NATIONAL COUNCIL FOR TECHNICAL AND VOCATIONAL EDUCATION AND TRAINING

JANUARY 2023

PROPOSED OCCUPATIONAL STANDARDS

OCCUPATION: CYBER SECURITY ENGINEER

LEVEL: NTA 8

TABLE OF CONTENT

CONTENTS

ABBREVIATIONS

CBET	Competency Based Education and Training
DTP	Data Transformation Protocol
GPA	Gatekeeper for Physical Access
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
NACTVET	National Council for Technical and Vocational Education and Training
NOS	National Occupational Standards
OS	Occupational Standards
TET	Technical Education and Training
TVET	Technical and Vocational Education and Training

GLOSSARY OF TERMS

Circumstantial Knowledge: Detailed knowledge, which allows the decision-making in regard to different circumstances and cross cutting issues.

Competence: The ability to use knowledge, understanding, practical, and thinking skills to perform effectively to the workplace standards required in employment.

Competency: A description of the ability one possesses when able to perform a given occupational task effectively and efficiently.

Competency-based Education: An instructional programme that derives its content from validated tasks and bases assessment on the learner's performance.

Curriculum: A description or composite of statements about "what is to be learned" by the trainee/student in a particular instructional programme; a product that states the "intended learning outcomes".

Educational/Training Programme: The complete curriculum and instruction (what and how) that is designed to prepare a person for employment in a job or other particular performance situation.

Occupation: A specific position requiring the performance of specific tasks – essentially the same tasks are performed by all employees having the same title. (Example: baker)

Occupational Area: This is a broad grouping of related jobs. (Example: food service)

Occupational Competence: The application of knowledge and skills that consistently meet the standards required by the work context.

Occupational Standards: Specific requirements of competences people are expected to demonstrate in a particular occupational area, including knowledge and relevant attitudes. They also act as a performance tool of assessment of the prescribed outcomes.

Occupational/Job Analysis: A process used to identify the tasks that are important to employees in any given occupation.

Performance Criteria: Indicate expected end results or outcomes in the form of evaluative statements.

Skills: The ability to perform occupational tasks with a high degree of proficiency within a given occupation. Skill is conceived of as a composite of three completely interdependent components: cognitive, affective, and psychomotor.

Standards: A set of statements, which if proved true under working conditions, means that an individual is meeting an expected level and type of performance.

Task Analysis: The process of analysing each task to determine the steps, circumstantial knowledge, attitudes, performance standards, tools and materials needed, as well as safety concerns required for the employees performing it.

Task: A work activity that has a definite beginning and ending, is observable or measurable, and consists of two or more definite steps that leads to a product, service, or decision.

Underpinning Knowledge: Crucial knowledge that an individual must acquire in order to demonstrate competences that are associated in performing a given task.

Verification Process: The process of having experts review and confirm the importance of the task (competency) statements identified through occupational analysis. Other questions, such as the degree of task learning difficulty are also frequently asked. This process is also sometimes referred to as validation.

1.0. INTRODUCTION

Technical Education and Training (TET) is one of the most important education sub-sectors in Tanzania, responsible for developing a skilled workforce to support the country's industrialization economic agenda. Tanzania's *Development Vision 2025* intends to raise the country's economy to a middle-income status. This requires a skilled workforce that is aligned with the needs of the public and private sectors of the economy. The National Council for Technical Education has begun the job of drafting Occupational Standards that will eventually be adopted as National Occupational Standards for TET in order to ensure that it meets the needs of the labour market and the country's economic agenda.

National Occupational Standards (NOS) are performance criteria that are matched with labour market demands. Each National Occupation Standard describes functions, performance standards, and knowledge/understanding for one important function or task. They combine skills, knowledge, and attitudes to describe best practice. They are useful tools for establishing job roles, personnel recruiting, supervision, and appraisal, as well as TET standards. They're also helpful for benchmarking and harmonizing qualifications on a national and international level. Standards, in general, provide a solid framework for high-quality TET that is labour market-relevant, current, and consistent in delivery across all public and private institutions.

However, it must be noted that, Occupational Standards and Training standards/qualifications standards are different. Occupational standards are defined in terms of activities performed by a person in a selected occupation (e.g., an electrical engineer designs electrical circuits, performs troubleshooting in electrical circuits, etc.) and they are usually defined by employers following procedures agreed upon by all stakeholders. Education and training standards are developed from the activities defined in occupational standards, and they include learning objectives to ensure that the necessary skills and knowledge are developed by a person to enable him or her to function at an agreed level in an occupation. Education and Training standards are used to define curricula in training institutions. It is however critical that there must be a direct link between the occupational standards and the training standards to respond to the demands of the labour market.

In TET delivery, Tanzania adopted the Competence Based Education and Training (CBET) approach. The CBET approach focuses on providing learners with the skills and knowledge required to meet the occupational standards. Occupational standards are thus the starting point for developing competency-based training (CBET) programmes. TET institutions will be required to benchmark their curricula with relevant occupational standards.

