الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

The Saudi Cybersecurity Higher Education Framework

(SCyber-Edu – 1: 2020)

Sharing Notice: White, Document Classification: Open

In The Name Of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red – Personal, Confidential and for Intended Recipient Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

Amber – Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green – Sharing within the Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White – No Restriction

Updates to Document

Version

1.0

Date

October 2020

Changes

Initial version

Table of Contents

1 Introduction

As per the mandate of the National Cybersecurity Authority (NCA) that was issued by the Royal Order number 6801, dated October 31, 2017, the NCA is mandated to build the national cybersecurity workforce; to participate in developing education and training programs; to prepare professional standards and frameworks; and to develop and run professional assessment tests related to cybersecurity. Therefore, and due to the importance of developing national high-quality academic programs in cybersecurity, the NCA has worked on the development of the "Saudi Cybersecurity Higher Education Framework (SCyber-Edu)" to be a guide that can be used for developing, evaluating and accrediting cybersecurity higher education programs. This framework was developed by the NCA in cooperation and coordination with the Ministry of Education and the Education and Training Evaluation Commission.

This framework contributes to setting the minimum curriculum requirements of cybersecurity higher education programs to assure their academic quality. The goal of this framework is to ensure that higher education programs in Saudi Arabia develop highly qualified cybersecurity professionals who can join and enrich the national cybersecurity workforce and contribute to the national efforts towards "A resilient, secure and trusted Saudi cyberspace that enables growth and prosperity".

SCyber-Edu is designed in alignment with the Unified Saudi Classification for Educational Levels and Specializations, the National Qualifications Framework (NQF) and the guidelines of the National Center for Academic Accreditation and Evaluation.

1.1 Scope

This framework covers the following degree programs in cybersecurity:

1. Intermediate Diploma
2. Bachelor
3. Higher Diploma
4. Master
5. Doctoral

The framework can be used and applied to cybersecurity degree programs offered by public and private post-secondary educational institutions in Saudi Arabia.

As of this first version of the document, the framework covers the general cybersecurity programs only. With the upcoming versions, the framework will evolve to cover more specialized cybersecurity programs. Since cybersecurity is a highly dynamic discipline, the curriculum requirements in this framework will be reviewed and updated periodically.

1.2 Methodology

Even though the field of cybersecurity is still evolving as compared to other well-established fields such as computer science, several international frameworks for cybersecurity education have been recently developed to ensure the quality of cybersecurity education programs. That include the framework of the National Centers of Academic Excellence in Cyber Defense (CAE-CD) Program[1], ABET Criteria for Accrediting Computing Programs, IEEE/ACM Cybersecurity Curricula 2017 and the framework of the NCSC-certified Higher Education Program[2] . These frameworks have major commonalities. These international frameworks have been studied to define the methodology for preparing the Saudi Cybersecurity Higher Education Framework by setting the minimum curriculum requirements for each degree program in cybersecurity in terms of Program Descriptors (PD), through which Program Learning Outcomes can be derived, and Knowledge Units (KUs) that students need to study in the program. As mentioned earlier, the SCyber-Edu is compatible with the Unified Saudi Classification for Educational Levels and Specializations, the National Qualifications Framework (NQF) and the guidelines of the National Center for Academic Accreditation and Evaluation.

The PDs correspond to NQF Level Descriptors which help academic organizations design the Program Learning Outcomes (PLOs) that comprise a set of knowledge, skills and values which graduates are expected to obtain upon completion of the program. The SCyber-Edu is intended to contribute to setting the minimum PDs that need to be considered in writing the PLOs for each degree program. However, an educational institution can add additional PLOs to its cybersecurity programs.

The KUs are thematic groupings that encompass multiple related topics; where the topics cover the required curricular content for each KU. Each KU contains a set of learning outcomes.

The KU-specific learning outcomes specify the minimum of what students should know or be able to do after successfully completing the KU. It is important for educational institutions to take into account the depth, expansion and progression of these learning outcomes to suit the level of the program; and to include learning

[1] The CAE-CD program is an initiative sponsored by the National Security Agency and the Department of Homeland Security in the United States of America.

[2] The NCSC-certified higher education program is developed by the National Cyber Security Center in the United Kingdom.

outcomes related to communication skills and values in the curricula. The SCyber-Edu sets the minimum core KUs that must be covered by the program and provides a list of elective KUs. Educational institutions can offer the desired elective KUs that are relevant to their programs and students can choose from them to complete their graduation requirements. It is important to note that a KU is not necessarily a credit course. A KU may be covered by one or more credit courses and a credit course may cover one or more KUs partially or completely.

For the bachelor's degree, this framework differentiates between a cybersecurity major degree program and an IT related major degree program with a cybersecurity track within the program.

The KUs are derived from the following sources:

1. The National Centers of Academic Excellence in Cyber Defense (CAE-CD) Designation Program Guidance and Knowledge Units 2019.
2. The IEEE/ACM Cybersecurity Curricula 2017.
3. The IEEE/ACM Computer Science Curricula 2013.

The necessary additions and modifications were made to meet the national needs in this field; and to comply with the relevant frameworks in the Kingdom.

For each degree program, SCyber-Edu sets three types of requirements:

1. Admission Requirements: A list of requirements that need to be met prior to admitting a student into the program.
2. Core KUs: Mandatory KUs that a student must complete as part of the graduation requirements.
3. Elective KUs: A list of optional KUs that an educational institution and/or a student can choose from. A minimum number of these elective KUs must be completed as part of the graduation requirements.

1.3 Prerequisites and Mathematics Requirements

Some KUs are considered to be prerequisites for other KUs. It is requested that such dependencies are reflected properly in the program of study.

Furthermore, there is a foundational connection between mathematics and many cybersecurity areas; and most undergraduate cybersecurity programs require some foundational mathematics knowledge units. However, the mathematics knowledge units required for a particular program depend heavily on the nature and focus of that

program. Therefore, post-secondary educational institutions offering undergraduate programs in cybersecurity are requested to include mathematics knowledge units that are relevant to their programs and that properly meet the prerequisites of the cybersecurity knowledge units in their programs.

1.4 Structure of the Document

The rest of this document is organized as follows. Section 2 presents the covered cybersecurity programs along with their targeted PDs and KUs requirements. Section 3 describes the details of all KUs.

2. Programs[3]

2.1 Intermediate Diploma[4]

2.1.1 Program Descriptors

Knowledge	Skills	Values, Autonomy and Responsibility
• General and interrelated knowledge and understanding of the foundations, theories, principles and technical concepts in the field of cybersecurity. • Knowledge and understanding of the analytical methodologies used in cybersecurity topics and the interpretation of information related to them.	• Use a range of theoretical and technical knowledge in related sciences; and adapt them to reflect theoretical understanding in specific and unfamiliar contexts in cybersecurity. • Apply critical thinking and creativity, for providing innovative practical solutions in moderately complex and unfamiliar contexts related to the field of cybersecurity. • Use study and investigation methodologies to benefit from their results to solve problems of moderate complexity in cybersecurity. • Select and use a variety of practices and technical tools; and adapt them to carry out practical moderately complex activities in the field of cybersecurity. • Communicate in appropriate forms to demonstrate understanding and knowledge transfer to the beneficiaries in the field of cybersecurity. • Analyze and interpret numerical data; and use graphical representations in moderately complex contexts associated with the field of cybersecurity.	• Adhere to cybersecurity ethics; and demonstrate responsible citizenship. • Manage learning and work independently; set goals and work towards achieving them; and take decisions regarding learning with moderate degree of autonomy. • Manage tasks and activities related to cybersecurity; and work under indirect supervision. • Work cooperatively and lead the teamwork to perform a range of tasks with moderate responsibility; and work towards achieving common goals effectively. • Promote health, psychological and social aspects related to the field of cybersecurity.

[3] The following references were used to prepare the content of the requirements for the programs: [1], [2].

[4] This program corresponds to the Diploma program at the fifth level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

2.1.2 Admission Requirements

- High school diploma or equivalent.

2.1.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)
- Cyber Threats (CTH)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Risk Analysis (SRA)

2.1.4 Elective Knowledge Units

- Elective KUs are all remaining KUs. Students must complete at least 3 elective KUs before graduation.

2.2 Bachelor (Cybersecurity Track)[5]

2.2.1 Program Descriptors

Knowledge	Skills	Values, Autonomy and Responsibility
• Knowledge of a broad and in-depth range of basic foundations, theories, principles and concepts in the field of cybersecurity. • In-depth knowledge and understanding of the processes, tools, techniques, policies and practices used in cybersecurity. • A set of specialized knowledge related to current and new developments in the field of cybersecurity.	• Analyze and evaluate various complex information in the field of cybersecurity. • Critically evaluate, select and use cybersecurity techniques, methodologies and tools to solve problems, reduce risks and perform cybersecurity work. • Use study, investigation and research methodologies in cybersecurity projects and activities. • Perform a range of tasks and procedures using cybersecurity tools in various complex operations. • Communicate in appropriate forms to demonstrate specialized knowledge and skills; and build professional and social relationships. • Use mathematical operations and quantitative methods to process data and information in various complex cybersecurity contexts.	• Adhere to the ethics and standards of the cybersecurity profession; and demonstrate responsible citizenship. • Take constructive decisions in situations that require self-reliance to work, learn and innovate with autonomy. • Manage cybersecurity related tasks with autonomy. • Work cooperatively and constructively, with the ability to lead, practice entrepreneurship and perform a range of tasks with responsibility. • Participate actively in developing the field of cybersecurity and community service.

2.2.2 Admission Requirements

- High school diploma or equivalent.

[5] This program corresponds to the Bachelor programs at the sixth level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

2.2.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)
- Cyber Threats (CTH)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Risk Analysis (SRA)
- Data Structures (DST)
- Databases (DAT)

2.2.4 Elective Knowledge Units

- Elective KUs are all remaining KUs. Students must complete at least 4 elective KUs before graduation.

2.3 Bachelor (Cybersecurity Major)[6]

2.3.1 Program Descriptors

Knowledge	Skills	Values, Autonomy and Responsibility
• Knowledge of a broad and in-depth range of basic foundations, theories, principles and concepts in the field of cybersecurity. • In-depth knowledge and understanding of the processes, tools, techniques, policies and practices used in cybersecurity. • A broad range of specialized knowledge related to current and emerging developments and advanced topics in the field of cybersecurity.	• Analyze and evaluate various complex information in the field of cybersecurity. • Critically evaluate, select and use cybersecurity techniques, methodologies and tools to solve problems, reduce risks and perform cybersecurity work. • Use study, investigation and research methodologies in cybersecurity projects and activities. • Perform a wide range of tasks and procedures using cybersecurity tools in various complex operations; innovate and invent in this aspect. • Communicate in appropriate forms to demonstrate knowledge, specialized skills and advanced concepts; and build professional and social relationships. • Use mathematical operations and quantitative methods to process data and information in various complex cybersecurity contexts.	• Adhere to the ethics and standards of the cybersecurity profession; and demonstrate responsible citizenship. • Take constructive decisions in situations that require self-reliance to work, learn and innovate with autonomy. • Manage cybersecurity related tasks with autonomy. • Work cooperatively and constructively, with the ability to lead, practice entrepreneurship and perform a wide range of tasks with responsibility. • Participate actively in developing the field of cybersecurity and community service.

2.3.2 Admission Requirements

- High school diploma or equivalent.

[6] This program corresponds to the Bachelor programs at the sixth level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

2.3.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)
- Cyber Threats (CTH)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Risk Analysis (SRA)
- Algorithms (ALG)
- Data Structures (DST)
- Databases (DAT)
- Network Technology and Protocols (NTP)
- Network Security Administration (NSA)
- Operating Systems Hardening (OSH)

2.3.4 Elective Knowledge Units

- Elective KUs are all remaining KUs. Students must complete at least 8 elective KUs before graduation.

