kasneb

bempowered

VOCATIONAL CERTIFICATE IN INFORMATION AND CYBER SECURITY (VCICS)

EXAMINATION SYLLABUS

JULY 2021

kasneb Towers, Hospital Road, Upper Hill
P.O. Box 41362 - 00100, Nairobi - Kenya
Tel: 254(020) 4923000
Cellphone: 0722-201214/0734-600624

E-mail: info@kasneb.or.ke Website: www.kasneb.or.ke

JULY 2021

FOREWORD

One of the cardinal objectives of any education system is to ultimately provide the economy with competent, self-driven and morally upright human capital for sustainable growth and prosperity. In order to effectively achieve this, it is important that the education system continuously adapts to market dynamics at global, regional and national levels.

For professional examination bodies such as the Kenya Accountants and Secretaries National Examinations Board (Kasneb), this translates to the need to regularly review their syllabuses to match and, in an ideal setting, surpass market expectations. The drivers of syllabuses change are wide and diverse and transcend various factors including economic, legal, social and technological spheres.

It is in the above context that The National Treasury and Planning, as the parent Ministry of Kasneb, is pleased to note the significant milestone in the completion of the major review process for Kasneb, having also participated with other stakeholders in the review process. This latest review has afforded Kasneb the opportunity to address emerging trends that define the next generation of professionals, including data mining and analytics, digital competence, soft skills and a global perspective in strategic decision making.

With the revised syllabuses, Kasneb is expected to continue playing a leading role in providing the economy with competent professionals in the areas of accounting, finance, governance and corporate secretarial practice, credit management, forensic investigations, information communication technology and related areas. This is further expected to boost the Government's development agenda as defined under the Kenya Vision 2030 development blueprint and the Big Four Agenda.

The successful implementation of the revised syllabuses will require the support of all stakeholders. I wish therefore to urge for the continued support to Kasneb including from various Government Ministries and Departments, regulatory bodies, employers, professional institutes, universities and other training institutions, among others.

It is my conviction that the revised syllabuses will reshape the professional qualifications frontier in the region and beyond and firmly place Kenya as one of the leading countries in the provision of globally competitive professionals.

Dr Julius M. Muia, PhD, CBS
The Principal Secretary/The National Treasury
The National Treasury and Planning

August 2021

PREFACE

Kasneb has been undertaking a major review of its examination syllabuses every five years and a mid-term review every two and a half years. The prime focus of the just completed major review was the need to produce enhanced, integrated and competence based curriculums whose graduates will remain well positioned to meet the dynamic global market demands for the next five years and beyond.

The major review process commenced in earnest in August 2019 with an intensive stakeholder engagement across various counties in Kenya. This was supplemented by study visits and surveys conducted in various parts of the globe, including in the USA, UK, Canada, Malaysia, Singapore, Australia and India. Further engagements with employers, practitioners and the market at large culminated in the development of a competence framework for the professional qualifications of Kasneb. A competence framework is a structure that sets out and defines each individual competency required by persons working in an organisation. The framework defines the knowledge, skills and attributes needed for people within an organization.

Complementing the competence framework were occupational standards developed for the vocational, certificate and diploma programmes. Similar to the competence frameworks for professionals, the occupational standards for various technician qualifications are statements of work performance reflecting the ability to successfully complete the functions required in an occupation, as well as the application of knowledge, skills and understanding in an occupation.

With the development of the competence frameworks and occupational standards, the next logical step was the development of the detailed syllabuses content addressing the identified required competencies. The syllabuses content was developed by various subject matter experts drawn from both public and private sectors, industry and academia, employers and practitioners among others.

As noted above, stakeholder engagement formed a critical pillar in each step of the review process. At the final stretch, stakeholders were invited to validate the syllabuses on Friday, 7 May 2021 during a national virtual conference. This paved the way for the launch of the syllabuses on Friday, 23 July 2021.

As part of the new competence-based system, Kasneb will use various assessment modes through a partnership model with other institutions to test the achievement of key competencies and skills. Among other key areas of focus is the introduction of practical experience and work-simulation, together with a requirement for students to attend workshops where matters of ethics, values, attitudes and other soft skills will be developed.

The major review of the syllabuses also witnessed the expansion of the qualifications spectrum for Kasneb to include four vocational courses, one certificate course, three diploma courses, five professional courses and one post-professional specialisation course.

We are confident that the new qualifications of kasneb will address the current and emerging skills requirements in the national, regional and international markets.

Finally, I wish to take this opportunity to thank all our partners and stakeholders for their contribution in various ways to the successful completion of the major syllabuses review.

Dr Nancy N. Muriuki, PhD
Chairman of the Board of Kasneb

August 2021

ACKNOWLEDGEMENT

I wish to take this opportunity to express our deepest appreciation to all our key stakeholders who, through their expert advice, comments, other feedback and general support contributed to the development of the revised syllabuses together with the supporting competence frameworks and occupational standards.

We are particularly grateful to the Government of Kenya through the National Treasury and Planning, the Ministry of Education, Ministry of Foreign Affairs incorporating various Kenyan Embassies and High Commissions, among others; various regulatory bodies including the Kenya National Qualifications Authority (KNQA), Technical and Vocational Education and Training Authority (TVETA), Commission for University Education (CUE), Central Bank of Kenya (CBK), Capital Markets Authority (CMA); professional bodies including the Institute of Certified Public Accountants of Kenya (ICPAK), Institute of Certified Secretaries (ICS), Institute of Certified Investment and Financial Analysts (ICIFA), Institute of Credit Management Kenya (ICM-K), Law Society of Kenya (LSK) - Nairobi Chapter; Federation of Kenya Employers (FKE) and individual employers; the Ethics and Anti-Corruption Commission (EACC); practitioners, subject matter experts and trainers, various consultants engaged; students, parents and guardians; past and present members of the Board, Committees and Sub-Committee; members of staff of Kasneb among other stakeholders.

We also extend our appreciation to all foreign regulatory and professional bodies who facilitated the study visits and provided valuable insights on global trends and emerging issues in areas relevant to the examinations of Kasneb. In this connection, we wish to highlight the following institutions for special mention:

1. United Kingdom (UK): Chartered Governance Institute; Chartered Institute of Management Accountants; Chartered Institute of Marketers; Institute of Chartered Accountants in England and Wales; Pearson Vue Limited.
2. United States of America (USA): American Institute of Certified Public Accountants; Chartered Financial Analysts Institute; International Federation of Accountants; Society for Corporate Governance.
3. Singapore and Malaysia: Chartered Secretaries Institute of Singapore; Malaysian Association of Chartered Secretaries and Administrators; Malaysian Institute of Accountants.
4. Canada: CPA Canada; Board of Canadian Registered Safety Professionals.
5. Australia: CPA Australia; Pearson Vue Australia.
6. India: Indira Gandhi National Open University; Institute of Chartered Accountants of India; Institute of Company Secretaries of India, Institute of Cost Accountants of India.
7. South Africa: South Africa Institute of Chartered Accountants (SAICA).