Occupational Standards are developed based on a given occupation's current and future demands. As a result, they serve as a means of bridging the gap between the worlds of employment and technical education and training (TET).

The Cyber Security Engineer Occupation has its own set of occupational standards. The document explains how the occupational standards were developed, as well as the scope, the occupational profile in the form of DACUM charts, and the Occupational Standards.

2.0. OCCUPATIONAL STANDARD DEVELOPMENT PROCESS

The Occupational standard development process began with an examination of major documents that guide Tanzanian skill development. The *10-year National Skills Development Strategy (2016-2026)* was one of the documents reviewed, and it outlined six (6) economic sectors that should be prioritized when developing skills development programmes.

These sectors include: Transport and Logistics, Tourism and Hospitality, Agribusiness, Construction, Energy and ICT. NACTE labour market reports were also used in the literature review to determine the skills demand in the Tanzanian labour market as a whole.

After the literature review, a workshop comprised of expert workers and educators with substantial knowledge and experience in the occupation conducted an occupational analysis utilizing the DACUM approach to produce the occupational profile. The analysis resulted in DACUM Charts, which are attached as **Appendix 1** to this document.

The occupational standards were then developed. Experts in Occupational Analysis and the Development of Occupational Standards facilitated the workshop. Interviews, online surveys, and a stakeholder forum were used to validate the Occupational Standards. Engineers, supervisory technicians on the job, and experienced Cyber Security Engineers were key informants in the survey to discover occupational trends. This information was used to gain insight from the workplaces regarding trends and changes in the profession, including how well graduates are prepared for working in the occupation. A total of ... online surveys were completed by experts from the labour market across the country. Apart from the surveys aiding in defining the scope for the occupational analysis, they also served to engage a wide cross-section of experts in the occupation. Apart from this, the stakeholders' forum was attended by ... participants from different parts of the country representing various companies.

3.0. THE SCOPE AND OVERVIEW OF THE OCCUPATION STANDARDS FOR CYBER SECURITY TECHNICIANS

The standards cover a broad range of duties and tasks that can be performed by a Cyber Security Engineer. However, the occupational standards are not meant to replace individual job descriptions. Instead, they are to be used for guidance in defining skill levels and knowledge for the technician in specific settings or positions. The Cyber Security Engineers may perform tasks in a number of key areas of the occupational standards, but not necessarily in all areas. For example, in large operations, other individuals may be employed or designated to perform specific tasks.

The Cyber Security Engineers shall help enterprises with cyber security planning, risk assessment, project management, security research and analysis of cases related to relevant laws and regulations. Therefore, in practice, engineers in this industry complete various tasks, ranging from cyber security risk assessment, planning and project management. Generally, the Cyber Security Engineer performs the following responsibilities:

a) Protection strategy planning

b) Protection strategy implementation and management

c) Operation manual development

d) Cyber security vulnerability detection and analysis

e) System penetration test and verification

f) System security risk analysis

g) Cyber security emergency tracking and monitoring

h) Cyber security emergency assessment and analysis

i) Cyber security emergency response

j) Cyber security emergency e-discovery

k) Training implementation

l) Technical guidance

m) Interpretation of common cyber security laws and regulations

n) Interpretation of intellectual property laws and regulations

o) Cyber security protection management

p) Cyber security test

q) Cyber security emergency handling

r) Cyber security training and guidance

s) Interpretation of cyber security-related intellectual property

t) Cyber security research

u) Cyber security planning

v) Project management

w) Cyber security risk assessment

x) Case study on cyber security laws and regulations

The Occupational standards have been clustered into NTA qualification levels, i.e. NTA level 7 and 8.

4.0. VALIDITY PERIOD

Due to the rapid development of technology, the validity period of occupational standards is 3-5 years. The review will proceed in the same manner as the one before it, with new occupational standards being developed based on current trends of the labour market.

5.0. OCCUPATIONAL STANDARDS

5.1 OCCUPATIONAL STANDARDS FOR CYBER SECURITY ENGINEER – NTA 8

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY RESEARCH	**DUTY NO.**	801
TASK TITLE	VULNERABILITY INFORMATION RESEARCH	**TASK NO.**	8011

PERFORMANCE CRITERIA	The person performing this task must be able to access vulnerability information through mainstream information platforms, analyse them, prepare vulnerability exploitation process reports, specify their levels, and propose solutions.
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office Word; 5. Penetration test tools such as Metasploit, Nmap, Burp Suite and Sqlmap; 6. Virtual machine; 7. Linux, Windows server, Windows10, Kali Linux and other operating systems.

