance and enhance security measures.

The **Alarm Monitoring** areas include AM Security Officer and AM Supervisor. Alarm monitoring in N801 focused on service security which does not involve the technical aspects on technology. In the Alarm Monitoring areas, Security Officers and Supervisors play integral roles in ensuring the constant surveillance and response to triggered alarms within various security systems. AM Security Officers are responsible for actively monitoring alarm systems, swiftly identifying any alerts or irregularities, and promptly investigating potential security breaches or incidents. They work diligently to verify alarms, assess the situation, and take appropriate action, which may involve contacting emergency services, dispatching security personnel, or notifying relevant stakeholders. AM Supervisors oversee the entire alarm monitoring operation, managing teams of Security Officers, developing protocols for alarm response, and conducting regular assessments to improve the efficiency and effectiveness of the alarm monitoring systems. They also collaborate with technical support teams to ensure the proper functioning of alarm systems and provide guidance and training to Security Officers to enhance their response capabilities in handling alarm-related situations.

The **Maritime Security** areas include Ship Security Officer (Control Centre)/ Operating Room Officer (Vessel), Unit Leader, Team Leader, Control Centre Supervisor, Maritime Operation Manager. In Maritime Security, a spectrum of vital roles is involved in ensuring the safety and security of ships, ports, and maritime operations. The Ship Security Officer oversees the implementation of security measures on vessels, conducts security assessments, and coordinates security-related activities onboard. The Unit Leader and Team Leader manage and supervise security teams, ensuring compliance with maritime security regulations and handling day-to-day security operations. Control Centre Supervisors oversee the overall security operations, including risk assessments and strategic planning. Operating Room Officers handle communications, coordinate responses to security incidents, and manage the command centre or operations room. The Maritime Operation Manager holds an overarching role, overseeing the entire maritime security operation, developing security

protocols, liaising with authorities, and ensuring compliance with international maritime security standards like the International Ship and Port Facility Security Code. Together, these roles collaborate to maintain the safety and security of maritime environments, vessels, and associated operations.

The **Aviation Security** area include Avsec Senior Specialist, Avsec Specialist, Avsec senior executive, Avsec executive, Avsec senior officer, Avsec officer and Avsec assistant. Aviation Security constitutes a multifaceted domain encompassing a range of pivotal roles essential for ensuring the safety and integrity of air travel. Within this sphere, positions such as the Avsec Senior Specialist take on a leadership role, overseeing strategic planning and implementing advanced security measures, while the Avsec Specialist focuses on specialized areas within aviation security protocols. The Avsec Senior Executive manages operational aspects, coordinates security functions, and ensures compliance with stringent aviation safety standards, whereas the Avsec Executive plays a hands-on role in executing these protocols efficiently. Working on the ground, the Avsec Senior Officer and Avsec Officer actively monitor and enforce security measures, ensuring strict adherence to procedures, while the Avsec Assistant supports the team in various capacities, contributing to the seamless implementation of aviation security measures. These roles collectively form an interconnected framework crucial in upholding safety standards, protecting passengers, and safeguarding the aviation industry against potential threats.

4.4.2 Security Systems Service Activities (N802)

The study identified three (3) distinct areas and fifteen (15) job titles within the domain of Security Systems Service Activities (N802). These areas encompass Security System Surveillance Operator, Security System Analyst, and Security System Technologist. Each of these areas is further delineated into eight specific levels, providing a detailed breakdown for comprehensive understanding. The subsequent sections elaborate on these levels and their corresponding descriptions.

The **Security System Surveillance Operator** areas include Operator, Senior Operator, Executives, Senior Executives and Manager. Within the domain of Security System Surveillance, various hierarchical roles encompass specific responsibilities crucial for effective monitoring and safeguarding. Operators are tasked with actively monitoring security systems, identifying, and responding to security alerts or irregularities, and ensuring adherence to

surveillance protocols. Monitoring security systems in N802 focused on the technical aspects of technology. Senior Operators possess advanced skills, oversee multiple surveillance systems simultaneously, and provide guidance to junior staff in handling complex situations. Executives manage the overall surveillance operations, including strategic planning, resource allocation, and coordination of surveillance activities. Senior Executives hold higher-level positions, overseeing multiple surveillance teams, contributing to decision-making processes, and aligning surveillance efforts with broader organizational goals. Managers play a pivotal role in overseeing the entire surveillance department, setting objectives, and ensuring the efficiency and effectiveness of surveillance operations. Collaboration among these levels is critical to maintaining a high level of security, promptly addressing threats, and ensuring the smooth functioning of surveillance systems to protect assets and personnel.

Table 4.8: Security Systems Service Activities Job Areas

SECTION	**N (Administrative Activities and Support Services)**		
DIVISION	**80 Security and Investigation Activities**		
GROUP	**802 (Security Systems Service Activities)**		
AREA / **LEVEL**	**Security System Surveillance Operator**	**Security System Analyst**	**Security System Technologist**
LEVEL 8	NJT	NJT	Chief Technical Officer ***
LEVEL 7	NJT	Specialist/ Senior Security Solutions/ Senior Manager***	Specialist Technical Deployment***
LEVEL 6	NJT	Manager / Security Solutions***	Head Technical Operation Executives***
LEVEL 5	Assistant Manager/ Supervisor***	Senior Analyst**	Senior Technical Executives***
LEVEL 4	Senior Executives**	Analyst**	Technical Executives**
LEVEL 3	Executives**	NJT	System Admin**
LEVEL 2	Senior Operator	NJT	NJT
LEVEL 1	Operator	NJT	NJT

The **Security System Analyst** areas include Analyst, Senior Analyst, Manager, Security Solutions and General Manager Security Solutions. In the domain of Security System Analysis, a structured hierarchy encompasses roles with specialized responsibilities crucial for evaluating, designing, and implementing robust security measures. Analysts are responsible for examining security systems, assessing vulnerabilities, and analyzing data to enhance security protocols. Senior Analysts possess advanced expertise, overseeing comprehensive

security analyses, and providing guidance to junior analysts in complex assessments. Managers in Security System Analysis oversee the department, setting strategic goals, managing resources, and ensuring the efficiency of security analyses. Security Solutions Managers focus on devising comprehensive security strategies, implementing innovative solutions, and aligning security measures with organizational needs. Senior Managers in Security Solutions hold senior leadership roles, overseeing multiple security departments, shaping overarching security strategies, and ensuring the alignment of security initiatives with broader organizational objectives. Collaboration across these hierarchical levels is pivotal for conducting thorough security analyses, implementing effective security solutions, and fortifying an organization's defenses against potential threats.

The **Security System Technologist** areas include System admin, Technical Executives, Chief Technical Officer, Specialist Technical Deployment, Head Technical Operation Executives and Senior Technical Executives. Within the domain of Security System Technology, a hierarchical structure comprises various roles with specialized functions essential for the deployment, maintenance, and advancement of robust security systems. System Administrators or Junior Engineers manage the day-to-day operations, handling basic technical tasks and assisting in system maintenance. Technical Executives or Engineers work on technical aspects, implementing solutions, and addressing system-related issues. Senior Technical Executives or Senior Engineers oversee comprehensive technical operations, guiding junior staff, and providing expertise in complex technical matters. Heads of Technical Operations or Lead Engineers take charge of the overall technical operations, supervising teams, ensuring system efficiency, and strategizing for technological advancements. Specialists focus on specific technical aspects, contributing expertise in niche areas of security system technology. Technical Deployment or Assistant Directors play a crucial role in managing large-scale deployments, coordinating teams, and overseeing project execution. Directors in Technical & Security Solutions hold high-level leadership positions, steering the technological and security solutions strategy, aligning it with organizational objectives, and ensuring the integration of cutting-edge technologies into security systems. Collaboration across these levels is pivotal for maintaining, advancing, and innovating security technologies to effectively protect assets and infrastructure against evolving threats.

4.4.3 Investigation Activities (N803)

The study identified one key area and six job titles within the realm of Investigation Activities (N803). These areas include Surveillance & Ground Investigation, Research & Analyst, Verify and Authenticate Information, Project Management, Corporate Management, and Project Management. Each of these areas is systematically subdivided into eight levels. The subsequent sections provide a detailed breakdown, offering comprehensive descriptions for each level within these areas.

Table 4.9: Investigation Activities Job Areas

SECTION	**N (Administrative Activities and Support Services)**
DIVISION	**80 Security and Investigation Activities**
GROUP	**803 (Investigation Activities)**
AREA / **LEVEL**	**Surveillance Investigation**
LEVEL 8	NJT
LEVEL 7	Investigation Technical Team Leader***
LEVEL 6	Investigation Team Leader***
LEVEL 5	Investigation Senior Analyst*
LEVEL 4	Investigation Junior Analyst*
LEVEL 3	Investigation Senior Operative*
LEVEL 2	Investigation Junior Operative*
LEVEL 1	NJT

The Surveillance Investigation areas include Investigation Junior Operative, Investigation Senior Operative, Investigation Junior Analyst, Investigation Senior Analyst, Investigation Team Leader and Investigation Technical Team Leader. The realm of Surveillance Investigation encompasses a spectrum of pivotal roles essential for probing and analyzing various incidents and matters requiring scrutiny. Within this domain, roles range from the Investigation Junior Operative, tasked with foundational investigative duties, to the Investigation Senior Operative, responsible for conducting advanced inquiries and employing specialized investigative techniques. The Investigation Junior and Senior Analysts play a crucial role in scrutinizing data, gathering intelligence, and drawing insightful conclusions, with the Senior Analyst assuming a more supervisory and analytical role. The Investigation Team Leader oversees the investigative process, coordinates efforts, and ensures efficient collaboration among team members, while the Investigation Technical Team Leader focuses on managing and applying technological tools and resources in the investigative process. These roles form a cohesive framework essential for thorough and effective surveillance

investigations, ensuring comprehensive analysis, and facilitating informed decision-making in complex situations. The summary of job titles for N80 is stated in the following table.

Table 4.10: Summary of Job Titles in N801

Job Area	Job Level							
	1	2	3	4	5	6	7	8
Guarding Services/ Security Operation Services	1	1	1	1	1	NJT	NJT	NJT
Armed Guarding	NJT	1	1	NJT	NJT	NJT	NJT	NJT
Close Protection	NJT	1	1	1	1	NJT	NJT	NJT
Cash Management/ Cash in Transit/ Value in Transit	1	1	1	NJT	NJT	NJT	NJT	NJT
K9 Service	NJT	1	NJT	NJT	NJT	NJT	NJT	NJT
Alarm Monitoring	NJT	1	1	NJT	NJT	NJT	NJT	NJT
Maritime Security (Control Centre/ Vessel)	1	1	1	1	1	NJT	NJT	NJT
Aviation Security (Avsec) (Operation, Intelligent and investigation)	1	1	1	1	1	1	1	NJT

Table 4.11: Summary of Job Titles in N802

Job Area	Job Level							
	1	2	3	4	5	6	7	8
Security System Surveillance Operator	1	1	1	1	1	NJT	NJT	NJT
Security System Analyst	NJT	NJT	NJT	1	1	1	1	NJT
Security System Technologist	NJT	NJT	1	1	1	1	1	1

Table 4.12: Summary of Job Titles in N803

Job Area	Job Level							
	1	2	3	4	5	6	7	8
Surveillance Investigation	NJT	1	1	1	1	1	1	NJT

4.5 The Responsibilities and Job Descriptions for Each Job Title

Objective 2 (b): To identify the responsibilities and job descriptions for each job title.

Identifying responsibilities and job descriptions associated with each job title involves a comprehensive analysis of the specific duties, tasks, and expectations tied to individual roles within an organization. This process typically entails delineating the key responsibilities, such as managerial oversight, operational execution, specialized tasks, and leadership responsibilities, attributed to each job title. It involves outlining the skills, qualifications, and experiences necessary to fulfill these roles effectively. By meticulously defining the responsibilities, functions, and hierarchical positioning of each job title, organizations ensure clarity in role expectations, facilitate efficient workflow management, support employee growth, and align organizational objectives with individual contributions, ultimately fostering a cohesive and productive work environment. The result of responsibilities and job descriptions for each job title as below:

4.5.1 The **Occupational Responsibilities (OR) in N801**

Table 4.13: Summary of Occupational Responsibilities (OR) in N801

SECTION	**N (Administrative Activities and Support Services)**		
DIVISION	**80 Security and Investigation Activities**		
GROUP	**801 (Private Security Activities)**		
AREA / **LEVEL**	**Guarding Services (GS)**	**Armed Guarding (AG)**	**Close Protection (CP)**
LEVEL 8	NJT	NJT	NJT
LEVEL 7	NJT	NJT	NJT
LEVEL 6	NJT	NJT	NJT
LEVEL 5	**GS Security Manager** • Develop and implement security policies and procedures. • Oversee and manage the entire security team. • Conduct risk assessments and security audits. • Provide leadership and guidance to security personnel. • Monitor and analyze security trends and incidents. • Coordinate with law enforcement and regulatory agencies. • Implement training programs for security staff. • Ensure compliance with security standards and regulations.	NJT	**CP Manager** • Develop and implement strategic plans for close protection operations. • Conspire with clients and security teams to understand specific protection needs. • Conduct comprehensive risk assessments for clients and their environments. • Formulate strategies to mitigate potential threats. • Recruit, train, and manage a team of close protection personnel • Assign duties and responsibilities to ensure effective protection. • Coordinate closely with local law enforcement and relevant authorities. • Oversee the planning and execution of protection operations. • Maintain regular communication with clients to understand their security concerns. • Provide updates on security measures and potential risks.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA LEVEL	Guarding Services (GS)	Armed Guarding (AG)	Close Protection (CP)
			• Develop and implement emergency response plans. • Coordinate responses to security incidents or threats. • Plan logistics for client movements, events, or travel. • Ensure the availability of necessary equipment and resources. • Ensure compliance with legal and regulatory requirements related to close protection. • Stay informed about changes in security laws and regulations.
LEVEL 4	**GS Security Executive** • Implement security measures and protocols.Monitor security systems and respond to alarms. • Conduct security briefings for security staff. • Conspire with external security agencies. • Perform risk assessments and vulnerability analyses. • Handle access control and identity verification processes. • Investigate security incidents and prepare reports. • Ensure emergency response and crisis management.	NJT	**CP Executive** • Provide close protection to clients in various environments. • Accompany clients during travel, events, and daily activities. • Continuously assess potential threats and risks. • Adjust protection strategies based on changing circumstances. • Maintain clear and constant communication with the close protection team. • Coordinate with the Close Protection Manager and other team members. • Conduct surveillance and monitoring of the client's surroundings. • Identify and respond to any suspicious activities. • Be prepared to respond swiftly to emergencies.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA LEVEL	Guarding Services (GS)	Armed Guarding (AG)	Close Protection (CP)
	• Maintain accurate documentation of security activities.		• Implement emergency evacuation or protection measures as needed.
LEVEL 3	**GS Security Supervisor** • Supervise security officers and guard operations. • Ensure the enforcement of security policies and procedures. • Conduct regular security drills and exercises. • Monitor and analyse security data for trends. • Assist in the development of security training programs. • Respond to and manage security incidents. • Coordinate with law enforcement and regulatory authorities. • Maintain accurate documentation and records. • Conduct routine inspections and patrols.	**AG Supervisor** • Supervise and lead a team of armed security personnel • Provide guidance and direction to security officers. • Conduct regular briefings and debriefings. • Oversee the training of armed security personnel. • Ensure that all team members are proficient in firearm use and safety. • Conduct ongoing training sessions to enhance skills. • Plan and organize security operations. • Develop security strategies to address potential threats. • Coordinate with other departments for seamless security integration. • Conduct risk assessments for various locations and situations. • Develop and implement risk mitigation strategies. • Coordinate emergency response plans and drills.	**CP Senior Bodyguard** • Execute close protection duties based on assigned roles and responsibilities. • Provide physical protection and ensure the safety of the client. • Lead and guide junior members of the close protection team. • Assist in coordinating protection efforts during assignments. • Interact with the client in a professional and discreet manner. • Address client concerns and ensure satisfaction. • Ensure advance planning for client movements or events. • Conduct reconnaissance and assess potential risks.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA LEVEL	Guarding Services (GS)	Armed Guarding (AG)	Close Protection (CP)
		• Lead the team in responding to security incidents or threats. • Ensure compliance with legal and regulatory requirements for armed security. • Stay updated on changes in laws related to armed security. • Ensure that all firearms and security equipment are well-maintained. • Conduct regular checks on the readiness of weapons and gear. • Oversee the documentation of security incidents. • Prepare detailed reports on security-related activities.	
LEVEL 2	**GS Security Officer** • Implement security measures to protect premises and assets. • Conduct security screenings of individuals and belongings. • Monitor surveillance systems for unusual activities. • Enforce access control and identification procedures. • Report and respond to security incidents. • Ensure security training programs.	**AG Security Officer** • Conduct armed patrols to secure assigned areas. • Monitor surveillance systems for unusual activities. • Enforce access control measures, ensuring only authorized personnel enter designated areas. • Verify identification and credentials of individuals. • Identify potential security threats and risks.	**CP Bodyguard** • Provide immediate and direct physical protection to the client. • Accompany the client during travel and public appearances. • Observe and report any unusual activities or potential threats. • Maintain vigilance to prevent security breaches. • Stay in constant communication with other members of the protection team. • Use communication devices effectively.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA LEVEL	Guarding Services (GS)	Armed Guarding (AG)	Close Protection (CP)
	• Conduct routine patrols and inspections. • Provide assistance during emergencies.	• Respond promptly to alarms and security breaches. • Respond to emergencies with appropriate use of force, if necessary • Implement emergency evacuation procedures. • Provide a visible and professional security presence. • Offer assistance and information to employees and visitors. • Maintain effective communication with team members and supervisors. • Use two-way radios and other communication devices. • Possess and use firearms responsibly and safely. • Follow proper procedures for carrying and using weapons. • Record and report all security-related incidents. • Complete detailed incident reports as necessary.	• Follow established protocols for emergency response. • Implement evacuation or protection measures as directed.
LEVEL 1	**GS Assistant Security Officer** • Assist in the implementation of security protocols.	NJT	NJT

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA LEVEL	Guarding Services (GS)	Armed Guarding (AG)	Close Protection (CP)
	• Perform security screenings and inspections. • Monitor surveillance cameras and report suspicious activities. • Assist in emergency response and evacuation procedures. • Support senior security personnel in daily operations. • Conduct routine security patrols. • Provide assistance during security drills and exercises. • Maintain accurate records of security activities.		

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA LEVEL	Cash Management (CM)	K9 Service (K9)	Alarm Monitoring (AM)
LEVEL 8	NJT	NJT	NJT
LEVEL 7	NJT	NJT	NJT
LEVEL 6	NJT	NJT	NJT
LEVEL 5	NJT	NJT	NJT
LEVEL 4	NJT	NJT	NJT
LEVEL 3	CM Supervisor	NJT	AM Supervisor

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA / LEVEL	Cash Management (CM)	K9 Service (K9)	Alarm Monitoring (AM)
	• Supervise and lead a team of security personnel involved in cash management activities. • Assign tasks and responsibilities to ensure efficient operations. • Ensure compliance with established cash handling and security protocols. • Enforce adherence to standard operating procedures. • Provide training to security staff on cash management procedures. • Conduct regular drills and training sessions to enhance skills. • Oversee security measures related to the transportation and handling of cash. • Implement strategies to safeguard assets against theft or unauthorized access. • Develop and implement emergency response plans for cash-related incidents. • Coordinate with local law enforcement when necessary. • Ensure proper maintenance and functionality of security equipment used in cash management.		• Provide leadership and guidance to the alarm monitoring team. Supervisors are responsible for Overseeing the work of alarm monitoring security officers. • Ensure that all alarm monitoring officers receive ongoing training • Create and manage work schedules for the alarm monitoring team • Monitor the performance of alarm monitoring officers • Provide technical assistance to alarm monitoring officers • Oversee the response to alarm activations • Maintain accurate records of alarm activities, incidents, and responses • Ensure that all alarm monitoring activities align with company policies • Identify areas for improvement in alarm monitoring procedures and implement changes as needed. • Maintain effective communication with other security personnel

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA / LEVEL	Cash Management (CM)	K9 Service (K9)	Alarm Monitoring (AM)
	• Conduct regular checks on surveillance systems, alarms, and other security devices. • Monitor and control inventory of cash-related supplies and equipment. • Replenish resources as needed to maintain operational readiness. • Interact with clients to understand their specific cash management requirements. • Provide updates and reports on security measures.		
LEVEL 2	**CM Security Officer** • Safely handle and transport cash according to established protocols. • Follow security procedures during cash-in-transit or cash handling operations. • Monitor and observe cash management activities through surveillance systems. • Identify and report any suspicious activities or security breaches. • Assist clients during cash-related transactions. • Provide a visible security presence to deter potential threats.	**K9 Security Officer** • Training and Handling Police Dogs • Patrol and Detection • Search and Rescue • Suspect Apprehension • Community Engagement • Maintaining Equipment • Report Writing • Continued Training • Adhering to Laws and Regulations • Work closely with other law enforcement officers	**AM Security Officer** • Monitor alarm systems • Respond promptly to alarm activations • Relay information to supervisors • Record details of alarm activations • Troubleshoot technical issues related to alarm systems • Conduct visual surveillance of monitored premises through security cameras and other monitoring tools. • Provide assistance and support • Follow established procedures and protocols • Ensure the proper functioning and maintenance of alarm monitoring equipment.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA / LEVEL	Cash Management (CM)	K9 Service (K9)	Alarm Monitoring (AM)
	• Maintain clear and timely communication with team members and supervisors. • Use communication devices effectively during operations. • Complete and maintain accurate records of cash management activities. • Prepare reports on incidents, discrepancies, or security concerns.		
LEVEL 1	**CM Assistant Security Officer** • Assist in various functions related to cash management security. • Support the supervisor and security officers in day-to-day operations. • Follow established security procedures for cash handling and transportation. • Learn and adhere to standard operating protocols. • Assist in the maintenance and inspection of security equipment • Report any issues with surveillance systems or alarms. • Ensure emergency response drills and activities. • Be prepared to assist during emergencies as directed.	NJT	NJT

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA / LEVEL	Cash Management (CM)	K9 Service (K9)	Alarm Monitoring (AM)
	• Observe and report any security-related incidents or concerns. • Maintain vigilance to prevent unauthorized access to cash or valuables.		

SECTION	N (Administrative Activities and Support Services)	
DIVISION	80 Security and Investigation Activities	
GROUP	801 (Private Security Activities)	
AREA / LEVEL	Maritime Security	Aviation Security (Avsec) (Operation, Intelligent and investigation)
LEVEL 8	NJT	NJT
LEVEL 7	NJT	**Avsec Senior Specialist** • Develop and implement aviation security policies and procedures. • Oversee and manage security programs at airports. • Conduct risk assessments and threat analyses. • Conspire with regulatory agencies to ensure compliance with aviation security standards. • Provide leadership and guidance to security personnel. • Investigate security incidents and breaches. • Implement training programs for security staff • Stay updated on the latest security technologies and industry best practices.
LEVEL 6	NJT	**Avsec Specialist**

SECTION	N (Administrative Activities and Support Services)	
DIVISION	80 Security and Investigation Activities	
GROUP	801 (Private Security Activities)	
AREA / LEVEL	Maritime Security	Aviation Security (Avsec) (Operation, Intelligent and investigation)
		• Implement security measures to safeguard airport facilities and operations. • Conduct security inspections and audits. • Monitor and analyze security threats and trends. • Refine and use relevant enforcement and regulatory agencies. • Train airport staff on security protocols. • Respond to and manage security incidents. • Ensure compliance with aviation security regulations. • Conduct security drills and exercises.
LEVEL 5	**Maritime Operation Manager** • Special briefing to the Team Leader of the Maritime operations team. • Communicate directly with Operations Room and Maritime Team Leader. • Holding operational briefings from time to time or according to the management's requirements. • Always ready at all times and ready to issue appropriate instructions according to the situation. • Fully understand the journeys, statistics, expectations and adhere to maritime operational procedures during threats. • Ensure that the details of the reports received are authentic and complete before issuing an order. • Manage Incidents • Issuing appropriate instructions according to relevant guidelines and laws. • Ensure all land support assistance and various appropriate assistance.	**Avsec Senior Executive** • Assist in the development and implementation of security strategies. • Supervise security personnel and operations. • Conduct regular security assessments and audits. • Coordinate with other departments to address security concerns. • Manage access control systems and surveillance technologies. • Investigate security incidents and prepare reports. • Provide training and awareness programs for employees. • Ensure compliance with aviation security policies.

SECTION	N (Administrative Activities and Support Services)	
DIVISION	80 Security and Investigation Activities	
GROUP	801 (Private Security Activities)	
AREA / LEVEL	Maritime Security	Aviation Security (Avsec) (Operation, Intelligent and investigation)
	• Submit all complete details of incident report and the work completion report to the relevant parties.	
LEVEL 4	**Maritime Control Centre Supervisor** • General security monitoring • Preparing and organising the Operation Room according to the S.O.P. • Ensure all points of contact according to the identified checklist. • Update all information and notifications according to the checklist. • Detect Security Threats • Acting as an intelligence officer. • Update briefly all Human Reliability Analysis (HRA) and latest events. • Advise the appropriate direction according to the threat received. • Manage incidents • Channelling authentic information about the incident to relevant channels. • Issuing appropriate instructions to the monitoring team and the maritime security team. • Provide complete reports to management, client and relevant security bodies.	**Avsec Executive** • Implement security measures and protocols at airports. • Monitor security systems and respond to alarms. • Conduct security briefings for airport staff • Conspire with external security agencies. • Perform risk assessments and vulnerability analyses. • Handle access control and identity verification processes. • Investigate security incidents and prepare reports. • Ensure emergency response and crisis management.
LEVEL 3	**Maritime Team Leader** • Detects Security Threats • Manage security personnel in security surveillance. • Act to advise the vessel master on the action to be taken. • Manage Security Teams • Coach security personnel • Conduct team briefings • Supervise security personnel.	**Avsec Senior Officer** • Supervise security operations at airports. • Ensure the enforcement of security policies and procedures. • Conduct regular security drills and exercises. • Monitor and analyze security data for trends. • Assist in the development of security training programs. • Respond to and manage security incidents. • Coordinate with law enforcement and regulatory authorities.

SECTION	N (Administrative Activities and Support Services)	
DIVISION	80 Security and Investigation Activities	
GROUP	801 (Private Security Activities)	
AREA / LEVEL	**Maritime Security**	**Aviation Security (Avsec) (Operation, Intelligent and investigation)**
	• Manage Incidents • Compile incident reports • Execute evacuation plans or exercises. • Handle medical incidents • Provide relevant information that are required by Ops Room officer relating to case management.	• Maintain documentation and records related to security activities.
LEVEL 2	**Maritime Unit Leader** • Provide Concierge Security Services • Attend to enquires from Vessel Master and Ops Room Officer. • Manage the assignments and supervision. • Ensure accurate reports are delivered promptly. • Detect Security Threats • Carry out instructions from the Team Leader. • Perform security surveillance on board the vessel. • Ensure communication tools operate well and are ready to use. • Manage Incidents • Assist ship's crew in law enforcement. • Provide quick response to incidents and emergencies. • Ready to act according to the right channel.	**Avsec Officer** • Implement security measures to protect airport assets. • Conduct security screenings of passengers and baggage.SEP Monitor surveillance systems for unusual activities. • Enforce access control and identification procedures • Report and respond to security incidents. • Ensure security training programs. • Conduct routine patrols and inspections.
LEVEL 1	**Maritime Ship Security Officer / Maritime Operating Room Officer** • Provide general security services • Carry out monitoring task as directed. • Assist in delivering situation reports according to SOP (Standard Operating Procedure) • To monitor environmental activities. • Detect Security Threats	**Avsec Assistant** • Assist in the implementation of security protocols. • Perform security screenings and inspections. • Monitor surveillance cameras and report suspicious activities. • Assist in emergency response and evacuation procedures. • Support senior security personnel in daily operations • Conduct routine security patrols. • Provide assistance during security drills and exercises.

