Co-funded by the
Erasmus+ Programme
of the European Union

lmpi
licence master professionnel
en protection informatique

LMPI - Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam

Project N° 573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

Survey for the identification of the target job profiles in IT security and corresponding training needs VIETNAM

1. Introduction

The project Erasmus + CBHE LMPI is a joint project for the modernization of educational programs in Engineering (administration of computer networks and systems), national priority for Moldova and Kazakhstan, regional priority for Vietnam. In each of the three countries, the goal is to overcome skills gaps on the intermediate levels (technicians, maintenance and protection of the systems and networks) and upper level (design, engineering for the protection of computer systems and networks) by improving the employability of students and perfecting technicians and executives in companies. Also, LMPI pursues setting up a Bachelor and a professional Master accessible in distance learning for the development, administration, management, protection of computer systems and networks in businesses in Moldova, Kazakhstan, Vietnam, and set up a training device throughout of life.

Among the important recommendations of the Bologna process is the professionalization of university curricula: a re-approchement between the knowledge taught and the skills required by the occupations/jobs. This imposes a paradigm shift: the curriculum instead of focusing on the teacher and his or her knowledge, focus on the skills expected at the end of the course. Any renovation of university courses must take into account the "exit profile/learning outcome" of the student. This expression means the set of skills and knowledge to be mastered by the student at the end of his / her training course so that the student can fit into a given occupation/job.

This document reports the results of the survey in Vietnam with the goal of (1) identify the occupations that will be targeted by the new university curricula (2) identify the skills required by these occupations/jobs and (2) identify the training needs required by these occupations/jobs.

2. Methodology of the survey

The survey includes 243 people working in the Information security environment and it took place during 3 months (July 2017- September 2017). The content of the survey was available online an it includes the following questions:

1. **Your Age.**
    - Choice: 20-30, 30-40, 40-50, 50+
2. **Your job.**
    - Choice: Engineer / Manager; Technician; Director; Student, Others
3. **Your own experience about Information Security.**
    - Choice: 1 - 5 years; 5 - 10 years; Over 10 years.
4. **What size is your business?**
    - Choice: Under 10 people; , 10 - 50 people; 50 - 100 people; 100 - 500 people; over 500 people.
5. **According to you, what aspects does Information Security specialize in? (you can choose more than 1 option).**
    - Choice: Telecommunication; Banking; Army; All companies using computers; Large companies; Public Administrations; Industry; Biotechnology; Small and Medium-sized companies of Service Production; Small and Medium-sized companies of Product Production; Others
6. **In your opinion, where are Information Security specialists needed the most? .**
    - Choice: Banking; Army; Telecommunication; Large companies; Public Administrations; All companies using computers; Computer Service and Consultant Companies; Industry; Biotechnology; Small and Medium-sized companies of Service Production; Small and Medium-sized companies of Product Production; Others
7. **Specify the activities that these specialists can carry out.**

- Choice: Implementation of intrusion detection, prevention and detection systems; Frequent detection, detection of system vulnerabilities; Implementation of information coding, authentication and construction of the PKI infrastructure; Implementation of the corrective system to the parts of the security flaws; Establishment of prevention mechanisms, restoration of the system and assurance of system continuity; Training security procedures to organizations' users; Network and system monitoring, incident response; Reporting, analysis, and prediction of attacks; Regular attendance of workshops, seminars on information security, updating information on security vulnerabilities in systems / software; Security audit; Security compliance implementation; Suggestion and Implementation of information security standards; Penetration testing; Others

8. **Describe what problems you encounter concerning with Information Security in your company**
    - Choice: Protecting Confidential Information; Low level of knowledge of all staff, management, not only IT teachers on the importance of information security; Adequate risk management strategy is not yet in place; Difficulties encountered by all staff, management in the development and implementation of security processes in data processing, data processing and the operating system; Difficulties (time, money, personnel) in implement and enforce security policies inside the company; Modifications information; Good combination on management policy and deployment technology is not yet done; Not enough resources to follow/implement security standards such as ISO 27001; Trade-off between security and usability; Difficulties encountered in implementing security processes in accordance with ISO 17799; Lack of commitment from top level managers to ensure security mechanism is in place; Lack of cooperation between business part and security part of the company; Identity Substitution; Others
9. **Specify the devices used for Information Security in your company (software and hardware)**
    - Choice: Counter viruses and malware; Controlled access; Data encryption; Software protection tools; Hardware protection tools; Legal, moral, ethical protection tools; Physical protection tools; Physical obstacle; Organizational protection tools; Others
10. **In your opinion, are there generic skills that an Information Security specialist must have?**
    - Choice: Ability to manage the urgent situations; Ability to analyze and synthesize; Ability to encounter risks; Respect of confidentiality; Effectiveness; Teamwork; Creativity; Initiative and ability for tasks; Ability to work in international circumstances; Ability to organize and make plans; Quality Concern; Ability to operate; Ability to communicate with diversity of people; Project concept and management; Reactivity; Others
11. **According to you, what can you get these generic skills from?**
    - Choice: Practical workshops; Case studies; Techniques; Multimedia; Theories; Training/Academic courses; Others
12. **In your view, which specific skills do specialists in Information Security need to have?**
    - Choice: Update security systems to meet new demands and latest technologies; Provide different solutions to the protection; Carry out the diagnostics in information systems; Ensure the sustainability of the security systems; Implement different security processes; Master the cryptology; Have knowledge of firewalls; Anticipate the negligence and errors; Design and implement hardware and software architecture; Identify the weaknesses; Implement and respect the security; Evaluate the necessity for the access of information and network of each service; Assess the network conformity with the expectation of traders by reports; Train employees on security rules; Draft the security policies and standards; Develop monitoring indicators; Develop Network; Write reports; Others
13. **In your opinion, what lessons can be learned to acquire these specific skills?**
    - Choice: Security policy; Security devices et equipment (VPN-Firewall, etc.); Cryptography; Network supervision and management; English; Security of servers and computers; Application layer security; Methods to implement a PSSI; Wireless et security; Internship; Audit/Pentesting network; Expression and Communication; High-speed telecommunication (3G, LTE); Configuration of routers; Project Implementation; Interior and exterior advanced storing and mailing; Hierarchical interconnection architecture; Administrative network

services; IPV6; Law; Supervised projects; Scripting (Shell, Python, Perl…); IP Telephony; Administrative systems; Economy and Gestures.

14. **According to you, what teaching methods do they need to acquire these specific skills?**
    - Choice: Internship; Case studies/Exercise; Techniques; Teamwork; Theories; Multimedia; Others
15. **As a professional, do you need an Information Security training course?**
    - Choice: Yes; No
16. **Would you be personally interested in Information security training?**
    - Choice: Yes; No
17. **Would you be interested in hosting Information security internship training?**
    - Choice: Yes; No
18. **If yes, what type of internship do you prefer?**
    - Choice: Functional internship to hire employees; Operational internship to develop its employment; Observational internship
19. **If yes, how long will your internship be**
    - Choice: 1 – 2 weeks; 1 month; 3 months; Over 3 months

The renovation team reviewed the today standards in the field of information security CV and two the three following documents as reference:

- *Cybersecurity: A Generic Reference Curriculum (October 2016). Developed by* Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group (ESCWG). This document is the result of the work of a multinational team of volunteer academics and researchers drawn from 17 nations associated with the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group (ESCWG). The aim was to produce a flexible and generally comprehensive approach to the issue of cybersecurity.
- NIST (National Institute of Standards & Technology). U.S. Department of Commerce. Special Publication 800-181. National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. William Newhouse; Stephanie Keith; Benjamin Scribner; Greg Witte. This publication describes the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), a reference structure that describes the interdisciplinary nature of the cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization. As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity workforce development, planning, training, and education.
- Toward Curricular Guidelines for Cybersecurity Report of a Workshop on Cybersecurity Education and Training (August 20113). Andrew McGettrick. Association for Computing Machinery (ACM). This document reports the work of a Core Leadership Group comprising cybersecurity experts in government, industry, and academia to discuss current cybersecurity education initiatives and make recommendations that will inform near-term and long-range curricular guidance in cybersecurity for colleges and universities. The group also discussed the roles for government and private industry to play in building a broad cybersecurity workforce ranging from proficient technicians and practitioners to policy makers and thought leaders. Workshop participants embraced the philosophy expressed by ACM's policy arm (USACM) and the Computing Research Association (CRA) that computer science and computer engineering graduates should possess a thorough education in cybersecurity and related fundamentals and principles as well as training in cybersecurity-specific technologies, tools, and skills. The balance between education and training may vary for particular knowledge areas or sub-specialties, but a strong underpinning of basic knowledge and principles to complement

technical skills should form the basis of a curriculum in cybersecurity. According to the specific characteristics of the Vietnamese University System and the national market needs in the survey, the renovator team took the NICE curricula guidelines by the NIST institute as main academic reference. NICE allowed to complement the perspective of professionals in the survey with a broader academic perspective which may guarantee the Curricula ability to anticipate likely developments and to give students the ability to adapt to these future developments.

3. Composition of the renovation group

Name	Position	Institution
Prof. Manuel Fernández Veiga	Head of Program Studies at the School of Communications Engineering	University of Vigo, Spain
Prof. Rebeca Díaz Redondo	Coordinator of BsC Program on Telecommunications Engineering	University of Vigo, Spain
Prof Ana Fernández Vilas	School of Communications Engineering Local Coordinator LMPI	University of Vigo, Spain
Prof. Thoai Nam	Dean, Faculty of Computer Science and Engineering	Ho Chi Minh City University of Technology
Prof. Pham Tran Vu	Vice-Dean, Faculty of Computer Science and Engineering	Ho Chi Minh City University of Technology
Dr, Truong Tuan Anh	Lecturer, Faculty of Computer Science and Engineering	Ho Chi Minh City University of Technology
Dr. Nguyen An Khuong	Lecturer, Faculty of Computer Science and Engineering	Ho Chi Minh City University of Technology
Prof. Ngo Hong Son	Dean, School of Information and Communication Technology	Hanoi University of Science and Technology
Prof. Huynh Thi Thanh Binh	Vice Dean, School of Information and Communication Technology	Hanoi University of Science and Technology
Dr. Tran Hoang Hai	Vice Director of Network Center	Hanoi University of Science and Technology
Dr. Tran Vinh Duc	Lecturer, SOICT	Hanoi University of Science and Technology
Dr. Tran Duc Quynh	Dean, Faculty of Information Technology	Vietnam National University of Agriculture
Dr. Pham Quang Dung	Vice-Dean, Faculty of Information Technology	Vietnam National University of Agriculture
Phan Trong Tien	Lecturer, Faculty of Information Technology	Vietnam National University of Agriculture

4. Analysis of the collected data from the survey

The complete results and analysis of the survey is included in Annex 1. These results were analysed and interpreted by the renovator team in order to identify the target occupation/jobs; the competences required in each kind of occupation and the training demand in each kind of occupation

4.1 Target occupations

According to the survey results to the question 7 7 (where are Information Security specialists needed the most?), the renovator team interpreted the market scenario as it is reflected in table

Table 1 Occupation Demand according to the survey

		(+) Demand according to the size of the company (-)		
(+) sector demand (-)		Large Companies	Public Administration	SME
	Banking	X	X	
	Army		X	
	Telecommunication	X	X	
	Consultants	X		X
	Computer Service	X		X
	Biotechnology	X		X
	Manufacturing	X	X	X

Taking into account the size and the ownership of the company, Security information profile is believed to be 5 times more demanded in public administration and large companies than in SME (either product or services). Taking into account the survey, the most demanding sector for Security Information profiles is Banking, closely follow by Army and Telecommunications. This result is clearly connected with the conclusions extracted according to the size of the company, as three of them (banking, Army and Telecommunication companies) are large-sized (either public or private).