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Access to publicly available vulnerability information; 2. Analyse vulnerabilities and prepare vulnerability exploitation process reports; 3. Define vulnerability levels; 4. Propose vulnerability solutions.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Access to publicly available vulnerabilities on mainstream information platforms; 1.2 Prepare vulnerability exploitation process reports; 1.3 Define vulnerability hazards and vulnerability rating; 1.4 Prepare vulnerability solutions. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of effectiveness;

	2.2 Principle of confidentiality; 2.3 Principle of controllability; 2.4 Principle of minimum impact. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 The use of mainstream vulnerability information sharing platforms and vulnerability principles; 3.2 Usage of penetration test tools; 3.3 Vulnerability types and basic solutions; 3.4 Definition standards of vulnerability levels; 3.5 Vulnerability type related requirements; 3.6 Basic requirements for databases; 3.7 Basic requirements for network service; 3.8 Basic methods of WEB programming. **4.0 Essential Skills** 4.1 Communication and teamwork skills; 4.2 Customer service skills; 4.3 Reading skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Vulnerability solutions are proposed in accordance with publicly available information on security vulnerabilities.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY RESEARCH	**DUTY NO.**	801
TASK TITLE	VULNERABILITY TOOL RESEARCH	**TASK NO.**	8012
PERFORMANCE CRITERIA	The person performing this task must be able to build vulnerability testing environment for disclosed vulnerability information, and validate and optimize disclosed vulnerability testing tools.		
RANGE STATEMENT	The task can be performed at the information system site under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office Word, Python, C; 5. Penetration test tools such as Metasploit, Nmap, Burp Suite and Sqlmap; 6. Virtual machine; 7. Linux, Windows server, Windows10, Kali Linux and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Retrieve disclosed vulnerability testing methods, tools; 2. Build the runtime environment required for vulnerability testing and testing tools; 3. Validate disclosed vulnerability testing tools; 4. Optimize publicly available vulnerability testing tools.	Detailed knowledge about: **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Select vulnerability testing methods and testing tools; 1.2 Build a vulnerability environment; 1.3 Validate penetration test tools; 1.4 Optimize vulnerability testing tools. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of effectiveness; 2.2 Principle of confidentiality; 2.3 Principle of comprehensiveness and depth; 2.4 Principle of non-destructiveness; 2.5 Principle of legality.

	3.0 Theories The person performing this task must be able to explain the following: 3.1 Principles of vulnerability testing tools and usage; 3.2 Requirements related to the preparation of vulnerability testing tools; 3.3 Operating system installation methods; 3.4 Requirements of relevant intellectual property and security laws and regulations; 3.5 Basic requirements for databases; 3.6 Basic requirements for network service; 3.7 Basic requirements of WEB programming. **4.0 Essential Skills** 4.1 Communication and teamwork skills; 4.2 Customer service skills; 4.3 Reading skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Optimization of testing tools for disclosed vulnerabilities is completed in accordance with operational requirements and specifications.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY PLANNING	**DUTY NO.**	802
TASK TITLE	TERMINAL SECURITY PLANNING	**TASK NO.**	8021
PERFORMANCE CRITERIA	The person performing this task must be able to assist the sales to complete the customer requirements information organisation, independently determine the terminal system environment and the number of terminals, determine the actual project construction objectives, prepare quotations and lists, and output the terminal security planning schemes.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Coordinate with sales for site visits and demand research; 2. Determine the terminal system environment and number of terminals by inspection; 3. Determine construction objectives; 4. Develop equipment lists and quotations; 5. Conduct planning on terminal antivirus; 6. Conduct planning on terminal access control; 7. Conduct planning on terminal secret release prevention; 8. Output terminal security planning scheme.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Coordinate with sales to organise information on customer demands; 1.2 Determine the terminal environment and number of terminals by inspection; 1.3 Determine construction objectives; 1.4 Develop equipment lists and quotations; 1.5 Conduct planning on terminal antivirus; 1.6 Conduct planning on terminal access control; 1.7 Conduct planning on terminal anti-confidentiality; 1.8 Prepare terminal security planning scheme. **2.0 Principles** The person performing this task must be able to explain the following principles:

	2.1 Principle of clarity of objectives; 2.2 Principle of practicability; 2.3 Principle of advancement; 2.4 Principle of consistency; 2.5 Principle of comprehensiveness and integrity. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Terminal antivirus technical requirements; 3.2 Terminal access control technical requirements; 3.3 Terminal secret release prevention technical requirements; 3.4 Requirements for cyber security level protection; 3.5 Related technical standards and specifications; 3.6 Requirements of cyber security laws and regulations. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Scheme document writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The preparation of terminal security planning schemes, project equipment lists and quotations are completed in accordance with technical requirements, site visits and customer demands.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY PLANNING	**DUTY NO.**	802
TASK TITLE	NETWORK BOUNDARY SECURITY PLANNING	**TASK NO.**	8022

PERFORMANCE CRITERIA	The person performing this task must be able to assist the sales to complete the customer requirements information organisation, independently determine the regional boundary security type, determine the actual project construction objectives, prepare equipment lists and quotations, firewall control policy planning, authentication security planning, data exchange system planning, data inspection and collection planning, and output network boundary security planning schemes.
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Coordinate with sales for site visits and demand research; 2. Determine the type of network boundary security; 3. Determine construction objectives; 4. Develop equipment lists and quotations; 5. Perform firewall control policy planning; 6. Perform authentication security planning; 7. Perform data exchange system planning; 8. Perform data testing and collection planning;	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Coordinate with sales to organise information on customer demands; 1.2 Determine the type of customer network boundary security; 1.3 Determine network boundary security planning objectives; 1.4 Prepare equipment lists and quotations for network boundary security equipment; 1.5 Perform firewall control policy planning; 1.6 Perform authentication security planning; 1.7 Perform data exchange system planning; 1.8 Perform data testing and collection planning;