SECTION	N (Administrative Activities and Support Services)	
DIVISION	80 Security and Investigation Activities	
GROUP	801 (Private Security Activities)	
AREA / LEVEL	Maritime Security	Aviation Security (Avsec) (Operation, Intelligent and investigation)
	• Assist Unit Leader to respond and report incidents. • Assist Unit Leader to perform security coverage. • Assist Unit Leader to closely monitor all threats. • Manage Incidents • Assist Unit Leader to provide quick response to incidents and emergencies. • Assist Unit Leader to assist authorities during incidents. • Ready to take defensive action according to R.O.E (Rules of Engagement). • Provide general security monitoring • Establish 24/7 security monitoring and impart security-related agencies. • Ensuring directive and monitoring of asset positions and intended movements such as route plans. • Monitor and channel all reports from assets, management, and enforcement agencies. • Detect security threats • Ensure accurate report data and channel it to specific channels. • Provide daily briefings for Ops Room Coordinator and Operation Manager. • Provide crisis management team briefings for Ops Room Coordinator and Operation Manager. • Manage incidents • Coordinate reports and actions with the SSO Team Leader. • Issue instructions in accordance with management approval regarding actions to be taken.	• Maintain accurate records of security activities.

4.5.2 The **Occupational Responsibilities (OR) in N802**

Table 4.14: Summary of Occupational Responsibilities (OR) in N802

SECTION	**N (Administrative Activities and Support Services)**		
DIVISION	**80 Security and Investigation Activities**		
GROUP	**802 (Security Systems Service Activities)**		
AREA / **LEVEL**	**Security System Surveillance Operator**	**Security System Analyst**	**Security System Technologist**
LEVEL 8	NJT	NJT	**Chief Technical Officer** • Oversee implementation of secure and resilient security systems, networks, and infrastructure. • Oversee integration of various security tools, technologies, and components to create a cohesive and effective security environment. • Oversee implementation of encryption protocols, multi-factor authentication, and access controls to safeguard data and resources. • Oversee penetration testing and vulnerability assessments to identify and address weaknesses in security systems. • Oversee plan innovation plan of emerging security technologies, providing recommendations for adoption based on organizational needs. • Oversee technical teams to ensure seamless integration of security measures into existing systems.
LEVEL 7	NJT	**Specialist/ Senior Security Solutions/ Senior Manager** • Develop the program to assess security threats, vulnerabilities, and risks to identify potential weaknesses in the security infrastructure.	**Specialist Technical Deployment** • Develop secure and resilient security systems, networks, and infrastructure. • Develop various security tools, technologies, and components to create a cohesive and effective security environment.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	802 (Security Systems Service Activities)		
AREA / LEVEL	Security System Surveillance Operator	Security System Analyst	Security System Technologist
		• Lead the development of security systems, networks, and applications to detect unauthorized access and potential breaches. • Verify security incidents, analyse data logs, and produce detailed reports on findings and recommendations. • Plan implementation of security measures with technical teams to ensure compliance with security policies. • Plan security assessments and audits to evaluate the effectiveness of existing security controls. • Innovate in accordance with emerging security trends, tools, and techniques to proactively address new threats. • Development of incident response plans and protocols. • Verify security awareness training to employees and promote a security-conscious culture.	• Develop security systems, firewalls, and intrusion detection/prevention systems in alignment with security policies. • Verify the Implementation of encryption protocols, multi-factor authentication, and access controls to safeguard data and resources. • Validate penetration testing and vulnerability assessments to identify and address weaknesses in security systems. • Innovate in accordance emerging security technologies, providing recommendations for adoption based on organizational needs. • Plan with other technical teams to ensure seamless integration of security measures into existing systems.
LEVEL 6	NJT	**Manager / Security Solutions** • Lead Surveillance Operations Monitoring security systems, including technology platforms, sensors, cameras, alarms, drone, robotics, and access control systems.	**Head Technical Operation Executives** • Plan the implementation of secure and resilient security systems, networks, and infrastructure. • Plan the integration of various security tools, technologies, and components to create a cohesive and effective security environment. Verify the configuration of security systems,

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	802 (Security Systems Service Activities)		
AREA / LEVEL	**Security System Surveillance Operator**	**Security System Analyst**	**Security System Technologist**
		• Plan and manage surveillance equipment to ensure continuous monitoring of designated areas. • Coordinate with other security personnel and law enforcement during incidents or emergencies. • Coordinate of security incidents reporting, maintaining accurate records of activities during shifts. • Plan routine maintenance and checks on surveillance equipment to ensure proper functioning. • Plan training program for new surveillance operators on protocols, equipment operation, and security procedures	firewalls, and intrusion detection/prevention systems in alignment with security policies. • Verify the implement of encryption protocols, multi-factor authentication, and access controls to safeguard data and resources. • Conduct penetration testing and vulnerability assessments to identify and address weaknesses in security systems. • Research and evaluate emerging security technologies, providing recommendations for adoption based on organizational needs. • Verify with other technical teams to ensure seamless integration of security measures into existing systems. • Develop documentation of security configurations, procedures, and system designs for future reference.
LEVEL 5	**Assistant Manager/ Supervisor** • Lead Surveillance Operations Monitoring security systems, including technology platforms, sensors, cameras, alarms, drone, robotics, and access control systems. • Plan and manage surveillance equipment to ensure continuous monitoring of designated areas.	**Senior Analyst** • Evaluate security threats, vulnerabilities, and risks to identify potential weaknesses in the security infrastructure. • Supervise security systems, networks, and applications to detect unauthorized access and potential breaches. • Supervise with the technical teams to implement security measures and ensure compliance with security policies.	**Senior Technical Executives** • Evaluate the implementation of secure and resilient security systems, networks, and infrastructure. • Verify the integration of various security tools, technologies, and components to create a cohesive and effective security environment. • Configure security systems, firewalls, and intrusion detection/prevention systems in alignment with security policies.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	802 (Security Systems Service Activities)		
AREA / LEVEL	**Security System Surveillance Operator**	**Security System Analyst**	**Security System Technologist**
	• Coordinate with other security personnel and law enforcement during incidents or emergencies. • Coordinate of security incidents reporting, maintaining accurate records of activities during shifts. • Plan routine maintenance and checks on surveillance equipment to ensure proper functioning. • Plan training program for new surveillance operators on protocols, equipment operation, and security procedures.	• Ensure security assessments and audits exercise to evaluate the effectiveness of existing security controls. • Ensure development and execution of incident response plans and protocols.	• Implement encryption protocols, multi-factor authentication, and access controls to safeguard data and resources. • Evaluate the penetration testing and vulnerability assessments to identify and address weaknesses in security systems. • Supervise implementation with other technical teams to ensure seamless integration of security measures into existing systems. • Evaluate documentation of security configurations, procedures, and system designs for future reference.
LEVEL 4	**Senior Executives** • Design Surveillance Operations Monitoring security systems, including technology platforms, sensors, cameras, alarms, drone, robotics, and access control systems. • Lead mobile surveillance of premises to identify and respond to any suspicious or unauthorized activities. • Verify surveillance equipment to ensure continuous monitoring of designated areas.	**Analyst** • Analyze security threats, vulnerabilities, and risks to identify potential weaknesses in the security infrastructure. • Analyze security systems, networks, and applications to detect unauthorized access and potential breaches. • Coordinate with technical teams to implement security measures and ensure compliance with security policies. • Observe the security assessments and audits exercise to evaluate the effectiveness of existing security controls. • Observe in the development and execution of incident response plans and protocols.	**Technical Executives** • Implement secure and resilient security systems, networks, and infrastructure. • Integrate various security tools, technologies, and components to create a cohesive and effective security environment. • Monitor the implementation of security systems, firewalls, and intrusion detection/prevention systems in alignment with security policies. • Coordinate with other technical teams to ensure seamless integration of security measures into existing systems.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	802 (Security Systems Service Activities)		
AREA / LEVEL	**Security System Surveillance Operator**	**Security System Analyst**	**Security System Technologist**
	• Coordinate with other security personnel and law enforcement during incidents or emergencies. • Approve security incidents report, maintaining accurate records of activities during shifts. • Verify routine maintenance and checks on surveillance equipment to ensure proper functioning. • Verify training program for new surveillance operators on protocols, equipment operation, and security procedures.		• Comply documentation of security configurations, procedures, and system designs for future reference.
LEVEL 3	**Executives** • Control Surveillance Operations Monitoring security systems, including technology platforms, sensors, cameras, alarms, drone, robotics, and access control systems. • Plan mobile surveillance of premises to identify and respond to any suspicious or unauthorized activities. • Organize and manage surveillance equipment to ensure continuous monitoring of designated areas.	NJT	**System Admin** • Administer, configure, and maintain security systems, including surveillance cameras, access control systems, and alarms • Ensure the proper functioning of security software and hardware. • Manage user accounts and permissions for security systems. • Provide access to authorized personnel and restrict access as necessary. • Identify and resolve technical issues with security systems promptly. • Conduct regular system checks and diagnostics to prevent malfunctions.

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	802 (Security Systems Service Activities)		
AREA / LEVEL	**Security System Surveillance Operator**	**Security System Analyst**	**Security System Technologist**
	• Validate security incidents, maintaining accurate records of activities during shifts. • Organize routine maintenance and checks on surveillance equipment to ensure proper functioning. • Conduct a training new surveillance operator on protocols, equipment operation, and security procedures.		• Keep security software up-to-date with the latest patches and updates. • Test and implement new features or enhancements. • Implement measures to secure and protect data collected by security systems. • Perform back up data to prevent loss in case of system failure. • Maintain accurate documentation of security system configurations, changes, and updates. • Create user manuals or guides for system operation. • Conduct regular security audits of system configurations and access logs. • Identify vulnerabilities and implement corrective actions. • Coordinate with vendors for technical support and issue resolution
LEVEL 2	**Senior Operator** • Ensure Surveillance Operations Monitoring security systems, including technology platforms, sensors, cameras, alarms, drone, robotics, and access control systems. • Ensure mobile surveillance of premises to identify and respond to	NJT	NJT

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	802 (Security Systems Service Activities)		
AREA / LEVEL	**Security System Surveillance Operator**	**Security System Analyst**	**Security System Technologist**
	any suspicious or unauthorized activities. • Communicate promptly to security alarms, incidents, and emergencies following established procedures. • Supervise and manage surveillance equipment to ensure continuous monitoring of designated areas. • Check report security incidents, maintaining accurate records of activities during shifts. • Maintain and checks on surveillance equipment to ensure proper functioning.		
LEVEL 1	**Operator** • Perform Surveillance Operations Monitoring security systems, including technology platforms, sensors, cameras, alarms, drone, robotics, and access control systems. • Perform mobile surveillance of premises to identify and respond to any suspicious or unauthorized activities. • Perform promptly to security alarms, incidents, and emergencies following established procedures.	NJT	NJT

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	802 (Security Systems Service Activities)		
AREA / LEVEL	Security System Surveillance Operator	Security System Analyst	Security System Technologist
	• Perform surveillance equipment to ensure continuous monitoring of designated areas. • Report security incidents, maintaining accurate records of activities during shifts. • Conduct routine maintenance and checks on surveillance equipment to ensure proper functioning.		

4.5.3 The **Occupational Responsibilities (OR) in N803**

Table 4.15: Summary of Occupational Responsibilities (OR) in N803

SECTION	N (Administrative Activities and Support Services)
DIVISION	80 Security and Investigation Activities
GROUP	803 (Investigation Activities)
AREA / LEVEL	Surveillance Investigation
LEVEL 8	NJT
LEVEL 7	**Investigation Technical Team Leader** • Design a technical investigation team. • Formulate guidance and mentorship to team members. • Planning and execution of complex investigations. • Ensure adherence to established protocols and procedures. • Design investigative technologies and tools. • Analyze technical data and digital evidence to support investigations.

SECTION	N (Administrative Activities and Support Services)
DIVISION	80 Security and Investigation Activities
GROUP	803 (Investigation Activities)
AREA LEVEL	Surveillance Investigation
	• Interpret and recommendations based on findings. • Formulate investigation technic, prepare detailed and accurate procedure, verify reports and investigative outcomes. • Corporate investigation (Technical forensic, Audit forensic, financial investigation, IT investigation)
LEVEL 6	**Investigation Team Leader** • Supervise a team of investigators and allocate tasks. • Ensure team members adhere to investigative standards. • Manage the progress of investigations and ensure timelines are met. • Prioritize cases based on urgency and impact. • Allocate resources effectively to support investigations. • Ensure proper documentation of investigative processes and findings. • Maintain records and case files. • Provide Support cross-functional investigations. • Verify quality checks on investigative work. • Implement corrective actions as needed. • Conduct a personal investigation (Matrimonial cases)
LEVEL 5	**Investigation Senior Analyst** • Analyze data and evidence related to investigations. • Provide expert insights into complex cases (Technical forensic, Audit forensic, Financial investigation, IT investigation) • Prepare detailed reports summarizing investigative findings.' • Ensure clarity and accuracy in documentation. • Handle and secure physical and digital evidence. • Follow chain of custody protocols. • Provide expert testimony in legal proceedings if required. • Communicate findings effectively to legal professionals.
LEVEL 4	**Investigation Junior Analyst** • Collect and compile data relevant to investigations. • Assist in the analysis of evidence.

SECTION	N (Administrative Activities and Support Services)
DIVISION	80 Security and Investigation Activities
GROUP	803 (Investigation Activities)
AREA LEVEL	Surveillance Investigation
	• Maintain accurate records of investigative activities • Support senior analysts in report preparation. • Conduct research on emerging investigative methodologies. • Assist in cross-functional initiatives.
LEVEL 3	**Investigation Senior Operative** • Conduct field investigations and gather on-site information. • Adhere to safety and legal protocols. • Perform surveillance activities as directed by team leaders. • Record observations and activities. • Communicate effectively with team members and leadership. • Provide timely updates on fieldwork. • Record findings and submit reports. • Ensure accuracy and completeness of reports (matrimonial cases) • Adhere to ethical and legal standards in investigative work by follow standard operating procedures.
LEVEL 2	**Investigation Junior Operative** • Assist in conducting field investigations and gathering information. • Ensure in surveillance activities, documenting observations. • Report findings accurately and promptly. • Maintain effective communication with the investigative team. • Provide updates on field activities and observations • Interpreting assigned tasks and activities as part of the investigation. • Contribute to the preparation of field reports. • Ensure in training sessions to enhance skills and knowledge.
LEVEL 1	NJT

4.6 The Critical Job, Job Relevant and Job Related with the Technology for N80

Objective 2 (c): To identify the critical job and the Job Description for N80 related to current developments in the industry.

Defining specific roles as "critical" within the security sector is justified for multifaceted reasons. Firstly, critical security jobs play a pivotal role in risk mitigation by actively engaging in tasks that contribute to the prevention of threats and the safeguarding of individuals, assets, and sensitive information from potential harm or unauthorized access. Second, certain positions are deemed critical due to their indispensable function in emergency response, requiring swift and effective action during crises such as security breaches, natural disasters, or other emergencies. Additionally, in many organizations, roles are considered critical as they are entrusted with the protection of vital assets, encompassing both physical entities like facilities and equipment and digital assets like sensitive information or data systems. Furthermore, certain security jobs directly contribute to public safety, including those in law enforcement, airport security, and other areas vital to the well-being of the general public. Moreover, critical security roles are often instrumental in ensuring regulatory compliance, as they navigate industry regulations, legal requirements, and standards, with non-compliance carrying severe consequences.

In the realm of cybersecurity, critical roles are acknowledged for their significance in protecting digital assets, sensitive information, and upholding the integrity of information systems amidst the escalating threat of cyberattacks. For national security, specific jobs within government or defence sectors are considered critical, involving tasks such as border protection, intelligence operations, and the safeguarding of critical infrastructure. Additionally, these roles contribute substantially to organizational resilience, with individuals tasked with developing and implementing security measures to ensure an organization can withstand and recover from disruptions. The high-level decision-making involved in certain security positions, where executives or leaders have a significant impact on an organization's overall security posture and strategy, further justifies their critical designation. Lastly, critical security jobs often demand specialized expertise in areas such as cybersecurity, threat analysis, or crisis management, making them indispensable for addressing specific security challenges. In essence, the classification of certain security roles as "critical" stems from their foundational role in risk management, emergency response, asset protection, and ensuring the safety and

security of individuals, organizations, and nations, underscoring their significance in the face of potential consequences of failure in their responsibilities.

In the security context, a "High Demand job" refers to a position within the security sector that is sought after and in great demand due to various factors. These factors can include the growing need for specialized skills, increased threats or risks that require additional security measures, or evolving industry trends. High demand security jobs are typically those for which there is a consistent and significant need, often driven by the critical nature of the responsibilities associated with the role. Examples of high demand security jobs may include cybersecurity experts, threat analysts, physical security specialists, and professionals with expertise in emerging technologies relevant to security, such as data protection or surveillance systems. The demand for these roles is often influenced by the dynamic nature of security challenges, advancements in technology, and the increasing recognition of the importance of robust security measures across various sectors.

Critical jobs, especially those related to technology, are assessed based on the outcomes of the focus group discussions (FGD) method. Critical jobs are marked with a single asterisk (*), jobs specifically associated with technology carry a double asterisk (**), and critical jobs directly related to technology are denoted with a triple asterisk (***).

4.6.1 Private Security Activities Critical job and Job Related to The Technology

Table 4.16: Private Security Activities Critical job and Job Related to The Technology

SECTION	**N (Administrative Activities and Support Services)**		
DIVISION	**80 Security and Investigation Activities**		
GROUP	**801 (Private Security Activities)**		
AREA **LEVEL**	***Critical Job**	****Jobs Relevant to Technology and Industrial Revolution**	*****Jobs Relevant to Technology and Industrial Revolution**
Guarding Services (GS)	• GS Security officer • GS Assistant Security Officer	• GS Security Manager • GS Security Executive • GS Security Supervisor	NJT
Armed Guarding (AG)	• AG Supervisor • AG Security Officer	NJT	NJT
Close Protection (CP)	• CP Senior Bodyguard	• CP Manager • CP Executive	NJT

SECTION	N (Administrative Activities and Support Services)		
DIVISION	80 Security and Investigation Activities		
GROUP	801 (Private Security Activities)		
AREA LEVEL	*Critical Job	**Jobs Relevant to Technology and Industrial Revolution	***Jobs Relevant to Technology and Industrial Revolution
	• CP Bodyguard		
Cash Management (CM)	NJT	NJT	NJT
K9 Service (K9)	K9 Security Officer	NJT	NJT
Alarm Monitoring (AM)	NJT	NJT	• AM Supervisor • AM Security Officer
Maritime Security	Team Leader	Control Center Supervisor	• Maritime Operation Manager
Aviation Security (Avsec) (Operation, Intelligent and investigation)	Avsec assistant	NJT	• Avsec executive • Avsec senior officer • Avsec officer

The 801 group, consisting of 29 distinct job titles, delineates various roles within an organizational framework. Among these titles, eight are designated as job area roles, serving as pivotal positions that define the broader scope of responsibilities within specific domains or departments. Additionally, four roles within this group are categorized as technology-related, highlighting their direct association with technological functions or expertise. Furthermore, six positions are identified as critical and possess a dual classification, being both essential to the organization's operations and deeply intertwined with technology-related tasks or advancements. This breakdown emphasizes the diversity and significance of roles within the 801 group, showcasing the crucial intersections between specialized job areas and the pivotal role technology plays across multiple functions within the organization.

4.6.2 Security Systems Service Activities Critical Job

Table 4.17: Security Systems Service Activities Critical Job

SECTION	**N (Administrative Activities and Support Services)**		
DIVISION	**80 Security and Investigation Activities**		
GROUP	**802 (Security Systems Service Activities)**		
AREA / **LEVEL**	***Critical Job**	****Jobs Relevant to Technology and Industrial Revolution**	*****Jobs Relevant to Technology and Industrial Revolution**
Security System Surveillance Operator	NJT	• Senior Executives • Executives	• Asistant Manager/ • Supervisor
Security System Analyst	NJT	• Senior Analyst • Analyst	• Specialist/ Senior Security Solutions/ Senior Manager • Manager / Security Solutions
Security System Technologist	NJT	• Technical Executives • System Admin	• Chief Technical Officer • Specialist Technical Deployment • Head Technical Operation Executives • Senior Technical Executives

Within the 802 group comprising eight distinct job areas, consensus among experts has identified six roles deemed recommended technology-related jobs, underscoring their strong association with technological expertise and functions. Moreover, within this group, seven positions have garnered a dual classification as both critical to the organization's operations and deeply intertwined with technology-related tasks and advancements. This classification highlights the strategic significance of these roles in leveraging and adapting to technological advancements, emphasizing their pivotal contribution to the organization's technological landscape while acknowledging their critical impact on the overall operational efficacy and success of the enterprise.

4.6.3 Investigation Activities Critical Job

Table 4.18: Investigation Activities Critical Job

SECTION	**N (Administrative Activities and Support Services)**		
DIVISION	**80 Security and Investigation Activities**		
GROUP	**803 (Investigation Activities)**		
AREA / **LEVEL**	***Critical Job**	****Jobs Relevant to Technology and Industrial Revolution**	*****Jobs Relevant to Technology and Industrial Revolution**
Surveillance Investigation	• Investigation Senior Analyst • Investigation Junior Analyst • Investigation Senior Operative • Investigation Junior Operative		• Investigation Technical Team Leader • Investigation Team Leader

The 803 group, comprising six distinct job titles, reflects an assessment where experts arrived at a consensus designating none of the roles as critical jobs within the organizational framework. However, within this subset, two specific positions were classified as critical jobs but with a discernible technology-related component. This assessment underscores a nuanced evaluation of roles within this group, indicating that while none of the positions are deemed critical in isolation, a subset of them holds critical significance when viewed through the lens of their technological involvement or influence. This delineation demonstrates the varying degrees of impact and importance associated with these roles within the organizational structure, emphasizing the specialized nature of certain positions that intertwine critical functions with technology-related expertise.

4.7 The Competency Needed to Address the Demand and Supply of the Industry in Malaysia

Objective 2 (d): To analyse the competency needed to address the demand and supply of the industry in Malaysia

Fuzzy Delphi Analysis

This study employed the Fuzzy Delphi technique to address objective (e), aiming to analyze the competencies required to meet the industry high demand and supply in Malaysia. The selection of this technique is made following the study's purpose to obtain expert consensus on the elements used in designing occupational framework. According to Mohd Jamil et al. (2017), this Fuzzy Delphi technique can be adopted to gain expert consensus on the itemization. The rationale for applying the Fuzzy Delphi technique compared to the Delphi technique is that it saves time and cost in handling questionnaires. It also allows experts to consistently provide their views (Mohd. Jamil et al., 2013). The minimum sample of experts in the Fuzzy Delphi studies is 10 to obtain high uniformity among experts (Adler & Ziglio, 1996; Jones & Twiss, 1978). Therefore, 23 experts were selected in this study using purposive sampling technique. They consisted of experts in security activities, system security activities and Investigation activities selected via purposive sampling technique (Chua, 2010). The experts had at least minimum of ten years of experience in the field. Expert selection criteria were in line with Berliner (2004) who stated that an individual is considered skilled in a field if he has had more than five years of experience in that field.

Questionnaire for Experts

The researchers used the literature review and interview to develop the research questionnaire for the Fuzzy Delphi method. The development of questionnaire items can be done based on literature review, pilot studies, and experiences (Skulmowski et al. 2007). Okoli and Pawlowski (2004) agree that the construction of items and content elements of a study should be done through a literature review within the study's scope. After adapting the questionnaire from literature, it was given to three experts for their feedback. Then, modifications were made to the questionnaire based on their feedback. It was also tested for reliability. To answer the research question, a five-point scale questionnaire, as stated in Table 4.19, was distributed to the experts to obtain consensus on the items.

Table 4.19: Five-Point Scale Fuzzy

Scale	Item	Triangular Fuzzy Number		
1	Strongly Disagree	0	0.1	0.2
2	Disagree	0.1	0.2	0.4
3	Moderate	0.2	0.4	0.6
4	Agree	0.4	0.6	0.8
5	Strongly Agree	0.6	0.8	1

Data Analysis Questionnaire

Data analysis was done systematically. The experts' views were carefully analysed using Microsoft Excel software as suggested by Ramlie et al. (2014), Mohd Jamil et al. (2017) and Mohd Jamil and Mat Noh (2020). The two main prerequisites that must be followed in the Fuzzy Delphi technique are the Triangular Fuzzy Number and the Defuzzification Process. Triangular Fuzzy Number has two conditions, first the value of Threshold (d) ≤ 0.25. The expert agreement is reached when the resulting value is smaller or equal to 0.25 (Cheng & Lin, 2002; Chen, 2000). The following formula is used:

$$d(\tilde{m},\tilde{n}) = \sqrt{\frac{1}{3}[(m_1 - n_1)^2 + (m_2 - n_2)^2 + (m_3 - n_3)^2]}$$

The second condition for the Triangular Fuzzy Number is to involve a percentage of expert agreement. The traditional Delphi technique stated that if the expert group agreement exceeds 70%, it is accepted (Chu & Hwang, 2008; Murray & Hammons, 1995). The determination of fuzzy (A) score value was made based on the following formula:

A= (1/3)*(m1 + m2 + m3)

Research Findings

Section 1: Demographic

The demographic details of the experts are presented in Table 4.11, indicating that each expert possesses over ten years of experience. The selected specialists are highly knowledgeable in Security Activities, System Security Activities, and Investigation Activities.

Table 4.20: Experts Demographic Information

AGE	
YEAR	Frequency
Above 50	14
40 to 49	6
30-39	3
Total	23
GENDER	
	Frequency
Male	21
Female	2
Total	23

WORKING EXPERIENCE	
YEAR	Frequency
Above 30	5
21 to 30	7
11 to 20	11
Total	23
CURRENT POSITION	
LEVEL	Frequency
Chief executive officer	5
Specialist/managing director/ general manager	15
Manager/human resource manager	3
Total	23
EXPERTISE	
FIELD OF EXPERT	Frequency
Security activities	9
Security system activities	7
Investigation activities	7
Total	23

Section 2: Competency in Demand

Analysis of Expert Consensus on knowledge competency for GROUP 801

In this knowledge competency construct, the items given to the experts are stated in Table 4.21.

Table 4.21: Items for the Aspect of Knowledge Competency in Demand Construct

ITEMS	
A1	Security threats
A2	Security personnel
A3	Medical incidents
A4	Case management
A5	Security surveillance
A6	Closed-Circuit Television (CCTV)
A7	Incidents and emergencies
A8	Traffic and crowds
A9	Security stakeholders
A10	Situational trend analyses
A11	Security operation audits
A12	Security risks
A13	Law enforcement

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.22.

Table 4.22: Findings of Expert Consensus on Knowledge Competency

ITEM	CONDITION OF DEFUZZIFICATION PROCESS		POSITION	EXPERTS CONSENSUS
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A5	89%	0.778	1	High Consensus
A1	100%	0.756	2	High Consensus
A6	100%	0.756	2	High Consensus
A12	100%	0.756	2	High Consensus
A7	100%	0.733	3	High Consensus
A2	89%	0.711	4	High Consensus
A10	100%	0.711	4	High Consensus
A8	100%	0.689	5	High Consensus
A9	100%	0.689	5	High Consensus
A13	89%	0.6889	5	High Consensus
A4	100%	0.667	6	High Consensus
A11	89%	0.667	6	High Consensus
A3	100%	0.489	7	High Consensus

Analyzing the results in Table 4.22, all 13 items have been accepted as knowledge competencies for security activities. All items have received unanimous agreement from experts, surpassing a threshold value of ≤ 0.25 with expert's consensus rate exceeding 70%. Notably, item A5 (Security Surveillance) holds the top position, attaining the highest fuzzy score.