Taking apart the size of the organization and the market sector, according to the survey (question 8), the target jobs demanded are ranked as follows:

1. Cybersecurity analyst
2. Secure-software developers
3. Data & information security engineer
4. System security engineer
5. Security managers & architects
6. Security audit engineer

After discussing again about the 6 resulting profiles, and taking into account the academic experience of the renovators, 4 job profiles we defined (2 Master level and 2 Bachelor Level)

- Engineer on Network security. This is considered a BsC level profile which integrates the sub-profiles 1,3.
- Engineer on Data & Application security. This is considered a BsC level profile which integrates the sub-profiles 2, 3.
- Expert on System & Data security. This is considered a MsC level profile which integrates the sub-profiles 4, 5
- Expert on Security management. This is considered a MsC level profile which integrates the sub-profiles 5, 6

4.2 Generic Competences (GC)

According to the survey results about market needs (question 11) and taking into account the NICE guidelines, the renovator team identified the following general competences (GC):

GC1. The ability to analyze systems, mechanisms and procedures related to protection of information entities and objects
GC2. Problem solving ability, design ability
GC3. Critical thinking
GC4. Creativity and Reactivity
GC5. Ability to apply theoretical knowledge to practice
GC6. Ability for self-study
GC7. Ability to work in a diversity group and in an international context (teamwork)
GC8. Ability to project organization and planning
GC9. Time management skill
GC10. Representation skill: Ability to represent, illustrate, convince
GC11. Skill in conducting trend analysis.

4.32 Specific Competences (SC)

According to the survey results about market needs (question 12) and taking into account the NICE guidelines, the renovator team identified the following general competences:

- To update security systems to meet new demands and latest technologies
- To design software/hardware security solutions
- To implement software/hardware security solutions
- To test software/hardware security solutions
- To carry out security diagnostics
- To ensure sustainability of the security systems
- To understand and apply cryptology
- To understand, configure and operate firewalls
- To apply vulnerability analysis
- To evaluate the accessibility level for information, network, and services
- To establish security policies and standards
- To assess networking compliance to internal policies and standards
- To make employees aware about corporate security policies and standards
- To design, develop and report monitoring indicators according to policies and standards

Taking the specific skills reported in the survey as a reference, the renovation team reviewed the NICE list of specific skills and, according to the 4 occupation profiles identified, they selected the following Specific Competences (SC):

SC01. To update security systems to meet new demands and latest technologies.
SC02. Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
SC03. Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
SC04. Skill in securing network communications.
SC05. Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
SC06. Skill in performing packet-level analysis.
SC07. Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).

SC08. Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
SC09. Skill in using Virtual Private Network (VPN) devices and encryption.
SC10. Skill in using incident handling methodologies.
SC11. Skill in preserving evidence integrity according to standard operating procedures or national standards.
SC12. Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
SC13. Skill in conducting vulnerability scans, recognizing and categorizing vulnerabilities in security systems.
SC14. To understand and to apply the up-to-date methods, tools, software and techniques to analyze risks, threats and protect the system.
SC15. The ability to understand security demands and design and implement software/hardware security solutions
SC16. Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
SC17. The ability to know, understand and apply code analysis techniques.
SC18. The ability to know, understand and apply security event correlation techniques and tools.
SC19. Skill in secure test plan design (e. g. unit, integration, system, acceptance).
SC20. Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.
SC21. Skill in analysing and predicting trends in security aspects.
SC22. Skill in analysing anomalous code as malicious or benign.
SC23. The ability to know, understand and apply binary analysis techniques and tools.
SC24. Skill in performing damage assessments.
SC25. Ability to evaluate risks (risk assessment)
SC26. To design/establish security policies, privacy policies and standards
SC27. To make employees aware about corporate security policies and standards
SC28. To design, develop and report monitoring indicators according to policies and standards
SC29. Ability to describe and illustrate the risks, threats and solutions
SC30. Skill in technical writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.
SC31. The ability to know, understand and apply database security techniques.
SC32. The ability to know, understand and apply cloud computing security solutions.
SC33. The ability to know, understand and apply the methods of cryptography and cryptanalysis, the digital identity fundamentals and the protocols of secure communications.
SC34. The ability to know, understand and apply privacy principles to organizational requirements.
SC35. The ability to understand security demands and design and implement software/hardware security solutions.
SC36. The ability to know, understand and apply the methods of networking protection.
SC37. Skill in assessing security controls based on cybersecurity principles and tenets.
SC38. Skill in assessing security systems designs.
SC39. Skill in using virtual machines.
SC40. Skill in creating policies that reflect the business's core privacy objectives.
SC41. Skill in designing the integration of hardware and software solutions.
SC42. Skill in creating policies that reflect system security objectives.
SC43. Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.
SC44. Skill to use cyber defence Service Provider reporting structure and processes within one's own organization.
SC45. Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
SC46. Skill in negotiating vendor agreements and evaluating vendor privacy practices.

SC47. Skill to extract information from available tools and applications associated with collection requirements and collection operations management.
SC48. Skill to evaluate requests for information to determine if response information exists.
SC49. Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed.
SC50. Skill to analyse target or threat sources of strength and morale.
SC51. Skill to analyse strategic guidance for issues requiring clarification and/or additional guidance.
SC52. Skill to access the databases where plans/directives/guidance are maintained.
SC53. Skill in utilizing feedback to improve processes, products, and services.
SC54. Skill in technical writing.
SC55. Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies).
SC56. Skill in target development in direct support of collection operations.
SC57. Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).
SC58. Skill in reviewing and editing plans.
SC59. Skill in reviewing and editing assessment products.
SC60. Skill in providing analysis to aid writing phased after action reports.
SC61. Skill in knowledge management, including technical documentation techniques.
SC62. Skill in identifying, locating, and tracking targets via geospatial analysis techniques
SC63. Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.
SC64. Skill in conducting non-attributable research.
SC65. Skill in developing and deploying signatures.
SC66. Skill in applying host/network access controls.
SC67. Skill in analysing network traffic capacity and performance characteristics.
SC68. Skill of identifying, capturing, containing, and reporting malware.
SC69. Skill to design incident response for cloud service models.
SC70. Skill to develop insights about the context of an organization's threat environment
SC71. Skill in writing about facts and ideas in a clear, convincing, and organized manner.
SC72. Skill in using research methods including multiple, different sources to reconstruct a target network.

Table 2 Identification of expected competencies for each of these occupations

Engineer on Network security (BsC).

- **General competence:** GC1, GC2, GC5, GC6, GC7, GC8, GC9, GC10
- **Specific competence:** SC01, SC02, SC03, SC04, SC05, SC06, SC07, SC08, SC09, SC10, SC11, SC12

Engineer on Data & Application security (BsC)

- **General competence:** GC1, GC2, GC4, GC5, GC6, GC7, GC8, GC9, GC10
- **Specific competence:** SC13, SC14, SC35, SC16, SC07, SC17, SC18, SC19, SC20, SC21, SC22, SC23, SC24, SC25, SC26, SC27, SC28, SC29, SC30, SC31, SC32

Expert on System & Data security (MsC)

- **General competence:** GC1, GC2, GC3, GC4, GC5, GC6, GC7, GC8, GC9, GC10, GC11
- **Specific competence:** SC02, SC03, SC04, SC05, SC06, SC07, SC08, SC09, SC10, SC11, SC12, SC64, SC20, SC16, SC65, SC66, SC67, SC68, SC44, SC69, SC70, SC71, SC72

Expert on Security management (MsC)

- **General competence:** GC1, GC2, GC3, GC4, GC5, GC6, GC7, GC8, GC9, GC10, GC11
- **Specific competence:** SC33, SC34, SC13, SC14, SC35, SC36, SC16, SC02, SC37, SC38, SC07, SC39, SC40, SC20, SC16, SC41, SC42, SC05, SC43, SC44, SC45, SC46, SC47, SC48, SC49, SC50, SC51, SC52, SC53, SC54, SC55, SC56, SC57, SC58, SC59, SC60, SC61, SC62, SC63

Table 3 Identification of training needs (from Annex 2)

Engineer on Network security (BsC).

- **Knowledges:** K07, K100, K103, K104, K105, K121, K13, K16, K17, K22, K23, K26, K27, K29, K30, K32, K33, K39, K48, K60, K64, K71, K73, K75, K78, K80, K83, K95

Engineer on Data & Application security (BsC)

- **Knowledges:** K01, K02, K05, K06, K09, K105, K106, K107, K109, K112, K113, K114, K116, K12, K120, K122, K123, K124, K19, K20, K22, K23, K26, K31, K33, K34, K35, K36, K37, K38, K41, K42, K43, K44, K45, K46, K47, K49, K50, K53, K56, K63, K65, K66, K67, K85, K86, K87, K88, K89, K91, K94, K96, K98, K99

Expert on System & Data security (MsC)

- **Knowledges:** K01, K05, K100, K104, K105, K111, K121, K16, K25, K29, K30, K32, K40, K41, K51, K57, K61, K63, K68, K70, K73, K74, K76, K79, K85, K87, K88, K91, K95, K97, K99

Expert on Security management (MsC)

- **Knowledges:** K01, K03, K04, K05, K06, K08, K10, K100, K101, K102, K104, K105, K106, K108, K11, K110, K111, K115, K116, K117, K118, K119, K14, K15, K16, K18, K19, K20, K21, K22, K24, K28, K29, K30, K31, K32, K33, K36, K40, K41, K51, K52, K53, K54, K55, K56, K57, K58, K59, K62, K63, K67, K68, K69, K70, K72, K73, K74, K77, K79, K81, K82, K84, K85, K86, K87, K88, K90, K91, K92, K93, K95, K96, K97, K99

5. Formalizing a synthesis of training needs

The training needs expressed by professionals	Engineer on Network security (BsC).	Engineer on Data & Application security (BsC)	Expert on System & Data security (MsC)	Expert on Security management (MsC)
Areas of common knowledge in the occupation	K01, K05, K06, K105, K106, K116, K19, K20, K22, K23, K26, K31, K33, K36, K41, K53, K56, K67, K85, K86, K87, K88, K91, K96, K99			
Areas of knowledge specific to each of the occupation	K07, K100, K103, K104, K121, K13, K16, K17, K27, K29, K30, K32, K39, K48, K60, K64, K71, K73, K75, K78, K80, K83, K95	K02, K09, K107, K109, K112, K113, K114, K12, K120, K122, K123, K124, K34, K35, K37, K38, K42, K43, K44, K45, K46, K47, K49, K50, K63, K65, K66, K89, K94, K98	K100, K104, K111, K121, K16, K25, K29, K30, K32, K40, K51, K57, K61, K63, K68, K70, K73, K74, K76, K79, K95, K97	K03, K04, K08, K10, K100, K101, K102, K104, K108, K11, K110, K111, K115, K117, K118, K119, K14, K15, K16, K18, K21, K24, K28, K29, K30, K32, K40, K51, K52, K54, K55, K57, K58, K59, K62, K63, K68, K69, K70, K72, K73, K74, K77, K79, K81, K82, K84, K90, K92, K93, K95, K97
Other observations				