9. Output network boundary security planning schemes.	1.9 Prepare network boundary security planning schemes. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of clarity of objectives; 2.2 Principle of practicability; 2.3 Principle of advancement; 2.4 Principle of consistency; 2.5 Principle of comprehensiveness and integrity. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Firewall technical requirements; 3.2 Authentication security technical requirements; 3.3 Data Transfer Protocol (DTP) requirements; 3.4 Data testing and collection requirements; 3.5 Gatekeeper for Physical Access (GPA) Requirements. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Scheme document writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The preparation of network boundary security planning schemes, project equipment lists and quotations are completed in accordance with technical requirements, site visits and customer demands.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY PLANNING	**DUTY NO.**	802
TASK TITLE	NETWORK ARCHITECTURE SECURITY PLANNING	**TASK NO.**	8023

PERFORMANCE CRITERIA	The person performing this task must be able to assist the sales to complete the customer requirements information organisation, independently determine the actual project construction objectives, prepare equipment lists and quotations, network exit security planning, server area security planning, network core layer security planning, network access layer security planning, cyber security management area planning, terminal secret release prevention regulations, and output network architecture security planning schemes.
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.

EVIDENCE REQUIREMENT

PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Coordinate with sales for site visits and demand research; 2. Determine construction objectives; 3. Develop equipment lists and quotations; 4. Perform network exit security planning; 5. Perform server area security planning; 6. Perform network core layer security planning; 7. Perform access layer security planning; 8. Perform security management area planning;	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Coordinate with sales to organise information on customer demands; 1.2 Determine network architecture security planning objectives; 1.3 Prepare equipment lists and quotations for network architecture security equipment; 1.4 Plan network exit security; 1.5 Plan network core layer security; 1.6 Plan network access layer security; 1.7 Plan cyber security management area; 1.8 Plan terminal secret release prevention;

9. Perform terminal data secret release prevention planning; 10. Output network architecture security planning schemes.	1.9 Prepare network architecture security planning schemes. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of clarity of objectives; 2.2 Principle of practicability; 2.3 Principle of advancement; 2.4 Principle of consistency; 2.5 Principle of comprehensiveness and integrity. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Network exit security technical requirements; 3.2 Server area security technical requirements; 3.3 Network core layer security technical requirements; 3.4 Network access layer security technical requirements; 3.5 Cyber security management area requirements; 3.6 Terminal data secret release prevention technical requirements; 3.7 Requirements for cyber security level protection; 3.8 Related technical standards and specifications; 3.9 Requirements of cyber security laws and regulations. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Scheme document writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The preparation of network architecture security planning schemes, project equipment lists and quotations are completed in accordance with technical requirements, site visits and customer demands.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:**

	1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY PLANNING	**DUTY NO.**	802
TASK TITLE	DATA CENTRE SECURITY PLANNING	**TASK NO.**	8024
PERFORMANCE CRITERIA	The person performing this task must be able to assist the sales to complete the customer requirements information organisation, determine the actual project construction objectives, prepare equipment lists and quotations, and output the data centre security planning schemes.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Coordinate with sales for customer communication and demand research; 2. Determine construction objectives; 3. Develop equipment lists and quotations; 4. Perform data rating planning; 5. Perform data confidentiality planning; 6. Perform data access control planning; 7. Perform data audit planning; 8. Perform data backup planning for disaster recovery; 9. Perform data security wiping planning; 10. Output data centre security planning schemes.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Coordinate with sales to organise information on customer demands; 1.2 Determine safety planning objectives; 1.3 Prepare equipment lists and quotations for data centre security equipment; 1.4 Perform data security rating; 1.5 Ensure data confidentiality; 1.6 Perform data access control; 1.7 Perform data audits; 1.8 Perform data backup for disaster recovery; 1.9 Perform data security wiping; 1.10Prepare data centre security planning schemes. **2.0 Principles** The person performing this task must be able to explain