2.4 Higher Diploma for IT Background[7]

2.4.1 Program Descriptors

Knowledge	Skills	Values, Autonomy and Responsibility
• In-depth and specialized range of theoretical and technical knowledge and understanding of key issues in cybersecurity to protect and defend cyber systems, respond to and recover from cyber incidents. • Rigorous knowledge and understanding of processes, techniques, policies and practices used in cybersecurity. • Deep understanding of new developments and advanced topics in cybersecurity.	• Select theoretical concepts, methodologies, techniques and tools for conducting cybersecurity work; assess and use them in complex and advanced contexts. • Evaluate the main concepts, principles and theories in cybersecurity; critically review them; and express opinion on them. • Provide and design innovative solutions in complex and advanced contexts for cybersecurity problems. • Communicate in various forms to demonstrate specialized knowledge and skills with different categories of beneficiaries. • Use quantitative and qualitative methods to process data and information in complex and advanced cybersecurity contexts.	• Adhere to the ethics and standards of the cybersecurity profession; and demonstrate integrity, values and responsible citizenship. • Initiate professional planning for learning, work and professional development; and participate in making strategic professional decisions with high autonomy. • Manage tasks effectively and with high autonomy in the field of cybersecurity. • Collaborate and participate effectively in professional projects, take a leadership role and take high responsibility. • Participate effectively in developing the field of cybersecurity and community service.

2.4.2 Admission Requirements

- Bachelor's degree in cybersecurity, computer science or related fields.
- English proficiency.

2.4.3 Core Knowledge Units

If one or more Core KUs of the Bachelor (Cybersecurity Track) program (which are listed in Section 2.2.3) are not completed by the student prior to admission, they must be completed in the program of study of this degree program.

[7] This program corresponds to the Higher Diploma program at the sixth level in the Unified Saudi Classification for Educational Levels and Specializations.

2.4.4 Elective Knowledge Units

- Students must complete at least 8 elective KUs before graduation. Elective KUs for this program include all KUs except for:
  - The Core KUs of the Bachelor (Cybersecurity Track) program (listed in Section 2.2.3).
  - The following KUs:
    - Awareness and Understanding (AUU)
    - Basic Cryptography (BCY)
    - Cyber Crime (CCR)
    - Component Procurement (CPP)
    - Cybersecurity Ethics (CSE)
    - Database Management Systems (DMS)
    - Linux System Administration (LSA)
    - Windows System Administration (WSA)

2.5 Higher Diploma for Non-IT Background[8]

2.5.1 Program Descriptors

Knowledge	Skills	Values, Autonomy and Responsibility
• A range of specialized theoretical knowledge and understanding of fundamental topics in cybersecurity to analyze risk; plan to protect and defend systems; and manage cyber incident and threat response. • Rigorous knowledge and understanding of the regulatory and ethical aspects, processes, policies, practices, governance, risk management and monitoring compliance with controls and standards in the field of cybersecurity. • Deep understanding of new developments in cybersecurity.	• Apply special principles, methodologies, concepts and tools in advanced cybersecurity contexts. • Analyze, build and update policies, organizational and ethical aspects, compliance, risk management and governance in the field of cybersecurity. • Evaluate and critically review the main concepts, principles and methodologies; express opinions on them; and provide creative solutions in complex and advanced contexts for problems in cybersecurity. • Perform a range of tasks and procedures using tools for assessing cyber risks. • Communicate in various forms to demonstrate specialized knowledge and skills with different categories of beneficiaries. • Use quantitative and qualitative methods to process data and information in advanced cybersecurity contexts.	• Adhere to the ethics and standards of the cybersecurity profession; and demonstrate integrity, values and responsible citizenship. • Initiate professional planning for learning, work and professional development; and participate in making strategic professional decisions with high autonomy. • Manage tasks effectively and with high autonomy in the field of cybersecurity. • Collaborate and participate effectively in professional projects, take a leadership role and take high responsibility. • Participate effectively in developing the field of cybersecurity and community service.

2.5.2 Admission Requirements

- Bachelor's degree.
- English proficiency.

[8] This program corresponds to the Higher Diploma program at the sixth level in the Unified Saudi Classification for Educational Levels and Specializations.

2.5.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Cyber Threats (CTH)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Risk Analysis (SRA)

2.5.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 2 elective KUs before graduation.

2.6 Master[9]

2.6.1 Program Descriptors

Knowledge	Skills	Values, Autonomy and Responsibility
• Knowledge of a broad and in-depth range of theoretical and technical topics in the field of cybersecurity. • Deep understanding of the processes and practices in cybersecurity to protect and defend cyber systems, respond to advanced cyber attacks and recover from them. • Deep understanding of modern and advanced developments and theories in cybersecurity.	• Use a wide range of specialized tools, methods and practices based on knowledge of the latest developments in the field of cybersecurity. • Plan and implement advanced cybersecurity research and innovative projects to develop cybersecurity products and services. • Use a wide range of techniques, methods and practices in complex and advanced cybersecurity contexts; evaluate and critically review them. • Use advanced and specialized processes, techniques and tools to perform complex work in cybersecurity. • Communicate in various forms to demonstrate specialized knowledge and skills with different categories of beneficiaries. • Use quantitative and qualitative methods to process data and information in complex and advanced cybersecurity contexts.	• Adhere to the ethics and standards of the cybersecurity profession; and demonstrate integrity, values and responsible citizenship. • Initiate professional planning for learning, work and professional development; and participate in making strategic professional decisions with high autonomy. • Manage tasks effectively and with high autonomy in the field of cybersecurity. • Collaborate and participate effectively in professional projects, take a leadership role and take high responsibility. • Participate effectively in developing the field of cybersecurity and community service.

2.6.2 Admission Requirements

- Bachelor's degree in cybersecurity, computer science or related fields.
- English proficiency.

[9] This program corresponds to the Master program at the seventh level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

2.6.3 Core Knowledge Units

- If one or more Core KUs of the Bachelor (Cybersecurity Track) program (which are listed in Section 2.2.3) are not completed by the student prior to admission, they must be completed in the program of study of this degree program.
- Completion of a thesis or a project in a cybersecurity topic.

2.6.4 Elective Knowledge Units

- Students must complete at least 7 elective KUs before graduation. Elective KUs for this program include all KUs except for:
    - The Core KUs of the Bachelor (Cybersecurity Track) program (listed in Section 2.2.3).
    - The following KUs:
        - Awareness and Understanding (AUU)
        - Basic Cryptography (BCY)
        - Cyber Crime (CCR)
        - Component Procurement (CPP)
        - Cybersecurity Ethics (CSE)
        - Database Management Systems (DMS)
        - Linux System Administration (LSA)
        - Windows System Administration (WSA)

2.7 Doctoral[10]

2.7.1 Program Descriptors

Knowledge	Skills	Values, Autonomy and Responsibility
• A substantial body of knowledge and thorough understanding of a broad range of topics in the field of cybersecurity, integrating advanced topics, specialized theories, pioneering principles and concepts necessary to create new and original knowledge, including the integration between disciplines. • Detailed critical knowledge and understanding of cybersecurity processes, technologies, policies and practices for protecting data, systems and networks. • Comprehensive knowledge and understanding of recent developments, emerging issues and challenges in cybersecurity.	• Evaluate, combine and critically review modern concepts, principles and theories; and develop innovative, creative and pioneering solutions to highly complex issues, problems, products and services of most advanced frontier in the field of cybersecurity. • Use a wide range of techniques, methods, policies and practices in the field of cybersecurity; evaluate and critically review them. • Develop, adapt and implement highly advanced research and investigation methodologies to create original knowledge that contribute significantly to cybersecurity. • Use highly advanced and new processes, technologies, tools and devices in the field of cybersecurity to carry out new, difficult and highly complex practical activities. • Communicate in numerous forms to disseminate and promote original knowledge and new insights; and conduct scientific and professional dialogue with peers, specialized groups and the society at large. • Process and interpret quantitative and qualitative data; and use it in highly complex research, projects or innovations of most advanced frontier related to the field of cybersecurity.	• Demonstrate high level of academic integrity and values in the field of cybersecurity when dealing with emerging ethical and professional issues, research and knowledge; and promote them. • Develop professional experience continuously; and take academic and professional strategic decisions with substantial autonomy. • Formulate or develop innovative solutions for complex tasks. • Cooperate and participate in various research and professional groups with high professionalism; take initiative and lead in them; and take full responsibility for the scientific activities. • Foster professional relationships and community service in the field of cybersecurity.

[10] This program corresponds to the Doctoral program at the eighth level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

2.7.2 Admission Requirements

- Master's degree in cybersecurity, computer science or related fields.
- English proficiency.

2.7.3 Core Knowledge Units

- If one or more Core KUs of the Bachelor (Cybersecurity Track) program (which are listed in Section 2.2.3) are not completed by the student prior to admission, they must be completed in the program of study of this degree program.
- Completion of a dissertation in a cybersecurity topic.

2.7.4 Elective Knowledge Units

- Students must complete at least 3 elective KUs before graduation. Elective KUs for this program include all KUs except for:
    - The Core KUs of the Bachelor (Cybersecurity Track) program (listed in Section 2.2.3).
    - The following KUs:
        - Awareness and Understanding (AUU)
        - Basic Cryptography (BCY)
        - Cyber Crime (CCR)
        - Component Procurement (CPP)
        - Cybersecurity Ethics (CSE)
        - Database Management Systems (DMS)
        - Linux System Administration (LSA)
        - Windows System Administration (WSA)

Figure 1: Summary of Admission Requirements, Core KUs and Elective KUs for all programs.

3 Knowledge Units (KUs)

Cybersecurity Foundations (CSF)

Description	This KU provides general knowledge of basic concepts in cybersecurity.
Topics	The following topics must be included in this KU: 1. The Importance of Cybersecurity 2. Cyber Risks, Threats and Vulnerabilities 3. Maintaining Confidentiality, Integrity and Availability 4. Control Access, Authentication, Authorization and Non-Repudiation 5. Encryption and Its Uses 6. Governance and Cyber Risk Management 7. Protecting Data, Systems and Networks 8. Security Know-How and Cyber Threats Monitoring 9. Detecting and Responding to Cyber Incidents 10. Technologies and Solutions Used in Cybersecurity 11. Social Engineering and the Role of the Human Element in Cybersecurity
Learning Outcomes	By completing this KU, students should be able to: 1. Explain basic terms and concepts in the field of cybersecurity. 2. Review cyber risks, threats and vulnerabilities. 3. Explain the methodologies and techniques used to protect data, systems and networks. 4. Discuss appropriate procedures for managing cyber risks and responding to cyber incidents.

Cybersecurity Design Principles (CDP)

Description	This KU includes the knowledge and skills of the fundamentals of secure-by-design for designing secure and reliable cyber systems.
Topics	The following topics must be included in this KU: 1. Fundamentals and Importance of the Secure Design for Programs and Systems 2. Separation of Duties 3. Isolation 4. Encapsulation 5. Modularity 6. Simplicity of Design 7. Minimization of Implementation 8. Open Design 9. Complete Mediation 10. Layering and Defense-in-Depth 11. Models of Systems Security Levels and Access Privileges 12. Fail Safe Defaults and Fail Secure 13. Least Astonishment 14. Minimize Trust Surface 15. Secure Design and Usability 16. Trust Relationships 17. Secure Coding Patterns
Learning Outcomes	By completing this KU, students should be able to: 1. Express the secure-by-design principles. 2. Explain the importance of cybersecurity design principles and how each principle is useful to design trusted systems. 3. Distinguish the violated design principle for common system security weaknesses. 4. Analyze the required cybersecurity design principles needed for a given setup. 5. Apply cybersecurity design principles to complex programs and / or systems.

The following references were used to prepare the content of this knowledge unit: [2] and [5].

IT Systems Components (ISC)

Description	This KU provides general introduction to common information technology systems components and general cybersecurity implications associated with them.
Topics	The following topics must be included in this KU: 1. Endpoint protection 2. Storage Devices 3. System Architectures 4. Virtualization and Cloud 5. SCADA, Real-Time and Critical Infrastructures Environments 6. LANs, Internet and Wireless Networks 7. Network Mapping 8. Network Security Components 9. Intrusion Detection and Prevention Systems 10. Incident Response 11. Managed Services 12. Software Security 13. Configuration Management 14. Patching 15. Vulnerability Scanning 16. People and Security 17. Physical and Environmental Security 18. Internet of Things (IOT)
Learning Outcomes	By completing this KU, students should be able to: 1. Identify common IT system components (both hardware and software) and illustrate their main functions. 2. Explain main cybersecurity implications of the current and future IT environments. 3. Express common cybersecurity systems, components, activities and their values to cybersecurity.