Kasneb remains forever grateful to all our stakeholders for your role in ensuring the development of quality and globally benchmarked syllabuses, competence frameworks and occupational standards. We look forward to your continued support in the implementation of the revised syllabuses.

Dr Nicholas K. Letting', PhD, EBS
Secretary/Chief Executive Officer, Kasneb

August 2021

TABLE OF CONTENTS

BACKGROUND INFORMATION ABOUT kasneb

1.1 Legal Foundation and Status of kasneb

kasneb was established as a state corporation under the National Treasury by the Government of Kenya on 24 July 1969. The establishment and operations of kasneb are governed by the following main Acts:

(a) The Accountants Act, No. 15 of 2008 (which repealed the Accountants Act, Cap 531 of 1977).
(b) The Certified Public Secretaries of Kenya Act, Cap 534 of 1988.
(c) The Investment and Financial Analysts Act, No. 13 of 2015.

1.2 Functions of kasneb

Section 17(1) of the Accountants Act, 2008 of the Laws of Kenya defines the functions of kasneb. These functions are:

(a) To prepare syllabuses for professional, diploma and certificate examinations in accountancy, company secretarial practice and related disciplines;
(b) To make rules with respect to such examinations;
(c) To arrange and conduct examinations and issue certificates to candidates who have satisfied examination requirements;
(d) To promote recognition of its examinations in foreign countries;
(e) To investigate and determine cases involving indiscipline by students registered with the Examinations Board;
(f) To promote and carry out research relating to its examinations;
(g) To promote the publication of books and other materials relevant to its examinations;
(h) To liaise with the Ministry of Education, Science and Technology in accreditation of institutions offering training in subjects examinable by the Examinations Board, and
(i) To do anything incidental or conducive to the performance of any of the preceding functions.

1.3 Professional Institutes/Registration Board for Kasneb graduates

1.3.1 Institute of Certified Public Accountants of Kenya (ICPAK)

ICPAK is established under Section 3 of the Accountants Act, 2008. One of the functions of ICPAK is to advise kasneb on matters relating to examination standards and policies. The Act also makes provisions for the establishment of a Registration and Quality Assurance Committee (Registration Committee) under Section 13. One of the functions of the Registration Committee is to register eligible persons as Certified Public Accountants.

1.3.2 Institute of Certified Secretaries (ICS)

ICS is established under Section 3 of the Certified Public Secretaries of Kenya Act (Cap. 534) of the Laws of Kenya. One of the functions of ICS is to advise kasneb on matters relating to examination standards and policies.

1.3.3 Registration of Certified Public Secretaries Board (RCPSB)

RCPSB is established under Section 11 of the Certified Public Secretaries of Kenya Act (Cap. 534) of the Laws of Kenya. One of the functions of RCPSB is to register eligible persons as Certified Secretaries.

1.3.4 Institute of Certified Investment and Financial Analysts (ICIFA)

ICIFA is registered under the Investment and Financial Analysts Act, No. 13 of 2015 of the Laws of Kenya. One of the functions of ICIFA is to advise

kasneb on matters relating to examination standards and policies. The Act also makes provisions for the establishment of a Registration Committee under Section 13. One of the functions of the Registration Committee is to register eligible persons as Certified Investment and Financial Analysts.

1.3.5 **Institute of Credit Management Kenya [ICM (K)]**

ICM (K) is registered under the Societies Act, (Cap.108) of the Laws of Kenya.

1.4 Vision, Mission, Mandate and Core Values

The vision, mission, mandate and core values of kasneb are as follows:

1.4.1 Vision

Global leader in examination and certification of business professionals.

1.4.2 Mission

Empowering professionals globally by offering quality examinations and undertaking research and innovation.

1.4.3 Mandate

The mandate of kasneb is the development of syllabuses; conduct of professional, diploma and certificate examinations and certification of candidates in accountancy, finance, credit, governance and management, information technology and related disciplines; promotion of its qualifications nationally, regionally and internationally and the accreditation of relevant training institutions in liaison with the ministry in charge of education.

1.4.4 Core Values

- Integrity
- Professionalism
- Customer focus
- Teamwork
- Innovativeness

2.0 EXAMINATIONS OF kasneb

kasneb currently offers the following examinations:

(a) **Vocational certificate courses**

These are short-term, skills-based programmes currently in the areas of entrepreneurship and innovation, graphic design, information and cyber security and block chain technology. The courses are ideal both for fresh high school graduates and established professionals in various areas willing to diversify their knowledge and competencies in the above areas.

The vocational certificate courses are administered in two levels, with each level requiring an average of three months, thus a total of six months.

Entrants with high school certificates will start with Level I which covers basic skills. Other entrants with post-high school qualifications covering the basic skills will enter at Level II.

The minimum entry for the vocational certificates is a KCSE certificate. The courses can be pursued through a tuition-based programme or privately. Tuition-based programmes (physical or virtual classes) are however recommended due to the interactiveness with facilitators and other students which are key in imparting the requisite technical and soft skills.

The examinations will be administered primarily on a computer-based platform.

The details on each of the vocational programmes are summarised below:

(i) **Vocational Certificate in Entrepreneurship and Innovation**

The course imparts basic knowledge, skills, values and attitudes to apply entrepreneurship skills and generate innovative ideas to start and manage a new business or grow an existing entity.

(ii) **Vocational Certificate in Graphic Design**

The course imparts basic knowledge, skills, values and attitudes to generate and enhance graphic designs according to set specifications.

(iii) **Vocational Certificate in Information and Cyber Security**

The course imparts basic knowledge, skills, values and attitudes to identify information and cyber threats and risks and implement programmes to protect information and databases.

(iv) **Vocational Certificate in Blockchain Technology**

The course imparts knowledge, skills, values and attitudes to develop a simple blockchain program and undertake blockchain transactions.

(b) **Certificate in Accounting and Management Skills (CAMS) course**

The course imparts knowledge, skills, values and attitudes to prepare basic accounts and financial statements for a small enterprise or non-complex environment and apply basic management and marketing skills in business.

The course is mainly for persons who wish to qualify and work as entry level accounting and management personnel.

The CAMS course is administered in two levels, with each level requiring an average of six months, thus a total of one year.

The minimum entry requirement is KCSE mean grade D or a vocational certificate.

The course is fully tuition based with requirements for students to sit for continuous assessment tests (CATs), which constitute 15% of the final score for assessment purposes.

The examinations will be administered primarily on a computer-based platform.

(c) **Diploma Courses**

Kasneb currently administers three diploma programmes; Accounting Technicians Diploma (ATD), Diploma in Data Management and Analytics (DDMA) and Diploma in Computer Networks and Systems Administration (DCNSA).

The diploma courses are administered in two levels, with each level requiring an average of one year, thus a total of two years.

The minimum entry for the diploma courses is KCSE mean grade C-. Persons with certificate and other higher qualifications from recognised institutions are also eligible for entry. The courses can currently be pursued through a tuition-based programme or privately. Tuition-based programmes (physical or virtual classes) are however recommended due to the interactiveness with facilitators and other students which are key in imparting the requisite technical and soft skills.

A summary on each of the diploma programmes is presented below:

(i) **Accounting Technicians Diploma (ATD) course**

The course imparts knowledge, skills, values and attitudes to prepare financial and management accounts and financial statements for small and medium sized enterprises and compute basic taxes for a business.

The course is aimed at persons who wish to qualify and work as middle level accountants providing technical support to professional accountants, auditors, tax practitioners and related areas.

(ii) **Diploma in Data Management and Analytics (DDMA) course**

The course imparts knowledge, skills, values and attitudes to undertake non-complex design of databases, mine and analyse data for decision making.
The DDMA will be administered on a computer-based platform.

(iii) **Diploma in Computer Networks and Systems Administration (DCNSA) course**

The course imparts knowledge, skills, values and attitudes to design, configure, test and secure and manage non-complex networks.

The DCNSA will be administered on a computer based platform.

(d) **Professional Courses**

Kasneb currently administers five professional courses, as summarised below:

(i) Certified Public Accountants (CPA)
(ii) Certified Secretaries (CS)
(iii) Certified Investment and Financial Analysts (CIFA)
(iv) Certified Credit Professionals (CCP)
(v) Certified Information Systems Solutions Expert (CISSE)

The professional courses are administered at Foundation, Intermediate and Advanced Levels. Each level requires an average of one year, though candidates are advised to provide for an additional one year to meet requirements for internship/practical experience

The minimum entry requirement for the professional courses is KCSE mean grade C+. Persons with diplomas or other higher-level qualifications from recognised institutions are also eligible for entry. The courses can be pursued through a tuition-based programme or privately. Tuition-based programmes (physical or virtual classes) are however recommended due to the interactiveness with facilitators and other students which are key in imparting the requisite technical and soft skills.
A summary on each of the professional courses is presented below:

(i) **Certified Public Accountants (CPA) course**

The course imparts knowledge, skills, values and attitudes to, among other competencies:

- Prepare accounts and financial statements including for complex entities in both the private and public sectors.
- Use computerised accounting systems
- Practically apply data analytical tools analyse data and reach conclusions.
- Undertake audit and assurance services
- Apply advanced financial management skills to evaluate various financial aspects of a business for decision making
- Prepare management accounts
- Apply leadership and management skills in practice to manage teams and achieve results

The course is aimed at persons who wish to qualify and work or practice as professional accountants, auditors, finance managers, tax managers and consultants in related areas in both public and private sectors.

Assessment will be conducted in a variety of ways, including examinations, practical papers, workshops attendance and practical experience.

In addition to the above papers, prior to certification, candidates will be required to

- Attend workshops on ethics, soft skills and emerging issues organised by Kasneb and ICPAK and earn IPD hours)
- Obtain 1-year practical experience, or alternatively attend workshops on work based simulation organised by Kasneb and ICPAK.

In order to assist CPA students to obtain the requisite practical experience and internship opportunities, they will be registered as student members of the Institute of Certified Public Accountants of Kenya (ICPAK) under a programme called the Trainee Accountants Practical Experience Programme (TAPEF). Through TAPEF, ICPAK working in consultation with Kasneb will assist students as much as possible to link with professional accountants who will mentor them towards obtaining the necessary practical experience.

(ii) **Certified Secretaries (CS) course**

The course imparts knowledge, skills, values and attitudes to, among other competencies:

- Practice and promote principles of good governance within public and private sector entities
- Implement and comply with legal, regulatory and ethical requirements in practice
- Ensure proper conduct and management of meetings
- Undertake consultancy and advisory services in corporate secretarial and related practices

- Manage boardroom dynamics
- Undertake governance and compliance audits

The course is aimed at persons who wish to qualify and work or practice as corporate secretaries, policy formulators and consultants in governance, governance and compliance auditors and administrators at county and national levels and in the private sector.

Assessment will be conducted in a variety of ways, including examinations, projects and workshops attendance.

(iii) **Certified Investment and Financial Analysts (CIFA) course**

The course imparts knowledge, skills, values and attitudes to, among other competencies:

- Apply financial tools and concepts in analysis and valuation of investment and securities
- Manage and grow portfolios of investments
- Analyse various types of investments including equity investments, fixed income investments and derivatives
- Manage corporate finances
- Apply financial modelling and analytical tools in investments analysis

The course is aimed at persons who wish to qualify and work or practice as investment, securities and financial analysts, portfolio managers, investment bankers, fund managers, consultants on national and global financial markets and related areas.

(iv) **Certified Credit Professionals (CCP) course**

The course imparts knowledge, skills, values and attitudes to, among other competencies:

- Manage the credit cycle for trade credit providers
- Manage credit risk for different entities
- Undertake credit analysis for various corporate entities
- Undertake debt collection in a professional manner
- Comply with various requirements in debt management including governance, ethical, legal and regulatory requirements.

The course is aimed at persons who wish to qualify and work or practice in various fields of credit management including credit analysis, debt management and recovery, corporate lending and related areas in both formal and informal sectors.

(v) **Certified Information Systems Solutions Expert (CISSE) course**

The course imparts knowledge, skills, values and attitudes to, among other competencies:

- Develop information systems solutions for a business
- Design and operationalise database management systems
- Design, configure and trouble shoot computer networks
- Implement ICT projects
- Manage and analyse big data

(e) **Post-professional specialisation course**

Kasneb has introduced the Certified Forensic Fraud Examiner (CFFE). The course imparts knowledge, skills, values and attitudes to, among other competencies:

- Apply analytical techniques in fraud detection
- Design and implement preventive and detective controls
- Apply and ensure compliance with the appropriate laws in fraud investigations

- Apply the burden and standards of proof in civil and criminal proceedings
- Apply the various methods and techniques of conducting fraud investigations
- Write standard investigations and expert witness reports
- Develop fraud prevention programs
- Conduct a fraud prevention health check up
- Develop and implement a fraud risk management program

The course is aimed at persons who wish to qualify and work or practice in the fields of financial fraud and corruption investigations, fraud prevention, fraud risk analysis and related areas.

The CFFE is administered in three modules, with an integrated case study and workshops at the end of the course. Each module is expected to last for three months. Examinations for the CFFE course will be administered three times in a year, thus the course is meant to last on average one year.

The minimum entry requirement to pursue the CFFE course is:
- Kasneb professional qualification; or
- Bachelor's degree from a recognised university; or
- Any other qualification considered equivalent to the above.

The course can be pursued through tuition-based learning or self-study.

Kasneb working with other partners will be rolling out another post-professional specialisation area in public financial management.

(f) **Examinations for holders of foreign qualifications wishing to be registered and practice in Kenya**

(i) **Examination for holders of foreign accountancy qualifications (FAQs)**
In consultation with the Council of ICPAK under Section 26 Sub-Sections (2) and (3) of the Accountants Act, 2008, kasneb examines holders of foreign accountancy qualifications who have applied for registration as Certified Public Accountants (CPAs) of Kenya and they are required to demonstrate their knowledge of local law and practice.

(ii) **Examination for holders of foreign secretaries qualifications (FSQs)**
In consultation with the Council of ICS under Section 20 Sub-Sections (2) and (3) of the Certified Public Secretaries of Kenya Act, Cap 534, kasneb examines holders of foreign secretaries qualifications who have applied for registration as Certified Secretaries (CSs) of Kenya and they are required to demonstrate their knowledge of local law and practice.

(iii) **Examination for holders of foreign investment and financial analysts qualifications (FIFAQs)**
In consultation with the Council of ICIFA under Section 16 Sub-Sections (2) and (3) of the Investment and Financial Analysts Act, No. 13 of 2015, kasneb examines holders of foreign qualifications who have applied for registration as Certified Investment and Financial Analysts (CIFA) and they are required to demonstrate their knowledge of local law and practice.

3.0 EXAMINATION RULES AND REGULATIONS

3.1 Registration and examination bookings

All applications for registration and examination booking must be in the prescribed manner. Students are advised to download the e-kasneb app for purposes of registration and examination booking. The deadline for registration and examination booking will be specified for each sitting but may not be later than thirty days to the date of the next examinations.

3.2 Exemptions

Exemptions may, on application, be granted to registered students who are holders of certain degrees and diplomas recognised by kasneb. Exemptions will be granted on a paper by paper basis. Details on available exemptions can be accessed on the kasneb website www.kasneb.or.ke.

3.3 Retention of Credits

Credits for papers passed by candidates will be retained without limit.

3.4 Progression Rule

A candidate will not be allowed to enter a higher level of the examination before completing the lower level.

3.5 Registration Renewal

3.5.1 A registered student must renew the studentship registration annually on the first day of July provided that newly registered students will be required to renew their registration on the first day of July following the examination sitting to which they are first eligible to enter.

3.5.2 A student who without good cause fails to renew the registration within three months of the renewal date will be deemed to have allowed the registration to lapse and may thus forfeit the right to write the examination until the renewal position is regularised. The registration number of a student who fails to renew the registration for three consecutive years will be deactivated, that is, removed from the register of students and will thus not be able to book for examinations until the registration number is reactivated.

3.5.3 A student whose registration number is deactivated for failure to renew the registration may apply for reactivation provided that if the application is accepted, the student shall:

(a) Pay the registration reactivation fee.
(b) Pay three years of registration renewal fees.

3.6 Rules Governing the Conduct of Students in the Examination Room

Kasneb will conduct examinations on both computer-based and paper-based platforms. The following rules mainly relate to paper-based examinations. Kasneb will be issuing additional rules specific to computer-based examinations in due course.

3.6.1 Candidates should present themselves for the examination at least 30 **minutes** before the scheduled time for the commencement of the examination they are taking.

3.6.2 A candidate who arrives half an hour or later after the commencement of the examination will not be allowed to take the examination nor will a candidate be

permitted to leave the examination room until after the end of the first half hour since the commencement of the examination.

3.6.3 Each candidate is assigned a registration number upon registration as a student of kasneb. The candidate must sit at the place indicated by that number in the examination room. The registration number must be entered in the space provided at the top right-hand corner of each answer sheet.

3.6.4 The name of the candidate **must not** appear anywhere on the answer sheet.

3.6.5 Each answer sheet has a serial number indicated on the top, left hand side of the answer sheet. Each candidate must indicate the serial number of the answer sheet(s) used for each examination paper in the signature register.

3.6.6 Examination stationery will be provided in the examination room, but candidates must bring their own blue or black ink pens, pencils, and rulers.

3.6.7 **Mobile phones are strictly not allowed in the examinations room.**

3.6.8 No stationery whatsoever may be removed from the examination room.

3.6.9 Candidates **must not** carry the examination question papers from the examination room.

3.6.10 Candidates are allowed to use calculators provided that such calculators are noiseless, cordless and non-programmable.

3.6.11 Candidates will be required to positively identify themselves to the chief invigilator by producing their student identification cards and the national identity cards. Non-Kenyan candidates will be required to produce other relevant identification documents such as passports.

3.6.12 Strict **silence** must be observed during the entire duration of the examination.

3.6.13 Candidates **must not** possess any notes, printed paper or books in the examination room, but must leave any such material with the chief invigilator. Candidates using clipboards must ensure that such clipboards have no writing on them whatsoever.

3.6.14 Smoking is **not** allowed in the examination room.

3.6.15 Candidates **must not** collude in the examination room by exchanging notes or keeping the answer booklet in such a way that another candidate can read or copy from the booklet.

3.6.16 Impersonation in the examination room is not only a serious offence but also a criminal offence.

3.6.17 During the course of the examination, no candidate may leave the examination room without permission from the chief invigilator. Any candidate who does so will not be allowed to return to the examination room.

3.6.18 Candidates who finish the paper before the chief invigilator announces the end of the examination and wish to leave the examination room while the examination is in progress must inform the invigilator and hand in their scripts to the invigilator before leaving the examination room. However, no candidate will be allowed to leave the examinations room during the last fifteen (15) minutes of the examination.

3.6.19 Candidates **must not** leave the examination room with any answer booklet or answer sheets.

3.6.20 Candidates **must not** leave the examination room before their answer booklets are collected by the invigilators.

3.6.21 Candidates **must not** write notes on the examination timetable (Authority to sit the Examination).

3.6.22 Candidates with confirmed disabilities may apply to kasneb to be allowed extra time during examinations. Such application should be made at least two months prior to the examination.

3.6.23 Candidates must produce the timetables (Authority to sit the Examination) in order to be allowed to take the examination. Candidates may download their timetables (Authority to sit the Examination) from the kasneb website or through the e-kasneb. The downloaded timetables may be used as authority to sit the examination.

3.7 **Action for Breach of Examination Rules and Regulations**

3.7.1 kasneb is mandated by the Accountants Act, 2008 under Section 17 (1)(e) to investigate and determine cases involving indiscipline by students registered with kasneb. Section 42 of the Act further defines examination offences that are punishable under the law and the applicable penalties.

3.7.2 Disciplinary action will be taken against candidates who breach the examination rules and regulations of kasneb. A breach of the examination rules and regulations of kasneb shall include but is not limited to the following:

(a) Deficiency in identification.
(b) Impersonation.
(c) Collusion.
(d) Possession of a mobile phone in the examination room.
(e) Possession of notes in the examination room.
(f) Taking away answer booklets.
(g) Writing of names on the scripts.
(h) Possession of mobile phones in the examination room.
(i) Carrying the examination question papers from the examination room.

3.7.3 The action for breach of the examination rules and regulations of kasneb shall include but not limited to the following:

(a) De-registration as a student of kasneb.
(b) Cancellation of registration number.
(c) Nullification of candidate's results.
(d) Prohibition from taking examinations of kasneb.
(e) Written reprimand and warning.

3.7.4 Certain breaches of the rules and regulations amount to breaches of the law. In such cases, candidates will be handed over to the police for investigations and appropriate legal action.

Section 42 of the Accountants Act, 2008 provides that a person who:

(a) gains access to examinations materials and knowingly reveals the contents, whether orally, in writing or through any other form, to an unauthorised party, whether a candidate or not;
(b) wilfully and maliciously damages examinations materials;
(c) while not registered to take a particular examination, with intent to impersonate, presents or attempts to present himself to take the part of an enrolled candidate;
(d) presents a forged certificate to a prospective employer or to an institution of learning with intent to gain employment or admission; or
(e) introduces unauthorised materials into the examinations room, whether in writing or in any other form, whether a candidate or not, commits an offence and is liable on conviction to imprisonment for a term not exceeding three years, or to a fine not exceeding one hundred thousand shillings, or to both.

LEVEL ONE

PAPER NO. 1 COMMUNICATION SKILLS AND ETHICS

Unit Description
This unit specifies competencies required to apply communication skills and ethics. It involves demonstrating concepts of communication skills and ethics, applying writing skills in communication, applying presentation skills, conducting interviews, conducting meetings, applying ethics in communication and applying ICT skills in communication.

Summary of Learning Outcomes
- Demonstrate concepts of communication skills and ethics
- Apply writing skills in communication
- Apply presentation skills
- Conduct interviews
- Conduct meetings
- Apply ethics in communication
- Apply ICT skills in communication

CONTENT:

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods

1. Demonstrate concepts of Communication Skills	• Meaning of communication
	• Purpose of communication
	• Elements of communication
	• Stages of the communication process
	  – Source
	  – Encoding
	  – Channel
	  – Decoding
	  – Feedback
	• Principles of effective communication
	• Formal and informal communication channels
	• Flow of formal communication
	• Forms of communication
	  – Oral communication
	  – Non-verbal communication
	  – Written communication
	  – Visual communication
	  – Audio-visual communication
	• Advantages and disadvantages of various forms of communication
	• Effective listening
	• Barriers to effective communication
	• Overcoming barriers to effective communication
		• Oral questioning
		• Written tests

Learning Outcome	Content	Suggested Assessment Methods
2. Apply writing skills in communication	• Steps in writing business documents – Prewriting – Drafting – Revising – Editing • Rules of writing business documents • Purposes of business documents – Business letters – Business reports – Memorandum – Circulars – Advertisements – Notices – E-mail	• Written tests • Oral testing
3. Apply presentation skills	• Definition of presentation • Uses of presentation • Presentation skills • Elements of a presentation • Methods of delivering a presentation – Manuscript – Memorised – Extemporaneous – Impromtu • Basic parts of a presentation • Importance of Audience analysis in presentation • Use of visual aids in presentation	• Written tests • Practical exercises • Demonstration
4. Conduct interviews	• Meaning of; – Interview – Interviewer – Interviewee • Purpose of interviews • Types of interviews – Unstructured – Semi-structured – Structured • Skills for effective interviewing • Importance of non- verbal communication in interviews • Purpose of maintaining of interview documents	• Written tests • Oral questioning
5. Conduct meeting	• Purpose of holding meetings in an organisation • Types of meetings – Formal – informal • Stages of conducting formal meeting	• Written tests • Oral questioning

Learning Outcome	Content	Suggested Assessment Methods
	• Importance of agenda of the meeting • Role of the chairperson and the secretary in a meeting • Importance of minutes • Online meetings – Video conferencing – Teleconferencing – Webinar	
6. Apply ethics in communication	• Meaning of ethics and integrity • Significance of ethics and integrity in communication • Principles of ethical communication • Purpose of employees' code of ethics • Factors influencing ethical communication • Ethical dilemmas in communication • Handling ethical dilemmas in communication	• Written tests • Oral questioning • Short tests to assess underpinned knowledge.
7. Apply ICT skills in communication	• Use of ICT skills in communication • Privacy and integrity of data in communication • Credibility and accuracy of • information • Ethical regulations in ICT • Advantages and disadvantages of digital communication	• Written tests • Oral questioning • Short tests to assess underpinned knowledge.

Suggested Methods of Delivery

- Role play
- Group discussions
- Presentations by both students and trainer;
- Guided learner activities and research to develop underpinning knowledge;

The delivery may also be supplemented and enhanced by the following, if the opportunity allows:

- Visiting media houses

Recommended Resources

Tools • Text books • Newspapers and Journals
Equipment Computers Mobile phones
Materials and supplies • Digital instructional material including DVDs and CDs • Sample of business documents and minute of the meetings
Reference materials 1. Warner, T. (Revised Edition). Communication Skills for Information Systems. Prentice Hall. 2. Sen. L. Communication Skills (2007). PHI Learning.

3. Payne, J. (Revised Edition). Communication for Personal and Professional Applications. Perfection Learning.
4. Kasneb e-learning resources (link on the Kasneb website).
5. Kasneb approved study packs.

PAPER NO. 2 INTRODUCTION TO COMPUTING SYSTEMS

Unit Description
This unit covers the competencies required to demonstrate foundational concepts of computers, operate computer hardware, identify computer software, perform data representation, identify computer networks, use the Internet and apply computer security.

Summary of Learning Outcomes
- Demonstrate foundational concepts of computers
- Operate computer hardware
- Identify computer software
- Perform Data representation
- Identify computer networks
- Use the Internet
- Apply Computer Security

CONTENT
Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Demonstrate foundational concepts of computers	• Computing terms – Computer – Input – Output – Hardware – Software – Data – Information • Computer booting process • Computer classification – Size – Type – purpose • Computer application areas – Commerce – Government – Education – Entertainment – Science and research – Communication – Trading/Marketing	• Practical • Oral questioning • Written tests
2. Operate computer hardware	• Computer components – Processor – Input – Output – Storage • Peripheral devices – Keyboard – Mouse – Monitor	• Written tests • Observation • Report writing • Practical
3. Identify computer software	• Computer software – System	• Practical • Oral questioning

Learning Outcome	Content	Suggested Assessment Methods
	– Application – Utility • Functions of operating system • File management using operating system – Files – Folders • Types of operating system – Batch Operating System. – Multitasking/Time Sharing – Multiprocessing – Real Time – Distributed – Network – Mobile • Creating user accounts in a stand alone computer • Programming languages – High level – Low level • Program translators – Interpreters – Compilers – Assembler • Software selection criteria – Functionality and ease of use – Vendor viability – Technology – Cost – Support and training – Industry expertise – Implementation	• Short tests to assess underpinning knowledge.
4. Perform Data representation	• Number systems – Decimal – Binary – Octal – Hexadecimal • Data conversions of number systems • Boolean – OR – AND – NOT • Truth tables	• Practical exercises • Oral questioning
5. Identify computer networks	• Definition of key terms – Computer network – Wide area network	• Practical exercises • Oral questioning

Learning Outcome	Content	Suggested Assessment Methods
	– Local area network • Types of computer networks – LAN – WAN – PAN • Components of computer network – Switch – Cable – Router – Hub	
6. Use the Internet	• Definition of key terms – Internet – Browser – World wide web – App – Domain – URL – Internet service provide • Communicating with internet – Email – Instant messaging – File transfer • Safety of Internet	• Practical exercises • Oral questioning
7. Apply Computer Security	• Key terms used in computer security – Computer security – Cloud – Domain – Virtual private network – Exploit – Breach – Firewall • Internet security – Threats – Countermeasures	• Practical exercises • Oral questioning

Suggested Methods of Delivery

- Presentations and practical demonstrations by trainer;
- Guided learner activities and research to develop underpinning knowledge;
- Supervised activities and projects in a computer laboratory;

The delivery may also be supplemented and enhanced by the following, if the opportunity allows:

- Visiting lecturer/trainer from the ICT sector;
- Industrial visits.

Recommended Resources

Tools
1. DVD containing operating system

Equipment Computer
Materials and supplies • Digital instructional material including DVDs and CDs
Reference materials 1. Laudon, K.C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm*. 16th Edition. Pearson Education Inc. 2. Rainer Jr. R. K., Prince, B. & Cegielski, C. (2015). *Introduction to Information System*s. 5th Edition. John Wiley & Sons, Inc. 3. Kroenke, D. M. & Boyle R. J. (2019): *Experiencing MIS*, 8th Edition. Pearson Education. 4. Kasneb e-learning resources (link on website) and approved study packs

PAPER NO. 3 NUMERICAL AND FINANCIAL LITERACY

Unit Description

This unit describes the competencies required by an entrepreneur/small trader to competently; Identify, use and interpret business data presented in numerical form; construct simple tables and graphs, identify and interpret information in graphs, identify and record basic cash transactions and determine a profit or loss.

Summary of Learning Outcomes

1. Identify, use and interpret data
2. Construct simple tables and graphs for work using familiar data
3. Identify and interpret information in familiar tables, graphs and charts for work
4. Record basic cash transactions (basic financial literacy)

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify, use and interpret data	● Whole numbers ● Simple fractions ● Decimals ● Percentages ● Sizes ● Recording and communicating numerical information	● Written ● Observation
2. Construct simple tables and graphs for work using familiar data	● Types of graphs ● Determination of data to be collected ● Selection of data collection method ● Collection of data ● Determination of variables from the data collected ● Order and collate data ● Construct a table and enter data ● Construct a graph using data from table ● Check results	● Written ● Observation
3. Identify and interpret information in familiar tables, graphs and charts for work	● Tables construction and labeling i.e. title, headings, rows and columns ● Interpreting information and data in simple tables ● Relaying information of relevant workplace tasks on/in a table ● Identify familiar graphs and charts in familiar texts and contexts ● Locate title, labels, axes, scale and key from familiar graphs and charts ● Identify and interpret information and data in familiar graphs and charts ● Relate information to relevant workplace tasks	● Written ● Observation

Learning Outcome	Content	Suggested Assessment Methods
4.Record basic cash transactions (basic financial literacy)	● Definition of terms - What is accounting - Accounting period - Accounting cycle - Income, expenses, asset, liability, capital ● Purpose and benefits of accounting ● Source documents; receipts, bills, invoices, statements, cheques ● Petty cash book ● Recording basic cash transactions: Capital, loans, cash, income, expenses, assets, liabilities ● Basic journals, ledgers and accounts ● Basic trial balance, income statement and statement of financial position ● Interpretation of basic financial statements	• Written • Observation

Suggested Delivery Methods

- Instructor led facilitation of theory
- Practical demonstration of tasks by trainer
- Practice by trainees/role play
- Discussion
- Observations and comments and corrections by trainers

Recommended Resources

- Standard operating and/or other workplace procedures manuals
- Specific job procedures manuals
- Mathematical tables

Reference materials

1. Lind, D. A., Marchal, W. G., & Wathen, S. A. (2021). Basic Statistics in Business and Economics (10th edition). New York: McGraw-Hill Education.
2. Wood, F & Robinson, S. (2018). Book-Keeping and Accounts (9th edition). Harlow. Pearson Education Ltd.
3. Kasneb e-learning resources (link on the Kasneb website).
4. Kasneb approved study packs

LEVEL TWO

PAPER NO. 4 CYBER SECURITY AND ETHICS

Unit Description

This unit covers the competencies required in applying basic skills in cyber security, applicable laws, policies and regulations and complying with ethical requirements. Competencies includes: Identify foundational concepts of Cyber Security, identify Concepts of Cyber Crime, identify Cyber Space Threats and Attacks and identify issues in Cyber Crime, identify basic issues of cyber security ethics, design cyber security policy and implement the policy.

Summary of Learning Outcomes

1. Identify foundational concepts of Cyber Security
2. Identify Concepts of Cyber Crime
3. Identify Cyberspace Threats and Attacks
4. Identify issues in Cyber Crime
5. Identify principles of Cyber Security Ethics
6. Develop Cyber Security policy
7. Implement Cyber Security policy and regulations

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify foundational concepts of Cyber Security	● Definition of key terms ○ Cyber security ○ Information ○ Cybercrime ○ Cybercriminal ○ Confidentiality ○ Integrity ○ Availability ● Types of cyber crime ○ Hacking ○ Virus dissemination ○ Logic bombs ○ Denial of service attack ○ Phishing ○ Email bombing and spamming ○ Web jacking ○ Cyber stalking ○ Data diddling ○ Identify theft ○ Salami slicing attack ○ Software piracy ● Information that is targeted through cybercrimes ○ Financial ○ Proprietary ○ Copyright	● Practical ● Oral questioning ● Written tests

2. Identify Concepts of Cyber Crime	● Dimension of cyber security ○ Integrity ○ Availability ○ Confidentiality ● Cybercrime classification ○ Crimes against individuals ○ Crimes against organisations ○ Crimes against society ● Cybercrime counter measures ○ Education ○ Legal responses ○ Patches ○ Backups ○ Access controls ○ Encryption ○ Intrusion detection and computer forensics ○ Honeypots ○ Intrusion prevention systems ○ Backtracing ○ Counterattacking	● Written tests ● Observation ● Report writing ● Practical
3. Identify Cyberspace Threats and Attacks	● Definition of key terms ○ Threats ○ Attacks ○ Counter measures ● Methods of identifying cybercrimes ○ Antispyware ○ Intrusion detection system ● Types of threat ○ Distributed denial of service (DDoS) ○ Man in the Middle (MitM) ○ Social engineering. ○ Malware and spyware. ○ Password attacks. ○ Advanced persistent threats ● (APT)	● Practical ● Oral questioning ● Short tests to assess underpinning knowledge.

4. Identify issues inCyber Crime	● Factors motivating cybercrime ● Effects of cybercrime in society ● Cyber terrorism ● Cyber warfare ● Cyber espionage ● Challenges in dealing with cybercrimes ● Artificial intelligence ● Internet of everything ● Big data	● Practical exercises ● Oral questioning

5. Identify principles of Cyber Security Ethics	● Definition of the key
	  ○ Term ethics
	  ○ Morality
	  ○ Moral system
	● Principles of ethics in cyber security
	● Ethical issues in cybersecurity
		● Practical
		● Oral questioning
		● Written tests

6. Develop Cyber Security policy	● Purpose.
	● Scope.
	● Information security objectives.
	● Authorization and access control policy.
	● Classification of data.
	  ○ Public
	  ○ Internal only
	  ○ Confidential
	  ○ Restricted
	● Data support and operations.
		● Written tests
		● Observation
		● Report writing
		● Practical

Suggested Methods of Delivery

- Presentations and practical demonstrations by trainer;
- Guided learner activities and research to develop underpinning knowledge;
- Supervised activities and projects in a computer laboratory;

The delivery may also be supplemented and enhanced by the following, if theopportunity allows:

- Visiting lecturer/trainer from the ICT sector;
- Industrial visits.

Recommended Resources

Tools

1. Monitoring tools
2. Firewalls
3. Antivirus
4. Anti-spy ware
5. Kali Linux
6. Cyber security policy template

Equipment

Computer

Materials and supplies

- Digital instructional material including DVDs and CDs

Reference materials

1. Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley.
2. Meeuwisse, R. (2017). Cybersecurity for Beginners (2nd edition). London: Cyber Simplicity Ltd.
3. Moschovitis, C. (2018). Cybersecurity Program Development for Business: The Essential Planning Guide. New Jersey: Wiley.
4. HBR, Blau, A., & Burt, A. (2019). Cybersecurity: The Insights You Need from Harvard Business Review. Boston: Havard Business Review.
5. Parenty, T. J., & Domet, J. J. (2019). A Leader's Guide to Cybersecurity: Why Boards Need to Lead--and How to Do It. Havard Business Review.
6. Kasneb e-learning resources (link on the Kasneb website).
7. Kasneb approved study packs.

PAPER NO. 5 ORGANISATION INFORMATION SECURITY

Unit Description
This unit covers the competencies required to manage organisation information security. Competencies include; Develop Organisation Information Security Policy, Classify Organisation Information and Assets and manage Organisation Information

Summary of Learnings Outcomes
1. Develop organisation information security policy.
2. Classify organisation information and assets
3. Manage organisation information

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Develop organisation information security policy.	● Definition of key terms ○ Law ○ Corporate strategy ○ Policy ○ Guidelines ○ Regulations ○ Stakeholders ○ Information security ● Legislation relevant to information security ● Elements of an information system security policy ○ Purpose ○ Audience ○ Information security objectives ○ Authority and access control policy ○ Data classification ○ Data support and operations ○ Security awareness and behavior ○ Responsibilities, rights, and duties of personnel	● Practical ● Oral questioning ● Written tests

2. Classify organisation information and assets.	● Definition of information asset
	● Information assets
	● Supporting assets
	  o Hardware
	  o Software
	  o People
	  o Buildings
	● Intangible assets
	● Aligning corporate strategy to the policy
	● Documenting assets
	  o Asset type
	  o Asset owner
	  o Asset classification
	  o Asset location
	  o Asset impact levels
	● Reviewing cyber security policy
		● Written tests
		● Observation
		● Report writing
		● Practical

3. Manage organisation information	● Definition of management
	● Duties of information system manager
	● Cyber security policies
	  o Change management policy
	  o Physical security policy
	  o Email policy
	  o Encryption policy.
	  o Vulnerability management policy media disposal policy
	  o Data retention policy
	  o Acceptable use policy
		● Practical
		● Oral questioning
		● Short tests to assess underpinning knowledge.

Suggested Methods of Delivery

- Presentations and practical demonstrations by trainer;
- Guided learner activities and research to develop underpinning knowledge;

The delivery may also be supplemented and enhanced by the following, if theopportunity allows:

- Visiting lecturer/trainer from the ICT sector;
- Industrial visits.

Recommended Resources

Tools 1.Cyber security policy template
Equipment Computer
Materials and supplies ● Digital instructional material including DVDs and CDs
Reference materials 1. Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley. 2. Meeuwisse, R. (2017). Cybersecurity for Beginners (2nd edition). London: Cyber Simplicity Ltd. 3. Moschovitis, C. (2018). Cybersecurity Program Development for Business: The Essential Planning Guide. New Jersey: Wiley. 4. HBR, Blau, A., & Burt, A. (2019). Cybersecurity: The Insights You Need from Harvard Business Review. Boston: Havard Business Review. 5. Parenty, T. J., & Domet, J. J. (2019). A Leader's Guide to Cybersecurity: Why Boards Need to Lead--and How to Do It. Havard Business Review. 6. Kasneb e-learning resources (link on the Kasneb website). 7. Kasneb approved study packs.

PAPER NO. 6 COMPUTER NETWORKS, OPERATIONS AND SECURITY

Unit Description

This unit covers the competencies required to identify network type, connect network , monitor the network, explore network infrastructure, analyse network security features, plan and design a solution and configure a network securitymeasure.

Summary of Learning Outcomes

1. Identify network type
2. Connect network devices
3. Configure a network
4. Monitor the network
5. Explore the network infrastructure
6. Analyse network security features
7. Plan and design a solution
8. Configure a network security feature

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify network type	● Uses of computer networks ● Network topologies ○ Physical ○ Logical ● Network components ○ Routers ○ Switches ○ Hub ○ RJ 45 connectors ○ Ports ○ Computers ○ Printers ● Types of network ○ Local area network ○ Personal area network ○ Metropolitan area network ○ Wide area network	● Practical ● Oral questioning ● Written tests

2. Connect network devices	● Network hardware
	  ○ Hub.
	  ○ Switch.
	  ○ Router.
	  ○ Bridge.
	  ○ Gateway.
	● Network operating software
	  ○ Functions
	  ○ Components
	● Connect hardware devices
	  ○ Computer
	  ○ Printer
	  ○ Switch
	  ○ Router
	● Testing network connectivity
	  ○ Software tools
	  ○ Hardware tools
	● Media management
	  ○ Network administration
	  ○ Network maintenance
	  ○ Network provisioning
		● Written tests
		● Observation
		● Report writing
		● Practical

3. Configure a network	● Network installation and configuration
	● IP addressing
	● Subnet masking
	● Configuring network
	  ○ DHCP
	  ○ IPv6
	  ○ DNS
	● Network segmentation
	● Setting privileges
		● Practical
		● Oral questioning
		● Short tests to assess underpinning knowledge.

4. Monitor the network	● Using network monitoring tools
	  ○ Ping
	  ○ Tracert
	  ○ Speed test
	● Switch / router monitoring
	● Network interface monitoring
	● Virtual private network monitoring
	● Other applicable monitorings	

5. Explore the network infrastructure	● Benefits of network ● Network topology ● Monitoring network speed ● Determining network users ● Security type o Firewalls o Intrusion detection system o Access control o Anti-malware software o Anomaly detection o Application security o Data loss prevent (DLP) o Email security o Endpoint security o Network segmentation o Security information and event management (SIEM) o Web security o Wireless security ● Network perimeter requirements ● Components of network perimeter o Border router intrusion prevention system	● Practical ● Oral questioning ● Written tests
6. Analyse network security features	● Types of network security protocols o Transmission Control Protocol (TCP) o Internet Protocol (IP) o User Datagram Protocol (UDP) o Post office Protocol (POP) o Simple mail transport Protocol (SMTP) o File Transfer Protocol (FTP) o Hyper Text Transfer Protocol (HTTP) o Hyper Text Transfer Protocol Secure (HTTPS) ● Applying network security protocols ● Intrusion prevention systems ● Creating security schedule ● Types of security testing ● Vulnerability scanning ● Security scanning ● Penetration scanning ● Risk assessment	● Written tests ● Observation ● Report writing ● Practical

	● Security auditing ● Posture assessment ● Ethical hacking ● Methodologies for security testing ● Tiger box ● Black box ● Grey box	
7. Plan and Design a Solution	● Types of network solutions ○ Firewalls ○ Email security ○ Anti-virus and anti-malware software ○ Network segmentation ○ Access control ○ Application security ○ Data loss prevention	● Practical ● Oral questioning ● Short tests to assess underpinning knowledge.
8. Configure a Network Security Measure	● Acquisition of security solution system ● Installing security solution ● Configuring security solution	● Practical ● Oral questioning ● Short tests to assess underpinning knowledge

Suggested Methods of Delivery

- Presentations and practical demonstrations by trainer;
- Guided learner activities and research to develop underpinning knowledge;
  The delivery may also be supplemented and enhanced by the following, if theopportunity allows:
- Visiting lecturer/trainer from the ICT sector;
- Industrial visits.

Recommended Resources

Tools 1.Cyber security policy template
Equipment Computer
Materials and supplies ● Digital instructional material including DVDs and CDs

Reference materials

1. Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley.
2. Meeuwisse, R. (2017). Cybersecurity for Beginners (2nd edition). London: Cyber Simplicity Ltd.
3. Moschovitis, C. (2018). Cybersecurity Program Development for Business: The Essential Planning Guide. New Jersey: Wiley.
4. HBR, Blau, A., & Burt, A. (2019). Cybersecurity: The Insights You Need from Harvard Business Review. Boston: Havard Business Review.
5. Parenty, T. J., & Domet, J. J. (2019). A Leader's Guide to Cybersecurity: Why Boards Need to Lead--and How to Do It. Havard Business Review.
6. Kasneb e-learning resources (link on the Kasneb website).
7. Kasneb approved study packs.

PAPER NO. 7 DATABASE DESIGN AND SECURITY

Unit Description
This unit covers competencies required to analyse user requirements, create databaseobjects, manipulate and test the database, explore the database, identify database vulnerability, enhance database security, perform audit trail and administer cyber security system

Summary of Learning Outcomes
1. Analyse user requirements
2. Create database objects
3. Manipulate the database
4. Test the database
5. Explore the database
6. Identify database vulnerabilities
7. Enhancing database security
8. Perform audit trail
9. Establish systems to be secured
10. Assess system's compatibility
11. Monitor performance using installed system
12. Document system security report

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Analyse user requirements	● Requirements definition ● Functional requirements ● Nonfunctional requirements ● Design objectives ● User requirement gathering techniques ○ Brainstorming ○ Document analysis ○ Focus group ○ Interface analysis ○ Interview ○ Observation ○ Prototyping ○ Requirement workshop. ● Documenting user requirements	● Practical ● Oral questioning ● Written tests

2. Create database objects	● Benefits of database systems ● Types of database ○ Hierarchical database ○ Network databasesystems ○ Object oriented database ● Database objects ○ Tables ○ Queries ○ Forms ○ Reports ○ Macros ● Database object tools ○ MySQL ○ PhpMyAdmin ● Creating objects	● Written tests ● Observation ● Report writing ● Practical
3. Manipulate the database	● Database manipulating tools ○ SQL ● Database manipulating techniques ○ Data manipulation language ● Creating database views	● Practical ● Oral questioning ● Short tests toassess underpinning knowledge.
4. Test a database	● Benefits of database testing ● Database testing prepare the environment ○ Run a test ○ Check test result ○ Validate according to the expected results ○ Reporting the findings ● Securing a database ○ Separate database servers and web servers ○ Using firewalls ○ Secure database user ● access	● Practical ● Oral questioning ● Short tests toassess underpinning knowledge
5. Explore the database	● Navigating database objects ● Application programs/ queries ● Query processing ● Data access	● Practical ● Oral questioning ● Written tests
6. Identify database vulnerabilities	● Database vulnerabilities ○ SQL injection ○ Buffer overflows ○ Privilege escalation ● Database countermeasures ○ Access control ○ Stored procedures	● Written tests ● Observation ● Report writing ● Practical

	○ Automatic auditing ○ Encrypting ● Training	
7. Enhancing database security	● Segmenting database ● Using passwords ● Database firewall ● Backup ● Authentication ● Authorisation short tests to assess underpinning knowledge.	● Practical ● Oral questioning
8. Perform audittrail	● Definition of database auditing ● Database auditing tools ○ SQL compliance manager ○ Triggers (Microsoft) ● Creating database auditingreport	● Practical ● Oral questioning ● Short tests to assess underpinning knowledge
9. Establish systems to be secured	● Types of information systems ○ Transaction processingSystems ○ Management information systems ○ Decision support systems. ○ Expert systems ● Types of threats ○ Malicious hackers ○ Industrial espionage ○ Employee sabotage ○ Fraud and theft ○ Loss of physical and infrastructure support ○ Errors and Omissions ● Vulnerabilities	● Practical ● Oral questioning ● Written tests
10. Monitor performance using installed system	○ Updating your operating system and patches ○ Audit and monitoring database activity ○ Test your database security o Encrypt data and backups o Cyber security system o Knowledge management system o Firewalls o Intrusion detection system	●

	● Hardware and software requirements	
11. Assess system's compatibility	● Assessing cyber security system ● Components specifications ○ Hardware specifications ○ Software specifications ● Assessing system using manufacturers manual	● Written tests ● Observation ● Report writing ● Practical
12. Monitor performance using installed System	● Threats ○ Malicious hackers ○ Industrial espionage ○ Employee sabotage ○ Fraud and theft ○ Loss of physical and infrastructure support ○ Errors and omissions ● Updating and patching system ● Enhancing system performance ● System security control measures ○ Preventive ○ Detective ● Responsive	● Practical ● Oral questioning ● Short tests to assess underpinning knowledge.
13. Document system Security report	● Documenting system performance ● System requirements ● Preparing installation and operation report	● Practical ● Oral questioning ● Short tests to assess underpinning ● knowledge

Suggested Methods of Delivery

- Presentations and practical demonstrations by trainer;
- Guided learner activities and research to develop underpinning knowledge;

The delivery may also be supplemented and enhanced by the following, if theopportunity allows:

- Visiting lecturer/trainer from the ICT sector;
- Industrial visits.

Recommended Resources

Tools

1. MySQL
2. Ms Access
3. User requirements template

Equipment
Computer

Materials and supplies

- Digital instructional material including DVDs and CDs

Reference materials

1. Connolly, T. M. & Begg, C. E. (2014): Database Systems – A Practical Approach to Design Implementation and Management (6th edition.). New Delhi: Pearson.
2. Date, C. J. (2003): An Introduction to Database Systems (8th Edition). Pearson.
3. Silberschatz, A., Korth, H. F & S. Sudarshan, S. (2019). Database System Concepts (7th edition). McGraw-Hill Higher Education.
4. Kasneb e-learning resources (link on the Kasneb website).
5. Kasneb approved study packs.