6. Summary of occupation profiles

Name of the occupation	Network Security
Professional sector	Banking, Army, Telecommunication, Consultants, Computer Service, Manufacturing
Terms of Access	Bachelor
Professional activities	• Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. (A22) • Coordinate with intelligence analysts to correlate threat assessment data. (A1) • Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. (A2) • Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. (A3) • Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. (A4) • Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). (A5) • Perform cyber defense trend analysis and reporting. (A6) • Conduct nodal analysis. (A7) • Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). (A8) • Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications. (A9) • Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. (A10) • Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunnelling). (A11) • Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. (A12) • Develop content for cyber defense tools. (A13) • Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives. (A14) • Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. (A15) • Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources. (A16) • Reconstruct networks in diagram or report format. (A17) • Review appropriate information sources to determine validity and relevance of information gathered. (A18) • Provide target recommendations which meet leadership objectives. (A19)

	• Profile targets and their activities. (A20) • Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. (A21)
General competences	• The ability to analyze systems, mechanisms and procedures related to protection of information entities and objects (GC1) • Problem solving ability, design ability (GC2) • Ability to apply theoretical knowledge to practice (GC5) • Ability for self-study (GC6) • Ability to work in a diversity group and in an international context (teamwork) (GC7) • Ability to project organization and planning (GC8) • Time management skill (GC9) • Representation skill: Ability to represent, illustrate, convince (GC10)
Specific competences	• To update security systems to meet new demands and latest technologies. (SC01) • Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (SC02) • Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). (SC03) • Skill in securing network communications. (SC04) • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. (SC05) • Skill in performing packet-level analysis. (SC06) • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). (SC07) • Skill in recognizing and categorizing types of vulnerabilities and associated attacks. (SC08) • Skill in using Virtual Private Network (VPN) devices and encryption. (SC09) • Skill in using incident handling methodologies. (SC10) • Skill in preserving evidence integrity according to standard operating procedures or national standards. (SC11) • Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). (SC12)
Knowledge	• Knowledge of computer networking concepts and protocols, and network security methodologies. (K16) • Knowledge of specific operational impacts of cybersecurity lapses. (K100) • Knowledge of cyber threats and vulnerabilities. (K29) • Knowledge of cybersecurity and privacy principles. (K32) • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). (K73) • Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). (K105) • Knowledge of data backup and recovery. (K33) • Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark- Wilson integrity model). (K95) • Knowledge of system administration, network, and operating system hardening techniques. (K104)

	• Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. (K121) • Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (K30) • Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). (K48) • Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). (K26) • Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks). (K39) • Knowledge of cyber defense and information security policies, procedures, and regulations. (K27) • Knowledge of cryptography and cryptographic key management concepts (K22) • Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems. (K103) • Knowledge of OSI model and underlying network protocols (e.g., TCP/IP). (K83) • Knowledge of network tools (e.g., ping, traceroute, nslookup) (K75) • Knowledge of operations security. (K80) • Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection). (K71) • Knowledge of malware analysis and characteristics. (K64) • Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering). (K60) • Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.). (K17) • Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.). (K13) • Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.). (K07) • Knowledge of operating system command-line tools. (K78) • Knowledge of cryptology. (K23)
Observations	

Name of the occupation	Data & Application Security
Professional sector	Banking, Army, Telecommunication, Consultants, Computer Service, Manufacturing
Terms of Access	Bachelor
Professional activities	• Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. (A22) • Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. (A23) • Assess and monitor cybersecurity related to system implementation and testing practices. (A24) • Coordinate with intelligence analysts to correlate threat assessment data. (A1) • Verify and update security documentation reflecting the application/system security design features. (A25) • Store, retrieve, and manipulate data for analysis of system capabilities and requirements. (A26) • Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications. (A9) • Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s). (A27) • Establish acceptable limits for the software application, network, or system. (A28) • Identify applications and operating systems of a network device based on network traffic. (A29) • Isolate and remove malware. (A30) • Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings). (A31) • Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration. (A32) • Examine recovered data for information of relevance to the issue at hand. (A33) • Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. (A34) • Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII). (A35) • Apply coding and testing standards, apply security testing tools including '"fuzzing" static- analysis code scanning tools, and conduct code reviews. (A36) • Determine and document software patches or the extent of releases that would leave software vulnerable. (A37)

	• Verify minimum security requirements are in place for all applications. (A38) • Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately. (A39) • Develop secure software testing and validation procedures. (A40) • Design to security requirements to ensure requirements are met for all systems and/or applications. (A41) • Consult with customers about software system design and maintenance. (A42) • Perform virus scanning on digital media. (A43) • Perform penetration testing as required for new or updated applications. (A44) • Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. (A45) • Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modelling, and defining any specific security criteria. (A46) • Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing. (A47) • Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures). (A48) • Perform hash comparison against established database. (A49) • Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system. (A50) • Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). (A51) • Implement specific cybersecurity countermeasures for systems and/or applications. (A52) • Implement new system design procedures, test procedures, and quality standards. (A53) • Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life. (A54) • Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development. (A55) • Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET). (A56)
General competences	• The ability to analyze systems, mechanisms and procedures related to protection of information entities and objects (GC1) • Problem solving ability, design ability (GC2) • Creativity and Reactivity (GC4) • Ability to apply theoretical knowledge to practice (GC5) • Ability for self-study (GC6) • Ability to work in a diversity group and in an international context (teamwork) (GC7) • Ability to project organization and planning (GC8) • Time management skill (GC9) • Representation skill: Ability to represent, illustrate, convince (GC10)

Specific competences	• Skill in conducting vulnerability scans, recognizing and categorizing vulnerabilities in security systems. (SC13) • To understand and to apply the up-to-date methods, tools, software and techniques to analyse risks, threats and protect the system. (SC14) • The ability to understand security demands and design and implement software/hardware security solutions. (SC35) • Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. (SC16) • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). (SC07) • The ability to know, understand and apply code analysis techniques. (SC17) • The ability to know, understand and apply security event correlation techniques and tools. (SC18) • Skill in secure test plan design (e. g. unit, integration, system, acceptance). (SC19) • Skill in developing, testing, and implementing network infrastructure contingency and recovery plans. (SC20) • Skill in analysing and predicting trends in security aspects. (SC21) • Skill in analysing anomalous code as malicious or benign. (SC22) • The ability to know, understand and apply binary analysis techniques and tools (SC23) • Skill in performing damage assessments. (SC24) • Ability to evaluate risks (risk assessment) (SC25) • To design/establish security policies, privacy policies and standards (SC26) • To make employees aware about corporate security policies and standards (SC27) • To design, develop and report monitoring indicators according to policies and standards (SC28) • Ability to describe and illustrate the risks, threats and solutions (SC29) • Skill in technical writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources. (SC30) • The ability to know, understand and apply database security techniques. (SC31) • The ability to know, understand and apply cloud computing security solutions. (SC32)
Knowledge	• Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. (K63) • Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). (K91) • Knowledge of an organization's information classification program and procedures for information compromise. (K01) • Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). (K105) • Knowledge of encryption algorithms (K41) • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) (K05) • Knowledge of Personal Health Information (PHI) data security standards.

	(K87) • Knowledge of Payment Card Industry (PCI) data security standards. (K85) • Knowledge of Personally Identifiable Information (PII) data security standards. (K88) • Knowledge of data backup and recovery. (K33) • Knowledge of cryptography and cryptographic key management concepts (K22) • Knowledge of penetration testing principles, tools, and techniques. (K86) • Knowledge of database systems. (K36) • Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). (K26) • Knowledge of controls related to the use, processing, storage, and transmission of data. (K19) • Knowledge of software engineering. (K99) • Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data. (K31) • Knowledge of application vulnerabilities. (K06) • Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). (K67) • Knowledge of cryptology. (K23) • Knowledge of systems security testing and evaluation methods. (K109) • Knowledge of system life cycle management principles, including software security and usability. (K106) • Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption. (K53) • Knowledge of software development models (e.g., Waterfall Model, Spiral Model). (K98) • Knowledge of server and client operating systems. (K96) • Knowledge of how to extract, analyze, and use metadata. (K50) • Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP). (K49) • Knowledge of data backup and restoration concepts. (K34) • Knowledge of ethical hacking principles and techniques. (K43) • Knowledge of basic system, network, and OS hardening techniques. (K09) • Knowledge of Windows/Unix ports and services. (K123) • Signature implementation impact for viruses, malware, and attacks. (K124) • Knowledge of encryption methodologies. (K42) • Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device). (K66) • Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro). (K65) • Knowledge of file type abuse by adversaries for anomalous behavior. (K45) • Knowledge of debugging procedures and tools. (K37) • Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark). (K46) • Knowledge of anti-forensics tactics, techniques, and procedures. (K02) • Knowledge of reverse engineering concepts. (K89) • Knowledge of data carving tools and techniques (e.g., Foremost). (K35) • Knowledge of critical information technology (IT) procurement requirements. (K20) • Knowledge of the organization's core business/mission processes. (K116) • Knowledge of security event correlation tools. (K94)

	• Knowledge of front-end collection systems, including traffic collection, filtering, and selection. (K47) • Knowledge of collection management processes, capabilities, and limitations. (K12) • Knowledge of deployable forensics. (K38) • Knowledge of types of digital forensics data and how to recognize them. (K112) • Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files. (K122) • Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies. (K120) • Knowledge of information security program management and project management principles and techniques. (K56) • Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip). (K44) • Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design. (K107) • Knowledge of the data flow from collection origin to repositories and tools. (K114) • Knowledge of the basic structure, architecture, and design of converged applications. (K113)
Observations	

Name of the occupation	Management Security
Professional sector	Banking, Army, Telecommunication, Consultants, Computer Manufacturing, Computer Services.
Terms of Access	Master
Professional activities	• Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). (A57) • Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. (A58) • Evaluate cost/benefit, economic, and risk analysis in decision-making process. (A59) • Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. (A60) • Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). (A8) • Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. (A15) • Manage Accreditation Packages (e.g., ISO/IEC 15026-2). (A61) • Establish acceptable limits for the software application, network, or system. (A28) • Assess all the configuration management (change configuration/release management) processes. (A62) • Assess the effectiveness of security controls. (A63) • Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. (A64) • Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). (A65) • Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. (A66) • Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals. (A67) • Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. (A68) • Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. (A69) • Verify and update security documentation reflecting the application/system security design features. (A25) • Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. (A70) • Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. (A71) • Recognize a possible security violation and take appropriate action to report the incident, as required. (A72) • Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program. (A73) • Establish overall enterprise information security architecture (EISA) with the

	organization's overall security strategy. (A74) • Ensure that security improvement actions are evaluated, validated, and implemented as required. (A75) • Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. (A76) • Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. (A77) • Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. (A78) • Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. (A79) • Apply security policies to applications that interface with one another, such as Business-to- Business (B2B) applications. (A80) • Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. (A81) • Establish a risk management strategy for the organization that includes a determination of risk tolerance. (A82)
General competences	• The ability to analyze systems, mechanisms and procedures related to protection of information entities and objects (GC1) • Problem solving ability, design ability (GC2) • Critical thinking (GC3) • Creativity and Reactivity (GC4) • Ability to apply theoretical knowledge to practice (GC5) • Ability for self-study (GC6) • Ability to work in a diversity group and in an international context (teamwork) (GC7) • Ability to project organization and planning (GC8) • Time management skill (GC9) • Representation skill: Ability to represent, illustrate, convince (GC10) • Skill in conducting trend analysis. (GC11)
Specific competences	• The ability to know, understand and apply the methods of cryptography and cryptoanalysis, the digital identity fundamentals and the protocols of secure communications. (SC33) • The ability to know, understand and apply privacy principles to organizational requirements. (SC34) • Skill in conducting vulnerability scans, recognizing and categorizing vulnerabilities in security systems. (SC13) • To understand and to apply the up-to-date methods, tools, software and techniques to analyze risks, threats and protect the system. (SC14) • The ability to understand security demands and design and implement software/hardware security solutions. (SC35) • The ability to know, understand and apply the methods of networking protection (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters, securing network communications, intrusion detection, VPN). (SC36) • Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. (SC16) • Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (SC02)

	• Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). (SC37) • Skill in assessing security systems designs. (SC38) • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). (SC07) • Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.). (SC39) • Skill in creating policies that reflect the business's core privacy objectives. (SC40) • Skill in developing, testing, and implementing network infrastructure contingency and recovery plans. (SC20) • Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. (SC16) • Skill in designing the integration of hardware and software solutions. (SC41) • Skill in creating policies that reflect system security objectives. (SC42) • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. (SC05) • Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations. (SC43) • Skill to use cyber defense Service Provider reporting structure and processes within one's own organization. (SC44) • Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience). (SC45) • Skill in negotiating vendor agreements and evaluating vendor privacy practices. (SC46) • Skill to extract information from available tools and applications associated with collection requirements and collection operations management. (SC47) • Skill to evaluate requests for information to determine if response information exists. (SC48) • Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed. (SC49) • Skill to analyze target or threat sources of strength and morale. (SC50) • Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance. (SC51) • Skill to access the databases where plans/directives/guidance are maintained. (SC52) • Skill in utilizing feedback to improve processes, products, and services. (SC53) • Skill in technical writing. (SC54) • Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies). (SC55) • Skill in target development in direct support of collection operations. (SC56) • Skill in tailoring analysis to the necessary levels (e.g., classification and organizational). (SC57) • Skill in reviewing and editing plans. (SC58) • Skill in reviewing and editing assessment products. (SC59) • Skill in providing analysis to aid writing phased after action reports. (SC60) • Skill in knowledge management, including technical documentation techniques (e.g., Wiki page). (SC61)

	• Skill in identifying, locating, and tracking targets via geospatial analysis techniques (SC62) • Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures. (SC63)
Knowledge	• Knowledge of computer networking concepts and protocols, and network security methodologies. (K16) • Knowledge of specific operational impacts of cybersecurity lapses. (K100) • Knowledge of cyber threats and vulnerabilities. (K29) • Knowledge of cybersecurity and privacy principles. (K32) • Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. (K63) • Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). (K91) • Knowledge of encryption algorithms (K41) • Knowledge of an organization's information classification program and procedures for information compromise. (K01) • Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures. (K62) • Knowledge of Personal Health Information (PHI) data security standards. (K87) • Knowledge of Payment Card Industry (PCI) data security standards. (K85) • Knowledge of Personally Identifiable Information (PII) data security standards. (K88) • Knowledge of network security architecture concepts (K72) • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). (K73) • Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. (K04) • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) (K05) • Knowledge of controls related to the use, processing, storage, and transmission of data. (K19) • Knowledge of embedded systems. (K40) • Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. (K21) • Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161) (K102) • Knowledge of the organization's enterprise information technology (IT) goals and objectives. (K115) • Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). (K105) • Knowledge of new and emerging information technology (IT) and cybersecurity technologies. (K77) • Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication,

	non-repudiation). (K30) • Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). (K119) • Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data. (K31) • Knowledge of business continuity and disaster recovery continuity of operations plans. (K10) • Knowledge of cryptography and cryptographic key management concepts (K22) • Knowledge of applicable business processes and operations of customer organizations. (K03) • Knowledge of penetration testing principles, tools, and techniques. (K86) • Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark- Wilson integrity model). (K95) • Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).64 (K92) • Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. (K74) • Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures. (K58) • Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). (K51) • Knowledge of operating systems. (K79) • Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). (K68) • Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities. (K24) • Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). (K57) • Knowledge of Risk Management Framework (RMF) requirements. (K90) • Knowledge of incident response and handling methodologies. (K54) • Knowledge of Security Assessment and Authorization process. (K93) • Knowledge of organization's enterprise information security architecture. (K81) • Knowledge of database systems. (K36) • Knowledge of data backup and recovery. (K33) • Knowledge of cyber defense and vulnerability assessment tools and their capabilities. (K28) • Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs. (K69) • Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. (K70) • Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption. (K53) • Knowledge of configuration management techniques. (K18) • Knowledge of various types of computer architectures. (K118) • Knowledge of service management concepts for networks and related

	standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). (K97) • Knowledge of system administration, network, and operating system hardening techniques. (K104) • Knowledge of critical information technology (IT) procurement requirements. (K20) • Knowledge of the organization's core business/mission processes. (K116) • Knowledge of information security program management and project management principles and techniques. (K56) • Knowledge of the systems engineering process. (K117) • Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing). (K111) • Knowledge of technology integration processes. (K110) • Knowledge of system life cycle management principles, including software security and usability. (K106) • Knowledge of systems diagnostic tools and fault identification techniques. (K108) • Knowledge of structured analysis principles and methods. (K101) • Knowledge of software engineering. (K99) • Knowledge of server and client operating systems. (K96) • Knowledge of parallel and distributed computing concepts. (K84) • Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). (K67) • Knowledge of industry-standard and organizationally accepted analysis principles and methods. (K55) • Knowledge of human-computer interaction principles. (K52) • Knowledge of installation, integration, and optimization of system components. (K59) • Knowledge of organization's evaluation and validation requirements. (K82) • Knowledge of computer algorithms. (K15) • Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware. (K11) • Knowledge of communication methods, principles, and concepts that support the network infrastructure. (K14) • Knowledge of application vulnerabilities. (K06) • Knowledge of authentication, authorization, and access control methods. (K08)
Observations	

Name of the occupation	**Data and System Security**
Professional sector	Financial, government, telecommunication, power, army
Terms of Access	Master
Professional activities	• Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). (A57) • Generate requests for information. (A83) • Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans. (A84) • Work with stakeholders to resolve computer security incidents and vulnerability compliance. (A85) • Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. (A86) • Assess and monitor cybersecurity related to system implementation and testing practices. (A24) • Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. (A22) • Assess adequate access controls based on principles of least privilege and need-to-know. (A87) • Analyze and report system security posture trends. (A88) • Analyze and report organizational security posture trends. (A89) • Coordinate with intelligence analysts to correlate threat assessment data. (A1) • Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. (A2) • Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. (A90) • Store, retrieve, and manipulate data for analysis of system capabilities and requirements. (A26) • Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. (A3) • Plan and recommend modifications or adjustments based on exercise results or system environment. (A91) • Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. (A23) • Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. (A58) • Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). (A5) • Perform cyber defense trend analysis and reporting. (A6)

	• Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. (A92) • Examine recovered data for information of relevance to the issue at hand. (A33) • Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. (A93) • Conduct nodal analysis. (A7) • Answer requests for information. (A94) • Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. (A79) • Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications. (A9) • Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. (A10) • Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunnelling). (A11) • Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects. (A95) • Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. (A12) • Develop content for cyber defense tools. (A13) • Apply security policies to applications that interface with one another, such as Business-to- Business (B2B) applications. (A80) • Apply coding and testing standards, apply security testing tools including "'fuzzing" static- analysis code scanning tools, and conduct code reviews. (A36) • Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support. (A96) • Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives. (A14) • Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date. (A97) • Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources. (A16) • Report intelligence-derived significant network events and intrusions. (A98) • Reconstruct networks in diagram or report format. (A17) • Review appropriate information sources to determine validity and relevance of information gathered. (A18) • Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. (A99) • Provide target recommendations which meet leadership objectives. (A19) • Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations. (A100) • Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations. (A101) • Provide evaluation and feedback necessary for improving intelligence

	production, intelligence reporting, collection requirements, and operations. (A102) • Provide current intelligence support to critical internal/external stakeholders as appropriate. (A103) • Profile targets and their activities. (A20)
General competences	• The ability to analyze systems, mechanisms and procedures related to protection of information entities and objects (GC1) • Problem solving ability, design ability (GC2) • Critical thinking (GC3) • Creativity and Reactivity (GC4) • Ability to apply theoretical knowledge to practice (GC5) • Ability for self-study (GC6) • Ability to work in a diversity group and in an international context (teamwork) (GC7) • Ability to project organization and planning (GC8) • Time management skill (GC9) • Representation skill: Ability to represent, illustrate, convince (GC10) • Skill in conducting trend analysis. (GC11)
Specific competences	• Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (SC02) • Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). (SC03) • Skill in securing network communications. (SC04) • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. (SC05) • Skill in performing packet-level analysis. (SC06) • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). (SC07) • Skill in recognizing and categorizing types of vulnerabilities and associated attacks. (SC08) • Skill in using Virtual Private Network (VPN) devices and encryption. (SC09) • Skill in using incident handling methodologies. (SC10) • Skill in preserving evidence integrity according to standard operating procedures or national standards. (SC11) • Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). (SC12) • Skill in conducting non-attributable research. (SC64) • Skill in developing, testing, and implementing network infrastructure contingency and recovery plans. (SC20) • Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. (SC16) • Skill in developing and deploying signatures. (SC65) • Skill in applying host/network access controls (e.g., access control list). (SC66) • Skill in analyzing network traffic capacity and performance characteristics. (SC67) • Skill of identifying, capturing, containing, and reporting malware. (SC68) • Skill to use cyber defense Service Provider reporting structure and processes within one's own organization. (SC44)

	• Skill to design incident response for cloud service models. (SC69) • Skill to develop insights about the context of an organization's threat environment (SC70) • Skill in writing about facts and ideas in a clear, convincing, and organized manner. (SC71) • Skill in using research methods including multiple, different sources to reconstruct a target network. (SC72)
Knowledge	• Knowledge of computer networking concepts and protocols, and network security methodologies. (K16) • Knowledge of specific operational impacts of cybersecurity lapses. (K100) • Knowledge of cyber threats and vulnerabilities. (K29) • Knowledge of cybersecurity and privacy principles. (K32) • Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. (K63) • Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). (K91) • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). (K73) • Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. (K70) • Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). (K51) • Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (K30) • Knowledge of an organization's information classification program and procedures for information compromise. (K01) • Knowledge of Personal Health Information (PHI) data security standards. (K87) • Knowledge of Payment Card Industry (PCI) data security standards. (K85) • Knowledge of Personally Identifiable Information (PII) data security standards. (K88) • Knowledge of operating systems. (K79) • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) (K05) • Knowledge of embedded systems. (K40) • Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark- Wilson integrity model). (K95) • Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. (K74) • Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). (K25) • Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing). (K111) • Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race

	conditions, covert channel, replay, return-oriented attacks, malicious code). (K105) • Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). (K68) • Knowledge of encryption algorithms (K41) • Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). (K97) • Knowledge of system administration, network, and operating system hardening techniques. (K104) • Knowledge of interpreted and compiled computer languages. (K61) • Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. (K121) • Knowledge of software engineering. (K99) • Knowledge of network traffic analysis methods. (K76) • Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). (K57)
Observations	

6. Conclusions

According to the survey and our analysis, the job demands for cybersecurity in Vietnam are in urgent, specially in Banking, Army, Telecommunication, Energy. However, current training programs do not provide enough skills and knowledges that meet the requirements from industry. Therefore, building new training programs in cybersecurity for both bachelor and master level is necessary. After the interpretation of the survey results, the renovator team defined four employment profiles and specified the skills, knowledges, and activities for them as listed in the annexes. Such employment profiles will guide the Vietnamese Universities to build the programs in cybersecurity for both bachelor and master level following the strategies and current situation of each university as follows.

HUST has currently both master and bachelor degrees in Computer Science. The bachelor program requires 4-year fulltime training while the master program takes 1.5-year fulltime training. Additionally, the university also offers some cybersecurity courses focusing on network security and system security to both bachelor and master students. Thus, the creation of any program in network security or system security majors is an advantage over other majors. Inspired from the above reasons, HUST is going to implement the two 2 programs on cybersecurity as follows:

- 4-year bachelor on Cybersecurity (focusing on the Network security employment profile), and
- 1.5-year master on Cybersecurity (focusing on the System & Data security employment profile).