The following reference was used to prepare the content of this knowledge unit: [2].

Basic Cryptography (BCY)

Description	This KU provides introduction to basic cryptographic algorithms and applications.
Topics	The following topics must be included in this KU: 1. Security Functions of Cryptography 2. Symmetric Cryptography 3. Block vs. Stream Data 4. Public Key Cryptography 5. Key Generation, Management, Exchange and Distribution 6. Digital Certificates 7. Hash Functions 8. Digital Signatures 9. Collision Resistance 10. Common Cryptographic Protocols and Standards 11. Types of Cryptographic Attacks 12. Cryptographic Implementation Failures 13. Certificateless Public Key Cryptography
Learning Outcomes	By completing this KU, students should be able to: 1. Explain the main components of any cryptographic system. 2. Differentiate between symmetric and asymmetric cryptography. 3. Propose an appropriate cryptographic mechanism for a given requirement and setup. 4. Demonstrate the use and strength of each cryptographic mechanism and associated implementation issues. 5. Explain the main security functions that cryptography can provide. 6. Illustrate the use of PKI to digitally sign and encrypt data. 7. Apply brute force, dictionary attack and frequency-based attacks to break encrypted data.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Basic Networking (BNW)

Description	This KU provides introduction to networks operations, components, layers, protocols, services, applications, tools and network security.
Topics	The following topics must be included in this KU: 1. ISO OSI and TCP/IP Networking models 2. Wired, Optical and Wireless Network Media 3. Network Architectures and Topologies 4. PAN, LAN, WAN, DMZ, VLAN and NAT 5. Subnetting and Supernetting 6. Common Network Devices: Routers, Switches and Firewalls 7. Network Protocols, Services and Applications: IP, TCP, UDP, ICMP, DNS, NTP, VLAN, SMTP, HTTP, VoIP, SSH, etc. 8. Basic network administration tools 9. Overview of Network Security Issues
Learning Outcomes	By completing this KU, students should be able to: 1. Explain foundational concepts of data networks including components, layers, protocols, services, applications and tools. 2. Propose a network design architecture for a given setup scenario. 3. Identify packets trace for simple connections. 4. Apply network tools to recognize packet flows. 5. Demonstrate how to perform network mapping. 6. Illustrate common network threats and vulnerabilities.

The following reference was used to prepare the content of this knowledge unit: [2].

Basic Scripting and Programming (BSP)

Description	This KU includes the knowledge and skills related to writing simple scripts and programs for implementing algorithms in order to solve given problems using programming languages according to general guidelines for writing secure software.
Topics	The following topics must be included in this KU: 1. Fundamentals of Software Development 2. Software Design Principles and Practices 3. Variables and Data Types 4. Statements and Expressions 5. Basic Logical Operations 6. Decisions and Branching 7. Loops in Programming and Their Types 8. Functions, Procedures and Calls 9. Debugging Techniques 10. Basic Data Structures and Algorithms 11. Strings, Arrays and Structures 12. Sequential and Parallel Execution 13. Scripting on Windows and Linux 14. Basic Concepts of Secure Coding: Permissions, Bounds Checking, Input Validation, Type Checking, Parameter Validation and Error Handling
Learning Outcomes	By completing this KU, students should be able to: 1. Design simple programs using secure coding principles and practices. 2. Develop and implement scripts and programs using compound conditions and loops in order to automate the tasks of a software system to solve given problems. 3. Develop and implement secure and reliable programs taking into account the characteristics of operating systems and environments.

The following references were used to prepare the content of this knowledge unit: [2] and [6].

Network Defense (NDF)

Description	This KU provides necessary concepts, skills, knowledge and tools to defend and protect a network against cyber threats.
Topics	The following topics must be included in this KU: 1. Network Attacks 2. Network Hardening 3. Minimizing Exposure, Attack Surface and Vectors 4. Defense in Depth 5. Implementing Firewalls 6. DMZs and Proxy Servers 7. VPNs 8. Honeypots and Honeynets 9. Implementing IDS/IPS 10. Network Security Monitoring 11. Network Traffic Analysis 12. Threat Hunting 13. Attack Pattern Detection 14. Network Access Control 15. Network Policy Development and Enforcement
Learning Outcomes	By completing this KU, students should be able to: 1. Illustrate main network defense concepts. 2. Demonstrate the use of network defense tools to protect a network from vulnerabilities, threats and attacks and to respond to incidents. 3. Analyze the security policies implementations to protect a network. 4. Examine network operations relevant to network defense.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Operating Systems Concepts (OSC)

Description	This KU provides a general introduction to the basic roles, functions and services of operating systems.
Topics	The following topics must be included in this KU: 1. Privileged and Non-Privileged States 2. Processes and Process Management 3. Threads and Concurrency 4. Scheduling 5. Memory Management 6. I/O Management 7. File systems 8. Virtualization and Hypervisors 9. Security Design in Operating Systems: Access controls, Domain Separation, Process Isolation, Resource Encapsulation and Least Privilege 10. Event Management
Learning Outcomes	By completing this KU, students should be able to: 1. Illustrate the basic roles, functions and services of operating systems. 2. Demonstrate operating systems interactions with hardware components and other software applications. 3. Explain main cybersecurity issues related to operating systems.

The following reference was used to prepare the content of this knowledge unit: [2].

Cyber Threats (CTH)

Description	This KU includes knowledge and skills about cyber threats and attacks.
Topics	The following topics must be included in this KU: 1. Models and Types of Cyber Threats 2. Cyber Adversary Model: Resources, Capabilities, Intent, Motivation, Risk Aversion and Access 3. Attack Techniques: Backdoors, Trojans, Viruses, Ransomware, Wireless Attacks, Social Engineering and Covert Channels 4. Password Guessing and Cracking 5. Data Interception, Spoofing and Session Hijacking 6. Data Disclosure, Alteration and Sabotage Threats 7. Repudiation Threats 8. Denial of Service Attacks, Distributed Denial of Service Attacks and Bots 9. MAC Spoofing, Web Application Attacks, Cloud Computing Attacks and Zero-Day Exploits 10. Advanced Persistent Threats (APT) 11. Attack Indication Events and Attack Timing 12. Attack Surfaces, Attack Vectors and Attack Trees 13. Insider Threats 14. Threat Information Sources 15. Strategies and Tools for Developing Cyber Threat Models 16. Cryptographic Threats 17. Legal Issues of Cyber Threats
Learning Outcomes	By completing this KU, students should be able to: 1. Categorize adversary resources, capabilities, techniques and motivations. 2. List, explain and compare types of cyber attacks. 3. Distinguish and identify attack indication events. 4. Use cyber threat modeling tools.

The following references were used to prepare the content of this knowledge unit: [2] and [7].

Cybersecurity Planning and Management (CPM)

Description	This KU provides necessary skills and abilities to design cybersecurity plans and processes for an organization.
Topics	The following topics must be included in this KU: 1. Cybersecurity Common Body of Knowledge (CBK) with Relation to Planning and Management 2. Operational, Tactical and Strategic Planning and Management 3. Cybersecurity Related C-Level Functions 4. Cybersecurity in the Core Strategy 5. Business Continuity and Disaster Recovery 6. Incident Response Processes and Procedures 7. Intellectual Property Protection Plan 8. Access Controls Implementation Management 9. Patch Management and Change Control
Learning Outcomes	By completing this KU, students should be able to: 1. Analyze system security functions and their strengths and weaknesses. 2. Design and prepare contingency plans including business continuity, disaster recovery and incident response. 3. Design patch and change management plan, intellectual property protection plan and access controls implementation plan. 4. Identify and illustrate the roles and responsibilities in cybersecurity planning and managing security.

The following reference was used to prepare the content of this knowledge unit: [2].

Policy, Legal, Ethics and Compliance (PLE)

Description	This KU provides knowledge related to cybersecurity laws, standards, regulations, guidelines, policies and ethics.
Topics	The following topics must be included in this KU: 1. Best Practices of Work Ethics in the Field of Cybersecurity for Organizations and Individuals 2. Issues Related to the Ethics and Practices of Using Social Media Platforms 3. National and International Legislation to Combat Cybercrimes 4. Judicial Authorities, Agreements, Treaties and International Organizations Related to Cybersecurity 5. National and International Cybersecurity Standards and Controls (e.g. Essential Cybersecurity Controls (ECC) issued by the National Cybersecurity Authority, HIPAA, ISO 27001, PCI DSS) 6. Privacy and Data Protection Legislation and Regulations (e.g. GDPR) 7. Intellectual Property Protection Legislation and Regulations 8. Guidelines and Best Practices in Recent Trends (e.g. BYOD, Internet of Things Protection Guidelines) 9. Best Practices for Aligning with Cybersecurity Legislation, Controls and Standards
Learning Outcomes	By completing this KU, students should be able to: 1. Discuss issues related to ethics and practices of using technology and cybersecurity. 2. Discussing legislation, regulations, guidelines and major policies in the field of cybersecurity. 3. Recognize important legislative and ethical issues when dealing with data. 4. Explain correct practices in alignment with cybersecurity legislation, controls and standards.

The following references were used to prepare the content of this knowledge unit: [2] and [8].

Security Program Management (SPM)

Description	This KU provides necessary knowledge to design, run and manage cybersecurity programs to protect and defend the organization in the cyberspace.
Topics	The following topics must be included in this KU: 1. Security Programs Goals and Objectives 2. Measuring Effectiveness 3. Roles and Responsibilities 4. Security Policies 5. Compliance with Applicable Laws and Regulations 6. Cybersecurity Best Practices and Frameworks 7. Cybersecurity Baselining 8. Program Monitoring and Control 9. Cybersecurity Awareness, Training and Education 10. Physical Security 11. Personnel Security 12. System and Data Identification 13. System Security Plans 14. Configuration and Patch management 15. System Documentation 16. Incident Response Program Management 17. Disaster Recovery Program Management 18. Certification and Accreditation
Learning Outcomes	By completing this KU, students should be able to: 1. Design, prepare and manage a security program with goals, objectives and metrics for a given organization. 2. Measure the effectiveness of a cybersecurity program.

The following reference was used to prepare the content of this knowledge unit: [2].

Security Risk Analysis (SRA)

Description	This KU includes the knowledge and skills of the models, methodologies and processes for assessing, managing and dealing with cyber risks.
Topics	The following topics must be included in this KU: 1. Principles and Concepts of Cybersecurity Risk Analysis and Management 2. Risk Management Lifecycle and Steps 3. Cyber Risk Assessment and Analysis Methodologies 4. Methodologies for Measuring and Evaluating Cyber Risks 5. Cyber Risk Management Standards and Frameworks 6. Cyber Risk Management Processes Across Levels in the Organization 7. Cyber Risks Mitigation Economics 8. Transference, Acceptance and Mitigation of Cyber Risks 9. Cyber Risks Policies for Technologies, Individuals and Entities 10. Characteristics of Organizations that Influence Cyber Risk Analysis and Management 11. Communication of Cyber Risks
Learning Outcomes	By completing this KU, students should be able to: 1. Relate risk to a cybersecurity policy. 2. Demonstrate the main risk management methodologies. 3. Evaluate and categorize risk with respect to technology, individuals and entities. 4. Choosing the appropriate methodology for dealing with cyber risks taking into consideration the advantages and disadvantages.

The following references were used to prepare the content of this knowledge unit: [2] and [9].

Advanced Algorithms (AAL)

Description	This KU provides the knowledge and skills to design, apply and analyze advanced optimization and approximation algorithms to correctly and effectively solve given problems.
Topics	The following topics must be included in this KU: 1. Bloom filters 2. Naive Bayes 3. Map-Reduce 4. Dynamic Programming algorithms 5. Markov Chain Monte Carlo 6. Coding and Compression 7. Artificial Intelligence algorithms 8. Max-Flow/Min-Cut and its applications 9. Stable Matching 10. NP-hardness 11. Linear Programming: Properties and Applications 12. Approximation Algorithms 13. Randomized Algorithms
Learning Outcomes	By completing this KU, students should be able to: 1. Design, apply and analyze advanced algorithms to optimally and efficiently solve real problems. 2. Explain the P, NP, NP-complete and NP-hard sets of problems. 3. Apply Bloom filters, Naive Bayes, Map-Reduce, Coding and Compression and AI algorithms to solve relevant problems. 4. Analyze the hardness of a problem. 5. Design approximation algorithms for NP-hard problems.