	the following principles: 2.1 Principle of clarity of objectives; 2.2 Principle of practicability; 2.3 Principle of advancement; 2.4 Principle of consistency; 2.5 Principle of comprehensiveness and integrity. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Data security rating standards; 3.2 Technical requirements for data confidentiality protection; 3.3 Data access control technical requirements; 3.4 Data auditing technical requirements; 3.5 Data backup technical requirements for disaster recovery; 3.6 Data security wiping technical requirements; 3.7 Requirements for cyber security level protection; 3.8 Related technical standards and specifications; 3.9 Requirements of cyber security laws and regulations. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Scheme document writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The preparation of data centre security planning schemes, project equipment lists and quotations are completed in accordance with technical requirements, site visits and customer demands.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY PLANNING	**DUTY NO.**	802
TASK TITLE	CYBER SECURITY SYSTEM PLANNING	**TASK NO.**	8025
PERFORMANCE CRITERIA	The person performing this task must be able to assist the sales to complete the customer requirements information organisation, independently determine the actual project construction objectives, prepare equipment lists and quotations, cyber security management system planning, technical system planning, operational system planning, and output cyber security system planning schemes.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Coordinate with sales for customer communication and demand research; 2. Determine construction objectives; 3. Develop equipment lists and quotations; 4. Perform cyber security management system planning; 5. Perform cyber security technical system planning; 6. Perform cyber security operation system planning; 7. Output cyber security system planning schemes.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Coordinate with sales to organise information on customer demands; 1.2 Determine safety planning objectives; 1.3 Prepare equipment lists and quotations for data centre security equipment; 1.4 Perform cyber security management system planning; 1.5 Perform cyber security technical system planning; 1.6 Perform cyber security operation system planning; 1.7 Prepare cyber security system planning schemes. **2.0 Principles** The person performing this task must be able to explain the following principles:

	2.1 Principle of clarity of objectives; 2.2 Principle of practicability; 2.3 Principle of advancement; 2.4 Principle of consistency; 2.5 Principle of comprehensiveness and integrity. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Cyber security management system framework requirements; 3.2 Cyber security technology (physical security technology, cyber security technology, host security technology, terminal security technology, application security technology, data security technology); 3.3 Knowledge of cyber security system operation and maintenance management; 3.4 Requirements for cyber security level protection; 3.5 Related technical standards and specifications; 3.6 Requirements of cyber security laws and regulations. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Scheme document writing skills; 4.4 Computer skills; 4.5 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The preparation of cyber security system planning schemes, project equipment lists and quotations are completed in accordance with technical requirements, site visits and customer demands.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	PROJECT MANAGEMENT	**DUTY NO.**	803
TASK TITLE	PROJECT MANAGEMENT PLAN PREPARATION	**TASK NO.**	8031
PERFORMANCE CRITERIA	The person performing this task must be able to develop a project management plan in accordance with the actual project.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Define, prepare, and coordinate all components of the project plan and integrate them into one comprehensive project management plan.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Define, prepare, and coordinate all components of the project plan. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of purpose; 2.2 Principle of systematicness; 2.3 Principles of economy; 2.4 Principle of dynamics. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Theoretical knowledge of project management. **4.0 Essential Skills**

	4.1 Communication skills;
	4.2 Customer service skills;
	4.3 Plan writing skills;
	4.4 Teamwork skills.

DESCRIPTION OF THE END PRODUCT / SERVICE	The project management plan is prepared in accordance with actual project requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	PROJECT MANAGEMENT	**DUTY NO.**	803
TASK TITLE	PROJECT IMPLEMENTATION AND MANAGEMENT	**TASK NO.**	8032
PERFORMANCE CRITERIA	The person performing this task must be able to purchase project equipment, audit the feasibility and reasonability of the project scheme, count and inspect the equipment and fill out the inspection form, and review the documents of the project implementation process.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Purchase equipment; 2. Arrange for a technical leader to perform the project site inspection; 3. Arrange for a technical leader to prepare the project implementation plan; 4. Audit the feasibility and reasonability of the project implementation scheme; 5. Count and inspect products and fill out inspection forms; 6. Track, review and report on overall project progress to achieve performance goals identified in the project management plan; 7. Review all change requests, approve changes, manage changes to deliverables, project documents, and project management plans, and communicate the results of change processing.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Purchase equipment; 1.2 Perform project site inspection; 1.3 Perform project implementation scheme review; 1.4 Count and inspect products and fill out inspection forms; 1.5 Track, review and report on overall project progress and determine performance goals; 1.6 Review all change requests, approve changes, and manage deliverables and project documents. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of integrity;

	2.2 Principle of unified command;
	2.3 Principle of scientificity;
	2.4 Principle of operability;
	
	3.0 Theories
	The person performing this task must be able to explain the following:
	3.1 Theoretical knowledge of project management.
	
	4.0 Essential Skills
	4.1 Communication skills;
	4.2 Customer service skills;
	4.3 Plan writing skills;
	4.4 Computer skills;
	4.5 Teamwork skills.