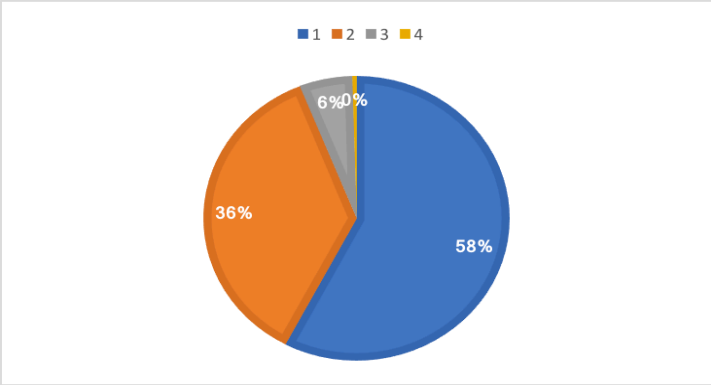
HCMUT has currently both master and bachelor degrees on computer science. The bachelor program requires 4-year fulltime training while the master degree takes 2-year fulltime training. The bachelor degree has been accredited by ABET organization and this leads to the difficulty in implementing a new bachelor-level program, including a new bachelor program on cybersecurity, at this time. This situation and other reasons according to the survey guide us to the implementation of the new master program only in the theme of this project. The implemented master-level program will be named as ¨Master in Cybersecurity¨ and includes two main majors, corresponding to the two high-level employment profiles identified in this document: System & Data Security and Security Management.

VNUA has 7 programs related with this area: (1) 4-year bachelor entitled BSc on Information Systems; (2) 4-year bachelor entitled BSc on Information Technology; (3) 4-year bachelor entitled BSc on Software Engineering; (4) 4-year bachelor entitled BSc on Applied Mathematics-Informatics (Professional-Oriented Higher Education – POHE); (5) 4-year bachelor entitled BSc on Computer Networking and Web (POHE); (6) 4-year bachelor entitled BSc on Software Engineering (POHE); (7) 2-year master entitled MSc on Information Technology. According to the demanding employment profiles, the aim is setting up a new BSc program entitled BSc on Information Security (focusing on Network security). With MSc level, we are creating a new track of Information Security (focusing on System and Data security) within the original 2-year program. We will do it by replacing some subjects with new ones of cyber-security field, and by suggesting a research orientation for the final theses to our master students.

Annex 1: Survey Results

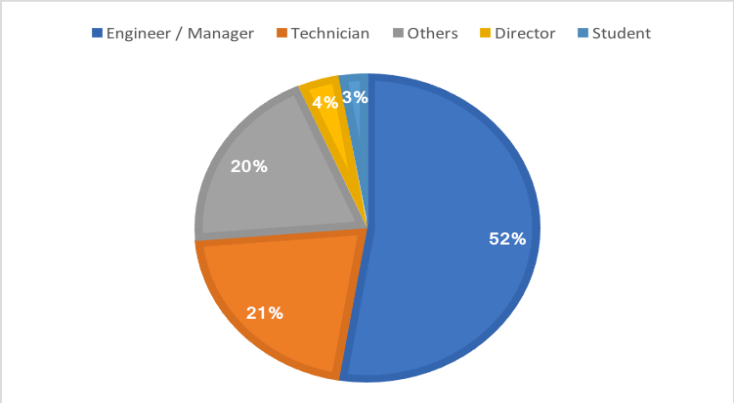
1. Your Age

Number	Choice	Quantity	Percent
1	20-30	135	57.69%
2	30-40	85	36.32%
3	40-50	13	5.56%
4	50+	1	0.43%



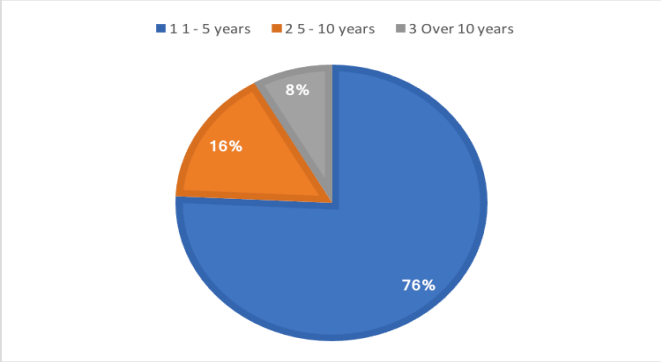
2. Your Job

Number	Choice	Quantity	Percent
1	Engineer / Manager	120	52.63%
2	Technician	48	21.05%
3	Others	45	19.74%
4	Director	9	3.95%
5	Student	6	2.63%



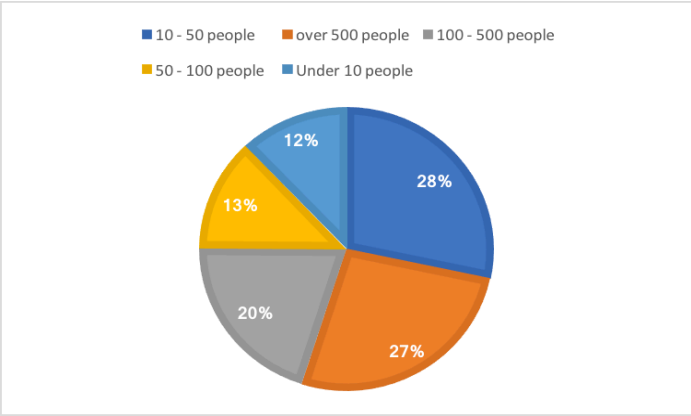
4. Your own experience about Information Security

Number	Choice	Quantity	Percent
1	1 - 5 years	175	75.76%
2	5 - 10 years	37	16.02%
3	Over 10 years	19	8.23%



5. What size is your business?

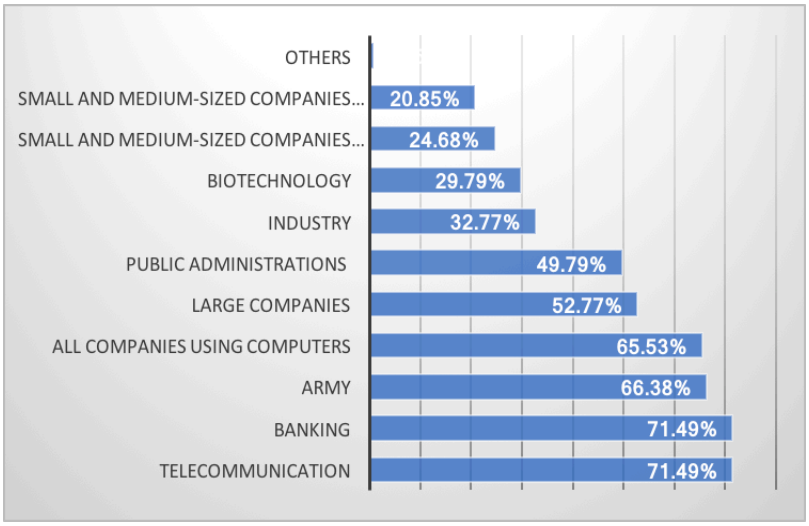
Number	Choice	Quantity	Percent
1	10 - 50 people	66	28.33%
2	over 500 people	62	26.61%
3	100 - 500 people	47	20.17%
4	50 - 100 people	30	12.88%
5	Under 10 people	28	12.02%



6. According to you, what aspects does Information Security specialize in? (you can choose more than 1 option)

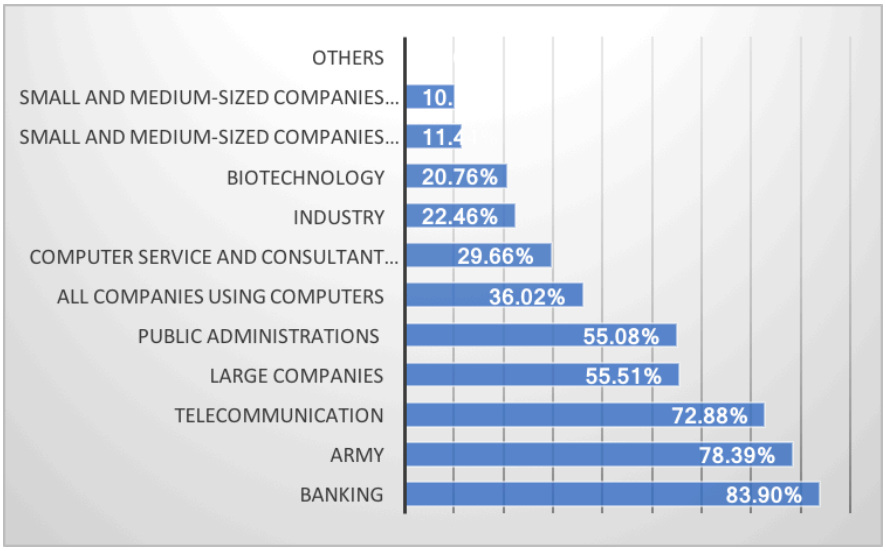
Number	Choice	Quantity	Percent
1	Telecommunication	168	71.49%
2	Banking	168	71.49%
3	Army	156	66.38%
4	All companies using computers	154	65.53%

5	Large companies	124	52.77%
6	Public Administrations	117	49.79%
7	Industry	77	32.77%
8	Biotechnology	70	29.79%
9	Small and Medium-sized companies of Service Production	58	24.68%
10	Small and Medium-sized companies of Product Production	49	20.85%
11	Others	2	0.85%



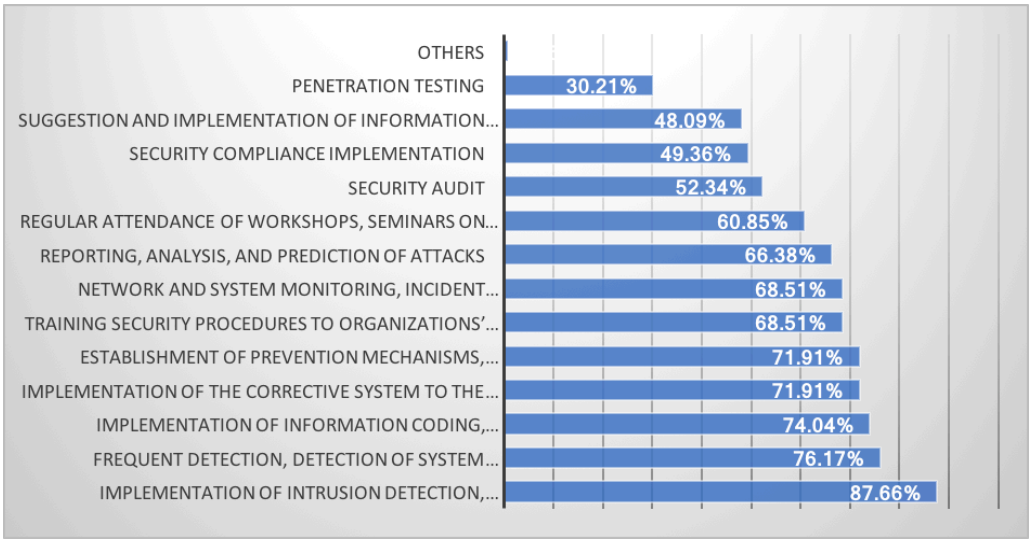
7. In your opinion, where are Information Security specialists needed the most?

Number	Choice	Quantity	Percent
1	Banking	198	83.90%
2	Army	185	78.39%
3	Telecommunication	172	72.88%
4	Large companies	131	55.51%
5	Public Administrations	130	55.08%
6	All companies using computers	85	36.02%
7	Computer Service and Consultant Companies	70	29.66%
8	Industry	53	22.46%
9	Biotechnology	49	20.76%
10	Small and Medium-sized companies of Service Production	27	11.44%
11	Small and Medium-sized companies of Product Production	24	10.17%
12	Others	0	0.00%



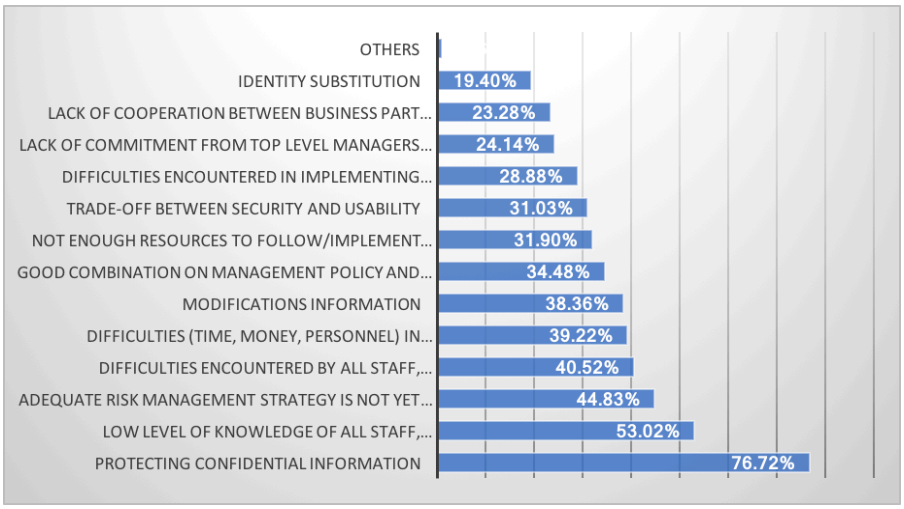
8. Specify the activities that these specialists can carry out

Number	Choice	Quantity	Percent
1	Implementation of intrusion detection, prevention and detection systems	206	87.66%
2	Frequent detection, detection of system vulnerabilities	179	76.17%
3	Implementation of information coding, authentication and construction of the PKI infrastructure	174	74.04%
4	Implementation of the corrective system to the parts of the security flaws	169	71.91%
5	Establishment of prevention mechanisms, restoration of the system and assurance of system continuity	169	71.91%
6	Training security procedures to organizations' users	161	68.51%
7	Network and system monitoring, incident response	161	68.51%
8	Reporting, analysis, and prediction of attacks	156	66.38%
9	Regular attendance of workshops, seminars on information security, updating information on security vulnerabilities in systems / software	143	60.85%
10	Security audit	123	52.34%
11	Security compliance implementation	116	49.36%
12	Suggestion and Implementation of information security standards	113	48.09%
13	Penetration testing	71	30.21%
14	Others	2	0.85%



9. Describe what problems you encounter concerning with Information Security in your company

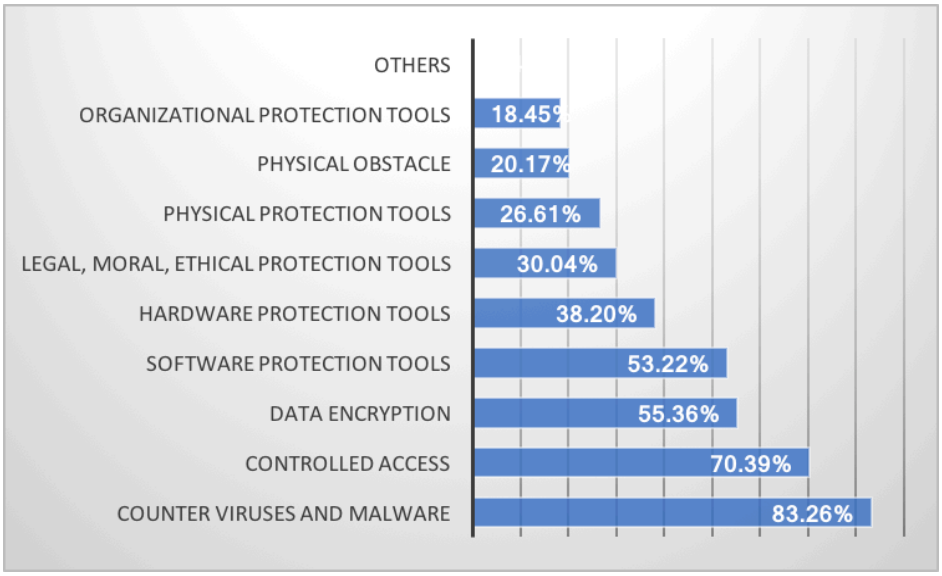
Number	Choice	Quantity	Percent
1	Protecting Confidential Information	178	76.72%
2	Low level of knowledge of all staff, management, not only IT teachers on the importance of information security	123	53.02%
3	Adequate risk management strategy is not yet in place	104	44.83%
4	Difficulties encountered by all staff, management in the development and implementation of security processes in data processing, data processing and the operating system	94	40.52%
5	Difficulties (time, money, personnel) in implement and enforce security policies inside the company	91	39.22%
6	Modifications information	89	38.36%
7	Good combination on management policy and deployment technology is not yet done	80	34.48%
8	Not enough resources to follow/implement security standards such as ISO 27001	74	31.90%
9	Trade-off between security and usability	72	31.03%
10	Difficulties encountered in implementing security processes in accordance with ISO 17799	67	28.88%
11	Lack of commitment from top level managers to ensure security mechanism is in place	56	24.14%
12	Lack of cooperation between business part and security part of the company	54	23.28%
13	Identity Substitution	45	19.40%
14	Others	2	0.86%



10. Specify the devices used for Information Security in your company (software and hardware)

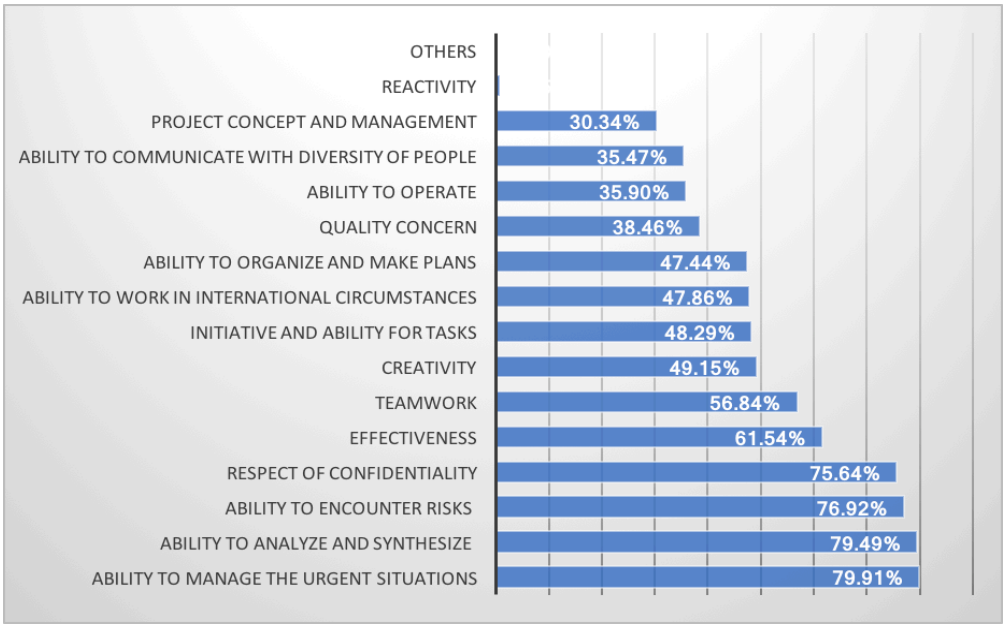
Number	Choice	Quantity	Percent
1	Counter viruses and malware	194	83.26%
2	Controlled access	164	70.39%
3	Data encryption	129	55.36%
4	Software protection tools	124	53.22%

5	Hardware protection tools	89	38.20%
6	Legal, moral, ethical protection tools	70	30.04%
7	Physical protection tools	62	26.61%
8	Physical obstacle	47	20.17%
9	Organizational protection tools	43	18.45%
10	Others	1	0.43%



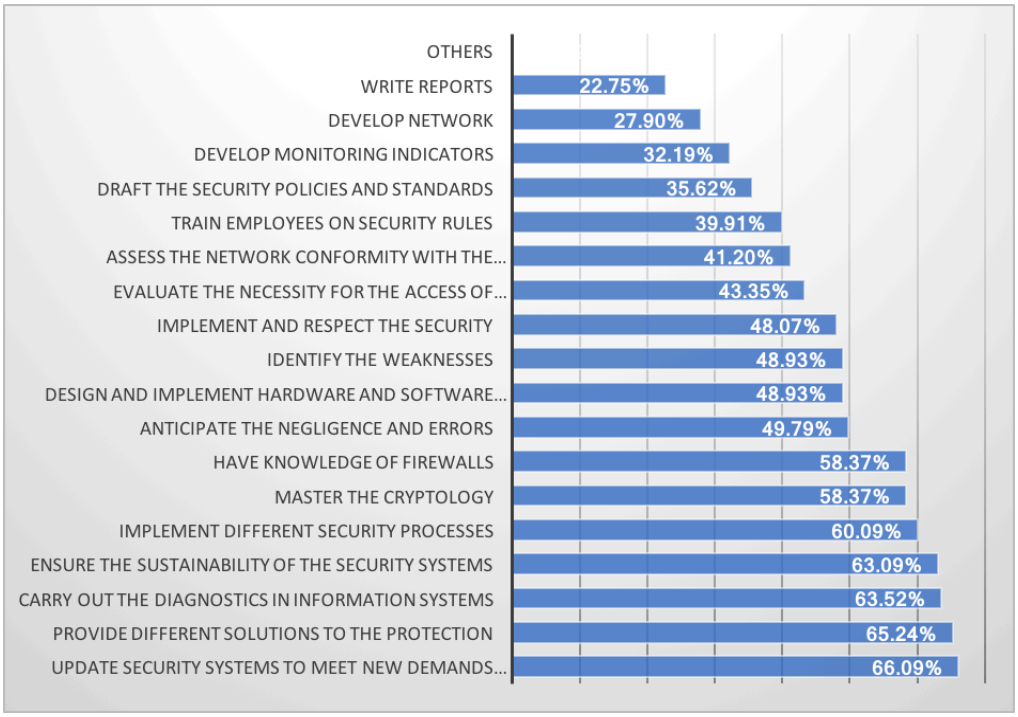
11. In your opinion, are there generic skills that an Information Security specialist must have?