The following references were used to prepare the content of this knowledge unit: [2] and [4].

Access Control (ACC)

Description	This KU provides knowledge of access control techniques.
Topics	The following topics must be included in this KU: 1. Physical Data Security: Data Center Security, Keyed Access, Key Cards, Video Surveillance, Rack-Level Security and Data Destruction 2. Logical Data Access Control: Access Control Lists, Group Policies, Passwords, Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Rule-Based Access Control (RAC), History-Based Access Control (HBAC), Identity-Based Access Control (IBAC), Organization-Based Access Control (OrBAC), Federated Identities and Access Control 3. Secure Architecture Design: Principles of a Security Architecture and Protection of Information in Computer Systems 4. Data Leak Prevention Techniques: Controlling Authorized Boundaries, Channels, Destinations and Methods of Data Sharing
Learning Outcomes	By completing this KU, students should be able to: 1. Explain access control list. 2. Explain physical and logical access control concepts. 3. Illustrate and compare authorization and authentication techniques.

The following reference was used to prepare the content of this knowledge unit: [3].

Advanced Cryptography (ACR)

Description	This KU provides knowledge of advanced cryptographic algorithms and applications.
Topics	The following topics must be included in this KU: 1. Review of the Number Theory 2. Review of Probability and Statistics 3. AES, RSA and EC 4. Naive RSA and padded RSA 5. Suite B Algorithms 6. Families of Attacks: Differential, Man-in-the-Middle, Linear 7. Hashing and Signatures 8. Key Management 9. Modes and Appropriate Uses 10. Classical Cryptanalysis 11. Side-Channel Attacks: Timing, Power-Consumption and Differential Fault Analysis Attacks 12. Identity-based Cryptography 13. Digital Signatures 14. Virtual Private Networks 15. Post Quantum Cryptography
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate the work of advanced cryptographic algorithms and protocols. 2. Analyze security levels considering cryptography. 3. Demonstrate the roles of cryptography in common applications. 4. Analyze error propagation through a cryptosystem. 5. Analyze the security strength in encryption algorithms. 6. Apply advanced encryption algorithms for given setup scenarios. 7. Perform classical cryptanalysis. 8. Explain how side-channel attacks work and how to be avoided.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Algorithms (ALG)

Description	This KU provides the knowledge and skills needed to design, apply and analyze algorithms to correctly and effectively solve computational problems.
Topics	The following topics must be included in this KU: 1. Function Growth 2. Algorithm Analysis 3. Searching Algorithms 4. Iteration and Recursion 5. Sorting Algorithms 6. Graph Algorithms 7. Divide and Conquer Algorithms 8. Greedy Algorithms 9. Dynamic Programming Algorithms 10. Computational Complexity and Complexity Classes (P, NP, NP-Complete NP-Hard)
Learning Outcomes	By completing this KU, students should be able to: 1. Explain methods of analyzing and designing algorithms. 2. Analyze algorithms and evaluate their effectiveness. 3. Design algorithms to solve computational problems in a correct and efficient way. 4. Classify computational problems according to complexity.

The following reference was used to prepare the content of this knowledge unit: [10].

Advanced Network Technology and Protocols (ANT)

Description	This KU provides knowledge of advanced networking concepts and complex network security issues.
Topics	The following topics must be included in this KU: 1. Advanced Routing algorithms and protocols: BGP, OSPF and MPLS 2. Software Defined Networking 3. IPv6 Networking 4. IPv6 Security Issues 5. Quality of Service 6. Network Services 7. Social Network Implementation and Security Issues 8. Voice over IP (VoIP) 9. Multicasting 10. Secure DNS 11. Network Address Translation 12. Deep Packet Inspection 13. Transport Layer Security
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate the work of common advanced network protocols. 2. Analyze the security of advanced network protocols. 3. Operate network tools to examine an advance network protocol behavior.

The following reference was used to prepare the content of this knowledge unit: [2].

Analog Telecommunications (ATC)

Description	This KU provides a general introduction to analog communications systems.
Topics	The following topics must be included in this KU: 1. Signaling Methods 2. Architecture 3. Trunks, Switching 4. Grade of Service 5. Blocking 6. Call Arrival Models 7. Interference Issues
Learning Outcomes	By completing this KU, students should be able to: 1. Illustrate the main components of analog communications systems and sketch block diagrams for such systems. 2. Differentiate between types of modulation and explain their advantages and applications.

The following reference was used to prepare the content of this knowledge unit: [2].

Analytical Tools (ATT)

Description	This KU provides knowledge, skills and ability to recognize, monitor, block, divert and respond to cyberattacks.
Topics	The following topics must be included in this KU: 1. Performance Measurements 2. Data Analytics 3. Cybersecurity Intelligence
Learning Outcomes	By completing this KU, students should be able to: 1. Design, implement and manage the use of specific measurements to determine the effectiveness of the overall security program. 2. Use approaches and techniques to define and evaluate the utility of performance measurements. 3. Use techniques to manipulate large volumes of data to recognize, block, divert and respond to cyberattacks. 4. Collection, analysis and dissemination of security information including but not limited to threats and adversary capabilities.

The following reference was used to prepare the content of this knowledge unit: [3].

Awareness and Understanding (AUU)

Description	This KU provides knowledge of risk, cyber hygiene, user education and vulnerabilities and threat awareness.
Topics	The following topics must be included in this KU: 1. Risk Perception and Communication 2. Cyber Hygiene 3. Cybersecurity User Education 4. Cyber Vulnerabilities and Threat Awareness
Learning Outcomes	By completing this KU, students should be able to: 1. Illustrate cyber hygiene, cybersecurity user education and cyber vulnerabilities and threat awareness. 2. Demonstrate Security Education, Training and Awareness (SETA) programs. 3. Explain risk perception and communication in cybersecurity and privacy.

The following reference was used to prepare the content of this knowledge unit: [3].

Business Continuity, Disaster Recovery and Incident Management (BDR)

Description	This KU provides knowledge of business continuity, disaster recovery and incident management techniques.
Topics	The following topics must be included in this KU: 1. Incident Response: Anticipate, Detect and Mitigate 2. Disaster Recovery: DR Plans 3. Business Continuity: Contingency Planning, Incident Response, Emergency Response, Backup and Recovery
Learning Outcomes	By completing this KU, students should be able to: 1. Explain what resilience is and identify the environments in which resilience is important. 2. Discuss the basics of a disaster recovery plan and business continuity plan. 3. Write case-based or actual plans for disaster recovery and business continuity. 4. Explain why backups pose a potential security risk.

The following reference was used to prepare the content of this knowledge unit: [3].

Cloud Computing (CCO)

Description	This KU provides a general introduction to cloud computing technologies, services, models and security.
Topics	The following topics must be included in this KU: 1. Virtualization Platforms 2. Cloud Services: SaaS, PaaS, DaaS and IaaS 3. Hypervisors and Cloud Computing Implementations 4. Service Oriented Architectures 5. Deployment Models: Private, Public, Community and Hybrid 6. Cloud Security 7. Storage 8. Legal and Privacy Issues
Learning Outcomes	By completing this KU, students should be able to: 1. Explain cloud computing services. 2. Discuss the advantages and disadvantages of virtualization. 3. Deploy a cloud-based application. 4. Efficiently allocate resources to users and applications. 5. Discuss the importance of resource management in cloud computing. 6. Explain the requirements for a secure cloud environment.

The following references were used to prepare the content of this knowledge unit: [2] and [4].

Cyber Crime (CCR)

Description	This KU provides general information about cybercrimes and abuses in the cyberspace.
Topics	The following topics must be included in this KU: 1. Cyber Crime Types: Intrusions, Ransomware, Espionage, Intellectual Property Theft, Fraud, Extortion, Services Disruption, Data Leakage, Data Destruction, Data Falsification 2. Cyber Stalking and Predators 3. Cyber Bullying 4. Identity Theft 5. Cyber Assisted Crimes 6. Cyber Terrorism 7. Cyber Crime Laws: National Laws, International Laws, Treaties
Learning Outcomes	By completing this KU, students should be able to: 1. Explain potential cybercrimes, cyber-stalking, cyber-bullying and other abusive behaviors in the internet. 2. Demonstrate the use of cybersecurity applications for defense against crime and abuse.

The following references were used to prepare the content of this knowledge unit: [2] and [11].

Component Procurement (CPP)

Description	This KU provides knowledge related to cybersecurity aspects and components security in procurement processes.
Topics	The following topics must be included in this KU: 1. Supply Chain Risks 2. Supply Chain Security 3. Supplier Vetting
Learning Outcomes	By completing this KU, students should be able to: 1. Describe hardware and software security threats and risks in component procurement. 2. Detect and prevent component security compromises. 3. Establish trusted components suppliers and transporters.

The following reference was used to prepare the content of this knowledge unit: [3].

Cybersecurity Ethics (CSE)

Description	This KU provides knowledge of ethical issues in cybersecurity.
Topics	The following topics must be included in this KU: 1. Maintaining Privacy and Confidentiality of Information in Cybersecurity 2. Protecting User Rights in Cybersecurity 3. Ethical Codes and Frameworks related to Cybersecurity Ethics 4. Ethical Aspects in Protecting Sensitive Systems and Networks That Has High Impact on Society and Individuals 5. The Balance between Protecting and Enabling Systems and Networks 6. National and Social Responsibility in Cybersecurity
Learning Outcomes	By completing this KU, students should be able to: 1. Explain basic topics in cybersecurity ethics. 2. Practicing cybersecurity work while adhering to the ethical aspects related to it.

Databases (DAT)

Description	This KU provides knowledge, skills and abilities to manage, use and protect database systems.
Topics	The following topics must be included in this KU: 1. Database Management Systems (DBMS) Types: Relational, Hierarchical, NoSQL Databases, Object-Based, Object-Oriented and Distributed 2. Database Security Models: Inference, Aggregation, Injection, Hashing, Encryption, Data Corruption, Unauthorized Access, Database Access Controls (DAC, MAC, RBAC, Clark-Wilson)
Learning Outcomes	By completing this KU, students should be able to: 1. Compare database models and implement given database requirements using a given model. 2. Illustrate security aspects related to databases and DBMS.

The following reference was used to prepare the content of this knowledge unit: [2].

Data Administration (DBA)

Description	This KU provides students with knowledge about data life cycle, data quality and data security.
Topics	The following topics must be included in this KU: 1. Data Lifecycle: Capture, Maintenance, Transformation, Usage, Distribution, Archival and Purging 2. Data Quality: Accuracy, Completeness, Relevance, Consistency, Integrity, Cleansing, Verification and Validation 3. Data Accessibility 4. Data Utility 5. Data Storage and Archiving: Data Warehousing, Long Term Archival and Big Data 6. Hadoop, MongoDB and HBASE 7. Data Control: Ownership, Stewardship, Management, Possession, Governance 8. Data Policies: Internal and External 9. Data Security: Access Control, Data Classification and Encryption
Learning Outcomes	By completing this KU, students should be able to: 1. Explain data lifecycle stages and discuss related security issues. 2. Analyze data quality, accessibility and utility. 3. Manage the creation, change, distribution, storage and termination of data in a secure way. 4. Discuss and explain data ownership, stewardship, management, possession and governance. 5. Illustrate the importance of data classification in cybersecurity.

The following reference was used to prepare the content of this knowledge unit: [2].

Digital Communications (DCO)

Description	This KU provides knowledge of digital communications systems and related protocols.
Topics	The following topics must be included in this KU: 1. Digital Communications System Components 2. Coding Schemes 3. Digital Signaling 4. Spread Spectrum Signals 5. Multi-User Communication Access: CDMA, TDMA, FDMA, SDMA, PDMA
Learning Outcomes	By completing this KU, students should be able to: 1. Illustrate digital communications systems, subsystems and modulations. 2. Demonstrate state of the art digital communications methods. 3. Differentiate between digital communications models and discuss pros and cons for each.

