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

Fiches métier LICENCE et MASTER

VIETNAM

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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	