Analysis of Expert Consensus on skills competency for GROUP 801

In this skills competency construct, the items given to the experts are stated in Table 4.23.

Table 4.23: Items for the Aspect of Skills Competency in Demand Construct

ITEMS	
A1	Interpersonal Communication
A2	Written Communication
A3	Critical Thinking
A4	Problem Solving
A5	Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results)
A6	Leadership
A7	Time management
A8	Aptitude for Technology and Equipment
A9	Intrapreneurship (Refers to employee initiatives in organisations to take something new, without being asked to do so)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.24.

Table 4.24: Findings of Expert Consensus on Skills Competency

ITEM	CONDITION OF DEFUZZIFICATION PROCESS		POSITION	EXPERTS CONSENSUS
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A3	100%	0.756	1	High Consensus
A4	100%	0.756	1	High Consensus
A6	100%	0.756	1	High Consensus
A7	100%	0.733	2	High Consensus
A1	100%	0.711	3	High Consensus
A5	100%	0.711	3	High Consensus
A8	89%	0.711	3	High Consensus
A2	100%	0.689	4	High Consensus
A9	44%	0.578	5	Low Consensus

Examining the outcomes in Table 4.24, one item out of the nine has been omitted as a skills competency for security activities. Specifically, item A9 (Intrapreneurship) has been excluded due to not meeting the 70% expert consensus with a ≤ 0.25 threshold value. It is noteworthy that items A3 (Critical Thinking), A4 (Problem Solving), and A6 (Leadership) hold the leading positions, achieving the highest fuzzy scores.

Analysis of Expert Consensus on attributes competency for GROUP 801

In this skills competency construct, the items given to the experts are stated in Table 4.25.

Table 4.25: Items for the Aspect of Attributes Competency in Demand Construct

ITEMS	
A1	Attention to details
A2	Team work
A3	Multi-tasking/ Flexibility
A4	Dependability (Trustworthy & Reliable)
A5	Work Ethics
A6	Professionalism
A7	Self-management/ independent
A8	Self-learning
A9	Agility (Ability to think and understand quickly)
A10	Ego-management (An exaggerated sense of self-worth based on one's extrinsic achievement)
A11	Career-management (career path and individual development, succession planning)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.26.

Table 4.26: Findings of Expert Consensus on Attributes Competency

ITEM	CONDITION OF DEFUZZIFICATION PROCESS		POSITION	EXPERTS CONSENSUS
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A1	100%	0.756	1	High Consensus
A7	100%	0.756	1	High Consensus
A2	100%	0.733	2	High Consensus
A5	100%	0.733	2	High Consensus
A9	100%	0.733	2	High Consensus
A4	100%	0.711	3	High Consensus
A6	100%	0.711	3	High Consensus
A3	100%	0.667	4	High Consensus
A8	89%	0.667	4	High Consensus
A11	44%	0.622	5	Low Consensus
A10	78%	0.556	6	High Consensus

Examining the outcomes in Table 4.26, one item out of the eleven has been omitted as attributes competency for security activities. Specifically, item A11 (Career-management) has been excluded due to not meeting the 70% expert consensus with a ≤ 0.25 threshold value. It is noteworthy that items A1 (Attention to details) and A7 (Self-management/ independent) hold the leading positions, achieving the highest fuzzy scores.

Analysis of Expert Consensus on skills gap for GROUP 801

In this skills gap construct, the items given to the experts are stated in Table 4.27.

Table 4.27: Items for the Aspect of Skills Gap Construct

ITEMS	
A1	Education or training mismatch
A2	Major changes in traditional training and new skills requirements
A3	Attitude (for example, lack of desire to work)
A4	Misalignment between how job seekers are communicating their skills in their CV
A5	Employers do not clarify the skills they require in the job specifications in the job advertisement

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.28.

Table 4.28: Findings of Expert Consensus on Skills Gap

ITEM	CONDITION OF DEFUZZIFICATION PROCESS		POSITION	EXPERTS CONSENSUS
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A3	100%	0.711	1	High Consensus
A1	89%	0.689	2	High Consensus
A2	89%	0.644	3	High Consensus
A4	67%	0.622	4	Low Consensus
A5	89%	0.533	5	High Consensus

Examining the outcomes in Table 4.28, one item out of the five has been omitted as skills gap for security activities. Specifically, item A4 (Misalignment between how job seekers are communicating their skills in their CV) has been excluded due to not meeting the 70% expert consensus with a ≤ 0.25 threshold value. It is noteworthy that items A3 (Attitude) hold the leading positions, achieving the highest fuzzy scores.

Section 3: Emerging Technical Skills

Analysis of Expert Consensus on Emerging Technical Skills for GROUP 801

In this emerging skills construct, the items given to the experts are stated in Table 4.29.

Table 4.29: Items for the Aspect of Emerging Technical Skills Construct

ITEMS	
A1	Drawing / designing 3D, Designing virtual environments, Applying virtual reality to training and design. Designing simulations, Designing artificial intelligent
A2	Design/Apply Green technology principles
A3	Digital skills
A4	Design/ Utilize software for autonomous technology, machine learning, data automation, and Internet of things (IoT)
A5	Environmental, social and governance (ESG)
A6	Design / Apply Robotics and Electronics

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.30.

Table 4.30: Findings of Expert Consensus on Emerging Technical Skills

ITEM	CONDITION OF DEFUZZIFICATION PROCESS		POSITION	EXPERTS CONSENSUS
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A3	67%	0.622	1	Low Consensus
A5	33%	0.611	2	Low Consensus
A4	44%	0.526	3	Low Consensus
A1	56%	0.522	4	Low Consensus
A6	78%	0.522	4	High Consensus
A2	22%	0.441	5	Low Consensus

Analyzing the results in Table 4.30, five out of the 6 items have been excluded as emerging skills for security activities. The excluded items are A1 (Drawing / designing 3D, Designing virtual environments, Applying virtual reality to training and design. Designing simulations, Designing artificial intelligent), A2 (Design/Apply Green technology principles), A3 (Digital skills), A4 (Design/ Utilize software for autonomous technology, machine learning, data automation, and Internet of things (IoT)) and A5 (Environmental, social and governance (ESG)) due to their failure to achieve a 70% expert consensus on ≤ 0.25 threshold value. Notably, item A3 (Digital skills) holds the top position, attaining the highest fuzzy score. Despite its elevated fuzzy value, this item is dismissed as it falls short of meeting the consensus among experts.

Section 4: Occupation Related to Technology

Analysis of Expert Consensus on occupation related to technology for GROUP 801

In this occupation related to technology construct, the items given to the experts are stated in Table 4.31.

Table 4.31. Items for the Aspect of Occupation Related to Technology Construct

ITEMS	
A1	The Industrial Revolution would have an impact on this industry
A2	Technology advancement directly affects the jobs in the industry
A3	Autonomous Robots (Coordinated and automated actions of robots to complete tasks intelligently, with minimal human input)
A4	Big Data Analytics (The analysis of ever larger volumes of data. Circulation, collection, and analysis of information is a necessity because it supports productivity growth based on a real-time decision-making process)
A5	Cloud Computing (Storing and accessing data and programs over the Internet instead of your computer's hard drive)

ITEMS	
A6	Internet of Things (IoT) (All machines and systems connected to the production plant (as well as other systems) must be able to collect, exchange and save these massive volumes of information, in a completely autonomous way and without the need of human intervention)
A7	Additive Manufacturing (3D Printing) (Use in prototyping, design iteration and small-scale production and often described as "rapid prototyping" - produce the desired components faster, more flexibly and more precisely than ever before)
A8	System Integration (The process of linking together different computing systems and software applications physically or functionally to act as a coordinated whole via Internet of Things-IoT)
A9	Cybersecurity (With the increased connectivity and use of standard communications protocols, the need to protect critical industrial systems and manufacturing lines from cybersecurity threats is increasing)
A10	Augmented Reality (Augmented-reality-based systems support a variety of services, such as selecting parts in a warehouse and sending repair instructions over mobile devices - provide workers with real-time information to improve decision making and work procedures)
A11	Simulation (Simulations will leverage real-time data to mirror the physical world in a virtual model, which can include machines, products, and humans. This allows operators to test and optimize the machine settings for the next product in line in the virtual world before the physical changeover, thereby driving down machine setup times and increasing quality)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.32.

Table 4.32: Findings of Expert Consensus on Occupation Related to Technology

ITEM	CONDITION OF DEFUZZIFICATION PROCESS		POSITION	EXPERTS CONSENSUS
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A1	89%	0.667	1	High Consensus
A2	89%	0.667	1	High Consensus
A4	56%	0.611	2	Low Consensus
A9	56%	0.611	2	Low Consensus
A8	33%	0.567	3	Low Consensus
A6	22%	0.552	4	Low Consensus
A11	78%	0.522	5	High Consensus
A3	100%	0.511	6	High Consensus
A5	67%	0.478	7	Low Consensus
A10	67%	0.411	8	Low Consensus
A7	89%	0.311	9	High Consensus

Analyzing the results in Table 4.32, six out of the 11 items have been excluded as occupation related to technology for security activities. The excluded items are A4 (Big Data Analytics), A5 (Cloud Computing), A6 (Internet of Things), A8 (System Integration), A9 (Cybersecurity) and A10 (Augmented Reality) due to their failure to achieve a 70% expert consensus on ≤ 0.25 threshold value. Notably, item A1 (Industrial Revolution) and A2 (Technology advancement) holds the top position, attaining the highest fuzzy score.

Section 5: Related Issues

Analysis of Expert Consensus on related issues for security services industry.

In these related issues construct, the items given to the experts are stated in Table 4.33.

Table 4.33: Items for the Aspect of Related Issues Construct

ITEMS	
A1	Insufficient number of skilled workers
A2	Insufficient number of certified workers
A3	Insufficient number of competence workers
A4	High dependence on foreign labour
A5	Underpayment of wages leads to high turnover
A6	Talent Gap among graduates
A7	Adaptation to technological changes
A8	Poor facilities and amenities for workers

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.34.

Table 4.34: Findings of Expert Consensus on Related Issues for Security Services Industry

ITEM	**CONDITION OF DEFUZZIFICATION PROCESS**		**POSITION**	**EXPERTS CONSENSUS**
	Percentage of Experts Group Consensus, %	**Fuzzy Score (A)**		
A2	100%	0.711	1	High Consensus
A1	89%	0.689	2	High Consensus
A3	78%	0.667	3	High Consensus
A5	22%	0.633	4	Low Consensus
A6	33%	0.600	5	Low Consensus
A7	11%	0.600	5	Low Consensus
A4	22%	0.585	6	Low Consensus
A8	100%	0.489	7	High Consensus

Analyzing the results in Table 4.34, four out of the eight items have been excluded as Related Issues for Security Services Industry. The excluded items are A4 (High dependence on foreign

labour), A5(Underpayment of wages leads to high turnover), A6 (Talent Gap among graduates), and A7(Adaptation to technological changes) due to their failure to achieve a 70% expert consensus on ≤0.25 threshold value. Notably, item A2 (Insufficient number of certified workers) holds the top position, attaining the highest fuzzy score.

Analysis of Expert Consensus on knowledge competency for GROUP 802

Section 2: Competency in Demand

In this knowledge competency construct, the items given to the experts are stated in Table 4.35.

Table 4.35 Items for the Aspect of Knowledge Competency in Demand Construct

ITEMS	
A1	Security system
A2	Security threats
A3	IT & Networking
A4	Analyse data logs
A5	Planning & Designing
A6	Project Management
A7	Maintenance & Service
A8	Security-conscious culture
A9	security policies.
A10	Security infrastructure
A11	Security controls

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.36.

Table 4.36: Findings of Expert Consensus on Knowledge Competency

Item	**Condition of Defuzzification Process**		**Position**	**Experts Consensus**
	Percentage of Experts Group Consensus, %	**Fuzzy Score (A)**		
A1	100%	0.743	1	High Consensus
A11	100%	0.743	1	High Consensus
A5	86%	0.686	2	High Consensus
A9	100%	0.686	2	High Consensus
A6	100%	0.657	3	High Consensus
A10	86%	0.657	3	High Consensus
A2	57%	0.629	4	Low Consensus
A8	57%	0.629	4	Low Consensus
A3	43%	0.600	5	Low Consensus

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A4	43%	0.600	5	Low Consensus
A7	43%	0.600	5	Low Consensus

Examining the outcomes in Table 4.36, five out of the eleven items have been omitted as knowledge competencies for security system activities. The excluded items are A2 (Security threats), A3 (IT & Networking), A4 (Analyze data logs), A7 (Maintenance & Service), and A8 (Security-conscious culture) due to their inability to secure a 70% expert consensus with a ≤0.25 threshold value. Noteworthy is that items A1 (Security system) and A11 (Security controls) claim the top positions, achieving the highest fuzzy scores.

Analysis of Expert Consensus on skills competency for GROUP 802

In this skills competency construct, the items given to the experts are stated in Table 4.37.

Table 4.37: Items for the Aspect of Skills Competency in Demand Construct

ITEMS	
A1	Interpersonal Communication
A2	Written Communication
A3	Critical Thinking
A4	Problem Solving
A5	Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results)
A6	Leadership
A7	Time management
A8	Aptitude for Technology and Equipment
A9	Intrapreneurship (Refers to employee initiatives in organisations to take something new, without being asked to do so)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.38.

Table 4.38. Findings of Expert Consensus on Skills Competency

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A4	86%	0.714	1	High Consensus
A6	100%	0.686	2	High Consensus
A8	86%	0.686	2	High Consensus
A3	71%	0.657	3	High Consensus
A5	86%	0.657	3	High Consensus
A7	86%	0.657	3	High Consensus
A9	86%	0.657	3	High Consensus
A1	71%	0.600	4	High Consensus
A2	57%	0.571	5	Low Consensus

Reviewing the outcomes in Table 4.38, one out of the nine items has been omitted as a skills competency for security system activities. The excluded item is A2 (Written Communication) due to its inability to secure a 70% expert consensus with a ≤0.25 threshold value. Notably, item A4 (Problem Solving) claims the top position, achieving the highest fuzzy score.

Analysis of Expert Consensus on attributes competency for GROUP 802

In this skills competency construct, the items given to the experts are stated in Table 4.39.

Table 4.39. Items for the Aspect of Attributes Competency in Demand Construct

ITEMS	
A1	Attention to details
A2	Teamwork
A3	Multi-tasking/ Flexibility
A4	Dependability (Trustworthy & Reliable)
A5	Work Ethics
A6	Professionalism
A7	Self-management/ independent
A8	Self-learning
A9	Agility (Ability to think and understand quickly)
A10	Ego-management (An exaggerated sense of self-worth based on one's extrinsic achievement)
A11	Career-management (career path and individual development, succession planning)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.40.

Table 4.40. Findings of Expert Consensus on Attributes Competency

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A4	100%	0.743	1	High Consensus
A5	100%	0.743	1	High Consensus
A2	100%	0.714	2	High Consensus
A3	100%	0.714	2	High Consensus
A6	100%	0.714	2	High Consensus
A9	100%	0.714	2	High Consensus
A1	100%	0.686	3	High Consensus
A7	86%	0.686	3	High Consensus
A8	86%	0.657	4	High Consensus
A11	57%	0.629	5	Low Consensus
A10	86%	0.571	6	High Consensus

Reviewing the outcomes in Table 4.40, one out of the eleven items has been omitted as a attributes competency for security system activities. The excluded item is A11 (Career-management) due to its inability to secure a 70% expert consensus with a ≤0.25 threshold value. Notably, item A4 (Dependability) and A5 (Work Ethics) claims the top position, achieving the highest fuzzy score.

Analysis of Expert Consensus on skills gap for GROUP 802

In this skills gap construct, the items given to the experts are stated in Table 4.41.

Table 4.41: Items for the Aspect of Skills Gap Construct

ITEMS	
A1	Education or training mismatch
A2	Major changes in traditional training and new skills requirements
A3	Attitude (for example, lack of desire to work)
A4	Misalignment between how job seekers are communicating their skills in their CV
A5	Employers do not clarify the skills they require in the job specifications in the job advertisement

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.42.

Table 4.42: Findings of Expert Consensus on Skills Gap

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A3	57%	0.629	1	Low Consensus
A2	57%	0.571	2	Low Consensus
A1	100%	0.514	3	High Consensus
A5	100%	0.514	3	High Consensus
A4	100%	0.486	4	High Consensus

Examining the outcomes in Table 4.42, two out of the five items have been omitted as skills gaps for security system activities. The excluded items are A2 (Major changes in traditional training and new skills requirements) and A3 (Attitude) due to their inability to secure a 70% expert consensus with a ≤0.25 threshold value. Notably, item A3 (Attitude, for example, lack of desire to work) claims the top position, achieving the highest fuzzy score. Despite its elevated fuzzy value, this item is dismissed as it falls short of meeting the consensus among experts.

Section 3: Emerging Skills

Analysis of Expert Consensus on Emerging Technical Skills for GROUP 802

In this emerging skills construct, the items given to the experts are stated in Table 4.43.

Table 4.43: Items for the Aspect of Emerging Skills Construct

ITEMS	
A1	Drawing / designing 3D, Designing virtual environments, Applying virtual reality to training and design. Designing simulations, Designing artificial intelligent
A2	Design/Apply Green technology principles
A3	Digital skills
A4	Design/ Utilize software for autonomous technology, machine learning, data automation, and Internet of things (IoT)
A5	Environmental, social and governance (ESG)
A6	Design / Apply Robotics and Electronics

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.44.

Table 4.44. Findings of Expert Consensus on Emerging Skills

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A3	86%	0.686	1	High Consensus
A4	43%	0.633	2	Low Consensus
A5	71%	0.600	3	High Consensus
A1	43%	0.576	4	Low Consensus
A6	14%	0.576	4	Low Consensus
A2	71%	0.519	5	High Consensus

Examining the outcomes in Table 4.44, three out of the six items have been excluded as emerging skills for security system activities. The excluded items are A1 (Drawing/Designing 3D, Designing virtual environments, Applying virtual reality to training and design, Designing simulations, Designing artificial intelligence), A4 (Design/Utilize software for autonomous technology, machine learning, data automation, and Internet of Things (IoT)), and A6 (Design/Apply Robotics and Electronics) due to their inability to secure a 70% expert consensus with a ≤0.25 threshold value. Notably, item A3 (Digital skills) claims the top position, achieving the highest fuzzy score.

Section 4: Occupation Related to Technology

Analysis of Expert Consensus on occupation related to technology for GROUP 802

In this occupation related to technology construct, the items given to the experts are stated in Table 4.45.

Table 4.45: Items for the Aspect of Occupation Related to Technology Construct

ITEMS	
A1	The Industrial Revolution would have an impact on this industry
A2	Technology advancement directly affects the jobs in the industry
A3	Autonomous Robots (Coordinated and automated actions of robots to complete tasks intelligently, with minimal human input)
A4	Big Data Analytics (The analysis of ever larger volumes of data. Circulation, collection, and analysis of information is a necessity because it supports productivity growth based on a real-time decision-making process)
A5	Cloud Computing (Storing and accessing data and programs over the Internet instead of your computer's hard drive)

ITEMS	
A6	Internet of Things (IoT) (All machines and systems connected to the production plant (as well as other systems) must be able to collect, exchange and save these massive volumes of information, in a completely autonomous way and without the need of human intervention)
A7	Additive Manufacturing (3D Printing) (Use in prototyping, design iteration and small scale production and often described as "rapid prototyping" - produce the desired components faster, more flexibly and more precisely than ever before)
A8	System Integration (The process of linking together different computing systems and software applications physically or functionally to act as a coordinated whole via Internet of Things-IoT)
A9	Cybersecurity (With the increased connectivity and use of standard communications protocols, the need to protect critical industrial systems and manufacturing lines from cybersecurity threats is increasing)
A10	Augmented Reality (Augmented-reality-based systems support a variety of services, such as selecting parts in a warehouse and sending repair instructions over mobile devices - provide workers with real-time information to improve decision making and work procedures)
A11	Simulation (Simulations will leverage real-time data to mirror the physical world in a virtual model, which can include machines, products, and humans. This allows operators to test and optimize the machine settings for the next product in line in the virtual world before the physical changeover, thereby driving down machine setup times and increasing quality)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.46.

Table 4.46. Findings of Expert Consensus on Occupation Related to Technology

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A1	100%	0.743	1	High Consensus
A2	100%	0.743	1	High Consensus
A9	100%	0.743	1	High Consensus
A8	100%	0.686	2	High Consensus
A4	71%	0.657	3	High Consensus
A5	71%	0.657	3	High Consensus
A6	71%	0.657	3	High Consensus
A3	43%	0.600	4	Low Consensus
A11	43%	0.600	4	Low Consensus
A10	86%	0.543	5	High Consensus
A7	57%	0.519	6	Low Consensus

Examining the outcomes in Table 4.46, three out of the eleven items have been omitted as occupations related to technology for security activities. The excluded items are A3 (Autonomous Robots), A7 (Additive Manufacturing), and A11 (unspecified) due to their inability to secure a 70% expert consensus with a ≤0.25 threshold value. Notably, items A1 (The Industrial Revolution would have an impact on this industry), A2 (Technology advancement directly affects the jobs in the industry), and A9 (Cybersecurity) claim the top positions, achieving the highest fuzzy scores.

Section 5: Related Issues

Analysis of Expert Consensus on related issues for security system services industry.

In these related issues construct, the items given to the experts are stated in Table 4.47.

Table 4.47. Items for the Aspect of Related Issues Construct

ITEMS	
A1	Insufficient number of skilled workers
A2	Insufficient number of certified workers
A3	Insufficient number of competence workers
A4	High dependence on foreign labour
A5	Underpayment of wages leads to high turnover
A6	Talent Gap among graduates
A7	Adaptation to technological changes
A8	Poor facilities and amenities for workers

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.48.

Table 4.48: Findings of Expert Consensus on Related Issues for Security System Services Industry

Item	**Condition of Defuzzification Process**		**Position**	**Experts Consensus**
	Percentage of Experts Group Consensus, %	**Fuzzy Score (A)**		
A3	86%	0.686	1	High Consensus
A2	57%	0.629	2	Low Consensus
A1	14%	0.600	3	Low Consensus
A7	43%	0.600	3	Low Consensus
A5	57%	0.571	4	Low Consensus

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A6	57%	0.571	4	Low Consensus
A4	43%	0.467	5	Low Consensus
A8	71%	0.462	6	High Consensus

Analyzing the results in Table 4.48, six out of the eight items have been excluded as related issues in security system services. The excluded items are A1 (Insufficient number of skilled workers), A2 (Insufficient number of certified workers), A4 (High dependence on foreign labour), A5(Underpayment of wages leads to high turnover), A6 (Talent Gap among graduates) and A7 (Adaptation to technological changes) due to their failure to achieve a 70% expert consensus on ≤0.25 threshold value. Notably, item A3 holds the top position, attaining the highest fuzzy score.

Analysis of Expert Consensus on knowledge competency for GROUP 803

Section 2: Competency in Demand

In this knowledge competency construct, the items given to the experts are stated in Table 4.49.

Table 4.49: Items for the Aspect of Knowledge Competency in Demand Construct

ITEMS	
A1	Monitoring and analyzing activities
A2	Surveillance operative
A3	Data collection and analysis
A4	Maintaining detailed records
A5	Research and analyze data patterns
A6	Evidence gathering
A7	Legal and ethical standards
A8	Investigative protocols
A9	Cost and profitability
A10	Risk Assessment and Mitigation

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.50.

Table 4.50: Findings of Expert Consensus on Knowledge Competency

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A10	100%	0.743	1	High Consensus
A3	86%	0.686	2	High Consensus
A4	86%	0.686	2	High Consensus
A5	86%	0.686	2	High Consensus
A6	86%	0.686	2	High Consensus
A7	86%	0.686	2	High Consensus
A8	86%	0.686	2	High Consensus
A9	86%	0.686	2	High Consensus
A1	86%	0.657	3	High Consensus
A2	57%	0.629	4	Low Consensus

Analyzing the results in Table 4.41, one out of the 11 items have been excluded as knowledge competencies for investigation activities. The excluded items are A2 (Surveillance operative) due to their failure to achieve a 70% expert consensus. Notably, item A10 (Risk Assessment and Mitigation) holds the top position, attaining the highest fuzzy score.

Analysis of Expert Consensus on skills competency for GROUP 803

In this skills competency construct, the items given to the experts are stated in Table 4.51.

Table 4.51: Items for the Aspect of Skills Competency in Demand Construct

ITEMS	
A1	Interpersonal Communication
A2	Written Communication
A3	Critical Thinking
A4	Problem Solving
A5	Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results)
A6	Leadership
A7	Time management

ITEMS	
A8	Aptitude for Technology and Equipment
A9	Intrapreneurship (Refers to employee initiatives in organisations to take something new, without being asked to do so)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.52.

Table 4.52: Findings of Expert Consensus on Skills Competency

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A6	29%	0.743	1	Low Consensus
A5	29%	0.714	2	Low Consensus
A8	100%	0.686	3	High Consensus
A9	43%	0.686	3	Low Consensus
A1	86%	0.657	4	High Consensus
A7	100%	0.657	4	High Consensus
A2	71%	0.629	5	High Consensus
A3	86%	0.629	5	High Consensus
A4	86%	0.571	6	High Consensus

Analyzing the results in Table 4.52, three out of the 9 items have been excluded as skills competencies for investigation activities. The excluded items are A5 (Agile Mindset), A6 (Leadership), and A9 (Intrapreneurship) due to their failure to achieve a 70% expert consensus. Notably, item A6 (Leadership) holds the top position, attaining the highest fuzzy score.

Analysis of Expert Consensus on attributes competency for GROUP 803

In this skills competency construct, the items given to the experts are stated in Table 4.53.

Table 4.53: Items for the Aspect of Attributes Competency in Demand Construct

ITEMS	
A1	Attention to details
A2	Team work
A3	Multi-tasking/ Flexibility
A4	Dependability (Trustworthy & Reliable)
A5	Work Ethics

ITEMS	
A6	Professionalism
A7	Self-management/ independent
A8	Self-learning
A9	Agility (Ability to think and understand quickly)
A10	Ego-management (An exaggerated sense of self-worth based on one's extrinsic achievement)
A11	Career-management (career path and individual development, succession planning)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.54.

Table 4.54: Findings of Expert Consensus on Attributes Competency

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A1	86%	0.771	1	High Consensus
A5	86%	0.771	1	High Consensus
A6	86%	0.771	1	High Consensus
A2	100%	0.743	2	High Consensus
A4	100%	0.743	2	High Consensus
A3	86%	0.714	3	High Consensus
A7	86%	0.714	3	High Consensus
A9	86%	0.714	3	High Consensus
A8	86%	0.657	4	High Consensus
A11	57%	0.629	5	Low Consensus
A10	57%	0.548	6	Low Consensus

Analyzing the results in Table 4.54, two out of the 11 items have been excluded as attributes competencies for security system activities. The excluded items are A10 (Ego-management) and A11 (Career-management) due to their failure to achieve a 70% expert consensus. Notably, item A4 (Dependability), A5 (Work Ethics) and A6 (Professionalism) holds the top position, attaining the highest fuzzy score.

Analysis of Expert Consensus on skills gap for GROUP 803

In this skills gap construct, the items given to the experts are stated in Table 4.55.