Number	Choice	Quantity	Percent
1	Ability to manage the urgent situations	187	79.91%
2	Ability to analyze and synthesize	186	79.49%
3	Ability to encounter risks	180	76.92%
4	Respect of confidentiality	177	75.64%
5	Effectiveness	144	61.54%
6	Teamwork	133	56.84%
7	Creativity	115	49.15%
8	Initiative and ability for tasks	113	48.29%
9	Ability to work in international circumstances	112	47.86%
10	Ability to organize and make plans	111	47.44%
11	Quality Concern	90	38.46%
12	Ability to operate	84	35.90%
13	Ability to communicate with diversity of people	83	35.47%
14	Project concept and management	71	30.34%
15	Reactivity	2	0.85%
16	Others	0	0.00%



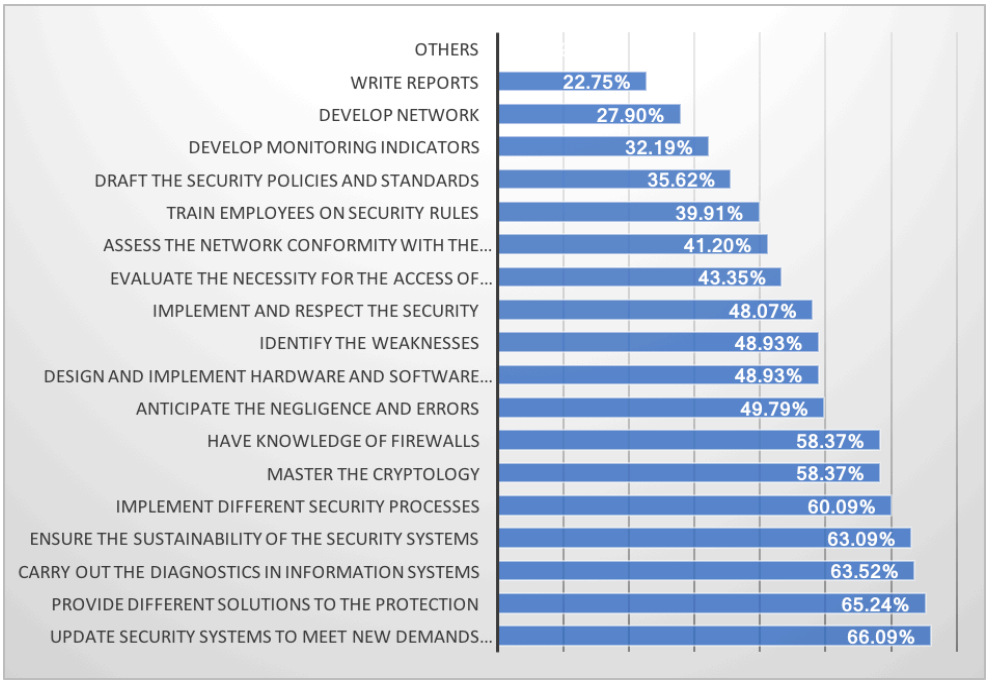
12. According to you, what can you get these generic skills from?

Number	Choice	Quantity	Percent
1	Practical workshops	118	48.16%
2	Case studies	55	22.45%
3	Techniques	26	10.61%
4	Others	24	9.80%
5	Multimedia	13	5.31%
6	Theories	8	3.27%
7	Training/Academic courses	1	0.41%



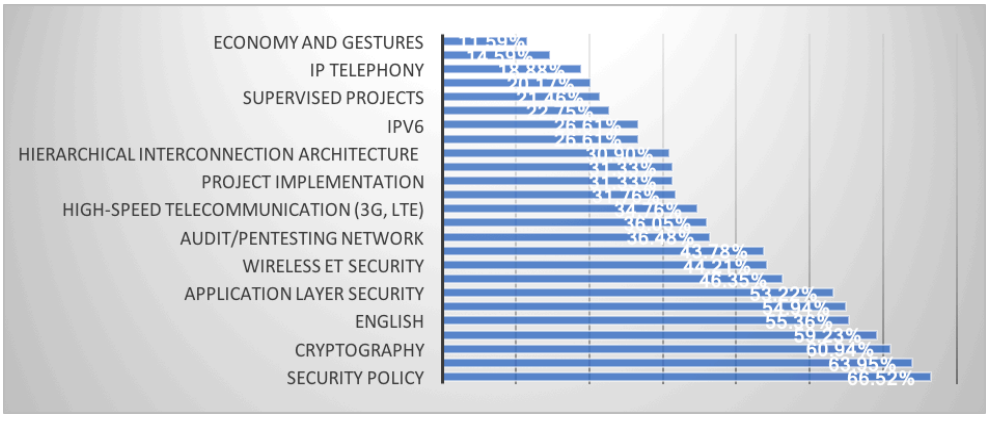
13. In your view, which specific skills do specialists in Information Security need to have?

Number	Choice	Quantity	Percent
1	Update security systems to meet new demands and latest technologies	154	66.09%
2	Provide different solutions to the protection	152	65.24%
3	Carry out the diagnostics in information systems	148	63.52%
4	Ensure the sustainability of the security systems	147	63.09%
5	Implement different security processes	140	60.09%
6	Master the cryptology	136	58.37%
7	Have knowledge of firewalls	136	58.37%
8	Anticipate the negligence and errors	116	49.79%
9	Design and implement hardware and software architecture	114	48.93%
10	Identify the weaknesses	114	48.93%
11	Implement and respect the security	112	48.07%
12	Evaluate the necessity for the access of information and network of each service	101	43.35%
13	Assess the network conformity with the expectation of traders by reports	96	41.20%
14	Train employees on security rules	93	39.91%
15	Draft the security policies and standards	83	35.62%
16	Develop monitoring indicators	75	32.19%
17	Develop Network	65	27.90%
18	Write reports	53	22.75%
19	Others	0	0.00%



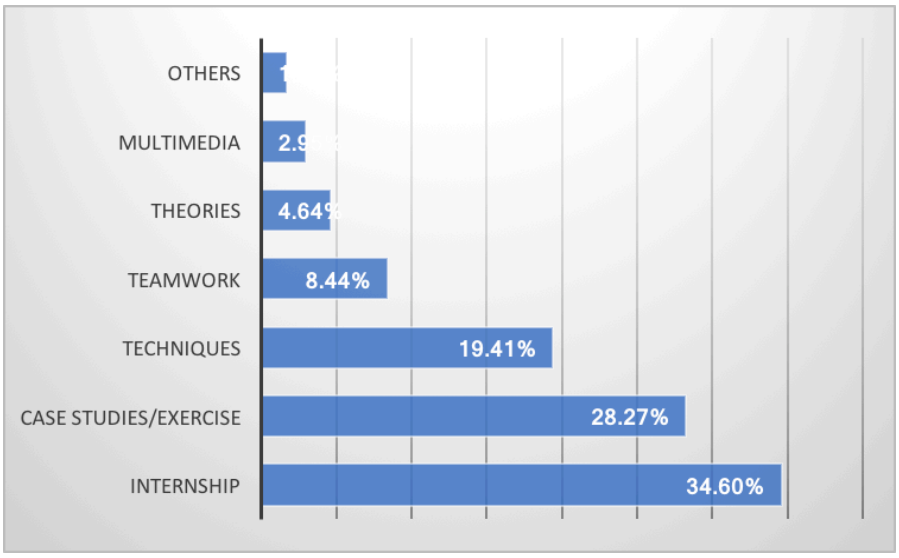
14. In your opinion, what lessons can be learned to acquire these specific skills?

Number	Choice	Quantity	Percent
1	Security policy	155	66.52%
2	Security devices et equipments (VPN-Firewall, etc.)	149	63.95%
3	Cryptography	142	60.94%
4	Network supervision and management	138	59.23%
5	English	129	55.36%
6	Security of servers and computers	128	54.94%
7	Application layer security	124	53.22%
8	Methods to implement a PSSI	108	46.35%
9	Wireless et security	103	44.21%
10	Internship	102	43.78%
11	Audit/Pentesting network	85	36.48%
12	Expression and Communication	84	36.05%
13	High-speed telecommunication (3G, LTE)	81	34.76%
14	Configuration of routers	74	31.76%
15	Project Implementation	73	31.33%
16	Interior and exterior avanced storing and mailing	73	31.33%
17	Hierarchical interconnection architecture	72	30.90%
18	Administrative network services	62	26.61%
19	IPV6	62	26.61%
20	Law	53	22.75%
21	Supervised projects	50	21.46%
22	Scripting (Shell, Python, Perl…)	47	20.17%
23	IP Telephony	44	18.88%
24	Administrative systems	34	14.59%
25	Economy and Gestures	27	11.59%



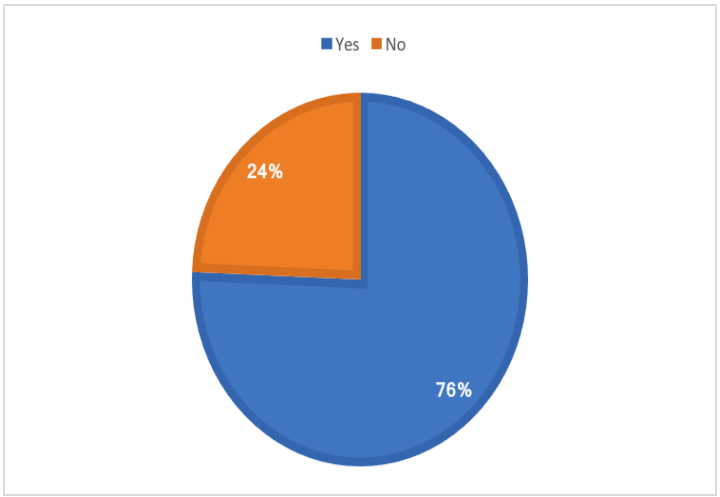
15. According to you, what teaching methods do they need to acquire these specific skills?

Number	Choice	Quantity	Percent
1	Internship	82	34.60%
2	Case studies/Exercise	67	28.27%
3	Techniques	46	19.41%
4	Teamwork	20	8.44%
5	Theories	11	4.64%
6	Multimedia	7	2.95%
7	Others	4	1.69%



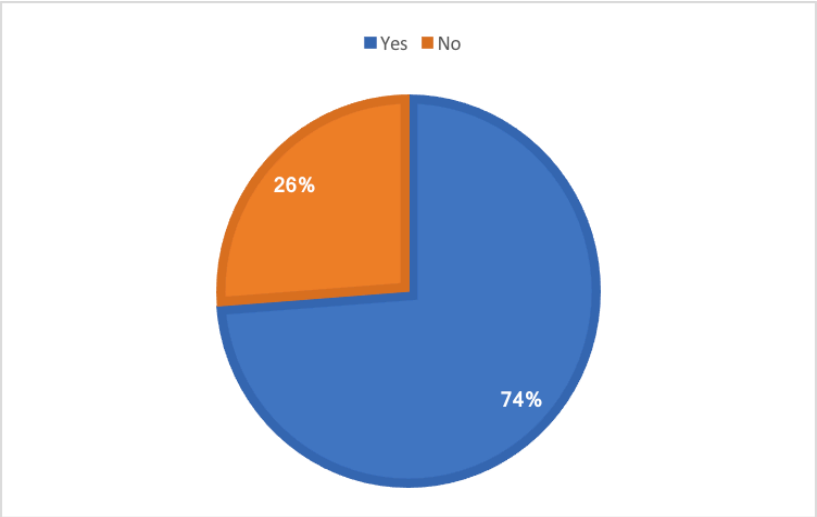
16. As a professional, do you need an Information Security training course?

Number	Choice	Quantity	Percent
1	Yes	174	75.65%
2	No	56	24.35%



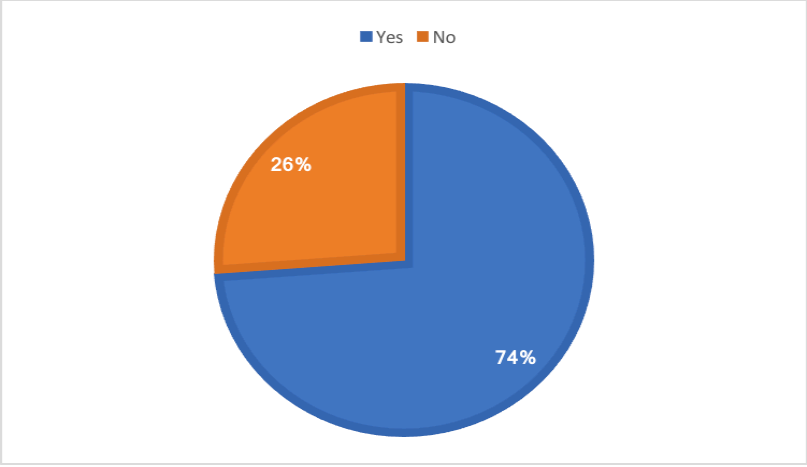
18. Would you be personally interested in Information security training?