DESCRIPTION OF THE END PRODUCT / SERVICE	Project implementers are supervised to complete the project based on the technical specifications and project management plan in accordance with the operational specifications and practical requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	PROJECT MANAGEMENT	**DUTY NO.**	803
TASK TITLE	PROJECT DELIVERY	**TASK NO.**	8033
PERFORMANCE CRITERIA	The person performing this task must be able to complete the organisation of project process documents, project experience summary, project handover, and questionnaires to measure stakeholder satisfaction.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computers; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Collect project or stage records, audit project success or failure, manage knowledge sharing and delivery, summarize experience and lessons learned, and archive project information; 2. Deliver products, service or results of the project to production and/or operation departments; 3. Collect suggestions for improving or updating organisational policies and procedures, and send them to the appropriate organisational department; 4. Use questionnaires to measure stakeholder satisfaction.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Collect project or stage records, audit project success or failure, manage knowledge sharing and delivery, summarize experience and lessons learned, and archive project information; 1.2 Deliver products, service or results of the project to production and/or operation departments; 1.3 Collect suggestions for improving or updating organisational policies and procedures, and send them to the appropriate organisational department; 1.4 Use questionnaires to measure stakeholder satisfaction. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of goal orientation; 2.2 Principle of transparency.

	3.0 Theories The person performing this task must be able to explain the following: 3.1 Theoretical knowledge of project management; 3.2 Application methods of technical standards and specifications. 3.3 Requirements of cyber security laws and regulations. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Plan writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Project delivery is completed in accordance with technical requirements and customer requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY RISK ASSESSMENT	**DUTY NO.**	804
TASK TITLE	CYBER SECURITY RISK ASSESSMENT PREPARATION	**TASK NO.**	8041

PERFORMANCE CRITERIA	The person performing this task must be able to collect information on project demands, prepare a cyber security risk assessment scheme.
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Collect information on project demands; 2. Prepare a cyber security risk assessment scheme.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Collect information on project demands using on-site observation and client interviews; 1.2 Prepare a cyber security risk assessment scheme. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of standard; 2.2 Principle of criticality; 2.3 Principle of minimum impact; 2.4 Principle of confidentiality. **3.0 Theories** The person performing this task must be able to explain the following:

	3.1 Basis for preparation of cyber security risk assessment scheme; 3.2 Requirements of cyber security laws and regulations; 3.3 Requirements for cyber security level protection; **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Scheme writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The cyber security risk assessment scheme is prepared in accordance with technical requirements and project requirement.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY RISK ASSESSMENT	**DUTY NO.**	804
TASK TITLE	CYBER SECURITY RISK ASSESSMENT IMPLEMENTATION	**TASK NO.**	8042
PERFORMANCE CRITERIA	The person performing this task must be able to prepare an assessment work plan, assign values to asset classification and its significance, confidentiality, and integrity, assign values to asset threat classification and asset threat likelihood, assign values to asset vulnerability severity, perform assessment of effectiveness of asset prevention and protection, and determine cyber security risk magnitude and level in accordance with the project scheme.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Metasploit; 6. Acunetix Web Vulnerability Scanner (AWVS); 7. sqlmap; 8. RayScan; 9. MSAT; 10. CRAMM; 11. Linux, Windows server, Windows10, Kali Linux and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Develop an assessment work plan; 2. Perform assignment of asset significance, confidentiality, and integrity; 3. Analyse the threat to the asset, assign values to asset threat classification and asset threat likelihood;	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Develop an assessment work plan; 1.2 Assign values to asset classification and its significance, confidentiality, and integrity; 1.3 Assign values to asset threat likelihood; 1.4 Assign values to asset vulnerability severity;

4. Analyse asset management and technical vulnerabilities and assign values to the asset vulnerability severity; 5. Assess the effectiveness of the various precautions and protections that have been put in place for the asset; 6. Select appropriate risk calculation methods or tools to determine the magnitude and level of cyber security risk using qualitative and quantitative analysis methods.	1.5 Assess the effectiveness of asset prevention and protection; 1.6 Determine the magnitude and level of risk. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of standard; 2.2 Principle of criticality; 2.3 Principle of minimum impact; 2.4 Principle of confidentiality. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Principles of cyber security risk assessment techniques and application methods; 3.2 Cyber security configuration methods; 3.3 Methods for qualitative and quantitative analysis of cyber security risks; 3.4 Cyber security risk value calculation methods; 3.5 Basic requirements for the use of security risk assessment tools. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Plan writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The cyber security risk assessment is implemented in accordance with technical requirements and customer requirements.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CYBER SECURITY RISK ASSESSMENT	**DUTY NO.**	804
TASK TITLE	CYBER SECURITY RISK ASSESSMENT REPORT PREPARATION	**TASK NO.**	8043
PERFORMANCE CRITERIA	The person performing this task must be able to list the distribution of important assets, vulnerability distribution and comprehensive threat distribution found in the risk assessment work, describe in detail the current status of security risks found and the results of the assessment and analysis, put forward the relevant risk control schemes, and prepare the cyber security risk assessment report.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computer; 2. Record book; 3. Pen; 4. Microsoft Office; 5. Windows10 and other operating systems.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. List the distribution of important assets, vulnerability distribution and comprehensive threat distribution found in the risk assessment work; 2. Describe the current status of security risks found and the results of the assessment and analysis; 3. Propose relevant risk control solutions and provide reasonable suggestions for subsequent reinforcement and rectification; 4. Output cyber security risk assessment reports.	**Detailed knowledge about:** **1.0 Methods** The person performing this task must be able to explain how to: 1.1 List the distribution of important assets, vulnerability distribution and comprehensive threat distribution found in the risk assessment work; 1.2 Describe the current status of security risks found and the results of the assessment and analysis; 1.3 Propose a risk control scheme; 1.4 Prepare a cyber security risk assessment report. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Principle of standard;