Table 4.55: Items for the Aspect of Skills Gap Construct

ITEMS	
A1	Education or training mismatch
A2	Major changes in traditional training and new skills requirements
A3	Attitude (for example, lack of desire to work)
A4	Misalignment between how job seekers are communicating their skills in their CV
A5	Employers do not clarify the skills they require in the job specifications in the job advertisement

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.56.

Table 4.56: Findings of Expert Consensus on Skills Gap

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A2	43%	0.600	1	Low Consensus
A3	43%	0.600	1	Low Consensus
A1	57%	0.571	2	Low Consensus
A4	86%	0.543	3	High Consensus
A5	86%	0.519	4	High Consensus

Analyzing the results in Table 4.56, three out of the 5 items have been excluded as skills gap for investigation activities. The excluded items are A1(Education or training mismatch), A2 (Major changes in traditional training and new skills requirements), and A3 (Attitude) due to their failure to achieve a 70% expert consensus. Notably, item A2 and A3 holds the top position, attaining the highest fuzzy score. Despite its elevated fuzzy value, this item is dismissed as it falls short of meeting the consensus among experts.

Section 3: Emerging Skills

Analysis of Expert Consensus on Emerging Skills for GROUP 803

In this emerging skills construct, the items given to the experts are stated in Table 4.57.

Table 4.57: Items for the Aspect of Emerging Skills Construct

ITEMS	
A1	Drawing / designing 3D, Designing virtual environments, Applying virtual reality to training and design. Designing simulations, Designing artificial intelligent
A2	Design/Apply Green technology principles
A3	Digital skills
A4	Design/ Utilize software for autonomous technology, machine learning, data automation, and Internet of things (IoT)
A5	Environmental, social and governance (ESG)
A6	Design / Apply Robotics and Electronics

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.58.

Table 4.58: Findings of Expert Consensus on Emerging Skills

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A3	86%	0.629	1	High Consensus
A4	71%	0.529	1	High Consensus
A5	57%	0.629	1	Low Consensus
A6	57%	0.448	2	Low Consensus
A1	43%	0.419	3	Low Consensus
A2	43%	0.400	4	Low Consensus

Analyzing the results in Table 4.58, four out of the 6 items have been excluded as emerging skills for investigation activities. The excluded items are A1 (Drawing / designing 3D, Designing virtual environments, Applying virtual reality to training and design. Designing simulations, Designing artificial intelligent), A2 (Design/Apply Green technology principles), A5 (Environmental, social & governance (ESG)) and A6 (Design / Apply Robotics and Electronics) due to their failure to achieve a 70% expert consensus. Notably, item A3, A4 and A5 holds the top position, attaining the highest fuzzy score.

Section 4: Occupation Related to Technology

Analysis of Expert Consensus on occupation related to technology for GROUP 803

In this occupation related to technology construct, the items given to the experts are stated in Table 4.59.

Table 4.59: Items for the Aspect of Occupation Related to Technology Construct

ITEMS	
A1	The Industrial Revolution would have an impact on this industry
A2	Technology advancement directly affects the jobs in the industry
A3	Autonomous Robots (Coordinated and automated actions of robots to complete tasks intelligently, with minimal human input)
A4	Big Data Analytics (The analysis of ever larger volumes of data. Circulation, collection, and analysis of information is a necessity because it supports productivity growth based on a real-time decision-making process)
A5	Cloud Computing (Storing and accessing data and programs over the Internet instead of your computer's hard drive)
A6	Internet of Things (IoT) (All machines and systems connected to the production plant (as well as other systems) must be able to collect, exchange and save these massive volumes of information, in a completely autonomous way and without the need of human intervention)
A7	Additive Manufacturing (3D Printing) (Use in prototyping, design iteration and small scale production and often described as "rapid prototyping" - produce the desired components faster, more flexibly and more precisely than ever before)
A8	System Integration (The process of linking together different computing systems and software applications physically or functionally to act as a coordinated whole via Internet of Things-IoT)
A9	Cybersecurity (With the increased connectivity and use of standard communications protocols, the need to protect critical industrial systems and manufacturing lines from cybersecurity threats is increasing)
A10	Augmented Reality (Augmented-reality-based systems support a variety of services, such as selecting parts in a warehouse and sending repair instructions over mobile devices - provide workers with real-time information to improve decision making and work procedures)
A11	Simulation (Simulations will leverage real-time data to mirror the physical world in a virtual model, which can include machines, products, and humans. This allows operators to test and optimize the machine settings for the next product in line in the virtual world before the physical changeover, thereby driving down machine setup times and increasing quality)

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.60.

Table 4.60: Findings of Expert Consensus on Occupation Related to Technology

Item	**Condition of Defuzzification Process**		**Position**	**Experts Consensus**
	Percentage of Experts Group Consensus, %	**Fuzzy Score (A)**		
A9	86%	0.643	1	High Consensus
A1	86%	0.629	2	High Consensus
A2	57%	0.629	2	Low Consensus

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A8	57%	0.557	3	Low Consensus
A6	86%	0.543	4	High Consensus
A5	71%	0.500	5	High Consensus
A4	71%	0.471	6	High Consensus
A11	71%	0.471	6	High Consensus
A10	71%	0.443	7	High Consensus
A7	71%	0.386	8	High Consensus
A3	57%	0.343	9	Low Consensus

Analyzing the results in Table 4.60, three out of the 11 items have been excluded as occupation related to technology for security activities. The excluded items are A2 (Technology advancement directly affects the jobs in the industry), A3 (Autonomous Robots), and A8 (System Integration) due to their failure to achieve a 70% expert consensus. Notably, item A9 holds the top position, attaining the highest fuzzy score.

Section 5: Related Issues

Analysis of Expert Consensus on related issues for investigation activities industry.

In these related issues construct, the items given to the experts are stated in Table 4.61.

Table 4.61: Items for the Aspect of Related Issues Construct

ITEMS	
A1	Insufficient number of skilled workers
A2	Insufficient number of certified workers
A3	Insufficient number of competence workers
A4	High dependence on foreign labour
A5	Underpayment of wages leads to high turnover
A6	Talent Gap among graduates
A7	Adaptation to technological changes
A8	Poor facilities and amenities for workers

The expert consensus percentage, defuzzification and item position for the above items are shown in Table 4.62.

Table 4.62: Findings of Expert Consensus on Related Issues for Investigation Activities Industry

Item	Condition of Defuzzification Process		Position	Experts Consensus
	Percentage of Experts Group Consensus, %	Fuzzy Score (A)		
A6	43%	0.600	1	Low Consensus
A1	43%	0.576	2	Low Consensus
A2	43%	0.576	2	Low Consensus
A3	43%	0.576	2	Low Consensus
A5	57%	0.571	3	Low Consensus
A7	86%	0.543	4	High Consensus
A4	57%	0.529	5	Low Consensus
A8	100%	0.486	6	High Consensus

Analyzing the results in Table 4.62, six out of the 8 items have been excluded as related issues in investigation activities. The excluded items are A1 (Insufficient number of skilled workers), A2 (Insufficient number of certified workers), A3 (Insufficient number of competence workers), A4 (High dependence on foreign labour), A5(Underpayment of wages leads to high turnover), and A6 (Talent Gap among graduates) due to their failure to achieve a 70% expert consensus. Notably, item A6 holds the top position, attaining the highest fuzzy score.

4.8 Validate the Security and Investigation Activities Industries in Malaysia

Objective 3: To validate the security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0.

Table 4.63: The security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0 in N801

SECTION	**N (Administrative Activities and Support Services)**							
DIVISION	**80 Security and Investigation Activities**							
GROUP	**801 (Private Security Activities)**							
AREA **LEVEL**	**Guarding Services (GS)**	**Armed Guarding (AG)**	**Close Protection (CP)**	**Cash Management (CM)**	**K9 Service (K9)**	**Alarm Monitoring (AM)**	**Maritime Security**	**Aviation Security (Avsec) (Operation, Intelligent and investigation)**
LEVEL 8	NJT	NJT	NJT	NJT	NJT	NJT	NJT	NJT
LEVEL 7	NJT	NJT	NJT	NJT	NJT	NJT	NJT	Avsec Senior
LEVEL 6	NJT	NJT	NJT	NJT	NJT	NJT	NJT	Avsec Specialist
LEVEL 5	GS Security Manager *Security Operation Management (DS-010-5:2013)*	NJT	CP Manager	NJT	NJT	NJT	Maritime Operation Manager	Avsec Senior Executive
LEVEL 4	GS Security Executive *Security Operation Management (DS-010-4:2013)*	NJT	CP Executive *Social Security Administration (NCS-012:2020)*	NJT	NJT	NJT	Maritime Control Centre Supervisor	Avsec Executive
LEVEL 3	GS Security supervisor Security *Services Supervision (DS-010-3:2013)*	AG Supervisor	CP Senior Bodyguard	CM Supervisor	NJT	AM Supervisor	Maritime Team Leader	Avsec Senior Officer

SECTION	**N (Administrative Activities and Support Services)**							
DIVISION	**80 Security and Investigation Activities**							
GROUP	**801 (Private Security Activities)**							
LEVEL 2	GS Security officer *Security Services Operation (DS-010-2:2013)*	AG Security Officer	CP Bodyguard	CM Security Officer	K9 Security Officer *Dog Unit Security Supervisor (K9) (SS-030-3)*	AM Security Officer	Maritime Unit Leader *Seaport Security Management (DS-012-5:2015)*	Avsec Officer
LEVEL 1	GS Assistant Security Officer *Security Assistant (SS-010-1)*	NJT	NJT	CM Assistant Security Officer	NJT	NJT	Maritime Ship Security Officer / Maritime Operating Room Officer *Seaport Security Surveillance (DS-012-3:2015) Seaport Security Control (DS-012-4:2015)*	Avsec Assistant

Table 4.64: The security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0 in N802

SECTION	**N (Administrative Activities and Support Services)**		
DIVISION	**80 Security and Investigation Activities**		
GROUP	**802 (Security Systems Service Activities)**		
AREA LEVEL	**Security System Surveillance Operator**	**Security System Analyst**	**Security System Technologist**
LEVEL 8	NJT	NJT	Chief Technical Officer
LEVEL 7	NJT	Specialist/ Senior Security Solutions/ Senior Manager	Specialist Technical Deployment *ICT System Security Technologist (IT-090-5)* *Telecommunications System and Network Security Technical Operation Management (J619-002-5:2021)*
LEVEL 6	NJT	Manager / Security Solutions	Head Technical Operation Executives *Telecommunications System and Network Security Technical Operation (J619-002-4:2021)*
LEVEL 5	Assistant Manager/ Supervisor	Senior Analyst	Senior Technical Executives *Security Senior Technician (Design) (EE-110-3)* *Cyber Security Penetration Testing & Assessment (J620-001-5:2019)*
LEVEL 4	Senior Executives	Analyst	Technical Executives *Electronic Security System Installation & Maintenance (DS-050-3:2013)*
LEVEL 3	Executives	NJT	System Admin
LEVEL 2	Senior Operator	NJT	NJT
LEVEL 1	Operator	NJT	NJT

Table 4.65: The security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0 in N803.

SECTION	**N (Administrative Activities and Support Services)**
DIVISION	**80 Security and Investigation Activities**
GROUP	**803 (Investigation Activities)**
AREA	**Surveillance Investigation**
LEVEL	
LEVEL 8	NJT
LEVEL 7	Investigation Technical Team Leader
LEVEL 6	Investigation Team Leader
LEVEL 5	Investigation Senior Analyst
LEVEL 4	Investigation Junior Analyst
LEVEL 3	Investigation Senior Operative *Investigation Detectives (SS-060-3)*
LEVEL 2	Investigation Junior Operative *Investigation Detectives (SS-060-3)*
LEVEL 1	NJT

All job categories within the Guarding services domain have been included in the existing NOSS. These encompass positions such as GS Security Manager, GS Security Executive, GS Security Supervisor, GS Security Officer, and GS Assistant Security Officer. However, certain roles remain absent from the current MOSQF, notably in areas like AG, where positions such as AG Supervisor and AG Security Officer are not covered. Similarly, within CP, only the CP Executive is addressed in the current MOSQF, leaving out roles like CP Manager, CP Senior Bodyguard, and CP Bodyguard. The CM) sector lacks coverage for positions like CM Supervisor, CM Security Officer, and CM Assistant Security Officer within the current MOSQF. Additionally, roles in K9 beyond K9 Security, AM roles such as AM Supervisor and AM Security Officer, as well as various roles in Maritime Security like Maritime Operation Manager, Maritime Control Centre Supervisor, and Maritime Team Leader, remain unaddressed. Lastly, within AVSEC, roles including Avsec Senior, Avsec Specialist, Avsec Senior Executive, Avsec Executive, Avsec Senior Officer, Avsec Officer, and Avsec Assistant across Operation, Intelligence, and Investigation sectors are not covered by the current MOSQF.

The existing MOSQF do not encompass all job categories within the domains of Security System Surveillance Operator and Security System Analyst. Security System Surveillance Operator roles such as Assistant Manager/Supervisor, Senior Executives, Executives, and Senior Operators, along with Security System Analyst positions involving

Specialists/Senior Security Solutions/Senior Managers, Managers/Security Solutions, Senior Analysts, and Analysts, remain outside the scope of the current MOSQF. However, several job categories within Security System Technologist are covered by the current MOSQF, including Specialist Technical Deployment, Head Technical Operation Executives, Senior Technical Executives, and Technical Executives. Nevertheless, roles like Chief Technical Officer and System Admin are not addressed within the existing MOSQF.

The present MOSQF cover merely two job categories within Surveillance Investigation. These include the roles of Investigation Senior Operative and Investigation Junior Operative. However, crucial positions such as Investigation Technical Team Leader, Investigation Team Leader, Investigation Senior Analyst, and Investigation Junior Analyst have not been incorporated into the existing standards.

CHAPTER V

DICUSSION AND CONCLUSION

5.1 Introduction

Chapter 5 represents the apex of this extensive inquiry, functioning as a consolidated repository of crucial insights gleaned from a meticulous and comprehensive examination carried out throughout this study. The study's summation provides a comprehensive overview, distilling the essence of the employed research methodologies, the overarching objectives pursued, and the pivotal constituents that shaped the investigation. This segment delves deeply into the discussion of findings, meticulously analyzing intricate details and discernible patterns extrapolated from the demographic profiles and exhaustive expert analyses encompassing diverse sectors such as Private Security Activities, Security Systems Service Activities, and Investigation Activities. These analyses aim to furnish a nuanced comprehension of the intricacies characterizing each domain, shedding light on their interrelationships within the broader industry landscape. The implications derived from these findings serve as guiding principles for potential industry advancements, regulatory refinements, and essential skill development initiatives necessary for fortifying the industry's resilience and adaptability in dynamic environments. Moreover, this chapter emphasizes the substantive contributions of the study in shedding light on previously unexplored facets, thereby fostering a more comprehensive understanding of industry dynamics, and subsequently laying the groundwork for future research pursuits. Ultimately, this chapter culminates by delineating valuable recommendations and avenues for prospective studies, advocating for sustained exploration into emergent trends, technological integrations, interdisciplinary collaborations, and the evolution of industry standards to facilitate the sustainable progression of security and investigation activities.

5.2 Summary of the Study

The investigation embarked on a comprehensive journey to unravel the intricate landscape of security and investigation activities in Malaysia, aiming to discern the evolving needs, job classifications, and inherent responsibilities within this dynamic industry. Commencing with a meticulous literature review, the study meticulously navigated through existing scholarly works, establishing a robust foundation steeped in the theoretical underpinnings and prior research associated with this field. This initial phase was instrumental in contextualizing the

subsequent research, providing insights into the prevailing discourse, gaps in knowledge, and guiding principles that underpin the realm of security and investigation activities.

Subsequently, employing a judicious mixed-methods approach, the study engaged in qualitative interviews and quantitative surveys conducted among seven experts in three distinct categories: Private Security Activities, Security Systems Service Activities, and Investigation Activities. This methodological approach was strategic in gathering rich qualitative insights while complementing them with quantitative data, fostering a comprehensive understanding of the nuances within each sector. The demographic profiles meticulously crafted for these experts aimed at ensuring a balanced and representative pool, capturing diverse expertise, experiences, and perspectives inherent in the multifaceted industry landscape.

Moreover, the study's exhaustive documentation and classification of job titles and classifications meticulously aligned with the National Occupational Skills Standard (NOSS) within the N80 sector. This meticulous effort extended to meticulously delineating the corresponding responsibilities and job descriptions affiliated with each identified job title, presenting an intricate tapestry of roles entrenched within the industry. Additionally, a critical analysis scrutinized the competencies requisite to address the industry's demands and supply dynamics, validating the security and investigation activities industries in Malaysia based on MSIC 2008 version 1.0. This multifaceted exploration aimed to validate and fortify the industry's foundational elements, paving the way for a more comprehensive comprehension of its intricacies and needs for future growth and development.

5.3 The Finding Discussion

The OF development in this study involved the exploration of needs within the N80 sector which align with the NOSS. These included Private Security Activities, Security Systems Service Activities, and Investigation Activities.

5.3.1 The Needs of the Current and Future Needs of the Industry Based on Previous Studies

Previous studies analyzing Security and Investigation Activities across the varied landscapes of Malaysia, US, UK, Indonesia, Singapore, China, Qatar, and Australia have spotlighted the critical role of eight distinct aspects in shaping national security measures. These aspects encompass Law Enforcement Agencies, Immigration and Border Control, Intelligence and Surveillance, Forensic Investigation, Counterterrorism, Cybersecurity, Private Security Companies, and Anti-Corruption Effort/Police Force. Notably, the comparative analysis

underscores Counterterrorism, Immigration and Border Control, and Private Security Companies as the three universal aspects accessible and integral across all eight countries. These aspects serve as foundational pillars in addressing immediate threats, controlling borders, and ensuring robust security mechanisms within the respective nations.

However, the disparities in the adoption and emphasis on the remaining aspects among the countries highlight the diverse regulatory environments and priorities embedded in each nation's security framework. Intelligence and Surveillance methodologies vary significantly due to distinct security threats, cultural contexts, and available resources within each country. Moreover, the focus on Forensic Investigation, Cybersecurity, and Anti-Corruption Efforts/Police Force reflects divergent priorities based on the unique challenges and strategic imperatives prevalent within each nation. Some countries might prioritize bolstering forensic investigative capabilities, while others may channel more resources into fortifying cybersecurity infrastructure or strengthening anti-corruption measures within law enforcement agencies, thereby shaping their individual approaches to security and investigation activities.

These findings underscore the nuanced nature of security strategies, where universality in certain aspects coexists with diversity and divergence in others, shaped by geopolitical, regulatory, and societal contexts. While three aspects serve as common denominators essential for all countries in addressing immediate security concerns, the divergent focus on the other aspects emphasizes the need for tailored and adaptive security measures that respond to the unique challenges faced by each nation, ultimately contributing to more effective and resilient national security frameworks.

5.3.2 Private Security Activities

In Private Security Activities, there are eight job areas namely Guarding Services/Security Operation Services, Guarding, Close Protection, Cash Management/Cash in Transit/Value in Transit, K9 Service, Alarm Monitoring, Maritime Security, and Aviation Security. Each area has different levels of job scope according to the needs. As an example, the area of guarding services required five levels of job scope namely security manager (level 5), security executive (level 4), security supervisor (level 3), security officer (level 2) and assistance security officer (level 1). The decision to determine the job scope in each area and level were based on the experts' suggestions according to the industry's need and the level of difficulties to operate the job area. The critical and demand job area required more job scope and all the scope in each level plays a significant role and correlates to each other's need.

All the job scope were divided accordingly into 4 categories which are critical job/high demands (*), jobs relevant to technology and industrial revolution (**), critical jobs and jobs relevant to technology and industrial revolution (***) and not applicable (no *). Based on the eight job areas in private security services, nine job scopes were categorized under critical job/high demands, three job scopes were categorized under jobs relevant to technology and industrial revolution, six job scopes categorized under jobs relevant to technology and industrial revolution and the rest of job scopes are not applicable under any categories. A critical job/high demands category requires vital professions essential for an organization. These are roles that, if left unfilled or not performed effectively, could have significant consequences. Meanwhile, jobs relevant to technology and the industrial revolution encompass employment opportunities closely tied to technological advancements and the ongoing industrial transformation. These roles contribute to innovative technologies, marking a key aspect of the Fourth Industrial Revolution, characterized by the integration of digital technologies, automation, and data-driven processes across sectors. Additionally, critical jobs and jobs relevant to technology and industrial revolution are those deemed essential for the overall well-being of an entity, and jobs relevant to technology and the industrial revolution are positions closely tied to advancements in technology and the ongoing transformation of industries. There can be an overlap when critical roles are also technologically driven, such as positions in emergency services that utilize advanced technologies.

Data gathered from Fuzzy Delphi technique presented the competency required to meet the industry demand and supply in Malaysia. The selection of this technique was to obtain expert consensus on the elements used in designing occupational framework. There are nine experts in the field of security activities with more than 11 years working experience who were involved in answering the survey questions. The competency in demand section was divided into several aspects include (1) Knowledge, (2) Skills, (3) Attributes, and (4) Skills Gap. This is followed by the Emerging skills and Occupation Related to Technology.

Results presented all thirteen items resulted high consensus as knowledge competencies for security activities as all the expert's consensus rate exceeds 70%. Notably, security surveillance holds the top position compared to other items. This indicates that security surveillance plays a crucial role in maintaining the safety and security of individuals, assets, and facilities by providing real-time monitoring and the ability to respond proactively to security threats.

In terms of skills competency, all the items resulted high consensus except for one item which is Intrapreneurship skill competency due to not meeting the 70% expert consensus. It is

remarkable that skill of critical thinking, problem solving, and leadership hold the top ranks, achieving the highest fuzzy scores. The insignificance of intrapreneurship skill reflects an unimportant ability of individuals within an organization to exhibit entrepreneurial traits and behaviors while working within the confines of a corporate environment. Meanwhile, the significance of critical thinking, problem solving, and leadership skills play a vital role in progressive organization. Critical thinking is essential in various aspects of life, including education, professional settings, decision-making, and problem-solving. It allows individuals to approach challenges with a thoughtful and analytical mindset, fostering a deeper understanding of issues and improving the quality of decision-making. The process of finding solutions to difficult or complex issues reflects the ability in problem solving skill. Each individual under this job scope should be capable in analyzing a situation, identifying the problem, and devising a strategy to address and overcome the challenge effectively. In aspect of leadership skill, they also should be able to guide, influence, and inspire others to achieve a common goal or vision. It involves taking charge, making decisions, and providing direction in a way that motivates and empowers individuals or a group to work together effectively. Leadership is not solely about holding a formal position of authority; it can manifest at various levels within an organization or community.

There are eleven questions asked for attributes competency. One item out of the nine, which is Career-management skill resulted in low consensus as attributes competency for security activities. The rest of the items are accepted. It is noteworthy that Attention to details and Self-management/ independent hold the heading positions, achieving the highest fuzzy scores. The elimination of career-management skills yields the less crucial in a competitive job market, even though individuals may experience multiple career transitions throughout their professional lives. In other words, everyone should take a proactive approach to navigating their own career journey, making informed decisions, and taking intentional steps to enhance career satisfaction and success. The significant of Attention to details and Self-management reinforce the unimportance of career management. Attention to detail is a valuable skill in various professions, including those that require accuracy, precision, and a low margin for error. Individuals with a high level of attention to detail are often sought, where accuracy are critical for success. In addition, self-management is a crucial aspect of personal development and is highly valued in various aspects of life, including education, career, relationships, and overall mental health. Individuals with strong self-management skills are often better equipped to navigate the complexities of modern life, set and achieve meaningful goals, and maintain a positive and productive mindset in the face of challenges.

In assessing the skills gap, one item focused on misalignment between how job seekers are communicating their skills in their Curriculum Vitae (CV) was excluded due to not meeting the 70% expert consensus and Attitude hold the important positions achieving the highest fuzzy scores. Data indicated that a discrepancy or mismatch in how individuals are presenting their skills and qualifications on their CV compared to what employers are seeking or expecting is unimportant. In other words, each individual probably is knowledgeable in conveying their abilities and what employers are looking for in a candidate through CV. In various contexts, including the workplace, a person's attitude can have a profound impact on their success, satisfaction, and well-being. Attitudes can be positive, negative, or neutral, and they play a significant role in shaping behavior, decision-making, and interpersonal relationships. Attitudes can be influenced by personal experiences, cultural background, upbringing, education, and external influences. Cultivating a positive and adaptive attitude is often considered beneficial for personal growth and resilience in the face of challenges.

Emerging skills in Private Security Activities require a question in term of drawing, designing, applying green technologies, digital skills including software, robotics and electronics. Five out of the 6 items were resulted as low consensus as emerging skills for security activities. The only high consensus item is Design/Apply Robotics and Electronic skills. This finding reflects the importance of individual ability to create, develop, and implement solutions related to robotics and electronic systems. This competency involves both the conceptualization and practical application of skills in these domains. The key components in these skills are design, application, robotic skills and electronic skills. In other words, Design/Apply Robotics and Electronic Skills suggests proficiency in both the conceptualization (design) and practical implementation (apply) of solutions involving robotics and electronic systems. Individuals with this skill set are capable of creating innovative designs, developing detailed plans, and successfully implementing and maintaining electronic and robotic technologies. This skill set is valuable in various industries, including manufacturing, automation, artificial intelligence, and emerging technologies.

Analysis of occupation related to technology is important to understand the connection and relevant of each skill related to advanced technologies including Autonomous Robot, Cloud Computing, Cybersecurity, Augmented Reality and etc. Finding presented six out of eleven items resulted as low consensus related to technology for security activities. The low consensus items are (1) Big Data Analytics, (2) Cloud Computing), (3) Internet of Things, (4) System Integration, (5) Cybersecurity and (6) Augmented Reality due to their failure to achieve

a 70% expert consensus. Notably, Industrial Revolution and Technology advancement holds the top position, attaining the highest fuzzy score. These findings indicate the importance of Industrial Revolution and Technology advancement compared to others related technologies. The Industrial Revolution was characterized by the widespread adoption of machinery, the growth of factories, and advancements in manufacturing processes. It played a pivotal role in shaping the modern industrialized world and had far-reaching impacts on economies, societies, and daily life. Technology advancement reflects continuous progress, improvement, and innovation in the development and application of various technologies. It signifies the evolution of tools, systems, methods, and devices that contribute to increased efficiency, functionality, and capabilities in diverse fields. Technological advancement often involves the refinement of existing technologies and the creation of new solutions to address challenges and improve various aspects of human life. As technology continues to advance, it shapes the way people live, work, and interact with the world, leading to constant changes and opportunities for progress.

Analysis of expert consensus on related issue in security services industry highlighted four high consensus items (insufficient number of skilled workers, insufficient number of certified workers, insufficient number of competence workers and poor facilities & amenities for workers) and four low consensus items (High dependence on foreign labour, Underpayment of wages leads to high turnover, Talent gap among graduates and Adaptation to technological changes)

5.3.3 Security Systems Service Activities

There are three job areas in security system security activities (N802), namely Security System Surveillance Operator, Security System Analyst and Security System Technologist. Each area has different levels of job scope according to the needs. Security System Surveillance Operator required five levels of job scope, Security System Analyst required four levels of job scope and Security System Technologist required six levels of job scope. The determination of job scope for each area and level was made in accordance with experts' recommendations, considering the industry's requirements and the operational challenges associated with each job area. Job areas with critical demand necessitated a broader scope, and the scope at each level is pivotal, as it aligns with the needs of other levels.