The following reference was used to prepare the content of this knowledge unit: [2].

Digital Forensics (DFS)

Description	This KU provides knowledge of forensics techniques and skills to apply them for investigation activities in a way that complies with the legal requirements.
Topics	The following topics must be included in this KU: 1. Digital Forensics Terminologies 2. Legal Compliance: Applicable Laws, Affidavits, Testimony, Testifying, Case Law and Chain of Custody 3. Investigatory Process 4. Acquisition and Preservation of Evidence: Write-blocking, Imaging Procedures, Live Forensics, Analysis and Authentication of Evidence (Hashing) 5. Analysis of Evidence: Root Cause Analysis, Metadata and File Carving 6. Reporting and Presentation of Results: Timeline and Attribution
Learning Outcomes	By completing this KU, students should be able to: 1. Solve a given cyber investigation problem using digital forensics techniques and tools. 2. Illustrate legal and regulation issues related to digital forensics and investigation according to the legislation, regulations, instructions and decisions in the Kingdom.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Data Integrity and Authentication (DIA)

Description	This KU provides knowledge of data integrity and authentication techniques.
Topics	The following topics must be included in this KU: 1. Authentication Strength: Multi-Factor Authentication, Cryptographic Tokens, Cryptographic Devices, Biometric Authentication, One-Time Passwords and Knowledge-Based Authentication 2. Password Attack Techniques: Dictionary Attack, Brute Force Attack, Rainbow Table Attack, Phishing, Social Engineering, Malware-Based Attack, Spidering, Off-line Analysis and Password Cracking Tools 3. Password Storage Techniques: Cryptographic Hash Functions, Collision Resistance, Salting, Iteration Count and Password-Based Key Derivation 4. Data integrity: Message Authentication Codes (HMAC, CBC-MAC), Digital Signatures, Authenticated Encryption and Hash Trees
Learning Outcomes	By completing this KU, students should be able to: 1. Explain the main concepts in authentication, authorization, access control and data integrity. 2. Illustrate strengths and weaknesses of authentication techniques. 3. Demonstrate common attacks on passwords.

The following reference was used to prepare the content of this knowledge unit: [3].

Deep Learning (DLL)

Description	This KU provides knowledge and skills for the development and application of modern neural networks.
Topics	The following topics must be included in this KU: 1. Neural Networks: Binary Classification, Logistic Regression, Logistic Regression Cost Function, Gradient Descent, Derivatives, Computation Graph, Vectorization 2. Shallow Neural Networks: Neural Network Representation, Activation Functions, non-linear Activation Functions, Derivatives of Activation Functions, Gradient descent, Forward Propagation, Backward Propagation and Computational Graphs 3. Convolutional Neural Networks: Classic Networks, Recurrent Neural Networks and Loss Functions and Optimization 4. Unsupervised Deep Learning 5. Deep Reinforcement Learning 6. Generative Adversarial Networks
Learning Outcomes	By completing this KU, students should be able to: 1. Explain the key fundamentals of deep learning and deep network architectures. 2. Define, train and use deep learning networks to solve problems. 3. Discuss the open issues and trends in deep learning research.

Database Management Systems (DMS)

Description	This KU provides students with knowledge about main concepts of database management systems in addition to skills and abilities to utilize database management systems.
Topics	The following topics must be included in this KU: 1. Database Types: Flat, Relational, Network, Hierarchical, Object-Oriented, Object-based, Key-Value and Distributed 2. SQL Data Manipulation Language: SELECT, INSERT, DELETE and UPDATE 3. SQL Data Definition Language 4. SQL Database Administration: User Creation and Deletion, Permissions and Access Controls 5. Database concepts: Indexing, Inference, Aggregation and Polyinstantiation 6. Database Security and Protection
Learning Outcomes	By completing this KU, students should be able to: 1. Differentiate between database models. 2. Differentiate between the roles of a database, a DBMS and a database server. 3. Create, administer and operate databases. 4. Manage DBMS access controls, privilege levels. 5. Sketch structures for storing data in DBMS. 6. Design and implement a database for a given application.

The following reference was used to prepare the content of this knowledge unit: [2].

Distributed Systems Architecture (DSA)

Description	This KU provides knowledge of distributed systems and how they are connected.
Topics	The following topics must be included in this KU: 1. Distributed Systems General Concepts 2. Examples of Distributed Systems 3. Protocols and Layering 4. High Performance Computing 5. Hypervisors and Cloud Computing Implementation 6. Vulnerabilities and Exploit Examples
Learning Outcomes	By completing this KU, students should be able to: 1. Describe the components and interfaces of a networking standard provided. 2. Explain a process in an operating system and introduce various architectures for running processes and enabling their communication. 3. Describe HPC and use cases that distinguish HPC from the standard Internet. 4. Examine the attack surfaces of the various distributed computing models emphasizing the fact that every interface introduces potential vulnerabilities.

The following reference was used to prepare the content of this knowledge unit: [3].

Data Structures (DST)

Description	This KU provides students with knowledge about abstract data types and the basic operations to manipulate them, as well as the skills to apply them to solve problems.
Topics	The following topics must be included in this KU: 1. Numerical 2. Strings 3. Lists: Linked List, Double Linked List and Hash Tables 4. Arrays 5. Vectors 6. Heaps 7. Queues 8. Stacks 9. Buffers 10. Trees 11. Objects 12. Data Formats in languages 13. Categories
Learning Outcomes	By completing this KU, students should be able to: 1. Implement common abstract data types. 2. Use given abstract data types and their operations to implement solutions to given problems. 3. Differentiate between different data structures and their uses, benefits and drawbacks. 4. Design specifications of a required data structure based on given needs. 5. Illustrate the abstraction concept and recognize abstract violations for given data structure specifications.

The following reference was used to prepare the content of this knowledge unit: [2].

Device Forensics (DVF)

Description	This KU provides skills and abilities to apply forensics techniques to investigate devices.
Topics	The following topics must be included in this KU: 1. Mobile Device Analysis: Smartphones and Tablets 2. Embedded Systems: GPS, Games Consoles and Smart TVs 3. Internet of Things Devices
Learning Outcomes	By completing this KU, students should be able to: 1. Perform forensics techniques and activities on mobile, embedded systems and IoT devices. 2. Discuss legal aspects linked to forensic operations on mobile, embedded systems and IoT devices.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Embedded Systems and Internet of Things (ESI)

Description	This KU provides knowledge about embedded systems, Internet of Things (IoT) and related security issues, as well as the skills and abilities needed to design and implement components of embedded systems and Internet of Things.
Topics	The following topics must be included in this KU: 1. The Uses and Applications of Embedded Systems and Internet of Things 2. The Basic Hardware and Software Components of Embedded Systems and Internet of Things 3. Communications and Networking between Embedded Systems Devices and Internet of Things 4. Interrupt Handling, Timing Issues and Resource Management in Embedded Systems and Internet of Things 5. Operating Systems for Embedded Systems and Internet of Things 6. Implementation of Embedded Systems and Internet of Things 7. Security Issues in Embedded Systems and Internet of Things
Learning Outcomes	By completing this KU, students should be able to: 1. Describe the components and applications of embedded systems and Internet of Things. 2. Explain aspects of operating systems, networks and communications in embedded systems and Internet of Things. 3. Design and implement embedded systems and Internet of things components.

Forensic Accounting (FAC)

Description	This KU provides knowledge about forensic techniques for financial investigations, in addition to the skills and abilities to apply them.
Topics	The following topics must be included in this KU: 1. Investigative Accounting 2. Fraudulent Financial Reporting 3. Misappropriation of Assets 4. Indirect Methods of Reconstructing Income 5. Money Laundering 6. Transnational Financial Flows 7. Litigation Services 8. Evidence Management 9. Economic Damages and Business Valuations
Learning Outcomes	By completing this KU, students should be able to: 1. Describe common financial statement fraud and their detection techniques. 2. Estimate concealed revenue and income. 3. Illustrate money laundering methods and their detection and prevention techniques. 4. Evaluate fraud and theft loss and damages.

The following reference was used to prepare the content of this knowledge unit: [2].

Formal Methods (FMD)

Description	This KU provides knowledge about the mathematical logic and skills needed to apply it in the design of secure systems.
Topics	The following topics must be included in this KU: 1. Concept of Formal Methods 2. Mathematical Logic 3. Role in System Design and Software Engineering 4. Limitations of Formal Methods 5. Bell-LaPadula 6. Automated Reasoning Tools 7. System Modeling and Specification 8. Proofs 9. Model Checkers and Model Finders 10. Program Assertion Languages
Learning Outcomes	By completing this KU, students should be able to: 1. Apply formal methods to real situations. 2. Illustrate the value of formal methods and analysis techniques over testing as software validation and verification techniques. 3. Apply formal methods to software designs. 4. Explain formal specification languages advantages and disadvantages. 5. Analyze software and systems security.

The following references were used to prepare the content of this knowledge unit: [2] and [4].

Fraud Prevention and Management (FPM)

Description	This KU provides knowledge and abilities to design plans and processes to prevent and mitigate fraud.
Topics	The following topics must be included in this KU: 1. Fraud Introduction and Terminologies 2. Fraud Prevention and Auditing: Scientific Method and Benford's Law 3. Dealing with Data: Collecting, Cleaning, Verifying and Normalizing 4. Understanding Data: Analysis, Visualization, Sorting, Indexing, Summarizing and Stratifying 5. Numeric Tests for Fraud: Frequently Used Values, Even Amounts, Rounding, Ratio/Variance Analysis, Testing for Outliers, Statistical Tests and Randomization Testing 6. Modeling Fraud: Machine Learning Techniques for Fraud Detection 7. Advanced Fraud Detection and Prevention
Learning Outcomes	By completing this KU, students should be able to: 1. Evaluate cost and effectiveness of fraud detection and prevention methods. 2. Explain legal and ethical issues related to fraud detection and prevention. 3. Apply fraud tools and techniques for detection and prevention.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Hardware Architecture (HAA)

Description	This KU provides introduction to the advantages of hardware architectures standards and potential vulnerabilities.
Topics	The following topics must be included in this KU: 1. Standard Architectures 2. Hardware Interface Standards 3. Common Architectures
Learning Outcomes	By completing this KU, students should be able to: 1. Understand the idea of standard architectures and the advantages of standardization. 2. Describe various hardware interface standards starting with IC package design, through busses such as ISA and PCI for integration platforms and ending with networking standards like IEEE 802.3.

The following reference was used to prepare the content of this knowledge unit: [3].

Hardware/Firmware Security (HFS)

Description	This KU provides knowledge of hardware/firmware components and the related security issues.
Topics	The following topics must be included in this KU: 1. Physical Vulnerabilities: Unused/Unsecured Communications Channels, Test Pads, Test Paths, Back Doors, Trojans, Hidden Circuits, Doping, Induced Faults, Reverse Engineering, Unauthorized Memory Access 2. Hardware Side Channel Attacks: Timing, Power Analysis, Electromagnetic, RF analysis, Hardware Insertion and Out-of-Band Channels 3. Sourcing Attacks: Pirated, Fake, Counterfeit Parts and Supply Chain Disruption 4. Equipment Destruction Attacks 5. Hardware Security Components: Verifiable Device IDs, Random Number Generators, Boot ROM Digital Signatures, Hardware-Base Encryption Modules, Security Controllers/Co-Processors and Encryption Accelerators 6. Physical Security Attributes: Device Validation, Open/Accepted Security Algorithms, Strong Random Number Generation, Secure Time Source, Standardized Developer Interface, Clear Documentation, Key Backup/Protection, Tamper-Resistance and Scalability 7. Bootloader Vulnerabilities: Boot Sector Attacks, Single User Mode, Boot to Non-Secure OS's and Boot Loader Reconfiguration 8. Microcode Vulnerabilities 9. Firmware Vulnerabilities: Reflashing BIOS/PROMs 10. Security Role of Intermediate Layers: Hardware Abstraction Layer and Virtualization Layers
Learning Outcomes	By completing this KU, students should be able to: 1. Illustrate main hardware vulnerabilities. 2. Utilize hardware security capabilities. 3. Explain systems initialization and software loading and validation. 4. Discuss the security role of hardware abstraction layers.