	2.2 Principle of criticality; 2.3 Principle of minimum impact; 2.4 Principle of confidentiality. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 Basis for preparation of cyber security risk assessment report; 3.2 Requirements for cyber security level protection; 3.3 Data processing, statistical analysis methods. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Plan writing skills; 4.4 Teamwork skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	The cyber security risk assessment report is prepared in accordance with technical requirements and assessment results.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

<table>
<tr><td><b>OCCUPATION</b></td><td colspan="2">CYBER SECURITY ENGINEER</td><td><b>OCCUPATION CODE</b></td><td></td></tr>
<tr><td><b>DUTY TITLE</b></td><td colspan="2">CASE STUDY ON LAWS AND REGULATIONS</td><td><b>DUTY NO.</b></td><td>805</td></tr>
<tr><td><b>TASK TITLE</b></td><td colspan="2">CASE STUDY RELATED TO THE CYBER SECURITY LAW</td><td><b>TASK NO.</b></td><td>8051</td></tr>
<tr><td><b>PERFORMANCE CRITERIA</b></td><td colspan="4">The person performing this task must be able to read cases related to the <i>Cyber Security Law</i>, interpret the laws and regulations involved in the cases, and propose preventive measures in accordance with technical requirements and security specifications.</td></tr>
<tr><td><b>RANGE STATEMENT</b></td><td colspan="4">The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers.
The tools and equipment to be used include:
1. Computers;
2. Projectors;
3. Black/white board, pens, brushes;
4. Microphones.</td></tr>
<tr><td colspan="5"><b>EVIDENCE REQUIREMENT</b></td></tr>
<tr><td colspan="2"><b>PRACTICAL PERFORMANCE</b></td><td colspan="3"><b>UNDERPINNING KNOWLEDGE</b></td></tr>
<tr><td colspan="2">The person performing this task must be able to do the following:
1. Read cases related to the <i>Cybersecurity Law</i>;
2. Interpret the cyber security laws and regulations involved in the cases;
3. Propose measures for combating and preventing the problem;
4. Prepare case study reports.</td><td colspan="3">Detailed knowledge about:
<b>1.0 Methods</b>
The person performing this task must be able to explain how to:
1.1 Read the case;
1.2 Interpret the case;
1.3 Propose preventive measures;
1.4 Prepare case study reports.

<b>2.0 Principles</b>
The person performing this task must be able to explain the following principles:
2.1 <i>Cyber Security Law</i>.

<b>3.0 Theories</b>
The person performing this task must be able to explain the following:
3.1 The current state of cyber security crimes;
3.2 Types and characteristics of cyber security crimes;</td></tr>
</table>

	3.3 Main causes of cyber security crimes; 3.4 Preventive measures against cyber security crimes; 3.5 Cyber security technical specification requirements; 3.6 Requirements of cyber security laws and regulations. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Teamwork skills; 4.4 Writing skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Preventive measures against cyber security crimes are proposed in accordance with technical requirements and cyber security laws and regulations.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

OCCUPATION	CYBER SECURITY ENGINEER	**OCCUPATION CODE**	
DUTY TITLE	CASE STUDY ON LAWS AND REGULATIONS	**DUTY NO.**	805
TASK TITLE	INTELLECTUAL PROPERTY-RELATED CASE STUDY	**TASK NO.**	8052
PERFORMANCE CRITERIA	The person performing this task must be able to read cases related to intellectual property, interpret the laws and regulations involved in the cases, and propose preventive measures in accordance with technical requirements and security specifications.		
RANGE STATEMENT	The task can be performed in the office and project site with a network environment under the supervision of senior cyber security engineers. The tools and equipment to be used include: 1. Computers; 2. Projectors; 3. Black/white board, pens, brushes; 4. Microphone.		

EVIDENCE REQUIREMENT	
PRACTICAL PERFORMANCE	**UNDERPINNING KNOWLEDGE**
The person performing this task must be able to do the following: 1. Read cases related to intellectual property; 2. Interpret the intellectual property laws and regulations involved in the cases; 3. Propose measures for combating and preventing the problem; 4. Prepare case study reports.	Detailed knowledge about: **1.0 Methods** The person performing this task must be able to explain how to: 1.1 Read the case; 1.2 Interpret the case; 1.3 Propose preventive measures; 1.4 Prepare case study reports. **2.0 Principles** The person performing this task must be able to explain the following principles: 2.1 Intellectual Property Law. **3.0 Theories** The person performing this task must be able to explain the following: 3.1 The current state of intellectual property crimes;

	3.2 Types and characteristics of intellectual property crimes; 3.3 Main causes of intellectual property crimes; 3.4 Preventive measures against intellectual property crimes; 3.5 Cyber security technical specification requirements; 3.6 Requirements of intellectual property laws and regulations. **4.0 Essential Skills** 4.1 Communication skills; 4.2 Customer service skills; 4.3 Teamwork skills; 4.4 Writing skills.
DESCRIPTION OF THE END PRODUCT / SERVICE	Preventive measures against intellectual property crimes are proposed in accordance with technical requirements and intellectual property laws and regulations.
CIRCUMSTANTIAL KNOWLEDGE	**Detailed knowledge about:** 1. Occupational health and safety; 2. Application of technical standards and specifications.