All the job scopes were divided accordingly into 4 categories which are critical job/high demands (*), jobs relevant to technology and industrial revolution (**), critical jobs and jobs relevant to technology and industrial revolution (***) and not applicable (no *). Based on the

three job areas in security system service activities, no job scopes were categorized under critical job/high demands, six job scopes were categorized under jobs relevant to technology and industrial revolution, seven job scopes categorized under jobs relevant to technology and industrial revolution and the rest of job scopes are not applicable under any categories. This security system service activity does not require a critical job/high demands category. This implies that certain roles, if left vacant or not executed optimally, may not result in significant consequences. In contrast, positions related to technology and the industrial revolution offer employment prospects intricately linked to technological progress and the ongoing transformation of industries. These roles contribute to innovative technologies, playing a crucial role in the Fourth Industrial Revolution characterized by the integration of digital technologies, automation, and data-driven processes across various sectors. It's important to note that critical jobs, as well as those pertinent to technology and the industrial revolution, are essential for the overall well-being of an entity. Positions in technology and the industrial revolution are closely associated with technological advancements and the ongoing industry transformation. There can be an intersection when critical roles are also technologically driven, such as positions in emergency services that leverage advanced technologies.

Data obtained through the Fuzzy Delphi technique has outlined the competencies necessary to address the industry's demand and supply in Malaysia. The rationale behind employing this technique was to garner expert consensus regarding the elements integral to shaping the occupational framework. Seven experts specializing in security system activities, each possessing over 11 years of work experience, participated in responding to the survey questions. The competency in demand section was categorized into four aspects, namely (1) Knowledge, (2) Skills, (3) Attributes, and (4) Skills Gap. Subsequently, the discussion delves into Emerging Skills, Occupations Related to Technology, and Jobs in Demand.

Results presented five out of the eleven items resulted as low consensus for knowledge competencies in security system services activities. The six items with high consensus are security system, planning & designing, project management, security policies, security infrastructure and security controls. Notably, security system and security controls hold the top position compared to other items. This indicates that security surveillance plays a crucial role in maintaining the safety and security of individuals, assets, and facilities by providing real-time monitoring and the ability to respond proactively to security threats.

In terms of skills competency, all the items resulted high consensus except for one item which is written communication skill competency due to not meeting the 70% expert consensus. It is remarkable that skill of problem solving hold the top ranks, achieving the

highest fuzzy scores. The insignificance of written communication skills reflects an unimportant ability of individuals to convey information, ideas, or messages effectively through the written word. Meanwhile, the significance of problem solving play a vital role in progressive organization. Critical thinking is essential in various aspects of life, including education, professional settings, decision-making, and problem-solving. It allows individuals to approach challenges with a thoughtful and analytical mindset, fostering a deeper understanding of issues and improving the quality of decision-making. The process of finding solutions to difficult or complex issues reflects the ability in problem solving skill. Each individual under this job scope should be capable in analyzing a situation, identifying the problem, and devising a strategy to address and overcome the challenge effectively.

There are eleven questions asked for attributes competency. One item out of the nine, which is Career-management skill was omitted as attributes competency for security system service activities. The rest of the items are accepted. It is noteworthy that Dependability and Work ethics hold the heading positions, achieving the highest fuzzy scores. The elimination of career-management skills yields the less crucial in a competitive job market, even though individuals may experience multiple career transitions throughout their professional lives. In other words, everyone should take a proactive approach to navigating their own career journey, making informed decisions, and taking intentional steps to enhance career satisfaction and success. Dependability reflects the quality of being reliable, trustworthy, and consistent in one's actions, responsibilities, and commitments. A dependable individual can be counted on to fulfill tasks, meet obligations, and deliver results consistently and in a timely manner. This trait implies a level of trustworthiness and a track record of being accountable for assigned duties. Dependability is a crucial characteristic in both personal and professional contexts, as it contributes to building trust, maintaining effective teamwork, and ensuring the successful completion of tasks and projects. Work ethics reflects moral principles and values that guide an individual's behavior, attitudes, and approach towards their work and professional responsibilities. It encompasses a range of qualities such as diligence, integrity, responsibility, professionalism, and a commitment to excellence. Having strong work ethics means adhering to a code of conduct that promotes honesty, accountability, and a strong work ethic fosters a positive work environment and contributes to individual and collective success within a professional setting. Individuals with strong work ethics are typically dedicated to achieving high standards, meeting deadlines, and conducting themselves with integrity in all work-related activities.

In assessing the skills gap, two item focused on major changes in traditional training and new skills requirement and Attitude posits a low consensus due to not meeting the 70% expert consensus and Education hold the important positions achieving the highest fuzzy scores. The insignificant of two items reflects the insignificant shifts or transformations in the conventional methods of training and the skills that are now deemed essential in response even though technology is evolving. This related to the insignificant of Attitude. In various contexts, including the workplace, a person's attitude can have a profound impact on their success, satisfaction, and well-being. Attitudes can be positive, negative, or neutral, and they play a significant role in shaping behavior, decision-making, and interpersonal relationships. Attitudes can be influenced by personal experiences, cultural background, upbringing, education, and external influences. Cultivating a positive and adaptive attitude is often considered beneficial for personal growth and resilience in the face of challenges. However, in this case, attitude does not play a vital role. On the other hand, Education appears as important role in assessing the skills gap. Education reflects the systematic process of acquiring knowledge, skills, values, and understanding through various formal or informal means. It involves the imparting and receiving of information, often in an organized and structured setting such as schools, colleges, universities, or other educational institutions. Education aims to promote intellectual, social, and emotional development, preparing individuals for responsible citizenship, professional roles, and a fulfilling life. It encompasses a broad range of subjects and disciplines, and it can occur through formal instruction, self-directed learning, or experiences in the real world. Education is a lifelong and dynamic process that plays a fundamental role in personal growth, societal progress, and the advancement of knowledge.

Emerging skills in security system security activities require a question in term of drawing, designing, applying green technologies, digital skills including software, robotics and electronics. Three items resulted high consensus and another three posits as low consensus in emerging skills for security activities. Notably, Digital Skills appear as the top position, achieving the highest fuzzy score. This finding reflects the importance of individual proficiency and knowledge necessary to use digital devices, software, and technologies effectively. These skills encompass a range of abilities, including the ability to navigate digital platforms, use software applications, understand basic coding concepts, and leverage online resources. Digital skills are essential in the contemporary world, as they empower individuals to access, analyze, and communicate information through digital channels. These skills are relevant across various domains, including education, employment, business, and daily life, and they play a crucial role in adapting to and participating in the digital age. Digital skills can

include competencies such as digital literacy, information literacy, and proficiency in using digital tools for communication, collaboration, and problem-solving.

Analysis of occupation related to technology is important to understand the connection and relevant of each skill related to advanced technologies including Autonomous Robot, Cloud Computing, Cybersecurity, Augmented Reality and etc. Finding presented three out of the eleven items resulted as low consensus in occupation related to technology for security system security activities. Notably, Industrial Revolution, Technology advancement and Cybersecurity holds the top position, attaining the highest fuzzy score. These findings indicate the importance of these three job aspects compared to others related technologies. The Industrial Revolution was characterized by the widespread adoption of machinery, the growth of factories, and advancements in manufacturing processes. It played a pivotal role in shaping the modern industrialized world and had far-reaching impacts on economies, societies, and daily life. Technology advancement reflects continuous progress, improvement, and innovation in the development and application of various technologies. It signifies the evolution of tools, systems, methods, and devices that contribute to increased efficiency, functionality, and capabilities in diverse fields. Technological advancement often involves the refinement of existing technologies and the creation of new solutions to address challenges and improve various aspects of human life. As technology continues to advance, it shapes the way people live, work, and interact with the world, leading to constant changes and opportunities for progress. In term of cybersecurity, it reflects the practice of protecting computer systems, networks, and digital infrastructure from security breaches, unauthorized access, data theft, and other cyber threats. It involves the implementation of measures, protocols, and technologies to safeguard information technology assets and ensure the confidentiality, integrity, and availability of data. Cybersecurity encompasses a wide range of strategies, including the use of firewalls, encryption, antivirus software, and other tools to detect, prevent, and respond to cyberattacks. As technology evolves, cybersecurity measures also adapt to address emerging threats, making it a dynamic and critical field in safeguarding digital assets and maintaining the overall security of information systems. All these skills should be mastered by employee for the progress of an organization.

An analysis of expert consensus in security system services industry highlighted two items with high consensus. This includes Insufficient number of competence workers in top position and Poor facilities and amenities for workers. This reflects situation where there is a shortage or inadequacy in the quantity of skilled and capable individuals within a specific workforce or industry. This deficit suggests that there are not enough workers with the

necessary skills, knowledge, and expertise to meet the demands or requirements of a particular job market, sector, or profession. This shortage can impact organizational productivity, hinder growth, and create challenges in addressing the needs of a rapidly evolving and specialized work environment. Addressing this issue often involves strategies such as workforce development, training programs, educational initiatives, and efforts to attract and retain skilled professionals. Ensuring a sufficient number of competent workers involves a strategic approach to workforce planning, development, and recruitment. By adopting a comprehensive approach that combines training, collaboration, and strategic planning, organizations can work towards ensuring a sufficient number of competent workers to meet current and future demands.

5.3.4 Security and Investigation Activities

Security and Investigation Activities posits three job areas, namely (1) Surveillance & Ground Investigation, (2) Research & Analyst, and Verify and Authenticate Information/Project Management. Each area has two levels of job scope according to the needs. Surveillance & Ground Investigation required level 2 and 3. Research & Analyst required job scope in level 4 and level 5. Meanwhile, Verify and Authenticate Information/Project Management required job scope level 6 and 7. Decisions regarding the delineation of job scopes in various areas and at different levels were guided by expert recommendations in alignment with industry requirements and the operational challenges specific to each job area. Job areas deemed critical and in high demand necessitated a broader job scope. The scopes at each level carry substantial importance, interconnecting to fulfill mutual needs. It is noteworthy that Level 8 represents the highest level, while Level 1 denotes the lowest.

All the job scope were divided accordingly into 4 categories which are critical job/high demands (*), jobs relevant to technology and industrial revolution (**), critical jobs and jobs relevant to technology and industrial revolution (***) and not applicable (no *). Among the three job areas within security and investigation activities, four job scopes were classified as critical/high demand. No job scopes fell into the category of positions relevant to technology and the industrial revolution, and two job scopes were assigned to the broader classification of jobs pertinent to technology and the industrial revolution. The remaining job scopes did not fall into any applicable categories. This security system service activity requires a critical job/high demands category. It indicated that certain roles that, if left unfilled or not performed effectively, could have significant consequences. On the other hand, this security and investigation activities does not require jobs relevant to technology and the industrial revolution. This indicated that job opportunities not intricately linked to technological progress

and the ongoing transformation of industries. Furthermore, critical jobs and jobs relevant to technology and industrial revolution are considered indispensable for the overall well-being of an entity. Jobs in this category are closely connected to technological advancements and the continuous evolution of industries. Notably, there can be an overlap when critical roles also involve significant technological components, as seen in positions within emergency services that leverage advanced technologies.

The data acquired through the application of the Fuzzy Delphi technique has delineated the competencies required to meet the industry's demand and supply in Malaysia. The rationale for utilizing this technique was to obtain expert consensus on the elements crucial for shaping the occupational framework. Seven experts specializing in security system activities, each with over 11 years of work experience, actively participated in responding to the survey questions. The section addressing competency in demand was subdivided into four aspects: (1) Knowledge, (2) Skills, (3) Attributes, and (4) Skills Gap. Following this, the discussion explores Emerging Skills and Occupations Related to Technology.

Results presented one out of the eleven items (Surveillance Operative) resulted in low consensus as knowledge competencies for security system activities. Notably, Risk Assessment and Mitigation hold the top position compared to other items. This indicates that Risk Assessment and Mitigation plays a crucial role in addressing potential risks and uncertainties associated with a particular project, decision, or activity are systematically identified, analyzed, and addressed to minimize their impact. Risk assessment and mitigation are integral parts of project management, strategy, and decision-making processes. By systematically addressing potential risks, organizations can enhance their ability to achieve objectives, protect assets, and respond effectively to unexpected challenges.

In terms of skills competency, all the items were in high consensus except for three items which are Agile Mindset, Leadership and Intrapreneurship competency due to not meeting the 70% expert consensus. It is remarkable that skill of Aptitude for technology and equipment hold the top position. This reflects the important of individual's inherent capability, inclination, or natural suitability for understanding, using, and adapting to various technological tools, devices, and equipment. It involves the ability to quickly grasp and apply concepts related to the operation, troubleshooting, and utilization of technological systems. An individual with a high aptitude for technology and equipment typically demonstrates a keen interest, ease of learning, and proficiency in working with a diverse range of technological tools and devices. This aptitude may extend to areas such as digital devices, software applications, machinery, and other technical systems. Having a strong aptitude for technology is often

considered advantageous in today's fast-paced and technology-driven environments, as it enables individuals to navigate and leverage advancements in various fields.

There are eleven questions asked for attributes competency. Two items out of the nine, which is Ego-management and Career-management skills resulted as low consensus in attributes competency for security activities. It is noteworthy that Dependability, Work Ethics and Professionalism hold the heading positions, achieving the highest fuzzy scores. The low consensus of Ego-management reflects the less crucial skill in personal and professional contexts, contributing to positive collaboration, teamwork, and the creation of a supportive and respectful environment. Career-management skills also yields the less crucial in a competitive job market, even though individuals may experience multiple career transitions throughout their professional lives. In other words, everyone should take a proactive approach to navigating their own career journey, making informed decisions, and taking intentional steps to enhance career satisfaction and success. In term of attributes competency, Dependability, Work Ethics and Professionalism plays a vital role. Dependability signifies the quality of being reliable, trustworthy, and consistent in one's actions, responsibilities, and commitments.

A dependable individual is someone who can be relied upon to fulfill tasks, meet obligations, and consistently deliver results in a timely manner. This trait suggests a high level of trustworthiness and a track record of being accountable for assigned duties. In both personal and professional contexts, dependability is a crucial characteristic that contributes to the establishment of trust, effective teamwork, and the successful completion of tasks and projects. Work ethics encompass the moral principles and values guiding an individual's behavior, attitudes, and approach to their work and professional responsibilities. This includes qualities such as diligence, integrity, responsibility, professionalism, and a commitment to excellence. Strong work ethics involve adhering to a code of conduct that promotes honesty and accountability, fostering a positive work environment. This commitment contributes to both individual and collective success within a professional setting, as individuals with strong work ethics are typically dedicated to achieving high standards, meeting deadlines, and conducting themselves with integrity in all work-related activities. On the other hand, Professionalism reflects to the behavior, and qualities that characterize a person in their professional or work-related endeavors. It encompasses a set of standards, ethics, and attitudes that reflect a commitment to excellence, integrity, and respect within a specific profession or occupational context. Professionalism extends beyond technical competence and includes aspects of interpersonal communication, ethical decision-making, and adherence to organizational norms.

In assessing the skills gap, two items focused on Attitude and Employers do not clarify the skills they require in the job specification in the job advertisement were resulted in high consensus. Data indicated the important of an individual's mindset, approach, and disposition toward their job, colleagues, tasks, and the overall work environment. It encompasses a person's feelings, beliefs, and behaviors in relation to their work responsibilities. A positive work attitude involves a constructive and proactive approach, while a negative attitude may manifest as apathy, resistance, or a lack of enthusiasm. On the other hand, item about Employers do not clarify the skills they require in the job specification in the job advertisement reflects a situation where job postings or vacancy announcements lack clear and detailed information about the specific skills and qualifications that are essential for the advertised position. In such cases, the employer may not provide a comprehensive breakdown of the skills, competencies, or expertise they are seeking in potential candidates. This lack of clarity can make it challenging for job seekers to understand the precise qualifications needed for the role, potentially leading to confusion and mismatches between applicants and job requirements. Clear and well-defined job specifications are crucial for attracting suitable candidates and ensuring a transparent and effective recruitment process.

Emerging skills in Private Security Activities require a question in term of drawing, designing, applying green technologies, digital skills including software, robotics and electronics. Four out of the six items resulted as low consensus in emerging skills for Security and Investigation Activities. The high consensus items are Designing simulations, designing artificial intelligent and Design/Apply Green technology principles. This finding reflects the importance of designing simulations that involves creating virtual or simulated environments that mimic real-world scenarios or systems. It also involves the development and creation of intelligent systems or machines that can perform tasks that typically require human intelligence. This encompasses various aspects, including defining algorithms, programming, and configuring systems to exhibit cognitive functions such as learning, problem-solving, perception, and language understanding. Besides, Design/Applying Green Technology Principles reflects the integration of environmentally sustainable practices and technologies in the planning, development, and implementation of systems, products, or processes. This approach aims to minimize the environmental impact, conserve resources, and promote ecological balance.

Analysis of occupation related to technology is important to understand the connection and relevant of each skill related to advanced technologies including Autonomous Robot, Cloud Computing, Cybersecurity, Augmented Reality and etc. Finding presented three out of

the eleven items have been excluded as occupation related to technology for Security and Investigation Activities. Notably, Cybersecurity holds the top position, attaining the highest fuzzy score. These findings indicate the importance of Cybersecurity compared to others related technologies. The increased connectivity and use of standard communications protocols arise the need to protect critical industrial systems and manufacturing lines from cybersecurity threats. Cybersecurity involves the implementation of measures, technologies, and best practices to safeguard digital assets and mitigate the risks associated with cyber threats. This field encompasses a wide range of strategies, including the use of firewalls, encryption, antivirus software, intrusion detection systems, and security protocols to defend against cyber-attacks. As technology evolves, cybersecurity measures also adapt to address emerging threats and vulnerabilities in the digital landscape. The goal of cybersecurity is to create a secure and resilient environment in which individuals, organizations, and governments can operate and communicate without compromising the integrity and security of their digital assets.

An analysis of expert consensus in security system services industry highlighted two items with high consensus which are Adaptation to technological changes and Poor facilities and amenities for workers. Adaptation to technological changes reflects the ability of individuals, organizations, or societies to adjust and respond effectively to advancements, innovations, and shifts in technology. This process involves embracing new technologies, modifying existing practices, and acquiring the necessary skills and knowledge to leverage the benefits of technological developments. Meanwhile, Poor facilities and amenities reflects the inadequate or substandard provisions in the workplace that are intended to support the well-being, comfort, and productivity of employees. This can encompass various aspects of the work environment, including physical infrastructure, amenities, and services. Addressing poor facilities and amenities is crucial for creating a positive work environment, enhancing employee satisfaction, and improving overall productivity and well-being in the workplace. Organizations that prioritize and invest in the comfort and needs of their workforce often experience higher levels of employee engagement and retention. These two aspects play a vital role in security system services industry.

5.3.5 Security and Investigation Activities Industries in Malaysia Based on MSIC 2008

Private security activities play an indispensable role in today's complex and ever-evolving security landscape. Guarding Services and Security Operation Services serve as the fundamental pillars, offering a wide spectrum of security measures tailored to diverse environments. These encompass not only surveillance and access control but also risk

assessment and crisis management strategies. Armed Guarding, a critical facet within this spectrum, involves extensively trained personnel equipped to handle and mitigate high-risk situations, adding an extra layer of defense against potential threats. Close Protection services, on the other hand, extend beyond conventional security measures, providing tailored and discreet security solutions for high-profile individuals, dignitaries, or individuals facing imminent risks, ensuring their safety without compromising their mobility or lifestyle.

Moreover, Cash Management, Cash in Transit, and Value in Transit services, essential for financial institutions and businesses, implement rigorous protocols and technologies to ensure the secure transportation and handling of cash and valuables. These services not only safeguard assets but also instill confidence in financial operations, reducing vulnerabilities to theft or unauthorized access during transit. K9 Services, leveraging the remarkable olfactory and auditory senses of specially trained dogs, contribute significantly to security efforts, detecting explosives, drugs, or unauthorized substances and bolstering patrol and search operations in diverse settings. Additionally, Maritime Security, covering both Control Centre operations and Vessel protection, addresses unique challenges specific to maritime environments, ensuring adherence to stringent safety protocols, safeguarding against piracy, theft, and unauthorized access, and maintaining compliance with international maritime laws, thereby fortifying security measures across various sectors and scenarios. The collective integration of these multifaceted services not only fortifies security measures but also adapts and evolves to meet the dynamic challenges posed by modern threats, contributing significantly to the overall safety and security of individuals, institutions, and critical infrastructure.

Security systems service activities operate at the core of safeguarding infrastructures by employing a specialized workforce proficient in distinct roles that collectively fortify the security apparatus. Alarm Monitoring serves as the first line of defense, requiring meticulous attention and swift action upon triggered alerts, enabling timely response protocols to potential threats. Concurrently, Security System Surveillance Operators act as vigilant custodians, actively monitoring live feeds from surveillance systems to swiftly identify and assess suspicious activities or breaches, facilitating immediate intervention when necessary. The critical role of Security System Analysts cannot be overstated; their expertise in assessing security requirements, devising robust strategies, and implementing optimized security systems ensures maximum efficacy against evolving threats. Simultaneously, Security System Technologists, with their specialized technical acumen, meticulously maintain, repair, and upgrade security hardware and software, ensuring seamless functionality and readiness against potential vulnerabilities. The synergy between these roles forms a cohesive unit essential for

the comprehensive operation, enhancement, and continuous fortification of security systems, mitigating risks and ensuring resilience against potential security breaches or weaknesses in the ever-evolving threat landscape.

Furthermore, the integration and collaboration among these roles extend beyond mere functionality, encompassing a proactive approach to anticipate and preempt security vulnerabilities. By continually analyzing and adapting security systems to emerging threats and technological advancements, these professionals not only ensure current efficacy but also spearhead innovation in security infrastructure. Their collective efforts lay the groundwork for adaptive security frameworks that not only respond to current challenges but also proactively evolve, staying ahead of potential risks. This collaborative synergy enables a dynamic security environment, reinforcing the defense against sophisticated threats while fostering a proactive stance in mitigating risks and vulnerabilities, thereby bolstering the resilience and effectiveness of security systems in safeguarding critical assets and environments.

Investigation and detective activities within aviation security (Avsec) extend beyond conventional security measures, involving multifaceted operations crucial for safeguarding airports and the aviation industry at large. Intelligence gathering and focused investigations lie at the forefront, constantly assessing potential threats, profiling passengers, and meticulously monitoring activities within airport premises. Surveillance units, employing cutting-edge monitoring technologies and ground investigation teams, maintain a watchful eye over airport areas, rigorously enforcing security protocols, and swiftly intervening in response to any suspicious activities or breaches, ensuring the safety and security of passengers and personnel.

Moreover, the contributions of research analysts are indispensable; their in-depth analysis of data, trends, and emerging threats provides vital insights that drive the formulation of robust security strategies and protocols. Verifying and authenticating information teams collaborate closely with intelligence units, employing stringent processes to ensure the integrity and reliability of gathered data, crucial for informed decision-making in high-stakes security scenarios. Additionally, project management assumes a pivotal role in Avsec, orchestrating the coordination among various operational aspects, ensuring the seamless implementation of security initiatives, and fostering cohesive collaboration among different units. This integrated approach not only upholds stringent aviation security standards but also enhances safety measures within the aviation industry, collectively contributing to fortifying airports and ensuring safe, secure travel experiences for passengers and personnel alike in an ever-evolving security landscape.

5.4 The Implication of Study

The implications derived from the comprehensive study of security and investigation activities within Malaysia are far-reaching and influential across various domains. Firstly, the study's findings offer invaluable insights into the evolving needs and requirements within the industry. By meticulously examining job classifications, responsibilities, and competencies essential in this sector, the study serves as a guiding compass for policymakers, industry regulators, and training institutions. These insights enable the identification of areas requiring immediate attention, allowing for targeted interventions and strategic planning to bridge skill gaps, align education programs, and shape policies that meet the industry's evolving demands. Moreover, the implications extend to professionals and aspiring individuals within the field, providing a clear understanding of the skill sets and competencies required for career advancement and personal development.

Secondly, the study's implications are instrumental in bolstering the industry's resilience and adaptability. The validation and documentation of job titles, classifications, and responsibilities aligning with MOSQF and industry validations based on MSIC 2008 version 1.0 offer a foundation for standardizing practices within the sector. This standardization not only enhances operational efficiency but also facilitates the harmonization of industry practices, fostering consistency and reliability in service delivery. Such implications serve as a catalyst for the industry's growth, encouraging innovation, and the adoption of best practices, thereby enhancing its competitiveness on both national and global platforms.

Furthermore, the study's implications resonate with the broader societal context, contributing to public safety and well-being. The insights garnered from the investigation activities and demographic profiles of experts across various domains provide a holistic understanding of the industry's landscape. This knowledge can be leveraged to enhance collaborative efforts between public and private entities, law enforcement agencies, and regulatory bodies, thereby bolstering efforts to combat emerging security threats, improve crime prevention strategies, and ensure a safer and more secure environment for citizens. Ultimately, the implications derived from this study serve as a cornerstone for informed decision-making, policy formulation, and strategic interventions that underpin the sustainable development and fortification of the security and investigation activities industry within Malaysia.

5.5 Suggestion for Future Study

The comprehensive research conducted on the landscape of security and investigation activities in Malaysia lays a solid foundation for future studies that could further enhance the understanding and development of this industry. Firstly, exploring the implications of emerging global trends on local security practices and investigative methodologies stands as a crucial avenue for future investigation. Given the increasing globalization and interconnectedness of economies, studying the impact of international events, geopolitical shifts, or technological advancements on local security needs and investigation procedures could provide valuable insights. Understanding how these external influences shape local practices and demand for specific skill sets could aid in developing more adaptive and responsive strategies within the Malaysian context.

Secondly, there is a need for in-depth research on the socio-economic impacts of the security and investigation activities industry. Examining the industry's role in contributing to employment, economic growth, and societal well-being could offer a comprehensive understanding of its significance beyond the realm of security alone. Exploring how the industry interfaces with other sectors, such as tourism, trade, or finance, and assessing its broader contributions to the national economy and social stability would be highly informative. This research could provide policymakers with a holistic perspective to formulate strategies that maximize the industry's positive impact on society while addressing any potential negative repercussions.

Additionally, conducting comparative studies between Malaysia and other countries or regions could yield valuable comparative insights. Analyzing the similarities, differences, and best practices adopted in security and investigation activities across different contexts could offer a benchmark for evaluating Malaysia's practices and identifying areas for improvement. Comparative studies could also facilitate knowledge exchange, enabling the adaptation of successful strategies from other regions to enhance the effectiveness and efficiency of local practices.

Future studies exploring the impact of global trends on local security practices, assessing the socio-economic contributions of the industry, and conducting comparative analyses between different contexts hold immense potential to deepen our understanding and further advance the security and investigation activities field in Malaysia. These avenues of research could pave the way for more robust, adaptive, and globally competitive practices within the country's security landscape.

Furthermore, the dedication of FGD's panel experts significantly impacts the study, as some individuals may face constraints participating in multiple sessions due to work obligations. This challenge hinders researchers in acquiring timely data and poses challenges in identifying alternative panel experts promptly. Moreover, the exclusive reliance on FGDs for data collection in this study results in a restricted pool of respondents. Subsequent research endeavors could explore diverse methodologies like surveys to enable the acquisition of data on a broader scale.

5.6 Conclusion

The meticulous development of an OF for Security and Investigation Activities serves as a cornerstone in standardizing, organizing, and professionalizing the diverse spectrum of roles within these crucial domains. This framework elucidates the competencies, skill sets, and qualifications necessary to excel in various facets of security and investigative functions, ensuring a structured pathway for career progression and skill development. By establishing clear guidelines and benchmarks, this framework not only fosters consistency and proficiency but also enhances the quality of personnel recruited, trained, and employed within these critical sectors. It underscores the significance of continuous learning, adaptability to evolving threats, and the amalgamation of practical expertise with theoretical knowledge, thereby contributing to a more robust and efficient workforce equipped to address the intricate challenges inherent in security and investigation activities.

REFERENCES

Adnan, N. A., Mahadzir, Z. 'Aqilah, Hashim, H., Mohd Yusoff, Z., Abdul Rasam, A. R., & Mokhtar, E. S. (2023). Road accessibility and safety analysis in gated and non-gated housing communities. *Planning Malaysia*, *21*(28). https://doi.org/10.21837/pm.v21i28.1318

Antoniou, G.S. (2018). A Framework for the Governance of Information Security: Can it be Used in an Organization. In SoutheastCon 2018 (pp. 1-30). IEEE

Anwar, A. Q., Ahmad Fuad, A. F., Ahmad, M. S., Said, M. H., & Kamis, A. S. (2023). Development of a conceptual framework of private maritime security company of Malaysia. *Australian Journal of Maritime & Ocean Affairs*, *15*(1), 12-24.

Buthelezi, M. P., Van Der Poll, J. A., & Ochola, E. O. (2016, December). Ambiguity as a barrier to information security policy compliance: A content analysis. In 2016 *International Conference on Computational Science and Computational Intelligence* (CSCI) (pp. 1360-1367). IEEE.

Castrillón Rias, J., & Guerra Molina, R. (2016). *A deep influence: United States-Colombia bilateral relations and security sector reform* (SSR), 1994-2002.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, 26(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9.

Dorn, N., & Levi, M. (2007). European Private Security, Corporate Investigation and Military Services: Collective Security, Market Regulation and Structuring the Public Sphere. *Policing and Society*, 17(3), 213–238. doi:10.1080/10439460701497303

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*, 17(5), 474-491.

England, M. L., & Center, H. L. S. (2009). Security sector governance and oversight: A note on current practice. Henry L. Stimson Center.

Ferreira, L. P. T. (2017). Cloud security risk and readiness. (*Doctoral dissertation*)

Firesmith, D.G. (2012) Engineering Safetyand Security-Related Requirements for Software-Intensive Systems. The 11th IASTED International Conference on Software Engineering (SE 2012) in Crete, Greece on 18 June 2012.

Gannapathy, V. R., Narayanamurthy, V., Subramaniam, S. K., Ibrahim, A. F. B. T., Isa, I. S. M., & Rajkumar, S. (2023). A Mobile and Web-Based Security Guard Patrolling, Monitoring and Reporting System to Maintain Safe and Secure Environment at Premises. *International Journal of Interactive Mobile Technologies*, *17*(11).

Gill, P., & Wilson, L. (2013). Intelligence and security sector reform in Indonesia. *Intelligence Elsewhere: spies and espionage outside the Anglosphere*, 157-80.

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4), 281–295. https://doi.org/10.1016/j.jsis.2010.10.002**.**

Gupta, A., Shakya, S., & Marasini, S. (2015). E-Readiness Assessment for Ministries of Nepal for Implementation of e-government. In 2015 *International Conference on Data Mining, Electronics and Information Technology* (DMEIT'15) (pp. 10-11).

Hu, L., Li, H., Wei, Z., Dong, S., & Zhang, Z. (2019). Summary of Research on IT Network and Industrial Control Network Security Assessment. *IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference* (ITNEC 2019), 1203-1210.

Ismail, Z., Masrom, M., Sidek, Z., & Hamzah, D. (2010). Framework to manage information security for malaysian academic environment. *Information Assurance & Cybersecurity*, *2010*, 1-16.

Javaida, M., Haleema, A., Singh, R.P., Suman, R., Gonzalez, E.S. (2022). Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. *Sustainable Operations and Computers*, 3, 203-2017.

Kamaruzaman, M. A., & Rashid, R. A. (2023, May). Supervisory mobile application for GuardExpert PRO security management system. In *AIP Conference Proceedings* (Vol. 2795, No. 1). AIP Publishing.

Kiplimo, A.E. (2018). A web-based model to determine cybersecurity readiness index for hospitals towards adoption of e-health, *Unpublished Dissertation*.

Manogaran, G., Thota, C., Lopez, D., Sundarasekar, R. (2017). Big Data Security Intelligence for Healthcare Industry 4.0. In: Thames, L., Schaefer, D. (eds) Cybersecurity for Industry 4.0. Springer Series in Advanced Manufacturing. *Springer*, Cham. https://doi.org/10.1007/978-3-319-50660-9_5

Mazlan, S. S., Mohamed , N. ., & Majid, F. F. . (2023). Development of Monitoring System using Raspberry Pi with Instant Notification. *Journal of Emerging Technologies and Industrial Applications*, *2*(1). Retrieved from http://jetia.mbot.org.my/index.php/jetia/article/view/15

Mehreza, A., & Bakria, A. (2019). The impact of human resource practices on job satisfaction and intention to stay in emerging economies: Model development and empirical investigation among high caliber governmental employees in Qatar.

Nalla, M. K., Lim, S. L. S., & Demirkol, I. C. (2015). The relationship between goal difficulty, goal specificity, rewards and job satisfaction: A study of Singapore security guards. *Security Journal*, 28, 392-409.

Novak, T., & Treytl, A. (2008). Functional safety and system security in automation systems - a life cycle model. *IEEE International Conference on Emerging Technologies and Factory Automation*, 311–318.

Othman, N., Bahri, M. S. S., Yahaya, H., & Jen, A. L. (2023). Terrorism & The Overview on Impacts Towards Government Policies in Malaysia, The United States and The United Kingdom. *Journal of the Malaysian Parliament*, *3*, 194-219.

Pan, D., & Liu, F. (2007). Influence between functional safety and security. *2nd IEEE Conference on Industrial Electronics and Applications*, 1323–1325.

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, 13, 1253–1260. doi:10.1016/j.promfg.2017.09.047

Prenzler, T., & Sarre, R. (2012). The evolution of security industry regulation in Australia: A critique. *International Journal for Crime, Justice and Social Democracy*, 1(1), 38-51.

Reichenbach, F., Endresen, J., Chowdhury, M. M. R., & Rossebø, J. (2012). A pragmatic approach on combined safety and security risk analysis. *IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, 239–244.

Samonas, S., Dhillon, G., & Almusharraf, A. (2020). Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management*, 50, 144–154. doi:10.1016/j.ijinfomgt.2019.04.011

Sahrir, M. S., Alias, N. A., Ismail, Z., & Osman, N. (2012). Employing design and development research (DDR) approaches in the design and development of online arabic vocabulary learning games prototype. *Turkish Online Journal of Educational Technology*, *11*(2).

Singh, A., Kumar, D., & H¨otzel, J. (2018). Iot based information and communication system for enhancing underground mines safety and productivity: Genesis, taxonomy and open issues. Ad Hoc Networks, 78,115–129. https://www.sciencedirect.com/science/article/pii/S1570870518303524

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, 22(1), 77-94.

Stiernstedt, P. (2019). Privatizing Police Discretion—"Private Security Criminal Investigations" in Sweden. *Policing: A Journal of Policy and Practice*, 15(4), 2210-2224. doi:10.1093/police/paz074

Tanner, M. S. (2002). Changing windows on a changing China: The evolving "think tank" system and the case of the public security sector. *The China Quarterly*, 171, 559-574.

Tomur, E., G¨ulen, U., Soykan, E. U., Ersoy, M. A., Karakoc, F., Karac¸ L., & C¸ omak, P. (2021). SoK: Investigation of Security and Functional Safety in Industrial IoT. 2021 *IEEE International Conference on Cyber Security and Resilience* (CSR), 226-233.

ANNEX 1 : QUESTIONNAIRE

Occupational Frameworks (N801)

UPUM Sdn. Bhd.
has been tasked to develop Occupational Frameworks in six (6) divisions of economic areas according to the Malaysia Standard Industrial Classification (MSIC) 2008, by the Department of Skills Development (DSD), Ministry of Human Resources.

The six divisions
are:

B09 - Mining
Support Service Activities

C15 -
Manufacturing of Leather and Related Product

C16 -
Manufacture of Wood and Products of Wood and Cork, except furniture; Manufacture of articles of straw and plating materials.

C17 -
Manufacture of paper And paper products

N80 - Security
and investigation activities

N81 - Service
to buildings and landscape activities

The research
aims to establish the occupational structure for these divisions by examining job areas, job titles, and levels; determine the occupational description and responsibilities for each job; examine the jobs and competencies in demand; identify critical job titles; and competency needed to address the demand and supply of the industry in Malaysia.

The Fuzzy
Delphi Instrument is used to achieve the following objectives:

a. To identify
the critical job and the Job Description for the six identified divisions
related to current developments in the industry

b. To analyse
the competency needed to address the demand and supply of the industry in Malaysia

Hence, we
welcome your feedback and responses as expert panel members.

The Fuzzy
Delphi Instrument consists of six (6) sections. Please attempt all sections and

fill in where applicable.

Section 1 :
Respondents Details.

Section 2 :
Competency in Demand

Section 3 :
Emerging Skills

Section 4 :
Occupation Related to Technology

Section 5
: Jobs in Demand

Section 6
: Related Issues

* Indicates required question

SURVEY RESPONDENT DETAIL

Please select only one item.

1. Age *

Mark only one oval.

- ◯ Below 20 years old
- ◯ 20 – 29 years old
- ◯ 30 – 39 years old
- ◯ 40 – 49 years old
- ◯ Above 50 years old

2. Gender *

Mark only one oval.

- ◯ Male
- ◯ Female

3. Overall number of years in the industry: * 1 point

Mark only one oval.

- ◯ Below 5 years
- ◯ 5 – 10 years
- ◯ 11 – 20 years
- ◯ 21 – 30 years
- ◯ Above 30 years

4. Position in the organization: * 1 point

Mark only one oval.

- ◯ Chief Executive Officer
- ◯ Specialist/Managing Director/General Manager
- ◯ Production Engineer/Engineer
- ◯ Manager/ Human Resource Manager

5. Others (please specify):

_____

6. Location of your organization in Malaysia (Please specify the state only): *

Mark only one oval.

- Perlis
- Kedah
- Penang
- Perak
- Selangor
- Negeri Sembilan
- Melaka
- Johor
- Pahang
- Terengganu
- Kelantan
- Sabah
- Sarawak
- Federal Territory of Kuala Lumpur
- Federal Territory of Putrajaya
- Federal Territory of Labuan

7. Expertise according to the Division in the Malaysia Standard Industrial Classification (MSIC) 2008 *

Mark only one oval.

- B09 – Mining Support Service Activities
- C15 - Manufacturing of Leather and Related Product
- C16 - Manufacture of Wood and Products of Wood and Cork, except furniture; Manufacture of articles of straw and plating materials.
- C17 – Manufacture of paper And paper products
- N80 – Security and investigation activities
- N81 – Service to buildings and landscape activities

8. Expertise according to Group in the Malaysia Standard Industrial Classification (MSIC) 2008 *

Mark only one oval.

- ◯ B091 – Support activities for Petroleum and Natural Gas Extraction
- ◯ B099 – Support activities for other mining and quarrying
- ◯ C151 – Tanning and dressing of leather; manufacture of luggage, handbags, saddlery and harness; dressing and dyeing of furon 3
- ◯ C152 – Manufacture of footware
- ◯ C161 – Sawmilling and planing of wood
- ◯ C162 – Manufacture of products of wood, cork, straw, and plaiting materials
- ◯ C170 – Manufacture of paper and paper products
- ◯ N801 – Private security activities
- ◯ N802 – Security systems service activities
- ◯ N803 – Investigation activities
- ◯ N811 – Combined facilities support activities
- ◯ N812 – Cleaning activities
- ◯ N813 – Landscape care and maintainence service activities

COMPETENCY IN DEMAND

INSTRUCTIONS: For each of the statements please indicate your level of agreement by selecting only one of the choices based on the Fuzzy scale below:

Strongly Disagree : 1
Disagree : 2
Moderately Agree : 3
Agree : 4
Strongly Agree : 5

According to your expert opinion, rank your agreement that the following competency is important to perform these jobs.

Knowledge (refer to Dictionary competency/ OR)

9. Security Threats *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

10. Security personnel *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

11. Medical incidents *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

12. Case management *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

13. Security surveillance *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

14. Closed-Circuit Television (CCTV) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

15. Incidents and emergencies *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

16. Traffic and crowds *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

17. Security stakeholders *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

18. Situational trend analyses *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

19. Security operation audits *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

20. Security risks *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

21. Law enforcement *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

Skills

22. Interpersonal Communication *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

23. Written Communication *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

24. Critical Thinking *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

25. Problem Solving *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

26. Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

27. Leadership *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

28. Time management *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

29. Aptitude for Technology and Equipment *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

30. Intrapreneurship (Refers to employee initiatives in organisations to take something new, without being asked to do so) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

31. Others (please specify)

_____

Attribute/Attitude (General)

32. Attention to details *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

33. Team work *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

34. Multi-tasking/ Flexibility *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

35. Dependability (Trustworthy & Reliable) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

36. Work Ethics *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

37. Professionalism *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

38. Self-management/ independent *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

39. Self-learning *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

40. Agility (Ability to think and understand quickly) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

41. Ego-management (An exaggerated sense of self-worth based on one's extrinsic achievement) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

42. Career-management (career path and individual development, succession planning) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

43. Others (please specify)

_____

According to your expert opinion, rank your agreement on the reason(s) for the skills gap.

44. Education or training mismatch *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

45. Major changes in traditional training and new skills requirements *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

46. Attitude (for example, lack of desire to work) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

47. Misalignment between how job seekers are communicating their skills in their CV *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

48. Employers do not clarify the skills they require in the job specifications in the job advertisement *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

49. Others (please specify)

EMERGING SKILLS

Emerging skills are skills that are expected to be important to the industry in the near future based on recent events, trends, government policies, or research. For example, the technology revolution, issues of sustainability, and many other things are examples of emerging skills.

According to your expert opinion, rank your agreement on the future emerging skills that affect the productivity of your current job.

50. Drawing / designing 3D, Designing virtual environments, Applying virtual reality to training and design. Designing simulations, Designing artificial intelligent *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

51. Design/Apply Green technology principles *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

52. Digital skills *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

53. Design/ Utilize software for autonomous technology, machine learning, data automation, and Internet of things (IoT) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

54. Environmental, social and governance (ESG) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

55. Design / Apply Robotics and Electronics *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

56. Other *(please specify)*:

_____

OCCUPATION RELATED TO TECHNOLOGY

According to your expert opinion, rank your agreement on the technology.

57. The Industrial Revolution would have an impact on this industry *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

58. Technology advancement directly affects the jobs in the industry *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

According to your expert opinion, rank your agreement on the technology that is influencing your industry/ job area.

59. Autonomous Robots *
(Coordinated and automated actions of robots to complete tasks intelligently, with minimal human input)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

60. Big Data Analytics *

(The analysis of ever larger volumes of data. Circulation, collection, and analysis of information is a necessity because it supports productivity growth based on a real-time decision-making process)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

61. Cloud Computing *

(Storing and accessing data and programs over the Internet instead of your computer's hard drive)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

62. Internet of Things (IoT) *

(All machines and systems connected to the production plant (as well as other systems) must be able to collect, exchange and save these massive volumes of information, in a completely autonomous way and without the need of human intervention)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

63. Additive Manufacturing (3D Printing) *

(Use in prototyping, design iteration and small scale production and often described as “rapid prototyping” - produce the desired components faster, more flexibly and more precisely than ever before)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

64. System Integration *

(The process of linking together different computing systems and software applications physically or functionally to act as a coordinated whole via Internet of Things-IoT)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

65. Cybersecurity *

(With the increased connectivity and use of standard communications protocols, the need to protect critical industrial systems and manufacturing lines from cybersecurity threats is increasing)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

66. Augmented Reality *

(Augmented-reality-based systems support a variety of services, such as selecting parts in a warehouse and sending repair instructions over mobile devices - provide workers with real-time information to improve decision making and work procedures)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

67. Simulation *

(Simulations will leverage real-time data to mirror the physical world in a virtual model, which can include machines, products, and humans. This allows operators to test and optimize the machine settings for the next product in line in the virtual world before the physical changeover, thereby driving down machine setup times and increasing quality)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

SECTION 5: JOBS IN DEMAND (801) According to your expert opinion, rank your agreement on the high manpower shortage for these jobs.

a. Guarding Services

68. Security supervisor *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

69. Security officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

70. Assistant Security officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

b. Security Operation Management

71. Operation director/MD *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

72. General manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

73. Senior Security manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

74. Security Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

75. Security Senior Executive *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

76. Security Executive *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

c. Armed Guarding

77. Supervisor *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

78. Security Officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

d. Close Protection

79. Close Protection Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

80. Close Protection Executive *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

81. Senior Bodyguard *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

82. Bodyguard *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

e. Cash Management/ Cash in Transit/ Value in Transit

83. Supervisor *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

84. Security Officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

f. K9 Service

85. Security Officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

g. Alarm Monitoring

86. Supervisor *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

87. Security Officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

h. Maritime Security

88. Maritime Operation Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

89. Operating Room Coordinator *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

90. Operating Room Officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

91. Ordnance officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

92. Operation Supervisor *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

93. Team Leader *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

94. Unit Leader *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

95. Ship Security Officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

i. Aviation Security (Admin, Training, Logistic & Support Services/ Operations/ Intelligence & Investigation)

96. Senior Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

97. Avsec Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

98. Avsec Executive *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

99. Avsec Senior Officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

100. Avsec Officer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

101. Avsec Assistant *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

102. General Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

103. State the reason for the high shortage of the Jobs-in demand

_____

RELATED ISSUES

According to your expert opinion, rank your agreement on the key issues affecting the workforce of the industry.

104. Insufficient number of skilled workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

105. Insufficient number of certified workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

106. Insufficient number of competence workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

107. High dependence on foreign labor *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

108. Underpayment of wages leads to high turnover *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

109. Talent Gap among graduates *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

110. Adaptation to technological changes *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

111. Poor facilities and amenities for workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

112. Others (please specify)

Occupational Frameworks (N802)

UPUM Sdn. Bhd.
has been tasked to develop Occupational Frameworks in six (6) divisions of economic areas according to the Malaysia Standard Industrial Classification (MSIC) 2008, by the Department of Skills Development (DSD), Ministry of Human Resources.

The six divisions
are:

B09 - Mining
Support Service Activities

C15 -
Manufacturing of Leather and Related Product

C16 -
Manufacture of Wood and Products of Wood and Cork, except furniture; Manufacture of articles of straw and plating materials.

C17 -
Manufacture of paper And paper products

N80 - Security
and investigation activities

N81 - Service
to buildings and landscape activities

The research
aims to establish the occupational structure for these divisions by examining job areas, job titles, and levels; determine the occupational description and responsibilities for each job; examine the jobs and competencies in demand; identify critical job titles; and competency needed to address the demand and supply of the industry in Malaysia.

The Fuzzy
Delphi Instrument is used to achieve the following objectives:

a. To identify
the critical job and the Job Description for the six identified divisions
related to current developments in the industry

b. To analyse
the competency needed to address the demand and supply of the industry in Malaysia

Hence, we
welcome your feedback and responses as expert panel members.

The Fuzzy
Delphi Instrument consists of six (6) sections. Please attempt all sections and

fill in where applicable.

Section 1 :
Respondents Details.

Section 2 :
Competency in Demand

Section 3 :
Emerging Skills

Section 4 :
Occupation Related to Technology

Section 5
: Jobs in Demand

Section 6
: Related Issues

* Indicates required question

SURVEY RESPONDENT DETAIL

Please select only one item.

1. Age *

Mark only one oval.

- ◯ Below 20 years old
- ◯ 20 – 29 years old
- ◯ 30 – 39 years old
- ◯ 40 – 49 years old
- ◯ Above 50 years old

2. Gender

Mark only one oval.

- ◯ Male
- ◯ Female

3. Overall number of years in the industry: 1 point

Mark only one oval.

- ◯ Below 5 years
- ◯ 5 – 10 years
- ◯ 11 – 20 years
- ◯ 21 – 30 years
- ◯ Above 30 years

4. Position in the organization: 1 point

Mark only one oval.

- ◯ Chief Executive Officer
- ◯ Specialist/Managing Director/General Manager
- ◯ Production Engineer/Engineer
- ◯ Manager/ Human Resource Manager

5. Others (please specify):

_____

6. Location of your organization in Malaysia (Please specify the state only):

Mark only one oval.

- ◯ Perlis
- ◯ Kedah
- ◯ Penang
- ◯ Perak
- ◯ Selangor
- ◯ Negeri Sembilan
- ◯ Melaka
- ◯ Johor
- ◯ Pahang
- ◯ Terengganu
- ◯ Kelantan
- ◯ Sabah
- ◯ Sarawak
- ◯ Federal Territory of Kuala Lumpur
- ◯ Federal Territory of Putrajaya
- ◯ Federal Territory of Labuan

7. Expertise according to the Division in the Malaysia Standard Industrial Classification (MSIC) 2008

Mark only one oval.

- ◯ B09 – Mining Support Service Activities
- ◯ C15 - Manufacturing of Leather and Related Product
- ◯ C16 - Manufacture of Wood and Products of Wood and Cork, except furniture; Manufacture of articles of straw and plating materials.
- ◯ C17 – Manufacture of paper And paper products
- ◯ N80 – Security and investigation activities
- ◯ N81 – Service to buildings and landscape activities

8. Expertise according to Group in the Malaysia Standard Industrial Classification (MSIC) 2008

Mark only one oval.

- ◯ B091 – Support activities for Petroleum and Natural Gas Extraction
- ◯ B099 – Support activities for other mining and quarrying
- ◯ C151 – Tanning and dressing of leather; manufacture of luggage, handbags, saddlery and harness; dressing and dyeing of furon 3
- ◯ C152 – Manufacture of footware
- ◯ C161 – Sawmilling and planing of wood
- ◯ C162 – Manufacture of products of wood, cork, straw, and plaiting materials
- ◯ C170 – Manufacture of paper and paper products
- ◯ N801 – Private security activities
- ◯ N802 – Security systems service activities
- ◯ N803 – Investigation activities
- ◯ N811 – Combined facilities support activities
- ◯ N812 – Cleaning activities
- ◯ N813 – Landscape care and maintainence service activities

9. Expertise according to Group in the Malaysia Standard Industrial Classification (MSIC) 2008 *

Mark only one oval.

- ◯ B091 – Support activities for Petroleum and Natural Gas Extraction
- ◯ B099 – Support activities for other mining and quarrying
- ◯ C151 – Tanning and dressing of leather; manufacture of luggage, handbags, saddlery and harness; dressing and dyeing of furon 3
- ◯ C152 – Manufacture of footware
- ◯ C161 – Sawmilling and planing of wood
- ◯ C162 – Manufacture of products of wood, cork, straw, and plaiting materials
- ◯ C170 – Manufacture of paper and paper products
- ◯ N801 – Private security activities
- ◯ N802 – Security systems service activities
- ◯ N803 – Investigation activities
- ◯ N811 – Combined facilities support activities
- ◯ N812 – Cleaning activities
- ◯ N813 – Landscape care and maintainence service activities

COMPETENCY IN DEMAND

INSTRUCTIONS: For each of the statements please indicate your level of agreement by selecting only one of the choices based on the Fuzzy scale below:

Strongly Disagree : 1
Disagree : 2
Moderately Agree : 3
Agree : 4
Strongly Agree : 5

According to your expert opinion, rank your agreement that the following competency is important to perform these jobs.

Knowledge (refer to Dictionary competency/ OR)

10. Security system *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

11. Security threats *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

12. IT & Networking *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

13. Analyse data logs *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

14. Planning & Designing *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

15. Project Management *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

16. Maintenance & Service *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

17. Security-conscious culture *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

18. Security policies *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

19. Security infrastructure *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

20. Security controls *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

Skills

21. Interpersonal Communication *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

22. Written Communication *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

23. Critical Thinking *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

24. Problem Solving *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

25. Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

26. Leadership *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

27. Time management *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

28. Aptitude for Technology and Equipment *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

29. Intrapreneurship (Refers to employee initiatives in organisations to take something new, without being asked to do so) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

30. Others (please specify)

_____

Attribute/Attitude (General)

31. Attention to details *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

32. Team work *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

33. Multi-tasking/ Flexibility *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

34. Dependability (Trustworthy & Reliable) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

35. Work Ethics *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

36. Professionalism *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

37. Self-management/ independent *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

38. Self-learning *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

39. Agility (Ability to think and understand quickly) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

40. Ego-management (An exaggerated sense of self-worth based on one's extrinsic achievement) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

41. Career-management (career path and individual development, succession planning) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

42. Others (please specify)

_____

According to your expert opinion, rank your agreement on the reason(s) for the skills gap.

43. Education or training mismatch *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

44. Major changes in traditional training and new skills requirements *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

45. Attitude (for example, lack of desire to work) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

46. Misalignment between how job seekers are communicating their skills in their CV *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

47. Employers do not clarify the skills they require in the job specifications in the job advertisement *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

48. Others (please specify)

_____

EMERGING SKILLS

Emerging skills are skills that are expected to be important to the industry in the near future based on recent events, trends, government policies, or research. For example, the technology revolution, issues of sustainability, and many other things are examples of emerging skills.

According to your expert opinion, rank your agreement on the future emerging skills that affect the productivity of your current job.

49. Drawing / designing 3D, Designing virtual environments, Applying virtual reality to training and design. Designing simulations, Designing artificial intelligent *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

50. Design/Apply Green technology principles *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

51. Digital skills *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

52. Design/ Utilize software for autonomous technology, machine learning, data automation, and Internet of things (IoT) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

53. Environmental, social and governance (ESG) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

54. Design / Apply Robotics and Electronics *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

55. Other *(please specify)*:

_____

OCCUPATION RELATED TO TECHNOLOGY

According to your expert opinion, rank your agreement on the technology.

56. The Industrial Revolution would have an impact on this industry *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

57. Technology advancement directly affects the jobs in the industry *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

According to your expert opinion, rank your agreement on the technology that is influencing your industry/ job area.

58. Autonomous Robots *
(Coordinated and automated actions of robots to complete tasks intelligently, with minimal human input)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

59. Big Data Analytics *

(The analysis of ever larger volumes of data. Circulation, collection, and analysis of information is a necessity because it supports productivity growth based on a real-time decision-making process)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

60. Cloud Computing *

(Storing and accessing data and programs over the Internet instead of your computer's hard drive)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

61. Internet of Things (IoT) *

(All machines and systems connected to the production plant (as well as other systems) must be able to collect, exchange and save these massive volumes of information, in a completely autonomous way and without the need of human intervention)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

62. Additive Manufacturing (3D Printing) *

(Use in prototyping, design iteration and small scale production and often described as “rapid prototyping” - produce the desired components faster, more flexibly and more precisely than ever before)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

63. System Integration *

(The process of linking together different computing systems and software applications physically or functionally to act as a coordinated whole via Internet of Things-IoT)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

64. Cybersecurity *

(With the increased connectivity and use of standard communications protocols, the need to protect critical industrial systems and manufacturing lines from cybersecurity threats is increasing)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

65. Augmented Reality *

(Augmented-reality-based systems support a variety of services, such as selecting parts in a warehouse and sending repair instructions over mobile devices - provide workers with real-time information to improve decision making and work procedures)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

66. Simulation *

(Simulations will leverage real-time data to mirror the physical world in a virtual model, which can include machines, products, and humans. This allows operators to test and optimize the machine settings for the next product in line in the virtual world before the physical changeover, thereby driving down machine setup times and increasing quality)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

JOBS IN DEMAND (802) According to your expert opinion, rank your agreement on the high manpower shortage for these jobs.

a. Security System Surveillance Operator

67. Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

68. Senior Executives *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

69. Executives *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

70. Senior Operator *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

71. Operator *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

b. Security System Analyst

72. General Manager Security Solutions *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

73. Manager, Security Solutions *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

74. Senior Analyst *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

75. Analyst *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

c. Security System Technologist

76. Director, Technical & Security Solutions *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

77. Specialist, Technical Deployment/ Assistant Director *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

78. Head, Technical Operation Executives / Senior engineer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

79. Senior Technical Executives/ Lead engineer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

80. Technical Executives / engineer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

81. System admin/ Junior engineer *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

82. State the reason for the high shortage of the Jobs-in demand

_____

RELATED ISSUES

According to your expert opinion, rank your agreement on the key issues affecting the workforce of the industry.

83. Insufficient number of skilled workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

84. Insufficient number of certified workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

85. Insufficient number of competence workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

86. High dependence on foreign labor *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

87. Underpayment of wages leads to high turnover *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

88. Talent Gap among graduates *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

89. Adaptation to technological changes *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

90. Poor facilities and amenities for workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

91. Others (please specify)

Occupational Frameworks (N803)

UPUM Sdn. Bhd.
has been tasked to develop Occupational Frameworks in six (6) divisions of economic areas according to the Malaysia Standard Industrial Classification (MSIC) 2008, by the Department of Skills Development (DSD), Ministry of Human Resources.

The six divisions
are:

B09 - Mining
Support Service Activities

C15 -
Manufacturing of Leather and Related Product

C16 -
Manufacture of Wood and Products of Wood and Cork, except furniture; Manufacture of articles of straw and plating materials.

C17 -
Manufacture of paper And paper products

N80 - Security
and investigation activities

N81 - Service
to buildings and landscape activities

The research
aims to establish the occupational structure for these divisions by examining job areas, job titles, and levels; determine the occupational description and responsibilities for each job; examine the jobs and competencies in demand; identify critical job titles; and competency needed to address the demand and supply of the industry in Malaysia.

The Fuzzy
Delphi Instrument is used to achieve the following objectives:

a. To identify
the critical job and the Job Description for the six identified divisions
related to current developments in the industry

b. To analyse
the competency needed to address the demand and supply of the industry in Malaysia

Hence, we
welcome your feedback and responses as expert panel members.

The Fuzzy
Delphi Instrument consists of six (6) sections. Please attempt all sections and

fill in where applicable.

Section 1 :
Respondents Details.

Section 2 :
Competency in Demand

Section 3 :
Emerging Skills

Section 4 :
Occupation Related to Technology

Section 5
: Jobs in Demand

Section 6
: Related Issues

* Indicates required question

SURVEY RESPONDENT DETAIL

Please select only one item.

1. Age *

Mark only one oval.

- ◯ Below 20 years old
- ◯ 20 – 29 years old
- ◯ 30 – 39 years old
- ◯ 40 – 49 years old
- ◯ Above 50 years old

2. Gender *

Mark only one oval.

- ◯ Male
- ◯ Female

3. Overall number of years in the industry: * 1 point

Mark only one oval.

- ◯ Below 5 years
- ◯ 5 – 10 years
- ◯ 11 – 20 years
- ◯ 21 – 30 years
- ◯ Above 30 years

4. Position in the organization: *

Mark only one oval.

- ◯ Chief Executive Officer
- ◯ Specialist/Managing Director/General Manager
- ◯ Production Engineer/Engineer
- ◯ Manager/ Human Resource Manager

5. Others (please specify):

_____

6. Location of your organization in Malaysia (Please specify the state only): *

Mark only one oval.

- Perlis
- Kedah
- Penang
- Perak
- Selangor
- Negeri Sembilan
- Melaka
- Johor
- Pahang
- Terengganu
- Kelantan
- Sabah
- Sarawak
- Federal Territory of Kuala Lumpur
- Federal Territory of Putrajaya
- Federal Territory of Labuan

7. Expertise according to the Division in the Malaysia Standard Industrial Classification (MSIC) 2008 *

Mark only one oval.

- B09 – Mining Support Service Activities
- C15 - Manufacturing of Leather and Related Product
- C16 - Manufacture of Wood and Products of Wood and Cork, except furniture; Manufacture of articles of straw and plating materials.
- C17 – Manufacture of paper And paper products
- N80 – Security and investigation activities
- N81 – Service to buildings and landscape activities

8. Expertise according to Group in the Malaysia Standard Industrial Classification (MSIC) 2008 *

Mark only one oval.

- B091 – Support activities for Petroleum and Natural Gas Extraction
- B099 – Support activities for other mining and quarrying
- C151 – Tanning and dressing of leather; manufacture of luggage, handbags, saddlery and harness; dressing and dyeing of furon 3
- C152 – Manufacture of footware
- C161 – Sawmilling and planing of wood
- C162 – Manufacture of products of wood, cork, straw, and plaiting materials
- C170 – Manufacture of paper and paper products
- N801 – Private security activities
- N802 – Security systems service activities
- N803 – Investigation activities
- N811 – Combined facilities support activities
- N812 – Cleaning activities
- N813 – Landscape care and maintainence service activities

9. Expertise according to Group in the Malaysia Standard Industrial Classification (MSIC) 2008 *

Mark only one oval.

- ◯ B091 – Support activities for Petroleum and Natural Gas Extraction
- ◯ B099 – Support activities for other mining and quarrying
- ◯ C151 – Tanning and dressing of leather; manufacture of luggage, handbags, saddlery and harness; dressing and dyeing of furon 3
- ◯ C152 – Manufacture of footware
- ◯ C161 – Sawmilling and planing of wood
- ◯ C162 – Manufacture of products of wood, cork, straw, and plaiting materials
- ◯ C170 – Manufacture of paper and paper products
- ◯ N801 – Private security activities
- ◯ N802 – Security systems service activities
- ◯ N803 – Investigation activities
- ◯ N811 – Combined facilities support activities
- ◯ N812 – Cleaning activities
- ◯ N813 – Landscape care and maintainence service activities

COMPETENCY IN DEMAND

INSTRUCTIONS: For each of the statements please indicate your level of agreement by selecting only one of the choices based on the Fuzzy scale below:

Strongly Disagree : 1
Disagree : 2
Moderately Agree : 3
Agree : 4
Strongly Agree : 5

According to your expert opinion, rank your agreement that the following competency is important to perform these jobs.

Knowledge (refer to Dictionary competency/ OR)

10. Monitoring and analyzing activities *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

11. Surveillance operative *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

12. Data collection and analysis *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

13. Maintaining detailed records *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

14. Research and analyze data patterns *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

15. Evidence gathering *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

16. Legal and ethical standards *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

17. Investigative protocols *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

18. Cost and profitability *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

19. Risk Assessment and Mitigation *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

Skills

20. Interpersonal Communication *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

21. Written Communication *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

22. Critical Thinking *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

23. Problem Solving *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

24. Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

25. Leadership *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

26. Time management *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

27. Aptitude for Technology and Equipment *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

28. Intrapreneurship (Refers to employee initiatives in organisations to take something new, without being asked to do so) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

29. Others (please specify)

_____

Attribute/Attitude (General)

30. Attention to details *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

31. Team work *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

32. Multi-tasking/ Flexibility *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

33. Dependability (Trustworthy & Reliable) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

34. Work Ethics *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

35. Professionalism *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

36. Self-management/ independent *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

37. Self-learning *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

38. Agility (Ability to think and understand quickly) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

39. Ego-management (An exaggerated sense of self-worth based on one's extrinsic achievement) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

40. Career-management (career path and individual development, succession planning) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

41. Others (please specify)

_____

According to your expert opinion, rank your agreement on the reason(s) for the skills gap.

42. Education or training mismatch *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

43. Major changes in traditional training and new skills requirements *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

44. Attitude (for example, lack of desire to work) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

45. Misalignment between how job seekers are communicating their skills in their CV *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

46. Employers do not clarify the skills they require in the job specifications in the job advertisement *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

47. Others (please specify)

_____

EMERGING SKILLS

Emerging skills are skills that are expected to be important to the industry in the near future based on recent events, trends, government policies, or research. For example, the technology revolution, issues of sustainability, and many other things are examples of emerging skills.

According to your expert opinion, rank your agreement on the future emerging skills that affect the productivity of your current job.

48. Drawing / designing 3D, Designing virtual environments, Applying virtual reality to training and design. Designing simulations, Designing artificial intelligent *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

49. Design/Apply Green technology principles *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

50. Digital skills *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

51. Design/ Utilize software for autonomous technology, machine learning, data automation, and Internet of things (IoT) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

52. Environmental, social and governance (ESG) *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

53. Design / Apply Robotics and Electronics *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

54. Other *(please specify)*:

_____

OCCUPATION RELATED TO TECHNOLOGY

According to your expert opinion, rank your agreement on the technology.

55. The Industrial Revolution would have an impact on this industry *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

56. Technology advancement directly affects the jobs in the industry *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

According to your expert opinion, rank your agreement on the technology that is influencing your industry/ job area.

57. Autonomous Robots *
(Coordinated and automated actions of robots to complete tasks intelligently, with minimal human input)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

58. Big Data Analytics *

(The analysis of ever larger volumes of data. Circulation, collection, and analysis of information is a necessity because it supports productivity growth based on a real-time decision-making process)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

59. Cloud Computing *

(Storing and accessing data and programs over the Internet instead of your computer's hard drive)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

60. Internet of Things (IoT) *

(All machines and systems connected to the production plant (as well as other systems) must be able to collect, exchange and save these massive volumes of information, in a completely autonomous way and without the need of human intervention)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

61. Additive Manufacturing (3D Printing) *

(Use in prototyping, design iteration and small scale production and often described as “rapid prototyping” - produce the desired components faster, more flexibly and more precisely than ever before)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

62. System Integration *

(The process of linking together different computing systems and software applications physically or functionally to act as a coordinated whole via Internet of Things-IoT)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

63. Cybersecurity *

(With the increased connectivity and use of standard communications protocols, the need to protect critical industrial systems and manufacturing lines from cybersecurity threats is increasing)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

64. Augmented Reality *

(Augmented-reality-based systems support a variety of services, such as selecting parts in a warehouse and sending repair instructions over mobile devices - provide workers with real-time information to improve decision making and work procedures)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

65. Simulation *

(Simulations will leverage real-time data to mirror the physical world in a virtual model, which can include machines, products, and humans. This allows operators to test and optimize the machine settings for the next product in line in the virtual world before the physical changeover, thereby driving down machine setup times and increasing quality)

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

JOBS IN DEMAND (803) According to your expert opinion, rank your agreement on the high manpower shortage for these jobs.

a. Surveillance & Ground Investigation

66. Senior Operative *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

67. Junior Operative *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

b. Research & Analyst

68. Senior Analyst *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

69. Junior Analyst *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

c. Verify and Authenticate Information

70. Team Leader *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

Untitled Title

d. Project Management

71. Project Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

e. Corporate and Project Management

72. General Manager *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

73. State the reason for the high shortage of the Jobs-in demand

RELATED ISSUES

According to your expert opinion, rank your agreement on the key issues affecting the workforce of the industry.

74. Insufficient number of skilled workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

75. Insufficient number of certified workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

76. Insufficient number of competence workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

77. High dependence on foreign labor *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

78. Talent Gap among graduates *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

79. Underpayment of wages leads to high turnover *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

80. Adaptation to technological changes *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

81. Poor facilities and amenities for workers *

Mark only one oval.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

82. Others (please specify)

ANNEX 2 : OCCUPATIONAL DESCRIPTION

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILITY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Guarding Services (GS)
JOB TITLE : GS Security Manager
LEVEL : 5

RESPONSIBILITIES:

The GS Security Manager plays a key role in overseeing and managing the entire security team. Their responsibilities include developing and implementing security policies and procedures, conducting risk assessments and security audits, and providing leadership and guidance to security personnel. The manager monitors and analyzes security trends and incidents, coordinates with law enforcement and regulatory agencies, and implements training programs for security staff. Additionally, they ensure compliance with security standards and regulations to maintain a robust and effective security framework.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILITY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Guarding Services (GS)
JOB TITLE : GS Security Executive
LEVEL : 4

RESPONSIBILITIES:

The GS Security Executive is responsible for implementing security measures and protocols, monitoring security systems, and responding to alarms. They conduct security briefings for staff and collaborate with external security agencies. The executive performs risk assessments and vulnerability analyses, handles access control and identity verification processes, and investigates security incidents, preparing comprehensive reports. Additionally, they ensure emergency response and crisis management procedures are in place and maintain accurate documentation of all security activities.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILITY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Guarding Services (GS)
JOB TITLE : GS Security supervisor
LEVEL : 3

RESPONSIBILITIES:

The GS Security Supervisor oversees security officers and guard operations, ensuring the enforcement of security policies and procedures. They conduct regular security drills, analyze security data for trends, and contribute to the development of security training programs. The supervisor responds to and manages security incidents, coordinates with law enforcement and regulatory authorities, and maintains accurate documentation and records. Additionally, they conduct routine inspections and patrols to maintain a high level of security effectiveness.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILITY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Guarding Services (GS)
JOB TITLE : GS Security officer
LEVEL : 2

RESPONSIBILITIES:

The GS Security Officer is responsible for implementing security measures to safeguard premises and assets. They conduct screenings of individuals and belongings, monitor surveillance systems for unusual activities, and enforce access control and identification procedures. The officer reports and responds to security incidents, ensures the implementation of security training programs, and conducts routine patrols and inspections. Additionally, they provide assistance during emergencies to maintain a secure environment.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILITY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Guarding Services (GS)
JOB TITLE : GS Assistant Security Officer
LEVEL : 1

RESPONSIBILITIES:

The GS Assistant Security Officer supports the implementation of security protocols, performs screenings and inspections, and monitors surveillance cameras for suspicious activities. They assist in emergency response and evacuation procedures, support senior security personnel in daily operations, and conduct routine security patrols. Additionally, they participate in security drills and exercises, ensuring accurate records of all security activities are maintained.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILITY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Armed Guarding (AG)
JOB TITLE : AG Supervisor
LEVEL : 3

RESPONSIBILITIES:

The AG Supervisor is responsible for leading and supervising an armed security team, providing guidance to officers, conducting briefings, overseeing training, and ensuring proficiency in firearm use. They plan and organize security operations, develop strategies for potential threats, and coordinate with other departments for seamless integration. Additionally, they conduct risk assessments, implement mitigation strategies, and coordinate emergency response plans. The supervisor ensures compliance with legal requirements, stays updated on relevant laws, maintains firearms and equipment, conducts readiness checks, oversees incident documentation, and prepares detailed security reports.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Armed Guarding (AG)
JOB TITLE : AG Security Officer
LEVEL : 2

RESPONSIBILITIES:

Responsibilities include conducting armed patrols to secure assigned areas, monitoring surveillance systems for unusual activities, enforcing access control measures to ensure only authorized personnel enter designated areas, verifying identification and credentials of individuals, identifying potential security threats and risks, responding promptly to alarms and security breaches, responding to emergencies with appropriate use of force if necessary, implementing emergency evacuation procedures, providing a visible and professional security presence, offering assistance and information to employees and visitors, maintaining effective communication with team members and supervisors using two-way radios and other communication devices, possessing and using firearms responsibly and safely, following proper procedures for carrying and using weapons, and recording and reporting all security-related incidents, completing detailed incident reports as necessary.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Close Protection (CP)
JOB TITLE : CP Manager
LEVEL : 5

RESPONSIBILITIES:

The responsibilities include developing and implementing strategic plans for close protection operations, collaborating with clients and security teams to understand specific protection needs, conducting comprehensive risk assessments for clients and their environments, formulating strategies to mitigate potential threats, recruiting, training, and managing a team of close protection personnel, assigning duties and responsibilities to ensure effective protection, coordinating closely with local law enforcement and relevant authorities, overseeing the planning and execution of protection operations, maintaining regular communication with clients to understand their security concerns, providing updates on security measures and potential risks, developing and implementing emergency response plans, coordinating responses to security incidents or threats, planning logistics for client movements, events, or travel, ensuring the availability of necessary equipment and resources, ensuring compliance with legal and regulatory requirements related to close protection, and staying informed about changes in security laws and regulations.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Close Protection (CP)
JOB TITLE : CP Executive
LEVEL : 4

RESPONSIBILITIES:

The responsibilities include providing close protection to clients in various environments, accompanying clients during travel, events, and daily activities, continuously assessing potential threats and risks, adjusting protection strategies based on changing circumstances, maintaining clear and constant communication with the close protection team, coordinating with the Close Protection Manager and other team members, conducting surveillance and monitoring of the client's surroundings, identifying and responding to any suspicious activities, and being prepared to respond swiftly to emergencies, including implementing emergency evacuation or protection measures as needed.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Close Protection (CP)
JOB TITLE : CP Senior Bodyguard
LEVEL : 3

RESPONSIBILITIES:

The responsibilities include executing close protection duties based on assigned roles and responsibilities, providing physical protection, and ensuring the safety of the client. The role also involves leading and guiding junior members of the close protection team, assisting in coordinating protection efforts during assignments, interacting with the client professionally and discreetly, addressing client concerns, ensuring advance planning for client movements or events, and conducting reconnaissance to assess potential risks.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Close Protection (CP)
JOB TITLE : CP Bodyguard
LEVEL : 2

RESPONSIBILITIES:

The responsibilities include providing immediate and direct physical protection to the client, accompanying the client during travel and public appearances, observing and reporting any unusual activities or potential threats, maintaining vigilance to prevent security breaches, staying in constant communication with other members of the protection team, using communication devices effectively, and following established protocols for emergency response. The CP Bodyguard is also responsible for implementing evacuation or protection measures as directed.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Cash Management (CM)
JOB TITLE : CM Supervisor
LEVEL : 3

RESPONSIBILITIES:

The responsibilities include supervising and leading a team of security personnel involved in cash management activities, assigning tasks and responsibilities to ensure efficient operations, ensuring compliance with established cash handling and security protocols, enforcing adherence to standard operating procedures, providing training to security staff on cash management procedures, conducting regular drills and training sessions to enhance skills, overseeing security measures related to the transportation and handling of cash, implementing strategies to safeguard assets against theft or unauthorized access, developing and implementing emergency response plans for cash-related incidents, coordinating with local law enforcement when necessary, ensuring proper maintenance and functionality of security equipment used in cash management, conducting regular checks on surveillance systems, alarms, and other security devices, monitoring and controlling inventory of cash-related supplies and equipment, replenishing resources as needed to maintain operational readiness, interacting with clients to understand their specific cash management requirements, and providing updates and reports on security measures.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Cash Management (CM)
JOB TITLE : CM Security Officer
LEVEL : 2

RESPONSIBILITIES:

The responsibilities include safely handling and transporting cash according to established protocols, following security procedures during cash-in-transit or cash handling operations, monitoring and observing cash management activities through surveillance systems, identifying and reporting any suspicious activities or security breaches, assisting clients during cash-related transactions, providing a visible security presence to deter potential threats, maintaining clear and timely communication with team members and supervisors, using communication devices effectively during operations, and completing and maintaining accurate records of cash management activities. Additionally, preparing reports on incidents, discrepancies, or security concerns is a part of the role.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Cash Management (CM)
JOB TITLE : CM Assistant Security officer
LEVEL : 1

RESPONSIBILITIES:

The responsibilities include assisting in various functions related to cash management security, supporting supervisors and security officers in day-to-day operations, following established security procedures for cash handling and transportation, learning and adhering to standard operating protocols, assisting in the maintenance and inspection of security equipment, reporting issues with surveillance systems or alarms, participating in emergency response drills and activities, being prepared to assist during emergencies, observing and reporting security-related incidents or concerns, and maintaining vigilance to prevent unauthorized access to cash or valuables.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : K9 Service (K9)
JOB TITLE : K9 Security Officer
LEVEL : 2

RESPONSIBILITIES:

The responsibilities include training and handling police dogs, engaging in patrol and detection activities, participating in search and rescue operations, apprehending suspects, engaging with the community, maintaining equipment, writing reports, undergoing continued training, adhering to laws and regulations, and collaborating closely with other law enforcement officers.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Alarm Monitoring (AM)
JOB TITLE : AM Supervisor
LEVEL : 3

RESPONSIBILITIES:

The responsibilities include providing leadership and guidance to the alarm monitoring team, overseeing the work of alarm monitoring security officers, ensuring ongoing training for all alarm monitoring officers, creating and managing work schedules, monitoring the performance of alarm monitoring officers, providing technical assistance, overseeing the response to alarm activations, maintaining accurate records of activities and incidents, ensuring alignment with company policies, identifying areas for improvement in procedures, and maintaining effective communication with other security personnel.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Alarm Monitoring (AM)
JOB TITLE : AM Security Officer
LEVEL : 2

RESPONSIBILITIES:

The responsibilities include monitoring alarm systems, responding promptly to alarm activations, relaying information to supervisors, recording details of alarm activations, troubleshooting technical issues related to alarm systems, conducting visual surveillance of monitored premises through security cameras and other monitoring tools, providing assistance and support, following established procedures and protocols, and ensuring the proper functioning and maintenance of alarm monitoring equipment.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Maritime Security
JOB TITLE : Maritime Operation Manager
LEVEL : 5

RESPONSIBILITIES:

The responsibilities include providing special briefings to the Team Leader of the Maritime operations team, communicating directly with the Operations Room and Maritime Team Leader, holding operational briefings as required by management, being ready at all times to issue appropriate instructions, fully understanding journeys, statistics, expectations, and adhering to maritime operational procedures during threats, ensuring the details of reports received are authentic and complete before issuing orders, issuing appropriate instructions according to relevant guidelines and laws during incidents, ensuring all land support assistance and various appropriate assistance, and submitting complete details of incident reports and work completion reports to relevant parties.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Maritime Security
JOB TITLE : Maritime Control Centre Supervisor
LEVEL : 4

RESPONSIBILITIES:

The responsibilities include general security monitoring, preparing and organizing the Operation Room according to the S.O.P., ensuring all points of contact according to the identified checklist, updating all information and notifications according to the checklist, acting as an intelligence officer, updating all Human Reliability Analysis (HRA) and latest events, advising the appropriate direction according to the threat received, channeling authentic information about the incident to relevant channels, issuing appropriate instructions to the monitoring team and the maritime security team, and providing complete reports to management, clients, and relevant security bodies.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Maritime Security
JOB TITLE : Maritime Team Leader
LEVEL : 3

RESPONSIBILITIES:

The responsibilities include detecting security threats, managing security personnel in security surveillance, advising the vessel master on the action to be taken, coaching security personnel, conducting team briefings, supervising security personnel, compiling incident reports, executing evacuation plans or exercises, handling medical incidents, and providing relevant information required by Ops Room officers related to case management.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Maritime Security
JOB TITLE : Maritime Unit Leader
LEVEL : 2

RESPONSIBILITIES:

The responsibilities include providing concierge security services, attending to inquiries from the Vessel Master and Ops Room Officer, managing assignments and supervision, ensuring accurate reports are delivered promptly, detecting security threats, carrying out instructions from the Team Leader, performing security surveillance on board the vessel, ensuring communication tools operate well and are ready to use, assisting the ship's crew in law enforcement, providing a quick response to incidents and emergencies, and being ready to act according to the right channel.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities
OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Maritime Security
JOB TITLE : Maritime Ship Security Officer / Maritime Operating Room Officer
LEVEL : 1

RESPONSIBILITIES:

The responsibilities include providing general security services, carrying out monitoring tasks as directed, assisting in delivering situation reports according to SOP (Standard Operating Procedure), monitoring environmental activities, detecting security threats, assisting the Unit Leader in responding to and reporting incidents, performing security coverage, closely monitoring all threats, managing incidents, providing quick response to incidents and emergencies, assisting authorities during incidents, and being ready to take defensive action according to R.O.E (Rules of Engagement).

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Aviation Security (Avsec) (Operation, Intelligent and investigation)
JOB TITLE : Avsec Senior Specialist
LEVEL : 7

RESPONSIBILITIES:

As an Avsec Senior Specialist, responsibilities include developing and implementing aviation security policies and procedures, overseeing and managing security programs at airports, conducting risk assessments and threat analyses, collaborating with regulatory agencies to ensure compliance with aviation security standards, providing leadership and guidance to security personnel, investigating security incidents and breaches, implementing training programs for security staff, and staying updated on the latest security technologies and industry best practices.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Aviation Security (Avsec) (Operation, Intelligent and investigation)
JOB TITLE : Avsec Specialist
LEVEL : 6

RESPONSIBILITIES:

As an Avsec Specialist, responsibilities include implementing security measures to safeguard airport facilities and operations, conducting security inspections and audits, monitoring and analyzing security threats and trends, coordinating with relevant enforcement and regulatory agencies, training airport staff on security protocols, responding to and managing security incidents, ensuring compliance with aviation security regulations, and conducting security drills and exercises.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Aviation Security (Avsec) (Operation, Intelligent and investigation)
JOB TITLE : Avsec senior executive
LEVEL : 5

RESPONSIBILITIES:

As an Avsec Senior Executive, responsibilities include assisting in the development and implementation of security strategies, supervising security personnel and operations, conducting regular security assessments and audits, coordinating with other departments to address security concerns, managing access control systems and surveillance technologies, investigating security incidents and preparing reports, providing training and awareness programs for employees, and ensuring compliance with aviation security policies.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Aviation Security (Avsec) (Operation, Intelligent and investigation)
JOB TITLE : Avsec Executive
LEVEL : 4

RESPONSIBILITIES:

The responsibilities include implementing security measures and protocols at airports, monitoring security systems, and responding to alarms. The Executive conducts security briefings for airport staff, collaborates with external security agencies, and performs risk assessments and vulnerability analyses. Additionally, the position involves handling access control and identity verification processes, investigating security incidents, preparing reports, and ensuring effective emergency response and crisis management.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Aviation Security (Avsec) (Operation, Intelligent and investigation)
JOB TITLE : Avsec Senior Officer
LEVEL : 3

RESPONSIBILITIES:

The key responsibilities involve supervising security operations at airports and ensuring the enforcement of security policies and procedures. The role includes conducting regular security drills and exercises, monitoring and analyzing security data for trends, and actively participating in the development of security training programs. The Senior Officer responds to and manages security incidents, coordinates with law enforcement and regulatory authorities, and maintains comprehensive documentation and records related to security activities to uphold a high standard of airport security.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Aviation Security (Avsec) (Operation, Intelligent and investigation)
JOB TITLE : Avsec Officer
LEVEL : 2

RESPONSIBILITIES:

The primary responsibilities include implementing security measures to safeguard airport assets, conducting security screenings of passengers and baggage, and monitoring surveillance systems for any unusual activities. The officer enforces access control and identification procedures, promptly reporting and responding to security incidents. Additionally, ensuring the effectiveness of security training programs and conducting routine patrols and inspections are integral aspects of the role to maintain a high level of security at the airport.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 801 (Private Security Activities)
AREA : Aviation Security (Avsec) (Operation, Intelligent and investigation)
JOB TITLE : Avsec Assistant
LEVEL : 1

RESPONSIBILITIES:

The role involves supporting the implementation of security measures through various tasks. This includes assisting in the implementation of security protocols, performing security screenings and inspections, and monitoring surveillance cameras to report any suspicious activities. The assistant plays a key role in emergency response and evacuation procedures and supports senior security personnel in their daily operations. Routine security patrols are conducted, and assistance is provided during security drills and exercises. Additionally, maintaining accurate records of all security activities is a crucial aspect of the role.

Knowledge:

• Security threats • Security personnel • Medical incidents • Case management • Security surveillance • Closed-Circuit Television (CCTV) • Incidents and emergencies • Traffic and crowds • Security stakeholders • Situational trend analyses • Security operation audits • Security risks • Law enforcement

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Ego-management (An exaggerated sense of self-worth based on one’s extrinsic achievement)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)
AREA : Security System Surveillance Operator
JOB TITLE : Assistant Manager/ Supervisor
LEVEL : 5

RESPONSIBILITIES:

Assistant Managers/Supervisors in security play a crucial role in overseeing surveillance operations. They lead the monitoring of security systems, including various technology platforms, sensors, cameras, alarms, drones, robotics, and access control systems. These professionals plan and manage surveillance equipment to ensure continuous monitoring of designated areas. They actively coordinate with other security personnel and law enforcement during incidents or emergencies. Additionally, Assistant Managers/Supervisors are responsible for coordinating security incident reporting, maintaining accurate records of activities during shifts. They strategically plan routine maintenance and checks on surveillance equipment to ensure its proper functioning. Moreover, these individuals contribute to the planning and execution of training programs for new surveillance operators, covering protocols, equipment operation, and security procedures.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)
AREA : Security System Surveillance Operator
JOB TITLE : Senior Executives
LEVEL : 4

RESPONSIBILITIES:

They design surveillance operations, overseeing the monitoring of security systems encompassing technology platforms, sensors, cameras, alarms, drones, robotics, and access control systems. These executives take a leadership role in mobile surveillance efforts to identify and respond to suspicious or unauthorized activities. They verify the functionality of surveillance equipment for continuous monitoring, coordinating with security personnel and law enforcement during incidents or emergencies. Senior Executives approve security incident reports, maintaining accurate records of activities during shifts. They also ensure routine maintenance and checks on surveillance equipment for proper functioning and verify training programs for new surveillance operators, covering protocols, equipment operation, and security procedures.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)
AREA : Security System Surveillance Operator
JOB TITLE : Executives
LEVEL : 3

RESPONSIBILITIES:

Executives are responsible for overseeing and managing surveillance operations, which includes monitoring security systems like technology platforms, sensors, cameras, alarms, drones, robotics, and access control systems. They strategically plan mobile surveillance activities to identify and respond to any suspicious or unauthorized activities on premises. Executives organize and manage surveillance equipment to ensure continuous monitoring of designated areas, validating security incidents and maintaining accurate records of activities during shifts. Additionally, they coordinate routine maintenance checks on surveillance equipment to ensure proper functioning. Executives also play a crucial role in conducting training for new surveillance operators, covering protocols, equipment operation, and security procedures.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)
AREA : Security System Surveillance Operator
JOB TITLE : Senior Operator
LEVEL : 2

RESPONSIBILITIES:

The key responsibilities involve overseeing and ensuring the effectiveness of surveillance operations. This includes monitoring a range of security systems, such as technology platforms, sensors, cameras, alarms, drones, robotics, and access control systems. The Senior Operator supervises mobile surveillance of premises to promptly identify and respond to any suspicious or unauthorized activities. They play a crucial role in communication, promptly responding to security alarms, incidents, and emergencies as per established procedures. Additionally, the Senior Operator supervises and manages surveillance equipment to guarantee continuous monitoring of designated areas. Maintenance checks on surveillance equipment are conducted regularly to ensure proper functioning, and meticulous records of security incidents and activities during shifts are maintained.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Surveillance Operator

JOB TITLE : Operator

LEVEL : 1

RESPONSIBILITIES:

In the role of an Operator, responsibilities include performing surveillance operations by monitoring various security systems such as technology platforms, sensors, cameras, alarms, drones, robotics, and access control systems. The operator engages in mobile surveillance of premises, promptly responding to any suspicious or unauthorized activities. Additionally, they are responsible for quick responses to security alarms, incidents, and emergencies, following established procedures. The operator ensures continuous monitoring of designated areas through the operation of surveillance equipment. Thorough documentation is maintained, with accurate records of security incidents and activities during shifts. Routine maintenance and checks on surveillance equipment are conducted to ensure proper functioning and overall effectiveness of the security systems.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Analyst

JOB TITLE : Specialist/ Senior Security Solutions/ Senior Manager

LEVEL : 7

RESPONSIBILITIES:

The individual is responsible for developing a comprehensive program to assess security threats, vulnerabilities, and risks to identify potential weaknesses in the security infrastructure. They lead the development of advanced security systems, networks, and applications to detect unauthorized access and potential breaches. The manager verifies security incidents, analyzes data logs, and produces detailed reports, contributing to a proactive response to potential security threats. Collaboration with technical teams is essential for planning and implementing security measures to ensure compliance with policies. Additionally, the role involves strategic planning for security assessments and audits to evaluate the effectiveness of existing controls. The individual innovates in alignment with emerging security trends, tools, and techniques to proactively address new threats and contributes to the development of incident response plans and protocols. Ensuring a security-conscious culture, the manager verifies security awareness training to employees. This role combines strategic planning, leadership, innovation, and proactive measures to strengthen the organization's overall security posture.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Analyst

JOB TITLE : Manager / Security Solutions

LEVEL : 6

RESPONSIBILITIES:

The individual oversees comprehensive surveillance operations by leading the monitoring of security systems, technology platforms, sensors, cameras, alarms, drones, robotics, and access control systems. They plan and manage surveillance equipment to ensure continuous monitoring of designated areas, coordinating with other security personnel and law enforcement during incidents or emergencies. The manager plays a key role in incident reporting, ensuring accurate records of activities during shifts. Additionally, they strategically plan routine maintenance and checks on surveillance equipment to maintain proper functioning. Moreover, the manager is responsible for planning training programs for new surveillance operators, focusing on protocols, equipment operation, and security procedures. This role involves leadership, coordination, and strategic planning to ensure effective security solutions within the organization.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Analyst

JOB TITLE : Senior Analyst

LEVEL : 5

RESPONSIBILITIES:

The individual holds a senior-level position with a focus on evaluating security threats, vulnerabilities, and risks to identify potential weaknesses in the security infrastructure. They take on a supervisory role in overseeing security systems, networks, and applications to detect unauthorized access and potential breaches. Collaboration with technical teams is emphasized, and the Senior Analyst actively supervises the implementation of security measures to ensure compliance with security policies. The role includes a commitment to ensuring the effectiveness of security controls through regular security assessments and audits exercises. Additionally, the Senior Analyst is responsible for overseeing the development and execution of incident response plans and protocols, showcasing a leadership role in maintaining a robust and responsive security posture within the organization.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Analyst

JOB TITLE : Analyst

LEVEL : 4

RESPONSIBILITIES:

The individual is responsible for analyzing security threats, vulnerabilities, and risks to identify potential weaknesses in the security infrastructure. They conduct in-depth analysis of security systems, networks, and applications to detect unauthorized access and potential breaches. Coordination with technical teams is essential to implement security measures and ensure compliance with established security policies. The Analyst actively observes security assessments and audits exercises to evaluate the effectiveness of existing security controls. They also play a role in observing the development and execution of incident response plans and protocols. This role requires a keen analytical mindset, collaboration with technical teams, and a proactive approach to maintaining and enhancing security measures within the organization.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Technologist

JOB TITLE : Chief Technical Officer

LEVEL : 8

RESPONSIBILITIES:

The individual holds a strategic oversight role in ensuring the implementation of secure and resilient security systems, networks, and infrastructure. The CTO oversees the integration of various security tools, technologies, and components to create a cohesive and effective security environment. Implementation of encryption protocols, multi-factor authentication, and access controls to safeguard data and resources is a key responsibility. The CTO provides oversight on penetration testing and vulnerability assessments to identify and address weaknesses in security systems. Strategic planning and innovation in accordance with emerging security technologies are overseen, with recommendations for adoption based on organizational needs. The CTO ensures that technical teams operate seamlessly to integrate security measures into existing systems. This leadership role demands a combination of strategic vision, technical expertise, and a proactive approach to maintaining a robust and evolving security infrastructure aligned with organizational objectives.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Technologist

JOB TITLE : Specialist Technical Deployment

LEVEL : 7

RESPONSIBILITIES:

Individuals are responsible for developing secure and resilient security systems, networks, and infrastructure. This includes the development of various security tools, technologies, and components to create a cohesive and effective security environment. The specialist actively contributes to the development of security systems, firewalls, and intrusion detection/prevention systems in alignment with security policies. Verification of the implementation of encryption protocols, multi-factor authentication, and access controls is a critical aspect of safeguarding data and resources. The specialist validates penetration testing and vulnerability assessments to identify and address weaknesses in security systems. Innovation is emphasized, aligning with emerging security technologies, and providing recommendations for adoption based on organizational needs. Collaborative planning with other technical teams ensures the seamless integration of security measures into existing systems. This role requires a combination of technical expertise, innovation, and collaboration to deploy advanced security solutions effectively.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Technologist

JOB TITLE : Head Technical Operation Executives

LEVEL : 6

RESPONSIBILITIES:

Individuals are responsible for planning the implementation of secure and resilient security systems, networks, and infrastructure. This involves planning the integration of various security tools, technologies, and components to create a cohesive and effective security environment. Verification of the configuration of security systems, firewalls, and intrusion detection/prevention systems is conducted in alignment with security policies. The implementation of encryption protocols, multi-factor authentication, and access controls is verified to safeguard data and resources. Head Technical Operation Executives conduct penetration testing and vulnerability assessments to identify and address weaknesses in security systems. They actively research and evaluate emerging security technologies, providing recommendations for adoption based on organizational needs. Verification with other technical teams ensures the seamless integration of security measures into existing systems. The development of documentation of security configurations, procedures, and system designs for future reference showcases their commitment to maintaining a robust and well-documented security infrastructure. This leadership role demands strategic planning, advanced technical knowledge, and a forward-looking approach to security technology.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Technologist

JOB TITLE : Senior Technical Executives

LEVEL : 5

RESPONSIBILITIES:

Senior Technical Executives play a crucial role in evaluating the implementation of secure and resilient security systems, networks, and infrastructure. They verify the integration of various security tools, technologies, and components to create a cohesive and effective security environment. Configuration of security systems, firewalls, and intrusion detection/prevention systems is carried out in alignment with established security policies. Implementation of encryption protocols, multi-factor authentication, and access controls is a key aspect to safeguard data and resources. Senior Technical Executives actively evaluate penetration testing and vulnerability assessments to identify and address weaknesses in security systems. They supervise the implementation with other technical teams, ensuring seamless integration of security measures into existing systems. The evaluation of documentation of security configurations, procedures, and system designs for future reference underscores their commitment to maintaining a high standard of security infrastructure. This role demands advanced technical expertise, leadership, and a proactive approach to security measures.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Technologist

JOB TITLE : Technical Executives

LEVEL : 4

RESPONSIBILITIES:

The individuals are tasked with implementing secure and resilient security systems, networks, and infrastructure. This involves integrating various security tools, technologies, and components to create a cohesive and effective security environment. Monitoring the implementation of security systems, firewalls, and intrusion detection/prevention systems is crucial, ensuring alignment with established security policies. Coordination with other technical teams is emphasized to ensure the seamless integration of security measures into existing systems. The Technical Executives are responsible for comprehensive documentation of security configurations, procedures, and system designs, ensuring future reference and facilitating effective management of security infrastructure. This role requires a combination of technical expertise, collaboration, and proactive measures to establish and maintain a robust security environment.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 802 (Security Systems Service Activities)

AREA : Security System Technologist

JOB TITLE : System Admin

LEVEL : 3

RESPONSIBILITIES:

The individual is responsible for the administration, configuration, and maintenance of security systems, encompassing surveillance cameras, access control systems, and alarms. Their duties involve ensuring the proper functioning of both security software and hardware. Management of user accounts and permissions for security systems is a key aspect, with a focus on providing access to authorized personnel and restricting access as necessary. The System Admin identifies and resolves technical issues promptly, conducts regular system checks and diagnostics, and keeps security software up-to-date with the latest patches and updates. They actively test and implement new features or enhancements, implementing measures to secure and protect data collected by security systems. Backup procedures are in place to prevent data loss in case of system failure. The System Admin maintains accurate documentation of security system configurations, changes, and updates, creating user manuals or guides for system operation. Regular security audits of system configurations and access logs are conducted to identify vulnerabilities, and corrective actions are implemented. Coordination with vendors for technical support and issue resolution is part of their responsibilities, showcasing a proactive approach to ensuring the security and reliability of the systems they administer.

Knowledge:

• Security system • Planning & Designing • Project Management • Security infrastructure • Security controls • Security policies.

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Agile Mindset (A thought process that involves understanding, collaborating, learning, and staying flexible to achieves high performing results) • Leadership • Time management • Aptitude for Technology and Equipment • Intrapreneurship

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly) • Career-management

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 803 (Investigation Activities)

AREA : Surveillance Investigation

JOB TITLE : Investigation Technical Team Leader

LEVEL : 7

RESPONSIBILITIES:

The individual holds a strategic role in designing a technical investigation team. They provide guidance and mentorship to team members, overseeing the planning and execution of complex investigations. Ensuring adherence to established protocols and procedures is a key responsibility. The team leader actively designs investigative technologies and tools, analyzing technical data and digital evidence to support investigations. They interpret findings and formulate recommendations, emphasizing the development of investigation techniques. The team leader is involved in preparing detailed and accurate procedures, verifying reports, and assessing investigative outcomes. Corporate investigations, spanning technical forensic, audit forensic, financial investigation, and IT investigation, fall within the purview of their responsibilities, showcasing a leadership role in the application of advanced technical expertise to investigative processes.

Knowledge:

• Monitoring and analyzing activities • Data collection and analysis • Maintaining detailed records • Research and analyze data patterns • Evidence gathering • Legal and ethical standards • Investigative protocols • Cost and profitability • Risk Assessment and Mitigation

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 803 (Investigation Activities)

AREA : Surveillance Investigation

JOB TITLE : Investigation Team Leader

LEVEL : 6

RESPONSIBILITIES:

The individual oversees and supervises a team of investigators, allocating tasks and ensuring adherence to investigative standards. They actively manage the progress of investigations, ensuring timelines are met and prioritizing cases based on urgency and impact. Effective resource allocation is a key responsibility to support investigations efficiently. The team leader ensures proper documentation of investigative processes and findings, maintaining records and case files. Additionally, they provide support for cross-functional investigations, verifying quality checks on investigative work and implementing corrective actions as needed. The team leader may also personally conduct investigations, particularly in matrimonial cases, showcasing a hands-on and leadership-oriented approach to ensuring the success and integrity of investigative efforts.

Knowledge:

• Monitoring and analyzing activities • Data collection and analysis • Maintaining detailed records • Research and analyze data patterns • Evidence gathering • Legal and ethical standards • Investigative protocols • Cost and profitability • Risk Assessment and Mitigation

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 803 (Investigation Activities)

AREA : Surveillance Investigation

JOB TITLE : Investigation Senior Analyst

LEVEL : 5

RESPONSIBILITIES:

The individual holds a pivotal role in analyzing data and evidence related to investigations. They provide expert insights into complex cases, spanning technical forensic, audit forensic, financial investigation, and IT investigation domains. The senior analyst is responsible for preparing detailed reports summarizing investigative findings, ensuring clarity and accuracy in documentation. Handling and securing both physical and digital evidence are crucial aspects, with a commitment to following chain of custody protocols. In legal proceedings, the senior analyst may provide expert testimony and effectively communicate findings to legal professionals. This role demands a high level of expertise, attention to detail, and effective communication skills in contributing to the resolution of complex investigative cases.

Knowledge:

• Monitoring and analyzing activities • Data collection and analysis • Maintaining detailed records • Research and analyze data patterns • Evidence gathering • Legal and ethical standards • Investigative protocols • Cost and profitability • Risk Assessment and Mitigation

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 803 (Investigation Activities)

AREA : Surveillance Investigation

JOB TITLE : Investigation Junior Analyst

LEVEL : 4

RESPONSIBILITIES:

The individual is tasked with collecting and compiling relevant data for investigations. They play a supporting role in the analysis of evidence and maintain accurate records of investigative activities. The junior analyst assists senior analysts in the preparation of reports, contributing to the overall investigative process. Additionally, they engage in research on emerging investigative methodologies, staying informed about the latest trends and techniques. The role involves active participation in cross-functional initiatives, showcasing a collaborative approach to investigative work. Overall, the Investigation Junior Analyst contributes to the investigative team by handling data, supporting analysis, and staying updated on evolving investigative practices.

Knowledge:

• Monitoring and analyzing activities • Data collection and analysis • Maintaining detailed records • Research and analyze data patterns • Evidence gathering • Legal and ethical standards • Investigative protocols • Cost and profitability • Risk Assessment and Mitigation

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 803 (Investigation Activities)

AREA : Surveillance Investigation

JOB TITLE : Investigation Senior Operative

LEVEL : 3

RESPONSIBILITIES:

The individual is responsible for conducting field investigations and gathering on-site information. Adherence to safety and legal protocols is paramount throughout the investigative process. The operative performs surveillance activities as directed by team leaders, meticulously recording observations and activities. Effective communication with team members and leadership is emphasized, with timely updates on fieldwork provided. The role includes recording findings and submitting reports, with a specific focus on ensuring accuracy and completeness in cases involving matrimonial matters. Moreover, a commitment to ethical and legal standards is maintained by following established standard operating procedures throughout the investigative work. This position requires a combination of investigative skills, attention to detail, and a commitment to professional standards.

Knowledge:

• Monitoring and analyzing activities • Data collection and analysis • Maintaining detailed records • Research and analyze data patterns • Evidence gathering • Legal and ethical standards • Investigative protocols • Cost and profitability • Risk Assessment and Mitigation

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly)

N80- Security and Investigation Activities

OCCUPATIONAL RESPONSIBILTY (OR)

MSIC GROUP : 803 (Investigation Activities)

AREA : Surveillance Investigation

JOB TITLE : Investigation Junior Operative

LEVEL : 2

RESPONSIBILITIES:

The role involves actively assisting in field investigations and gathering information. This includes ensuring surveillance activities are carried out effectively, with a focus on meticulously documenting observations. Accuracy and prompt reporting of findings are crucial aspects of the job. The individual maintains effective communication within the investigative team, providing regular updates on field activities and observations. Interpretation of assigned tasks and activities as integral to the investigation is emphasized. Additionally, the role includes contributing to the preparation of comprehensive field reports and actively participating in training sessions to enhance skills and knowledge. This multifaceted position underscores the importance of attention to detail, effective communication, and continuous improvement in contributing to the success of field investigations.

Knowledge:

• Monitoring and analyzing activities • Data collection and analysis • Maintaining detailed records • Research and analyze data patterns • Evidence gathering • Legal and ethical standards • Investigative protocols • Cost and profitability • Risk Assessment and Mitigation

Skills:

• Interpersonal Communication • Written Communication • Critical Thinking • Problem Solving • Time management • Aptitude for Technology and Equipment

Attributes:

• Attention to details • Team work • Multi-tasking/ Flexibility • Dependability (Trustworthy & Reliable) • Work Ethics • Professionalism • Self-management/ independent • Self-learning • Agility (Ability to think and understand quickly)

ANNEX 3 : LIST OF CONTRIBUTERS

N80 - SECURITY AND INVESTIGATION ACTIVITIES

RESEARCHERS

NO.	NAME	POSITION	ORGANISATION
1	Prof. Dr Norlidah Alias	Lead Researcher	UPUM Sdn. Bhd.
2	Assoc. Prof. Dr Zainuddin Ibrahim	Researcher	UITM
3	Assoc. Prof. Dr Hutkemri Zulnaidi	Researcher	UPUM Sdn. Bhd.
4	Ts. Ihsanulfitri Zahedi	Project Manager	UPUM Sdn. Bhd.

EXPERT PANELIST

NO.	NAME	POSITION	ORGANISATION
1	Dato' Habibullah Bin Dato' Haji Ahmad	Setiausaha Kehormat	Class A Security Sdn Bhd
2	En. Che Mohamad Noor Husain	Pengerusi Negeri Terengganu	Bintara Camar Security Sdn Bhd
3	Puan Siti Subaidah Mustaffa	Pengarah Urusan	Corporate Risks Consulting Sdn Bhd
4	Tuan Jeff Nor Jettey	Pengurus Besar	Persatuan Industri Keselamatan Malaysia
5	En. Paramjeet Singh	Pengarah	MVD International Sdn Bhd
6	Lt. Col. Ahmad Zubir Mohamed	Pengarah Urusan	Saza Security Sdn Bhd
7	En. Shaharuddin Samsi	Pengarah	Muhafiz Security Sdn Bhd
8	En. M. Afiq Hazman	Chief Operating Officer	Tracker Hero
9	En. Muhamad Adli Zulkifli	General Manager	Ultrack Technology Sdn Bhd
10	Puan Aini Suraya Osman	Pengarah Urusan	RSS Security Sdn Bhd
11	Dato' Mohd Khaidzir Fahmi	Principal	Tropical Quantum
12	En. Mohd Roselee Abdul Ghani	Pengarah Urusan	Tropical Quantum

NO.	NAME	POSITION	ORGANISATION
13	Ts Samuel Lim	Pengarah	FL Group Distribution
14	En. Wan Zairi Afhtar Ishak	Managing Consultant	MY Private Eye Consulting Sdn Bhd
15	En. Shahfik Mohd Sawardi	Manager	Aviation Security, Malaysia Airports Holdings Berhad (MAB)
16	En. Barathan Muniyandy	Chief Executive Officer	Handal Asia Pacific Sdn Bhd
17	En. Hafiz Rahman	Senior Executive	System Consultancy Services
18	En. Haidil Hazha Bin Husaini	Technical Manager	AE Security System Sdn Bhd
19	En. Hong Chee Choong	Business Development Manager	Beyondsensor Sdn. Bhd
20	En. Muhd Hafizuddin Bin Hamzah	Regional Director of Security & Investigations - APAC	AstraZeneca
21	Dr. Balasubramaniam Rajoo	General Manager of Security	Digital Nasional Berhad

OCCUPATIONAL FRAMEWORK ASSESSMENT TECHNICAL COMMITTEE (JTPOF 1) – 14th September 2023

NO.	NAME	POSITION	ORGANISATION
1	Pn. Khadijah Isaak	Ketua Penolong Pengarah, Unit Pengurusan Kerangka Pekerjaan - Chairman-	Jabatan Pembangunan Kemahiran
2	En. Nazrul Hilmi Mohammad	Penolong Pengarah, Unit Pengurusan Kerangka Pekerjaan - Secretariat-	Jabatan Pembangunan Kemahiran

NO.	NAME	POSITION	ORGANISATION
3	Ts. Nor Aini Binti Abdullah	Pegawai Kanan Pembangunan Kemahiran, Unit Pengurusan Kerangka Pekerjaan - Secretariat-	Jabatan Pembangunan Kemahiran
4	En. Ahmad Azran Ranaai	Ketua Penolong Pengarah, Unit Pengurusan Kerangka Pekerjaan - Secretariat-	Jabatan Pembangunan Kemahiran
5	Pn. Emmylia Cetena Lee Binti Anuar Lee	Unit Agensi Persendirian	Kementerian Dalam Negeri (KDN)
6	En. Muhammad Ubaidillah bin Iman	President	PIKM
7	ACP Dr. Paru Suraman Subramaniam	Deputy Chairperson of Investigatory Chambers of Ethics	PDRM
8	Pn. Sharifah Sajidah Binti Syed Noor Mohammad	Head of Department Human Capital Development	CyberSecurity Malaysia
9	Pn. Nurmadihah binti Mat Daud	MYSTEP	Kementerian Sumber Manusia
10	En. Suraimey Sulaiman	Penolong Pengarah Perangkaan	Department of Statistics Malaysia
11	Pn. Sharifah Rohaiza Binti Syed Rozali	Pengarah Penguatkuasaan dan Kawalan (PKK) Wilayah Persekutuan Kuala Lumpur,	Bahagian Penguatkuasaan Dan Kawalan (KDN))

OCCUPATIONAL FRAMEWORK ASSESSMENT TECHNICAL COMMITTEE (JTPOF 2) – 11th January 2024

NO.	NAME	POSITION	ORGANISATION
1	Dr. Sulaiha Binti Ali	Timbalan Pengarah, Cawangan Kurikulum TVET -Chairman-	Jabatan Pembangunan Kemahiran
2	En. Ahmad Azran Ranaai	Ketua Penolong Pengarah, Unit Pengurusan Kerangka Pekerjaan -Secretariat-	Jabatan Pembangunan Kemahiran

NO.	NAME	POSITION	ORGANISATION
3	Ts. Nor Aini Binti Abdullah	Pegawai Kanan Pembangunan Kemahiran, Unit Pengurusan Kerangka Pekerjaan -Secretariat-	Jabatan Pembangunan Kemahiran
4	En. Muhammad Ubaidillah bin Iman	President	PIKM
5	Pn. Saliza Abdullah	Vice President	PIKM
6	Pn. Siti Hawa Binti Lah	Penolong Pengarah	Kementerian Dalam Negeri (KDN)
7	Pn. Sharifah Rohaiza Binti Syed Rozali	Pengarah Penguatkuasaan dan Kawalan (PKK) Wilayah Persekutuan Kuala Lumpur,	Bahagian Penguatkuasaan Dan Kawalan (KDN))
8	En. Suraimey Sulaiman	Penolong Pengarah Perangkaan	Department of Statistics Malaysia
9	Pn. Samsinahajar Binti Mohd Ibrahim	Pembantu Perhubungan Perusahaan	Kementerian Sumber Manusia
10	ACP Dr. Paru Suraman Subramaniam	Deputy Chairperson of Investigatory Chambers of Ethics	PDRM
11	En. Paramjeet Singh	Mnaging Director	MVD International Sdn. Bhd.
12	Pn. Aini Suraya binti Datuk Osman	Naib Presiden	PIKM
13	En. Zaidel Baharuddin	Business Development	System Consultancy Services Sdn Bhd

OCCUPATIONAL FRAMEWORK INTERNAL TECHNICAL COMMITTEE

NO.	NAME	POSITION	ORGANISATION
1	En. Yuslan Yasok	Timbalan Pengarah Unit Pengurusan Kerangka Pekerjaan	JPK
2	Pn. Wan Suriani Bt. Wan Yusoff	Ketua Pembantu Tadbir	CIAST
3	Dr. Muhamad Azuddin Bin Hassan	Ketua Penyelaras Program (Penyelidikan)	CIAST

NO.	NAME	POSITION	ORGANISATION
4	Pn. Fairus Atida Binti Said	Penolong Kanan Pengarah	JPK
5	Dr. Sulaiha Binti Ali	Timbalan Pengarah, Cawangan Kurikulum TVET	JPK

OCCUPATIONAL FRAMEWORK DEVELOPMENT SECRETARIAT

No.	Name	Position
1.	Pn. Khadijah binti Isaak	Ketua Penolong Pengarah, Unit Pengurusan Kerangka Pekerjaan
2.	En. Ahmad Azran bin Ranaai	Penolong Kanan Pengarah, Unit Pengurusan Kerangka Pekerjaan
3.	Ts. Nor Aini binti Abdullah	Pegawai Kanan Pembangunan Kemahiran, Unit Pengurusan Kerangka Pekerjaan
4.	En. Nazrul Hilmi bin Mohammad	Penolong Pengarah, Unit Pengurusan Kerangka Pekerjaan
5.	Pn. Wan Suraini binti Wan Yusoff	Pegawai Pembangunan Kemahiran, Unit Pengurusan Kerangka Pekerjaan

Department of Skills Development
Ministry of Human Resources
Level 7-8, Block D4, Complex D,
Federal Government Administrative Centre
62530 Putrajaya, Malaysia
Tel : 603-8886 5589
Fax : 603-8889 2423
Email : jpk@mohr.gov.my
Website : https://www.dsd.gov.my

OCCUPATIONAL FRAMEWORK
MSIC N80
SECTION N : ADMINISTRATIVE AND SUPPORT ACTIVITIES
DIVISION 80 : SECURITY AND INVESTIGATION ACTIVITIES

2024