The following reference was used to prepare the content of this knowledge unit: [2].

Host Forensics (HOF)

Description	This KU provides skills and ability to investigate a network host using forensics techniques.
Topics	The following topics must be included in this KU: 1. File Systems and File System Forensics 2. Hypervisor Analysis 3. Cryptanalysis 4. Rainbow Tables 5. Known File Filters (KFF) 6. Steganography 7. File Carving 8. Live System Investigations 9. Timeline Analysis
Learning Outcomes	By completing this KU, students should be able to: 1. Identify retrievable data from multiple operating system environments. 2. Demonstrate host forensics methodologies.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Hardware Reverse Engineering (HRE)

Description	This KU provides knowledge, abilities and skills to determine the functionality, input, output and stored data of given hardware components using reverse engineering procedures and techniques.
Topics	The following topics must be included in this KU: 1. Reverse Engineering Principles 2. Stimulus, Data Collection and Data Analysis 3. Specification Development 4. Capability Enhancement and Modification Techniques 5. Detecting Modification 6. Stimulation Methods and Instrumentation 7. JTAG IEEE 1149.1 Standards 8. Defining and Enumerating Interfaces 9. Functional Decomposition
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate hardware reverse engineering techniques. 2. Apply probing, measuring and data collection to identify the functionality of a given hardware component.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Information Assurance Architectures (IAA)

Description	This KU provides knowledge of security architectures used for protecting information systems.
Topics	The following topics must be included in this KU: 1. Defense in Depth 2. DMZs 3. Proxy Servers 4. Composition and Security 5. Cascading 6. Emergent Properties 7. Dependencies 8. TCB Subsets 9. Enterprise Architectures and Security Architectures 10. Secure Network Design
Learning Outcomes	By completing this KU, students should be able to: 1. Differentiate and relate between Information Assurance (IA) architecture stages and components. 2. Demonstrate knowledge of the capabilities and limitations of current methods for evaluating, planning, implementing and maintaining IA Architectures solutions. 3. Examine potential vulnerabilities for a given architecture. 4. Design information assurance architectures for given applications.

The following reference was used to prepare the content of this knowledge unit: [2].

Information Assurance Compliance (IAC)

Description	This KU provides knowledge of rules, regulations and issues related to the audit and compliance with applicable laws and regulations related to cybersecurity.
Topics	The following topics must be included in this KU: 1. Relationship Between Compliance and Audit 2. Audit Types: Internal and External 3. Audit Purposes: Requirements, Specifications, Policy, Standards, Laws, Regulatory and Internal Controls 4. Audit Process: Charter, Baseline, Activities, Reporting, Results, Recommendations, Response and Mitigation Strategy 5. Compliance Monitoring 6. Compliance Training
Learning Outcomes	By completing this KU, students should be able to: 1. Differentiate between mandatory and optional compliance requirements. 2. Design, plan and perform audits to examine compliance.

The following reference was used to prepare the content of this knowledge unit: [2].

Information Assurance Standards (IAS)

Description	This KU provides knowledge of information assurance standards.
Topics	The following topics must be included in this KU: 1. National standards related to cybersecurity 2. International regulations and standards related to cybersecurity (e.g. NIST) 3. Commercial Standards (e.g. PCI/DSS) 4. Open Standards (e.g. OWASP)
Learning Outcomes	By completing this KU, students should be able to: 1. Compare different types of national and international laws, regulations, policies, frameworks and standards. 2. Explain the impact of standards on given systems. 3. Illustrate standards implications on sub-contractors and customers. 4. List and explain main standards provisions.

The following reference was used to prepare the content of this knowledge unit: [2].

Industrial Control Systems (ICS)

Description	This KU provides knowledge of industrial control systems and their potential vulnerabilities.
Topics	The following topics must be included in this KU: 1. Hardware Components of ICS 2. Ladder Logic 3. Programmable Logic Controllers (PLCs) 4. Protocols (MODBUS, PROFINET, DNP3, OPC, ICCP, SERIAL) 5. Networking (RS232/485, ZIGBEE, 900MHz, Bluetooth, X.25) 6. Types of ICSs (e.g., Power Distribution Systems, Manufacturing) 7. Models of ICS systems: Time Driven vs. Event Driven 8. Common Vulnerabilities in Critical Infrastructure Systems 9. SCADA Security Components
Learning Outcomes	By completing this KU, students should be able to: 1. Describe the application of PLCs for automation. 2. List, explain and discuss industrial control systems components and applications. 3. Describe control schemes and differentiate between them. 4. Implement and evaluate security functionality within an industrial network. 5. Demonstrate and compare popular ICS protocols.

The following reference was used to prepare the content of this knowledge unit: [2].

Independent/Directed Study/Research (IDR)

Description	This KU provides knowledge of emerging issues related to cybersecurity.
Topics	The following topics must be included in this KU: 1. Emerging Technologies with Relevant Security Issues 2. Emerging Tools, Techniques and Methods Related to Cybersecurity
Learning Outcomes	By completing this KU, students should be able to: 1. Discuss advanced and emerging technologies related to cybersecurity. 2. Apply, demonstrate and discuss the use of emerging and advanced cybersecurity tools, methods and techniques.

The following reference was used to prepare the content of this knowledge unit: [2].

Intrusion Detection/Prevention Systems (IDS)

Description	This KU provides knowledge about methods and techniques to detect and analyze vulnerabilities and threats, as well as the skills to utilize them to mitigated associated risks.
Topics	The following topics must be included in this KU: 1. Deep Packet Inspection 2. Log File Analysis 3. Log Aggregation 4. Cross Log Comparison and Analysis 5. Anomaly Detection: Establishing Profiles, Anomaly Algorithms, Statistical Techniques, Correlation Techniques, Fuzzy Logic Approaches, Artificial Intelligence, Filtering Algorithms and Neural Networks 6. Misuse Detection: Signature Detection 7. Specification-Based Detection 8. Host-Based Intrusion Detection and Prevention 9. Network-Based Intrusion Detection and Prevention: Stealth mode 10. Distributed Intrusion Detection 11. Hierarchical IDS's 12. Honeynets/Honeypots 13. Intrusion Response: Device Reconfiguration, Notifications, Logging, SNMP Trap, Email, Visual/Audio Alert, Trace Recording, Opening Application, Session Interruption and Reach Back
Learning Outcomes	By completing this KU, students should be able to: 1. Detect and respond to host and network intrusions. 2. Apply tools to detect malware and unauthorized devices on a network. 3. Design corrective procedures to respond to discovered intrusions. 4. Setup, install and configure intrusions detection/prevention system; and optimize their performance and accuracy.

The following reference was used to prepare the content of this knowledge unit: [2].

Identity Management (IMM)

Description	This KU provides knowledge of identity management techniques.
Topics	The following topics must be included in this KU: 1. Identification and Authentication: People and Devices, Network Access Control (NAC), Identity Access Management (IAM), Roles, Multi-Method Identification and Authentication Systems, Biometric Authentication Systems, Accuracy/FAR/FRR, Resistance, Privacy, Usability and Tolerability of the Methods 2. Physical and Logical Assets Control: System Hardware, Network Assets, Backup/Storage Devices, Rules-Based Access Control (RAC), Role based Access Control (RBAC), Inventory Tracking Methods, Identity Creation Methods 3. Identity as a Service (IaaS) 4. Third-Party Identity Services 5. Access Control Attacks and Mitigation Measures: Password, Dictionary, Brute Force, Spoofing Attacks, Multi-Factor Authentication, Strong Password Policy, Secure Password Files and Restrict Access to Systems
Learning Outcomes	By completing this KU, students should be able to: 1. Differentiate between identification, authentication and access authorization. 2. Discuss the audit trails and logging importance in identification and authentication. 3. Apply least privilege and segregation of duties concepts. 4. Explain access control attacks and discuss mitigation measures.

The following reference was used to prepare the content of this knowledge unit: [3].

Information Storage Security (ISS)

Description	This KU provides knowledge of information storage security techniques.
Topics	The following topics must be included in this KU: 1. Disk and File Encryption: Hardware vs. Software Encryption 2. Data Erasure: Overwriting, Degaussing, Physical Destruction Methods and Memory Remanence 3. Data Masking: for Testing, for Obfuscation and for Privacy 4. Database Security: Access, Authentication, Auditing and Application Integration Paradigms
Learning Outcomes	By completing this KU, students should be able to: 1. Describe hardware and software encryption for disks and files. 2. Describe data erasure techniques. 3. Explain data masking applications. 4. Discuss database access, authentication, auditing and application integration.

The following reference was used to prepare the content of this knowledge unit: [3].

Introduction to the Theory of Computation (ITC)

Description	This KU provides knowledge of finite automata and their role and use in computation. It also provides the skills and abilities to analyze the complexity of computation problems.
Topics	The following topics must be included in this KU: 1. Automata 2. Turing Machines 3. Deterministic and Non-Deterministic Finite Automata 4. Formal Language Theory 5. Computability and Non-Computability 6. Turing Computability 7. Analysis of Algorithms 8. Complexity Measures: Time, Storage, Communications and Numbers of Processors 9. Big O Notation 10. Best, Worst and Average Complexity 11. Upper and Lower Bounds on Complexity 12. Classes of Complexity: P, NP and Intractability
Learning Outcomes	By completing this KU, students should be able to: 1. Explain abstract machines theory and automata. 2. Differentiate between computable and incomputable functions. 3. Explain complexity and quantify resources requirements for problems computation. 4. Analyze given problems using deterministic and non-deterministic finite automata.

The following references were used to prepare the content of this knowledge unit: [2] and [4].

Life-Cycle Security (LCS)

Description	This KU provides knowledge of security principles and skills to apply them to improve security throughout the system or product lifecycle.
Topics	The following topics must be included in this KU: 1. System Life-Cycle Phases and Issues: Initiation, Requirements, Design, Development, Testing, Deployment, Operations, Maintenance and Disposal 2. Vulnerability Mapping, Management and Tractability 3. Threat Modeling 4. Software Assurance Maturity Model 5. Role of Project/Program Management 6. Role of Process Management 7. Importance of Culture and Training 8. Development Processes and Paradigms 9. Configuration Management 10. Developmental Threats
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate and apply practices, processes and methodologies to secure software. 2. List system life-cycle phases and explain each phase along with security related issues. 3. List and explain maturity model elements.

The following reference was used to prepare the content of this knowledge unit: [2].

Low Level Programming (LLP)

Description	This KU provides skills to securely perform low level operations using low level programing languages.
Topics	The following topics must be included in this KU: 1. Low Level Access Support in C 2. Programing in Assembly 3. Library Functions Security 4. Pointers and Pointer Manipulation 5. Modularization in Low Level Programs 6. Defensive Programming Techniques 7. Compile, Assemble and Link Object Files 8. Calls in Assembly
Learning Outcomes	By completing this KU, students should be able to: 1. Apply low level programming to implement OS components and hardware drivers. 2. Discuss the benefits and the risks of using low level programming.

The following reference was used to prepare the content of this knowledge unit: [2].

Linux System Administration (LSA)

Description	This KU provides skills to perform basic operations in LINUX system administration.
Topics	The following topics must be included in this KU: 1. OS Installation 2. User Accounts Management: Access Control, Password Policies, Authentications Methods and Group Policies 3. Command Line Interfaces 4. Configuration Management 5. Updates and Patches 6. Event Logging and Auditing 7. Managing System Services 8. Virtualization 9. Backup and Restoring Data 10. File System Security 11. Network Configuration 12. Host Intrusion Detection 13. Security Policy Development
Learning Outcomes	By completing this KU, students should be able to: 1. Install, configure, operate and maintain LINUX OS in a secure way. 2. Setup user accounts, develop authentication policies and implement them. 3. Design and implement audit configurations. 4. Perform backup and restore operations. 5. Demonstrate the importance of reviewing security logs and installing updates and patches periodically.

The following reference was used to prepare the content of this knowledge unit: [2].