TABLE 1: DACUM CHARTS FOR CYBER SECURITY ENGINEER - NTA 8

DUTIES	TASKS	ENABLERS
1.0 Cyber security research	1.1 Vulnerability information research.	**General skills and knowledge** · Communication and teamwork skills · Skills in using mainstream vulnerability information sharing platforms or vulnerability bases · Mainstream vulnerability information sharing platforms or vulnerability bases · Vulnerability report combing skills · Publicly available vulnerability validation programme retrieval skills · Vulnerability level definition methods **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity
	1.2 Vulnerability tool research.	**General skills and knowledge** · Communication and teamwork skills · Vulnerability testing environment setup method · Vulnerability triggering principle **Tools and equipment** · Computers **Requirements for employees**

DUTIES	TASKS	ENABLERS
		· Teamwork, punctuality and integrity
2.0 Cyber security planning	2.1 Terminal security planning.	**General skills and knowledge** · Communication and teamwork skills · Requirement analysis skills · Terminal security analysis skills · Terminal firewall · Terminal secret release prevention · Terminal access control **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity
	2.2 Network architecture security planning.	**General skills and knowledge** · Communication and teamwork skills · Requirement analysis skills · Network architecture security analysis skills · Firewall control strategy · Authentication security · Data inflow detection · Data Transformation Protocol · Data collection **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity

DUTIES	TASKS	ENABLERS
	2.3 Network boundary security planning.	**General skills and knowledge** · Communication and teamwork skills · Requirement analysis skills · Network boundary security analysis skills · Exit safety · Vulnerability scanning system · Bastion host · Audit system · IPS · IDS · Terminal access system · Situation awareness · Anti-leakage system **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity
	2.4 Data centre security planning.	**General skills and knowledge** · Communication and teamwork skills · Requirement analysis skills · Data centre security analysis skills · Data grading · Data confidentiality · Data access control · Data audit · Data backup for disaster recovery · Secure data erasure **Tools and equipment**

DUTIES	TASKS	ENABLERS
		· Computers **Requirements for employees** · Teamwork, punctuality and integrity
	2.5 Cyber security architecture.	**General skills and knowledge** · Communication and teamwork skills · Requirement analysis skills · Security management system · Security technology system · Safety operation system · Overall strategy **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity
3.0 Project management	3.1 Project management plan preparation.	**General skills and knowledge** · Communication and teamwork skills · Terminal security analysis skills · Cost budget · Risk control · Quality control · Plan management **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity
	3.2 Project implementation and management.	**General skills and knowledge**

DUTIES	TASKS	ENABLERS
		· Communication and teamwork skills · Equipment procurement · Equipment inspection · Project implementation and management · Project testing **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity
	3.3 Project delivery.	**General skills and knowledge** · Communication and teamwork skills · Training organisation · Project document review · Project acceptance · Project delivery **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity
4.0 Cyber security risk assessment	4.1 Cyber security risk assessment scheme preparation.	**General skills and knowledge** · Communication and teamwork skills · Demand analysis capacity · Scheme writing skills **Tools and equipment** · Computers **Requirements for employees**

DUTIES	TASKS	ENABLERS
		· Teamwork, punctuality and integrity
	4.2 Cyber security risk assessment implementation.	**General skills and knowledge** · Communication and teamwork skills · Cyber security risk analysis and assessment skills · Plan writing skills · Management competence · Asset identification · Threat identification · Vulnerability identification **Tools and equipment** · Computers **Requirements for employees** · Teamwork, punctuality and integrity
	4.3 Cyber security risk report.	**General skills and knowledge** · Communication and teamwork skills · Analysis skills · Project document review · Report writing skills · Expression skills **Tools and equipment** · Computers, projectors **Requirements for employees** · Teamwork, punctuality and integrity
5.0 Case study on laws and regulations	5.1 Case study related to the *Cyber Security Law*.	**General skills and knowledge** · Communication and teamwork skills · *Cyber Security Law* · Case study skills

DUTIES	TASKS	ENABLERS
		· Expression skills **Tools and equipment** · Computers, projectors **Requirements for employees** · Teamwork, punctuality and integrity
	5.2 Intellectual property-related case study.	**General skills and knowledge** · Communication and teamwork skills · Internet intellectual property · Case study skills · Expression skills **Tools and equipment** · Computers, projectors **Requirements for employees** · Teamwork, punctuality and integrity