Number	Choice	Quantity	Percent
1	Yes	169	73.80%
2	No	60	26.20%



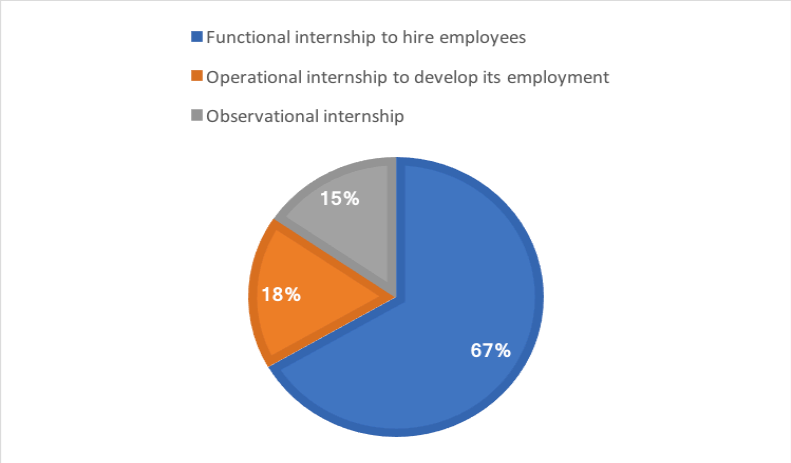
20. Would you be interested in hosting Information security internship training?

Number	Choice	Quantity	Percent
1	Yes	183	80.26%
2	No	45	19.74%



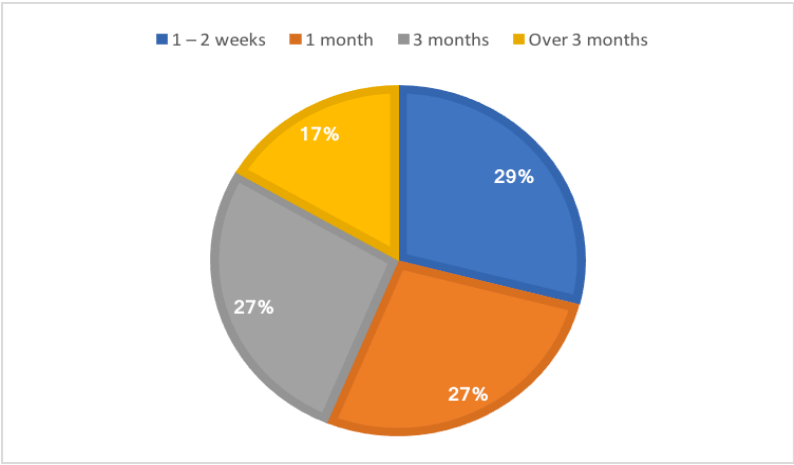
21. If yes, what type of internship do you prefer?

Number	Choice	Quantity	Percent
1	Functional internship to hire employees	142	66.36%
2	Operational internship to develop its employment	38	17.76%
3	Observational internship	33	15.42%



22. If yes, how long will your internship be

Number	Choice	Quantity	Percent
1	1 – 2 weeks	63	29.03%
2	1 month	59	27.19%
3	3 months	59	27.19%
4	Over 3 months	36	16.59%



Annex 2: Knowledge & Activities

According to the NICE guidelines, the renovator team sletected the following lists of Knowledges and competences. The selection was based on the 4 identified profiles.

Knowledges

K01	Knowledge of an organization's information classification program and procedures for information compromise.
K02	Knowledge of anti-forensics tactics, techniques, and procedures.
K03	Knowledge of applicable business processes and operations of customer organizations.
K04	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
K05	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
K06	Knowledge of application vulnerabilities.
K07	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).
K08	Knowledge of authentication, authorization, and access control methods.
K09	Knowledge of basic system, network, and OS hardening techniques.
K10	Knowledge of business continuity and disaster recovery continuity of operations plans.
K11	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
K12	Knowledge of collection management processes, capabilities, and limitations.
K13	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K14	Knowledge of communication methods, principles, and concepts that support the network infrastructure.
K15	Knowledge of computer algorithms.
K16	Knowledge of computer networking concepts and protocols, and network security methodologies.
K17	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).
K18	Knowledge of configuration management techniques.
K19	Knowledge of controls related to the use, processing, storage, and transmission of data.
K20	Knowledge of critical information technology (IT) procurement requirements.
K21	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.
K22	Knowledge of cryptography and cryptographic key management concepts
K23	Knowledge of cryptology.
K24	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.
K25	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K26	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
K27	Knowledge of cyber defense and information security policies, procedures, and regulations.

K28	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K29	Knowledge of cyber threats and vulnerabilities.
K30	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
K31	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
K32	Knowledge of cybersecurity and privacy principles.
K33	Knowledge of data backup and recovery.
K34	Knowledge of data backup and restoration concepts.
K35	Knowledge of data carving tools and techniques (e.g., Foremost).
K36	Knowledge of database systems.
K37	Knowledge of debugging procedures and tools.
K38	Knowledge of deployable forensics.
K39	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
K40	Knowledge of embedded systems.
K41	Knowledge of encryption algorithms
K42	Knowledge of encryption methodologies.
K43	Knowledge of ethical hacking principles and techniques.
K44	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
K45	Knowledge of file type abuse by adversaries for anomalous behavior.
K46	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).
K47	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.
K48	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
K49	Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).
K50	Knowledge of how to extract, analyze, and use metadata.
K51	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
K52	Knowledge of human-computer interaction principles.
K53	Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.
K54	Knowledge of incident response and handling methodologies.
K55	Knowledge of industry-standard and organizationally accepted analysis principles and methods.
K56	Knowledge of information security program management and project management principles and techniques.
K57	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K58	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
K59	Knowledge of installation, integration, and optimization of system components.
K60	Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).
K61	Knowledge of interpreted and compiled computer languages.
K62	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.

K63	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K64	Knowledge of malware analysis and characteristics.
K65	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).
K66	Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).
K67	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).
K68	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
K69	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.
K70	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K71	Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
K72	Knowledge of network security architecture concepts
K73	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
K74	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
K75	Knowledge of network tools (e.g., ping, traceroute, nslookup)
K76	Knowledge of network traffic analysis methods.
K77	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
K78	Knowledge of operating system command-line tools.
K79	Knowledge of operating systems.
K80	Knowledge of operations security.
K81	Knowledge of organization's enterprise information security architecture.
K82	Knowledge of organization's evaluation and validation requirements.
K83	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K84	Knowledge of parallel and distributed computing concepts.
K85	Knowledge of Payment Card Industry (PCI) data security standards.
K86	Knowledge of penetration testing principles, tools, and techniques.
K87	Knowledge of Personal Health Information (PHI) data security standards.
K88	Knowledge of Personally Identifiable Information (PII) data security standards.
K89	Knowledge of reverse engineering concepts.
K90	Knowledge of Risk Management Framework (RMF) requirements.
K91	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K92	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).64
K93	Knowledge of Security Assessment and Authorization process.
K94	Knowledge of security event correlation tools.
K95	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark- Wilson integrity model).
K96	Knowledge of server and client operating systems.
K97	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).
K98	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).

K99	Knowledge of software engineering.
K100	Knowledge of specific operational impacts of cybersecurity lapses.
K101	Knowledge of structured analysis principles and methods.
K102	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
K103	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
K104	Knowledge of system administration, network, and operating system hardening techniques.
K105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K106	Knowledge of system life cycle management principles, including software security and usability.
K107	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.
K108	Knowledge of systems diagnostic tools and fault identification techniques.
K109	Knowledge of systems security testing and evaluation methods.
K110	Knowledge of technology integration processes.
K111	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).
K112	Knowledge of types of digital forensics data and how to recognize them.
K113	Knowledge of the basic structure, architecture, and design of converged applications.
K114	Knowledge of the data flow from collection origin to repositories and tools.
K115	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.
K116	Knowledge of the organization's core business/mission processes.
K117	Knowledge of the systems engineering process.
K118	Knowledge of various types of computer architectures.
K119	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
K120	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
K121	Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities.
K122	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
K123	Knowledge of Windows/Unix ports and services.
K124	Signature implementation impact for viruses, malware, and attacks.

Activities

A1	Coordinate with intelligence analysts to correlate threat assessment data.
A2	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
A3	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
A4	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
A5	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
A6	Perform cyber defense trend analysis and reporting.
A7	Conduct nodal analysis.
A8	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
A9	Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.
A10	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
A11	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
A12	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
A13	Develop content for cyber defense tools.
A14	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
A15	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
A16	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.
A17	Reconstruct networks in diagram or report format.
A18	Review appropriate information sources to determine validity and relevance of information gathered.
A19	Provide target recommendations which meet leadership objectives.
A20	Profile targets and their activities.
A21	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.
A22	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
A23	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
A24	Assess and monitor cybersecurity related to system implementation and testing practices.
A25	Verify and update security documentation reflecting the application/system security design features.
A26	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
A27	Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).
A28	Establish acceptable limits for the software application, network, or system.

A29	Identify applications and operating systems of a network device based on network traffic.
A30	Isolate and remove malware.
A31	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).
A32	Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.
A33	Examine recovered data for information of relevance to the issue at hand.
A34	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
A35	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).
A36	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.
A37	Determine and document software patches or the extent of releases that would leave software vulnerable.
A38	Verify minimum security requirements are in place for all applications.
A39	Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.
A40	Develop secure software testing and validation procedures.
A41	Design to security requirements to ensure requirements are met for all systems and/or applications.
A42	Consult with customers about software system design and maintenance.
A43	Perform virus scanning on digital media.
A44	Perform penetration testing as required for new or updated applications.
A45	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
A46	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.
A47	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.
A48	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).
A49	Perform hash comparison against established database.
A50	Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.
A51	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
A52	Implement specific cybersecurity countermeasures for systems and/or applications.
A53	Implement new system design procedures, test procedures, and quality standards.
A54	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.
A55	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.
A56	Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP

	SECRET).
A57	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
A58	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
A59	Evaluate cost/benefit, economic, and risk analysis in decision-making process.
A60	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
A61	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
A62	Assess all the configuration management (change configuration/release management) processes.
A63	Assess the effectiveness of security controls.
A64	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
A65	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).
A66	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.
A67	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.
A68	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
A69	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
A70	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
A71	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
A72	Recognize a possible security violation and take appropriate action to report the incident, as required.
A73	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program.
A74	Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.
A75	Ensure that security improvement actions are evaluated, validated, and implemented as required.
A76	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.
A77	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
A78	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.
A79	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
A80	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
A81	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.
A82	Establish a risk management strategy for the organization that includes a determination of

	risk tolerance.
A83	Generate requests for information.
A84	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.
A85	Work with stakeholders to resolve computer security incidents and vulnerability compliance.
A86	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
A87	Assess adequate access controls based on principles of least privilege and need-to-know.
A88	Analyze and report system security posture trends.
A89	Analyze and report organizational security posture trends.
A90	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
A91	Plan and recommend modifications or adjustments based on exercise results or system environment.
A92	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.
A93	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.
A94	Answer requests for information.
A95	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.
A96	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
A97	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.
A98	Report intelligence-derived significant network events and intrusions.
A99	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
A100	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.
A101	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.
A102	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.
A103	Provide current intelligence support to critical internal/external stakeholders as appropriate.