Media Forensics (MEF)

Description	This KU provides skills and ability to investigate media using forensics techniques.
Topics	The following topics must be included in this KU: 1. Drive Acquisition 2. Evidence Authentication: Verification, Validation and Hashing 3. Metadata: Modification, Access or Change (MAC) Timestamps 4. Live vs. Static Acquisition 5. Sparse vs. Full Imaging 6. Slack Space 7. Hidden Files, Clusters and Partitions
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate forensic analysis techniques on given media. 2. Apply forensic methods on specified media.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Machine Learning (MLL)

Description	This KU provides knowledge of machine learning algorithms and mathematical and statistical models. It also provides the skills to use these algorithms and models in machine learning applications.
Topics	The following topics must be included in this KU: 1. Linear Regression 2. Linear Classification 3. Logistic Regression 4. K-Nearest Neighbors 5. Evaluation Metrics: AUC, Precision, Recall, Specificity, MSE, MAPE and RMSE 6. Hypothesis Testing 7. Gradient Descent 8. Decision Trees 9. Random Forest 10. Support Vector Machines 11. Probabilistic Classifiers 12. Artificial Neural Networks 13. Clustering 14. Singular Value Decomposition (SVD), Principal Component Analysis (PCA) and Autoencoders 15. Reinforcement Learning
Learning Outcomes	By completing this KU, students should be able to: 1. Apply machine learning algorithms and models to classification, regression and clustering problems. 2. Evaluate and interpret the results of the algorithms. 3. Analyze and handle large data sets.

Mobile Technologies (MOT)

Description	This KU provides knowledge of mobile technologies including their hardware, communications, management and programing environments.
Topics	The following topics must be included in this KU: 1. 2G, 3G, 4G/LTE and 5G: Standards Heritage and Core Architecture Evolution 2. Design Choices 3. Encryption 4. Mobile Use of SS7 5. RRC Signaling 6. Billing/Charging 7. Mobile Security
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate how mobile systems function to secure voice and data access. 2. Explain how network connectivity is maintained during motion. 3. Discuss main techniques to secure mobile systems and communications.

The following reference was used to prepare the content of this knowledge unit: [2].

Network Security Administration (NSA)

Description	This KU provides knowledge related to the administration and maintenance of enterprise security infrastructures.
Topics	The following topics must be included in this KU: 1. Mapping Business Objectives to Technology Objectives 2. Main Security Solutions and Product Categories and Features 3. Information Security Conflicts with Potential Solutions 4. Cybersecurity Best Practices 5. Applying Network Security Policies 6. Risk Posture and Risk Appetite 7. Network and Systems Monitoring Tools 8. Issue Evaluation, Response and Management 9. Incident Identification 10. Incident Response Processes and Management 11. Deployment and Upgrade Processes 12. User Acceptance Testing 13. Blackout Plans 14. Maintenance Windows and Management
Learning Outcomes	By completing this KU, students should be able to: 1. Analyze needs and recommend solutions, products and technologies. 2. Select best security practices to satisfy business objectives according to risk assumptions. 3. Protect IT assets and infrastructure from potential threats. 4. Perform systems monitoring for anomalies and periodically perform system updating and patching. 5. Practice incident response activities to breaches, intrusions and theft. 6. Plan, test, implement and evaluate software and hardware deployment.

The following reference was used to prepare the content of this knowledge unit: [2].

Network Technology and Protocols (NTP)

Description	This KU provides knowledge of network protocols and components. It also provides skills to use tools to monitor and analyze a network.
Topics	The following topics must be included in this KU: 1. Network Switching: ARP, RARP and Layer 2 Security Issues 2. IPv4 Suite: IPv4 Addressing 3. IPv6 Suite: IPv6 Addressing 4. Routing in IPv4 and IPv6: Routing Tables and Metrics, Layer 3 Security Issues and IPsec 5. Network Naming: DNS and NetBIOS 6. Network Analysis and Troubleshooting: Netflow
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate and explain layer 2 networking. 2. Illustrate IPv4 and IPv6 structure. 3. Discuss common network vulnerabilities. 4. Detect and mitigate layer 2 and layer 3 security issues. 5. Apply networks analysis tools for troubleshooting.

The following reference was used to prepare the content of this knowledge unit: [2].

Network Forensics (NWF)

Description	This KU provides skills and ability to investigate and analyze network traffic using forensic techniques.
Topics	The following topics must be included in this KU: 1. Packet Capture and Analysis 2. Intrusion Detection and Prevention 3. Interlacing of Device and Network Forensics 4. Log File Analysis
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate network forensic methodologies. 2. Analyze network traffic. 3. Detect malicious and anomalous activities and their effects.

The following reference was used to prepare the content of this knowledge unit: [2].

Operating Systems Administration (OSA)

Description	This KU provides knowledge and skills to perform basic operations in operating systems administration.
Topics	The following topics must be included in this KU: 1. OS Installation 2. User Accounts Management: Access Control, Password Policies, Authentications Methods and Group Policies 3. Command Line Interfaces 4. Configuration Management 5. Updates and Patches 6. Event Logging and Auditing 7. Managing System Services 8. Virtualization 9. Backup and Restoring Data 10. File System Security 11. Network Configuration 12. Host Intrusion Detection 13. Security Policy Development
Learning Outcomes	By completing this KU, students should be able to: 1. Setup user accounts, develop authentication policies and implement them. 2. Design and implement audit configurations. 3. Perform backup and restore operations. 4. Review security and system logs. 5. Install patches and updates.

The following reference was used to prepare the content of this knowledge unit: [2].

Operating Systems Hardening (OSH)

Description	This KU provides knowledge, skills and abilities to improve the security and robustness of operating systems.
Topics	The following topics must be included in this KU: 1. Secure Installation 2. Removing Unnecessary Components 3. File System Maintenance: Isolation of Sensitive Data 4. User Restrictions: Access and Authorizations 5. User, Group and File Management 6. Password Standards and Requirements 7. Shutting Down Unnecessary and Unneeded Services 8. Closing Unnecessary and Unneeded Ports 9. Patch Management and Software Updates 10. Virtualization 11. Vulnerability Scanning
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate hardening steps for a given OS according to given applications. 2. Perform secure OS installation and disable unneeded components, services and ports. 3. Perform OS patching and updating periodically.

The following reference was used to prepare the content of this knowledge unit: [2].

Operating Systems Theory (OST)

Description	This KU provides knowledge of operating system concepts, components and interfaces.
Topics	The following topics must be included in this KU: 1. Privilege States 2. Processes, Threads and Process/Thread Management 3. Memory Management and Virtual Memory 4. Inter-Process Communications 5. Concurrency, Synchronization and Deadlocks 6. File Systems 7. Input and Output 8. Real-time Operating Systems and Security Issues 9. Distributed OS Architectures and Security Issues 10. Race Conditions 11. Buffer Overflows 12. Virtualization 13. Clear Interface Semantics
Learning Outcomes	By completing this KU, students should be able to: 1. Illustrate and demonstrate operating systems theory and implementation. 2. Design and implement OS architectural changes.

The following reference was used to prepare the content of this knowledge unit: [2].

Privacy (PRI)

Description	This KU provides knowledge and skills about the concepts and principles of privacy, methods of assessing their preservation, assistive techniques in privacy, best practices, standards and relevant privacy legislation and enforcement.
Topics	The following topics must be included in this KU: 1. Privacy Concepts and Principles 2. Privacy and Data Preservation 3. Data Ownership and Classifications 4. Personally Identifiable Information (PII) 5. Practices Related to Preserving Privacy (Determining the Purpose for Storing or Sharing Data, Reducing Data Saved by Purpose, Transparency, Requesting Consent to Share, Restricting Use, Data Quality, Integrity, Confidentiality, Accountability and Auditing) 6. Risks and Types of Attacks on Privacy 7. Methods of Assessing Privacy Impact 8. International Laws, Regulations and Legislation for Privacy: such as GDPR, HIPPA, Data Protection Act and Others 9. Tools and Techniques for Improving and Preserving Privacy 10. Policies and Procedures for Maintaining Privacy in Organizations 11. Privacy Issues in Emerging Technologies such as: Internet of Things, FinTech and Others
Learning Outcomes	By completing this KU, students should be able to: 1. Explain the concepts and principles of privacy. 2. Clarify the difference between preserving privacy and protecting data. 3. Identify tools and techniques that improve privacy preservation. 4. Discuss the impact of national and international privacy legislation and regulations on the work of organizations and individuals. 5. Assess privacy impact on given examples. 6. Discuss contemporary issues related to privacy at the national and international levels.

Penetration Testing (PTT)

Description	This KU provides knowledge of methods to exploit vulnerabilities to gain control or access to systems and networks. It also provides skills and ability to utilize and apply these methods.
Topics	The following topics must be included in this KU: 1. Flaw Hypothesis Methodology 2. Other Methodologies (e.g., OSSTMM) 3. Identifying Flaws from Documentation 4. Identifying Flaws from Source Code Analysis 5. Vulnerability Scanning 6. Families of Attacks 7. Flaws that Lead to Vulnerabilities 8. Enumeration and Footprinting 9. Attack Surface Discovery 10. Attack Vectors
Learning Outcomes	By completing this KU, students should be able to: 1. Plan and perform penetration testing on a system or a network. 2. Discuss and compare families of attacks. 3. Explain different types of vulnerabilities and how they may be exploited.

The following reference was used to prepare the content of this knowledge unit: [2].

QA/Functional Testing (QAT)

Description	This KU provides knowledge of methods used to assess the extent to which a requirement is met by a functional unit.
Topics	The following topics must be included in this KU: 1. Testing Methodologies: White, Grey and Black Box Testing 2. Test Coverage Analysis 3. Automatic and Manual Generation of Test Inputs 4. Test Execution 5. Validation of Results
Learning Outcomes	By completing this KU, students should be able to: 1. Design and develop effective, structured and organized tests. 2. Perform security functional testing to demonstrate that security policies and mechanisms are completely and correctly implemented. 3. Perform functional testing to validate security policies implementation.

The following reference was used to prepare the content of this knowledge unit: [2].

Radio Frequency Principles (RFP)

Description	This KU provides knowledge about radio frequency communications.
Topics	The following topics must be included in this KU: 1. Basics of Electromagnetic Radiation 2. Antennas 3. Information Modulation 4. Digital Modulation 5. Spectral Representation 6. Bandwidth 7. BER 8. Eb/No vs. S/N 9. Limiting Access in RF 10. Propagation Principles
Learning Outcomes	By completing this KU, students should be able to: 1. Explain isolating RF emissions methods. 2. Explain obfuscating RF transmissions techniques. 3. Demonstrate the tradeoffs related to bandwidth data rate, modulation, complexity, acceptable BER and signal spreading.

The following reference was used to prepare the content of this knowledge unit: [2].

Software Assurance (SAS)

Description	This KU provides knowledge of methods and techniques for software assurance.
Topics	The following topics must be included in this KU: 1. Security Principles: Segregation, Isolation, Encapsulation, Least Privilege, Simplicity, Minimization, Fail Safe Defaults, Fail Secure, Modularity, Layering, Least Astonishment, Open Design, Usability and Reduce Attack Surfaces 2. Security of Alternative Designs 3. Review Secure Design Patterns 4. Levels of security requirements for system data 5. Audit Trail 6. Security Modeling Techniques and Vulnerability Mapping 7. Resiliency Increase 8. Design Reviews
Learning Outcomes	By completing this KU, students should be able to: 1. Apply security design principles. 2. Illustrate the effects of system design and architecture on security. 3. Design a given system to optimally satisfy security requirements. 4. Construct a secure design using modeling and vulnerability assessment. 5. Discuss how Design Reviews can significantly help improving security.

The following reference was used to prepare the content of this knowledge unit: [2].

System Control (SCC)

Description	This KU provides knowledge of system control techniques including detecting, compensating for, defending against and preventing attacks.
Topics	The following topics must be included in this KU: 1. Access control: Controlling Access to Resources and the Integrity of the Controls 2. Authorization Models: Management of Authorization across many Systems and the Distinction from Authentication 3. Intrusion Detection: Anomaly, Misuse [Rule-Based, Signature-Based] and Specification-Based Techniques 4. Attacks: Trees and Graphs and Specific attacks 5. Defenses: ASLR, IP Hopping and Intrusion Tolerance 6. Audit: Logging, Log Analysis and Relationship to Intrusion Detection 7. Malware: Viruses, Worms and Ransomware 8. Vulnerabilities Models: RISOS and PA, CVE and CWE 9. Penetration Testing: Flaw Hypothesis Methodology, ISSAF, OSSTMM, GISTA, PTES 10. Forensics: System Requirements for Forensics 11. Recovery and Resilience: Availability Mechanisms
Learning Outcomes	By completing this KU, students should be able to: 1. Examines the security considerations involved in controlling the system itself. 2. Detect, compensate for, defend against and prevent attacks related to system control.

The following reference was used to prepare the content of this knowledge unit: [3].

Secure Communication Protocols (SCP)

Description	This KU provides knowledge of secure communication protocols.
Topics	The following topics must be included in this KU: 1. Application and transport layer protocols: HTTP, HTTPS, SSH and SSL/TLS 2. Attacks on TLS: Downgrade Attacks, Certificate Forgery, Implications of Stolen Root Certificates and Certificate Transparency 3. Internet/Network Layer: IPsec and VPN 4. Privacy Preserving Protocols: Mixnet, Tor, Off-the-Record Message and Signal 5. Data Link Layer: L2TP, PPP and RADIUS
Learning Outcomes	By completing this KU, students should be able to: 1. Practice secure communication protocols (e.g. HTTPS, SSH, SSL/TLS, IPsec, VPN, L2TP, PPP and RADIUS protocols). 2. Illustrate common attacks on various communication protocols and how to protect against them.

The following reference was used to prepare the content of this knowledge unit: [3].

Supply Chain Security (SCS)

Description	This KU provides knowledge of security issues related to third-party components used in building complex systems.
Topics	The following topics must be included in this KU: 1. Supply Chain Risks: Cybersecurity Risks Related to Third-Party in the Supply Chain and Best Practices to Manage Them 2. Global Development Trends 3. Offshore Production 4. Transport and Logistics of IT Components 5. Evaluation of 3rd Party Development Practices 6. Capabilities and limitations of Software and Hardware Reverse Engineering 7. Procurement Process: Physical Security, Split Manufacturing, Traceability, Cargo Screening and Validation
Learning Outcomes	By completing this KU, students should be able to: 1. Discuss cybersecurity issues related to outsourcing hardware, software development and integration. 2. List and explain common vulnerabilities in supply chain components. 3. Demonstrate methods to mitigate supply chain cybersecurity risks and explain the challenges of these mitigation methods.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Systems Programming (SPG)

Description	This KU provides knowledge, skills and ability to develop complex and low-level software.
Topics	The following topics must be included in this KU: 1. Hardware and Software Interfaces and Interactions 2. Types of Systems Programs: Development Environments, Operating Systems, Utilities, Networking Functions, Device Drivers, Storage Frameworks and Gaming Engines 3. Layered Services Design 4. Application Programming Interfaces (API's) 5. Programming Operating Systems Internal Interfaces 6. Low Level Programming: Assembly, C 7. Resource Optimization 8. Resource Management 9. Runtime Overhead Minimization 10. Direct Control of Memory Access and Flow Control 11. Memory Management in Systems Software 12. Security Concerns in Systems Software 13. Monitoring and Logging Systems Software
Learning Outcomes	By completing this KU, students should be able to: 1. Develop programs that can correctly operate under limited resources. 2. Apply a layered approach for API's access. 3. Implement new functions in an OS kernel or device driver. 4. Implement systems functions without using external libraries.

The following reference was used to prepare the content of this knowledge unit: [2].

Secure Programming Practices (SPP)

Description	This KU provides knowledge skills and abilities needed to develop and implement secure software.
Topics	The following topics must be included in this KU: 1. Common Software Vulnerabilities and Best Practices to Avoid Them 2. Defensive Programming Practices 3. Uses of Cryptography in Programming 4. Methodologies for Checking and Reviewing Programs in Terms of Cybersecurity 5. Software Static and Dynamic Analysis 6. Implementing Software Functions Securely and with Proper Access Control 7. Input Testing and Validation 8. Data Type Checking and Data Range Validation
Learning Outcomes	By completing this KU, students should be able to: 1. Explain common software vulnerabilities. 2. Discuss best practices and methodologies for developing and testing secure software. 3. Design and develop secure software that meets its functional requirements.

Software Reverse Engineering (SRE)

Description	This KU provides skills and ability to perform reverse engineering of executable code to determine its function, effect and implementation details.
Topics	The following topics must be included in this KU: 1. Malware Analysis 2. Reverse Engineering Tools & Techniques 3. Static vs Dynamic Analysis 4. Sandboxing 5. Anti-Reverse Engineering Techniques
Learning Outcomes	By completing this KU, students should be able to: 1. Practice software reverse engineering techniques. 2. Apply software reverse engineering tools to discover functionality and implementation details of software or malware.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Software Security Analysis (SSA)

Description	This KU provides knowledge of tools and methods used to analyze the security of software in binary or source code form. It also provides skills and abilities to use these tools and methods for software security analysis.
Topics	The following topics must be included in this KU: 1. Testing Methodologies 2. Source and Binary Code Analysis 3. Static and Dynamic Analysis Techniques 4. Sandboxing 5. Common Analysis Tools and Methods
Learning Outcomes	By completing this KU, students should be able to: 1. Describe tools and techniques used for software security analysis. 2. Apply software security analysis tools to analyze unknown software components.

The following reference was used to prepare the content of this knowledge unit: [2].

Systems Security Engineering (SSE)

Description	This KU provides skills to participate in the development of large-scale secure systems using related techniques and methods throughout the entire system life-cycle.
Topics	The following topics must be included in this KU: 1. Testing Design 2. Testing methodologies 3. Emergent Properties 4. Systems Engineering 5. System Integration 6. Make or Buy Analysis 7. Systems Security Analysis 8. Enterprise System Components
Learning Outcomes	By completing this KU, students should be able to: 1. Participate in the development of system components by collecting and analyzing requirements along with designing, implementing, testing and maintaining components. 2. Analyze system components in a composed system and how they interact. 3. Analyze a given system design and assess its compliance with the system security requirements.

The following reference was used to prepare the content of this knowledge unit: [2].

Vulnerability Analysis (VLA)

Description	This KU provides knowledge and skills related to detection, identification, root cause determination and mitigation of system and network vulnerabilities.
Topics	The following topics must be included in this KU: 1. Vulnerability Definition 2. System Modeling Techniques 3. Vulnerability Mapping 4. Vulnerability Characteristics and Classification. 5. Taxonomy: Buffer Overflows, Privilege Escalation, Rootkits, Trojans, Backdoors, Viruses, Return Oriented Programming, Social Engineering Vulnerabilities and Administrative Privileges Effect on Vulnerabilities 6. Vulnerabilities Root Causes 7. Mitigation Strategies 8. Countermeasure Analysis 9. Vulnerability Disclosure 10. Vulnerabilities Detection Tools and Techniques
Learning Outcomes	By completing this KU, students should be able to: 1. Apply vulnerabilities detection tools and techniques. 2. Construct vulnerability map of a given system. 3. Trace vulnerabilities to identify their root causes. 4. Demonstrate countermeasures for vulnerabilities mitigation and analyze these countermeasures. 5. Discuss scenarios when vulnerabilities must be disclosed.

The following references were used to prepare the content of this knowledge unit: [2] and [3].

Virtualization Technologies (VTT)

Description	This KU provides knowledge of modern host virtualization and its implementation, deployment, use, system components and security.
Topics	The following topics must be included in this KU: 1. Virtualization Architectures 2. Virtualization Techniques for Code Execution 3. Memory Management in Virtual Environments 4. Networking in Virtual Environments 5. Storage in Virtual Environments 6. Scheduling of Virtual Machines 7. Migration and Snapshots 8. Virtual Management Layers 9. Digital Forensics in Virtual Environments
Learning Outcomes	By completing this KU, students should be able to: 1. Explain virtualization concepts. 2. Explain virtualization architectures and compare them. 3. Design, construct, implement and configure virtualization environments.

The following reference was used to prepare the content of this knowledge unit: [2].

Web Application Security (WAS)

Description	This KU provides knowledge of technology, tools and practices related to web applications. It also provides skills to apply these tools and practices to develop and deploy secure web applications.
Topics	The following topics must be included in this KU: 1. Web Application Technologies: HTTP Protocol, Encoding Schemes, Web Application Architectures, AJAX, XML and JSON 2. Server-Side Controls 3. Authentication 4. Session Management 5. Access Controls 6. Client-Side Controls 7. Input-Based Vulnerabilities: SQL Injection, Blind SQL Injection, Cross-Site Scripting and Cross-Site Request Forgery 8. JavaScript and Cookies Attack 9. Function-Specific Input Vulnerabilities 10. Attacking Application Logic 11. Recent Attack Trends 12. Shared Hosting Vulnerabilities 13. Application Server Vulnerabilities
Learning Outcomes	By completing this KU, students should be able to: 1. Demonstrate common web application technologies and explain security issues related to them. 2. Develop and deploy secure web applications. 3. Illustrate web applications security principles.

The following reference was used to prepare the content of this knowledge unit: [2].

Windows System Administration (WSA)

Description	This KU provides knowledge and skills to perform basic operations in Microsoft Windows system administration.
Topics	The following topics must be included in this KU: 1. OS Installation 2. User accounts management: Access controls, Password Policies, Authentications Methods and Group Policies 3. Command Line Interfaces 4. Configuration Management 5. Updates and Patches 6. Event Logging and Auditing 7. Managing System Services 8. Virtualization 9. Backup and Restoring Data 10. File System Security 11. Network Configuration: Port Security 12. Host Intrusion Detection 13. Security Policy Development
Learning Outcomes	By completing this KU, students should be able to: 1. Install, configure, operate and maintain MS Windows OS in a secure way. 2. Setup user accounts, develop authentication policies and implement them. 3. Design and implement audit configurations 4. Perform backup and restore operations. 5. Demonstrate the importance of reviewing security logs and installing updates and patches periodically.

The following reference was used to prepare the content of this knowledge unit: [2].

Wireless Sensor Networks (WSN)

Description	This KU provides knowledge of wireless sensor networks principles, the challenges and cybersecurity aspects related to them.
Topics	The following topics must be included in this KU: 1. Wireless Sensor Devices 2. Wireless Sensor Networks Applications 3. Deploying Wireless Sensor Networks: Structured, Randomized, Topology, Signal Strength Control, Coverage, Mobility 4. Localization 5. Synchronization 6. Wireless Transmission Characteristics 7. Channel Access 8. Sleep Scheduling 9. Effective Energy Consumption 10. Data-Centric Network Services 11. Congestion Control and Transport Reliability 12. Security Aspects Associated with Wireless Sensor Networks
Learning Outcomes	By completing this KU, students should be able to: 1. Perform simulations of wireless sensor networks for given scenarios. 2. Perform real experiments of secure wireless sensor networks based on given settings. 3. Apply efficient mechanism of localization, synchronization and power consumption.

The following reference was used to prepare the content of this knowledge unit: [12].

References

[1] National Qualifications Framework (NQF), Education and Training Evaluation Commission, 2020.

[2] The National Centers of Academic Excellence in Cyber Defense (CAE-CD) Designation Program Guidance and Knowledge Units, 2019.

[3] The IEEE/ACM Cybersecurity Curricula, 2017.

[4] The IEEE/ACM Computer Science Curricula, 2013.

[5] E. Fernandez-Buglioni, Security Patterns in Practice: Designing Secure Architectures Using Software Patterns, Wiley, 2013.

[6] S. McConnell, Code Complete: A Practical Handbook of Software Construction, 2nd ed., Microsoft Press, 2004.

[7] Shostack, Threat Modeling: Designing for Security, John Wiley & Sons Inc., 2014.

[8] Reynolds, Ethics in Information Technology, 5th ed., Cengage Learning, 2014.

[9] J Martin and M Talabis, Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, 2013.

[10] T. H. Cormen, C. E. Leiserson and R. L. Rivest, Introduction to Algorithms, The MIT Press, 2009.

[11] Anti-Cyber Crime Law in the Kingdom of Saudi Arabia.

[12] B. Krishnamachari, Networking Wireless Sensors, Cambridge University Press, 2009.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority