EC-Council

NICE Cybersecurity Workforce Framework (NCWF) and EC-Council Certification Mapping

National Initiative for Cybersecurity Education (NICE)

About NICE

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Located in the Information Technology Laboratory at NIST, the NICE Program Office operates under the Applied Cybersecurity Division, positioning the program to support the country's ability to address current and future cybersecurity challenges through standards and best practices.

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure.

NICE Strategic Plan

The NICE Strategic Plan is the result of engagement and deliberation among NICE partners in government, academia, and industry. The overall intent of the Strategic Plan is to provoke a national conversation and guide action on how to address the critical shortage of a skilled cybersecurity workforce.

Values:

- Seek Evidence – inform actions or decisions with data and pursue objective and reliable sources of information
- Pursue Action – create concrete steps towards deliverable outcomes to achieve mission and goals
- Challenge Assumptions – examine rationale for past and present education, training, and workforce approaches and apply critical analysis to future solutions
- Drive Change – seek creative and innovative solutions that might disrupt or defy the status quo
- Stimulate Innovation – inspire and experiment with new approaches to education, training, and skills development
- Foster Communication – raise awareness of cybersecurity education and workforce issues and encourage openness to build trust
- Facilitate Collaboration – combine the knowledge and skills of multiple stakeholders with multiple viewpoints to achieve the best outcomes
- Share Resources – leverage, support, and raise awareness of community-developed approaches and solutions
- Model Inclusion – encourage participation from stakeholders with diverse backgrounds and viewpoints
- Measure Results – assess the effectiveness of results through both quantitative metrics and qualitative measures

National Initiative for Cybersecurity Education (NICE)

Goal #1 Accelerate Learning and Skills Development

Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers

Objectives:

1.1 Stimulate the development of approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers

1.2 Advance programs that reduce the time and cost for obtaining knowledge, skills, and abilities for in-demand work roles

1.3 Engage displaced workers or underemployed individuals who are available and motivated to assume cybersecurity work roles

1.4 Experiment with the use of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skills

1.5 Explore methods to identify gaps in cybersecurity skills and raise awareness of training that addresses identified workforce needs

Goal #2 Nurture a Diverse Learning Community

Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce

Objectives:

2.1 Improve education programs, co-curricular experiences, and training and certifications

2.2 Encourage tools and techniques that effectively measure and validate individual aptitude, knowledge, skills, and abilities

2.3 Inspire cybersecurity career awareness with students in elementary school, stimulate cybersecurity career exploration in middle school, and enable cybersecurity career preparedness in high school

2.4 Grow creative and effective efforts to increase the number of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce

2.5 Facilitate the development and dissemination of academic pathways for cybersecurity careers

Goal #3 Guide Career Development and Workforce Planning

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent.

Objectives:

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers

3.2 Publish and raise awareness of the National Cybersecurity Workforce Framework and encourage adoption

3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals

3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning

NICE Working Group

The NICE Working Group (NICEWG) has been established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.

NICE Working Group Structure and Leadership

The NICE Working Group is led by three co-chairs, each representing Academia, Private Industry, or Government. The current co-chairs are:

- Academic: Kathi Hiyane-Brown, President of Whatcom Community College
- Industry: Andre Thornton, Founder and CEO of Whitman Consulting
- Government: Rodney Petersen, Director of NICE at the National Institute of Standards and Technology

The NICE Working Group is comprised of five sub-working groups. Each subgroup meets independent of the NICEWG and reports out at the NICEWG Meetings. The subgroups are:

- K-12
- Collegiate
- Competitions

- Training and Certifications
- Workforce Management

NICE Interagency Coordinating Council

The NICE Interagency Coordinating Council (ICC) convenes federal government partners of NICE for consultation, communication, and coordination of policy initiatives and strategic directions related to cybersecurity education, training, and workforce development.

NICE Cybersecurity Workforce Framework (NCWF)

Introduction to NICE Cybersecurity Workforce Framework (NCWF)

The NCWF can be viewed as a cybersecurity workforce dictionary, and consumers of the NCWF can reference it for different workforce development, education, and/or training purposes. For instance, it provides a starting point and helps set standards for developing academic pathways, career pathways, position descriptions, and training content. The NCWF helps to ensure our nation is able to educate, recruit, train, develop, and retain a highly-qualified cybersecurity workforce. It serves several key audiences within the cybersecurity community including:

- **Employers**, to help assess their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and improve position descriptions;
- **Current and future employees**, to help explore Tasks and Work Roles and assist with understanding the KSAs that are being valued by employers for in-demand cybersecurity jobs and positions. The NCWF also enables staffing specialists and guidance counsellors to use the NCWF as a resource to support these employees or job seekers;
- **Training and certification providers** who desire to help current and future members of the cybersecurity workforce gain and demonstrate the KSAs;
- **Education providers** who may use the NCWF as a reference to develop curriculum, courses, seminars, and research that cover the KSAs and Tasks described; and
- **Technology providers** who can identify cybersecurity Work Roles and specific Tasks and KSAs associated with services and hardware/software products they supply.

As a mechanism to organize information technology (IT), cybersecurity, and cyber-related work, the NCWF helps organizations to organize roles and responsibilities through the following components:

- **Categories** – A high-level grouping of common cybersecurity functions;
- **Specialty Areas** – Distinct areas of cybersecurity work;
- **Work Roles** – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks;
- **Tasks** – Specific work activities that could be assigned to a professional working in one of the NCWF's Work Roles; and
- **Knowledge, Skills, and Abilities (KSAs)** – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.

The NCWF components work together to describe the range of cybersecurity work, from a high level to the very granular. Each Category contains Specialty Areas, each of which contains one or more Work Roles. Each Work Role is composed of numerous Tasks and KSAs. Providing this range of detail helps organizations to systematically build their cybersecurity workforce, which, in turn, enables improved performance, cost-effective workforce management, and continuous readiness.

While some of the NCWF is based on federal government programs, any organization with cybersecurity workforce needs will benefit from the standards described and can customize the NCWF as needed.

NICE Cybersecurity Workforce Framework (NCWF)

Using the NCWF as described above will help strengthen an organization's cybersecurity workforce. Investment in the existing workforce, such as through initiatives focused on training and retaining existing talent, will help the organization to prepare for and realize its risk management objectives. The common language provided by the NCWF also helps bridge workforce needs to external frameworks, such as the Cybersecurity Framework (CSF), the U.S. Department of Labor Competency Models, the U.S. Department of Education Employability Skills Framework, and the National Security Agency(NSA)/Department of Homeland Security(DHS) National Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units.

The NCWF builds upon decades of industry research into how to effectively manage the risks to valuable organizational electronic and physical information. Cybersecurity tactics are ever-changing, always identifying new ways to gain information advantage through technology. As we evolve, the ways we perform cybersecurity functions continue to evolve, as must the components of the NCWF. As part of an ongoing collaborative approach, NICE will periodically consider recommendations received and will update the NCWF publication(s). Additionally, new reference materials or tools will be developed to cross-reference elements of the NCWF. To the extent possible, digital reference materials will be posted to the NICE website as an aid to applying and utilizing NCWF and associated materials.

NICE Cybersecurity Workforce Framework (NCWF)

The seven categories and a description of the types of specialty areas included in each are below.

SECURELY PROVISION (SP) - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).

OPERATE AND MAINTAIN (OM) - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

OVERSEE AND GOVERN (OV) - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

PROTECT AND DEFEND (PR) - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

ANALYZE (AN) - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

COLLECT AND OPERATE (CO) - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

INVESTIGATE (IN) - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

About NICE | Introduction to NCWF | About EC-Council | EC-Council Career Tracks | EC-Council Programs

About NICE, NCWF and EC-Council | Methodology and Mapping Summary | Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV) | Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO) | Investigate (IN)

EC-Council at a Glance

EC-Council Group is a multidisciplinary institution of global Information Security professional services.

EC-Council Group is a dedicated Information Security organization that aims at creating knowledge, facilitating innovation, executing research, implementing development, and nurturing subject matter experts in order to provide their unique skills and niche expertise in cybersecurity.

Some of the finest organizations around the world such as the US Army, US Navy, DoD, the FBI, Microsoft, IBM, and the United Nations have trusted EC-Council to develop and advance their security infrastructure.

ICECC
International Council of E-Commerce Consultants
EC-Council Group

ECC
EC-Council Training & Certification
Division of Professional Workforce Development

EGS
EC-Council Global Services
Division of Corporate Consulting & Advisory Services

ECCU
EC-Council University
Division of Academic Education

EGE
EC-Council Global Events
Division of Conferences, Forums, Summits, Workshops & Industry Awards

ECF
EC-Council Foundation
Non-Profit Organization for Cyber Security Awareness Increase.

15+
YEARS EXPERIENCE

40+
TRAINING & CERTIFICATION PROGRAMS

145+
COUNTRIES

350+
SUBJECT MATTER EXPERTS

700+
TRAINING PARTNERS WORLDWIDE

3000+
TOOLS & TECHNOLOGIES

220,000+ CERTIFIED MEMBERS

Your Learning Options

Instructor-led Training

EC-Council has a large network of Accredited Training Centers (ATC) spread across 145 countries. Each center has a certified trainer to deliver the entire EC-Council program from a training facility in your city.

Online Training

iLearn online training is a distance learning program designed for those who cannot attend a live course. The program is for the people who have a very busy schedule and want to learn at their own pace through self-study. This modality is also available from our enterprise teams.

Mobile Learning

Our world class content is also available on a mobile device, allowing our students to learn on the go. This program is designed for those who are cannot attend a live course, but are keen to improve their cyber security skills. This modality is also available from our enterprise teams.

Computer-based Training

For people who work in secure facilities with limited or no access to the internet, we offer computer-based training (CBT) options delivered in an HD DVD format. The DVDs are an upgrade/add-on to the base iLearn program and are not sold independently. This modality is also available from our enterprise teams.

Hands-on Experience with the EC-Council Cyber Range (iLabs)

EC-Council iLabs allows students to dynamically access a host of virtual machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere. Our simplistic web portal enables the student to launch an entire range of target machines and access them remotely with one simple click. It is the most cost-effective, easy to use, live range lab solution available. *Most of our courses are equipped with iLabs, but iLabs can be purchased independently as well.*

Customized Learning

Love a course we offer, but want it customized? No problem! EC-Council has a dedicated team to cater to your needs. We have access to the largest pool of EC-Council certified instructors via our ATC channel. Let us know where and when you want the training delivered, and we will arrange for an instructor and all that's required for a course to be taught at a location of your choice. Contact our accredited training partners for a custom solution.

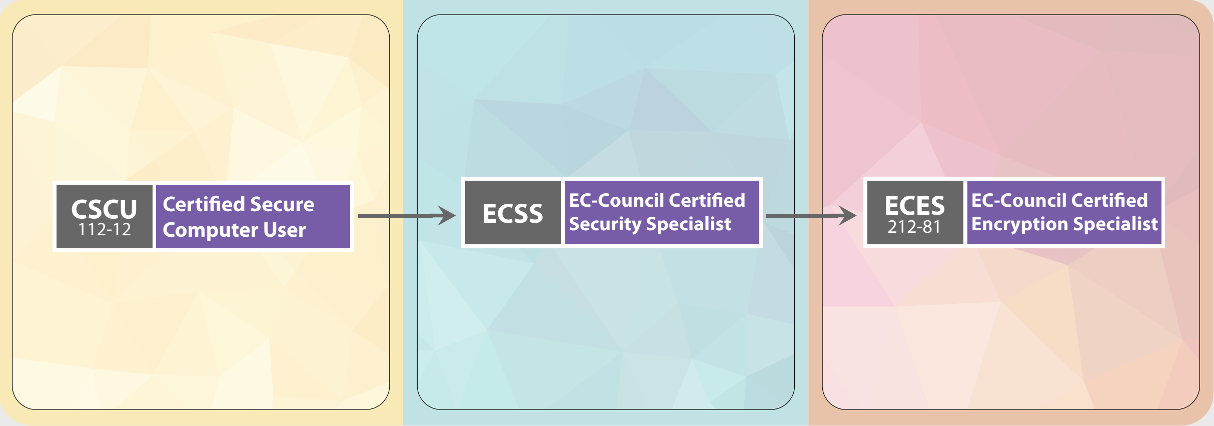
EC-Council client-site training includes official courseware, certification exam (ECC-Exam or VUE), iLabs, online labs (wherever available), and our test-pass guarantee.

Live Online Training

If self-study or self-paced learning does not fit into your personal learning style, we offer you our live online model, iWeek.

With iWeek, an instructor will teach you live online while you are seated in the comfort of your home. This training method gives you the freedom to get trained from a location of your choice. Individuals who choose this delivery method consistently attribute their choice to the preference of having a live instructor available for which questions can be asked and answered. We offer early-bird rates, group rates, and get even private courses delivered anytime.

Foundation Track


CSCU
112-12
Certified Secure Computer User
ECSS
EC-Council Certified Security Specialist
ECES
212-81
EC-Council Certified Encryption Specialist

Target Audience

This track focuses on todays' computer users who use the internet extensively to work, study and play.

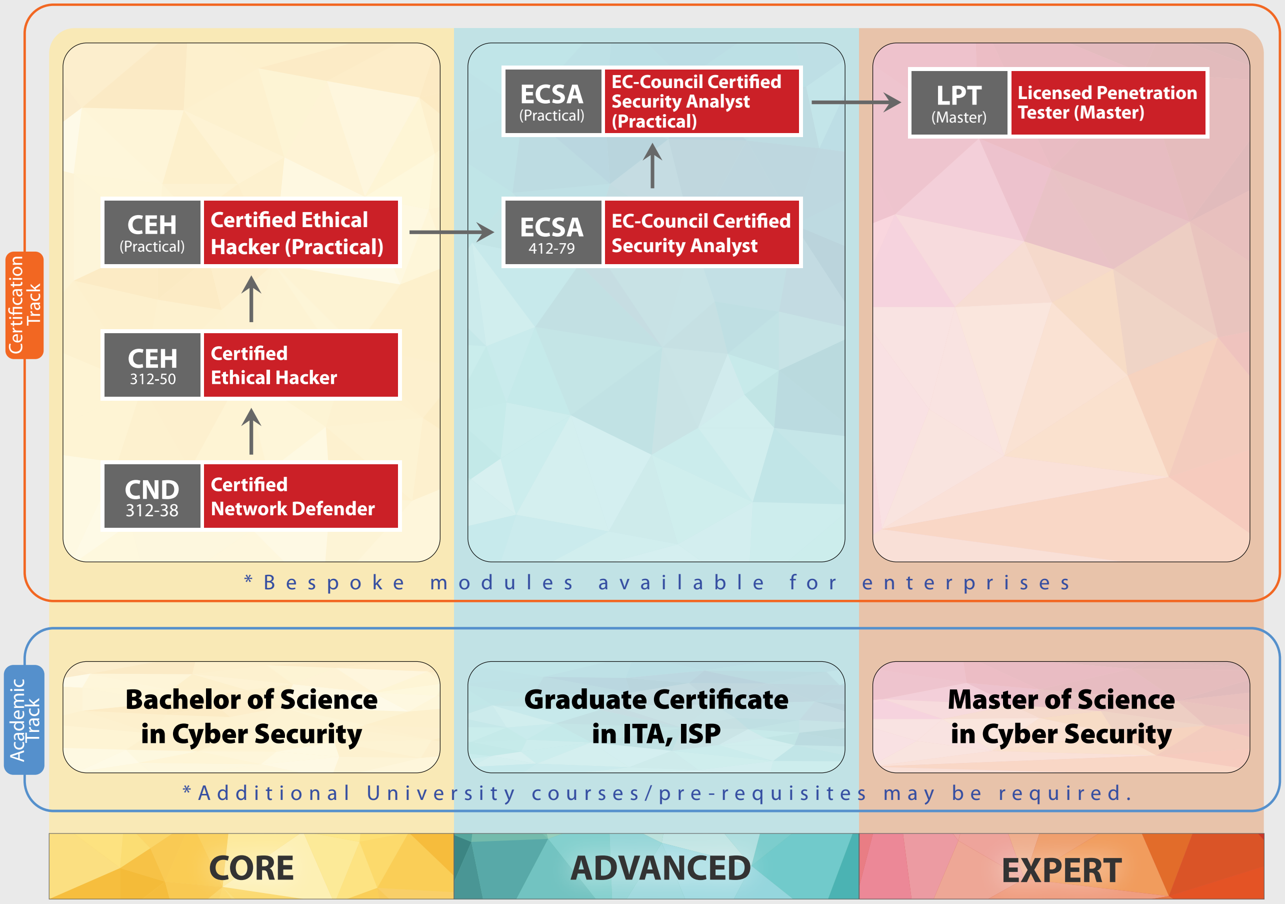
What will You Learn

Cloud Security	Password Security	Social Engineering Countermeasures	Mitigating Identity Theft	Email Security	Safe Browsing
Data Protection	Physical Security	Mobile Device Security	Encryption	Social Network Security	Antiviruses Protection
Disaster Recovery	Internet Security	Credit Card Security	Monitoring Kids Online	Wireless & Home Network Security	OS Security

Our Certified Foundation Professionals are Employed at:

Caritas Microfinance Bank, Grant Thornton, IBM, PALADION, Poly technique, Unique Academy, Ministry of Defence, NTT Data, CIT Group of Institutions, happiest minds, ingenia, icddr,b, Bank DCB Commercial Bank Plc, vodafone, UNP Universitas Negeri Padang, Reliance, core4 factory, Nestlé, • • •

Vulnerability Assessment & Penetration Testing (VAPT)



Certification Track
CEH (Practical) Certified Ethical Hacker (Practical)
CEH 312-50 Certified Ethical Hacker
CND 312-38 Certified Network Defender
ECSA (Practical) EC-Council Certified Security Analyst (Practical)
ECSA 412-79 EC-Council Certified Security Analyst
LPT (Master) Licensed Penetration Tester (Master)
*Bespoke modules available for enterprises
Academic Track
Bachelor of Science in Cyber Security
Graduate Certificate in ITA, ISP
Master of Science in Cyber Security
*Additional University courses/pre-requisites may be required.
CORE
ADVANCED
EXPERT

Job Roles

- Information Assurance (IA) Security Officer
- Information Security Analyst/Administrator
- Information Security Manager/Specialist
- Information Systems Security Engineer/Manager
- Security Analyst
- Information Security Officers
- Information Security Auditors
- Risk/Vulnerability Analyst

Our Certified VAPT Professionals are Employed at:

CISCO, EY, Microsoft, accenture, Infosys, amazon, AIG, hp, Bank of America, Booz | Allen | Hamilton, Capgemini, Deloitte., NEC, bugcrowd, TATA, lastline, axiata, U.S. ARMY, Marriott, Hero

This track maps to NICE's Specialty Areas:

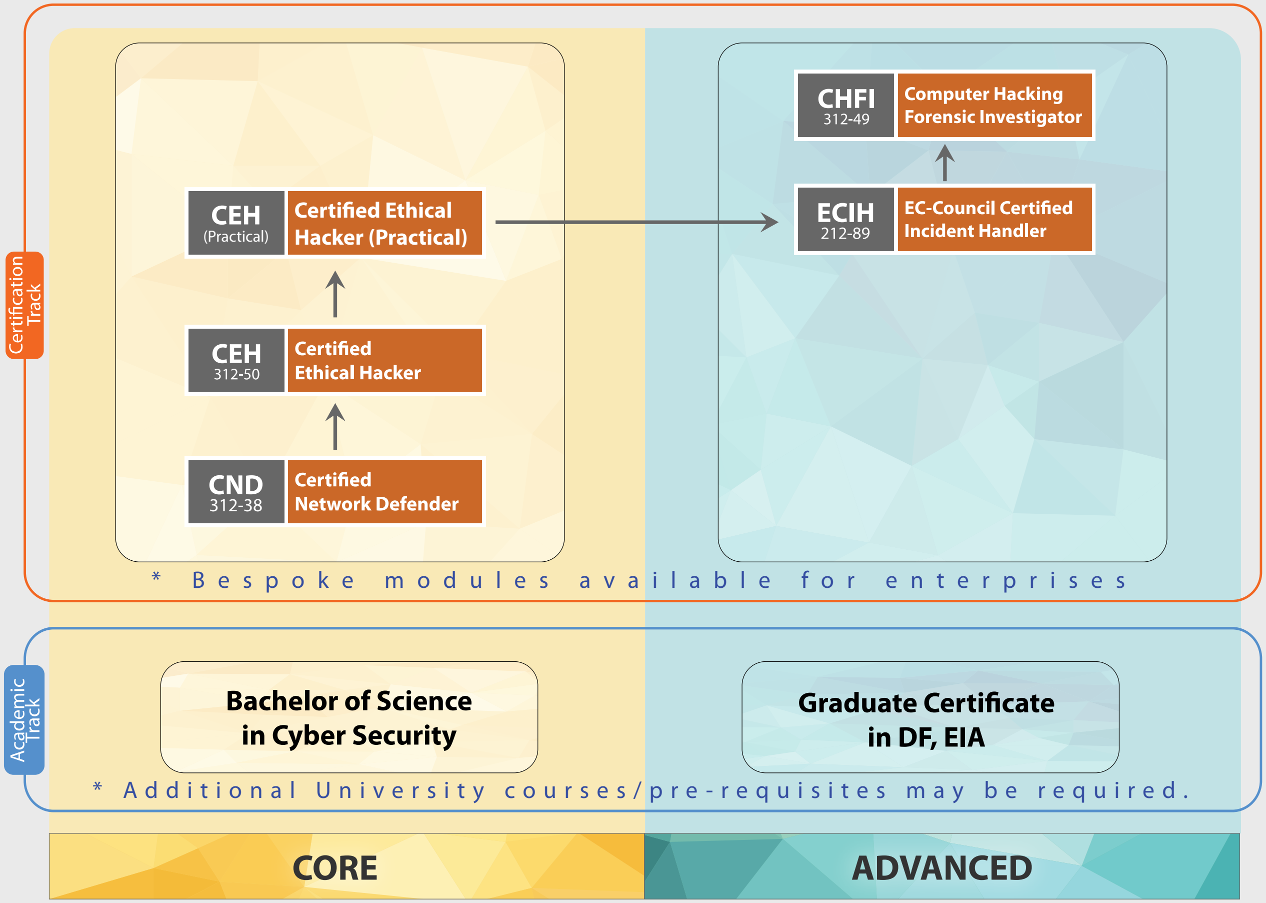
1. Protect and Defend (PR)
   a. Cybersecurity Defense Analysis (DA)
   b. Cybersecurity Defense Infrastructure Support (INF)
   c. Incident Response (IR)
   d. Vulnerability Assessment and Management (VA)

2. Securely Provision (SP)
   a. Test and Evaluation

3. Analyze (AN)
   a. Threat Analysis (TA)
   b. Exploitation Analysis (XA)

About NICE | Introduction to NCWF | About EC-Council | EC-Council Career Tracks | EC-Council Programs
About NICE, NCWF and EC-Council | Methodology and Mapping Summary | Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV) | Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO) | Investigate (IN)

Cyber Forensics



Certification Track

CEH (Practical) Certified Ethical Hacker (Practical)

CEH 312-50 Certified Ethical Hacker

CND 312-38 Certified Network Defender

CHFI 312-49 Computer Hacking Forensic Investigator

ECIH 212-89 EC-Council Certified Incident Handler

* Bespoke modules available for enterprises

Academic Track

Bachelor of Science in Cyber Security

Graduate Certificate in DF, EIA

* Additional University courses/pre-requisites may be required.

CORE

ADVANCED

Job Roles

- Computer Forensic Analyst
- Computer Network Defense (CND)
- Forensic Analyst
- Digital Forensic Examiner

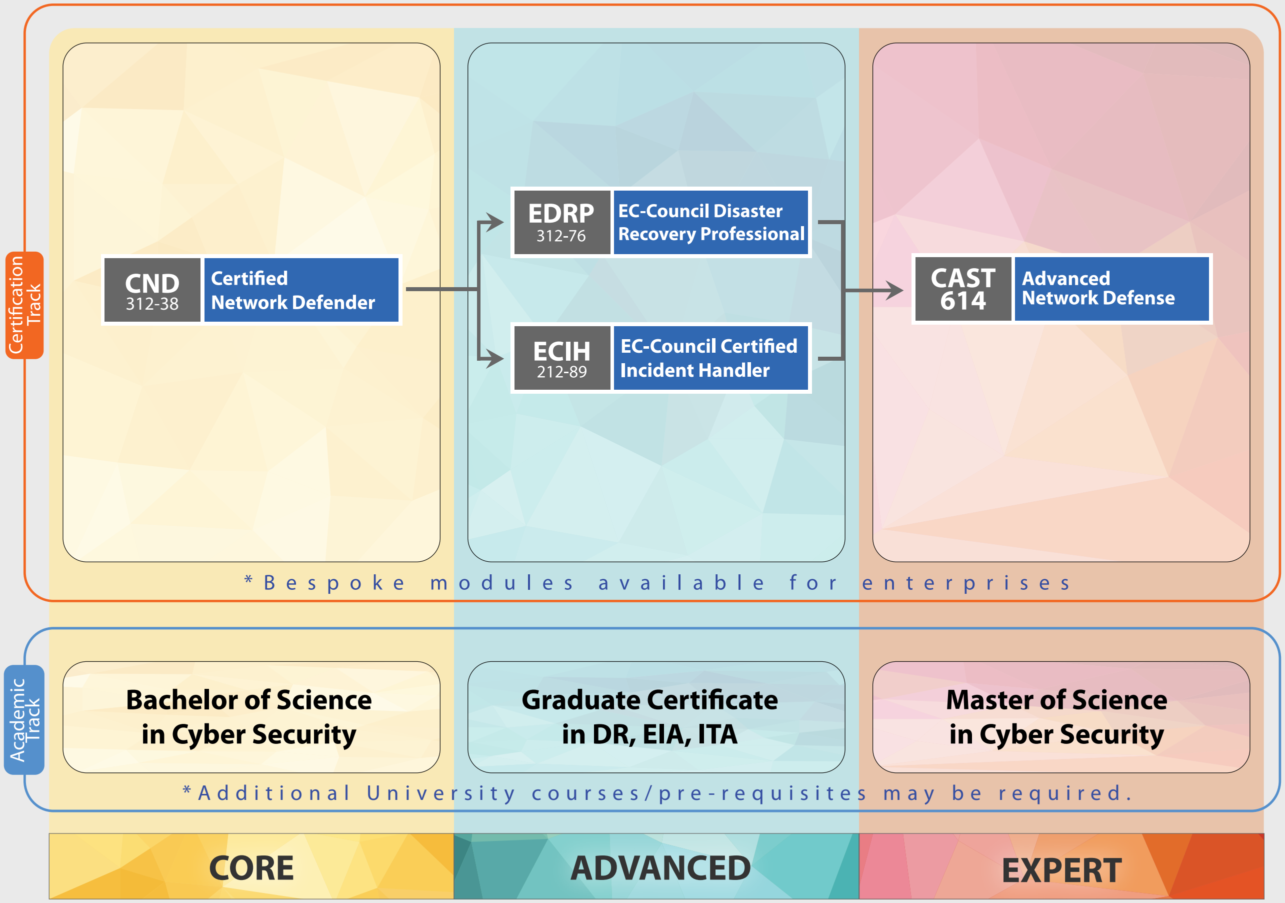
Our Certified Cyber Forensic Professionals are Employed at:

BARCLAYS, AIG, accenture, Infosys, U.S.ARMY, ICICI Bank, Bank of America, HDFC BANK, h+k, BMC SWITZERLAND, Telkom Indonesia, LEXINGTON MEDICAL CENTER, pwc, du, HSBC, WIPRO Applying Thought, • • •

This Track Maps to NICE's Specialty Areas:

1. **Securely Provision (SP)**
   a. Risk Management (RM)
   b. Test and Evaluation
   c. Systems Analysis (AN)
2. **Operate and Maintain (OM)**
   a. Network Services (NET)
   b. Systems Administration (SA)
3. **Oversee and Govern (OV)**
   a. Cybersecurity Management (MG)
4. **Protect and Defend (PR)**
   a. Cybersecurity Defense Analysis (DA)
   b. Cybersecurity Defense Infrastructure Support (INF)
   c. Incident Response (IR)
   d. Vulnerability Assessment and Management (VA)
5. **Analyze (AN)**
   a. Threat Analysis (TA)
   b. Exploitation Analysis (XA)

Network Defense and Operations



Certification Track

CND 312-38 Certified Network Defender

EDRP 312-76 EC-Council Disaster Recovery Professional

ECIH 212-89 EC-Council Certified Incident Handler

CAST 614 Advanced Network Defense

*Bespoke modules available for enterprises

Academic Track

Bachelor of Science in Cyber Security

Graduate Certificate in DR, EIA, ITA

Master of Science in Cyber Security

*Additional University courses/pre-requisites may be required.

CORE

ADVANCED

EXPERT

Job Roles

- Network Security Administrators
- Network Security Engineer/Specialist
- Network Defense Technicians
- Security Analyst
- Security Operator
- Computer Network Defense(CND) Analyst
- Cybersecurity Intelligence Analyst
- Enterprise Network Defense(END) Analyst

Our Certified Network Defense Professionals are Employed at:

بنك الخليج الأول FGB

IBM

KPMG

DISA

mitra solusi telematika

Ameriprise Financial

COMCAST

Florida State University 1851

NCB الأهلي

IPDC FINANCE

Johnson Controls

sopra steria CONSULTING

Rockwell Automation

MAPFRE

• • •

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
  a. Risk Management (RM)
  b. Test and Evaluation (TE)

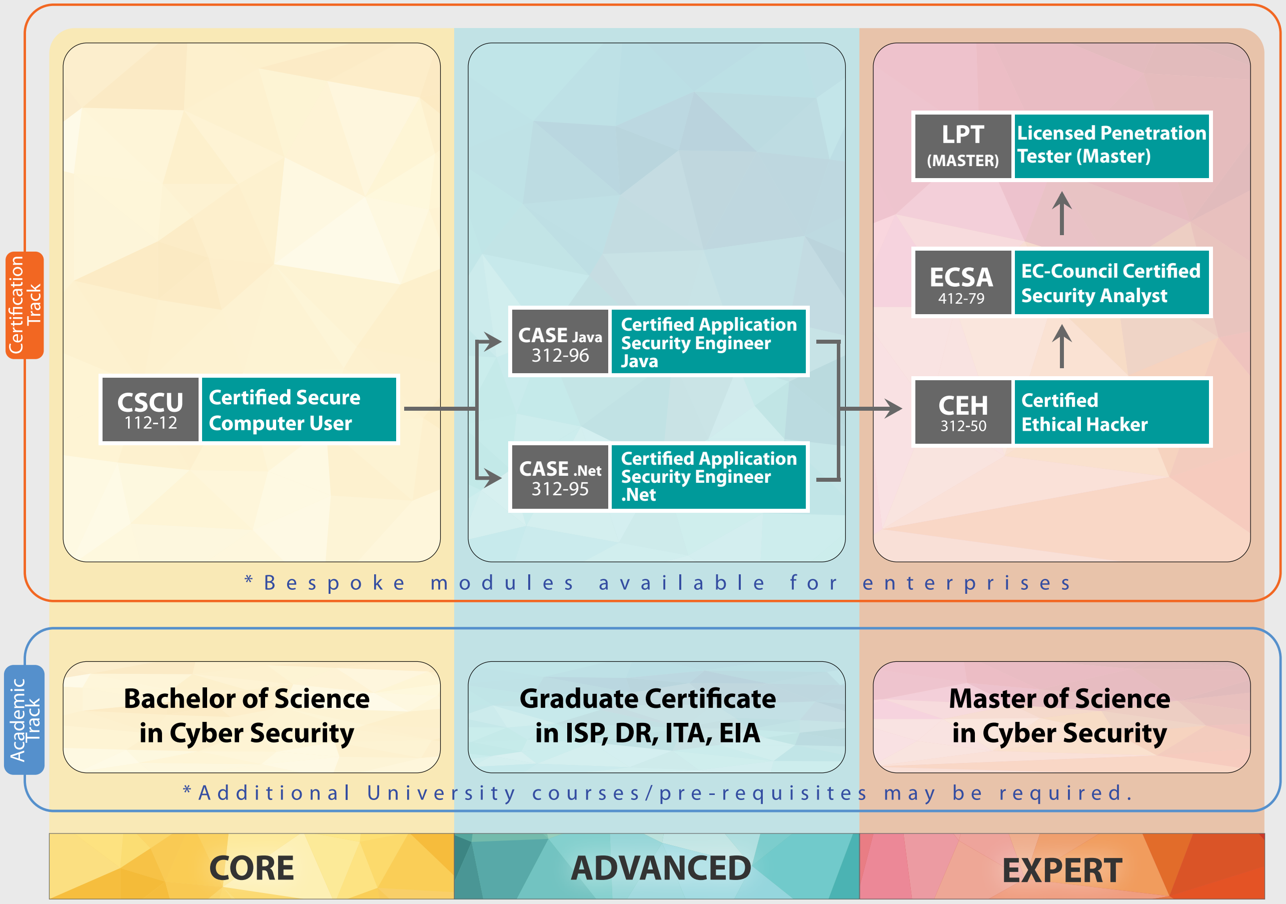
2. Operate and Maintain (OM)
  a. Network Services (NET)
  b. Systems Administration (SA)
  c. Systems Analysis (AN)

3. Oversee and Govern (OV)
  a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
  a. Cybersecurity Defense Analysis (DA)
  b. Cybersecurity Defense Infrastructure Support (INF)
  c. Incident Response (IR)
  d. Vulnerability Assessment and Management (VA)

5. Analyze (AN)
  a. Threat Analysis (TA)

Software Security


Certification Track
CSCU 112-12
Certified Secure Computer User
CASE Java 312-96
Certified Application Security Engineer Java
CASE .Net 312-95
Certified Application Security Engineer .Net
CEH 312-50
Certified Ethical Hacker
ECSA 412-79
EC-Council Certified Security Analyst
LPT (MASTER)
Licensed Penetration Tester (Master)
*Bespoke modules available for enterprises
Academic Track
Bachelor of Science in Cyber Security
Graduate Certificate in ISP, DR, ITA, EIA
Master of Science in Cyber Security
*Additional University courses/pre-requisites may be required.
CORE
ADVANCED
EXPERT

This Track Maps to NICE's Specialty Areas:

1. Securely Provision
  a. Software Development (DEV)
  b. Technology R&D (RD)

2. Operate and Maintain (OM)
  a. Data Administration (DA)
  b. Systems Analysis (AN)

3. Oversee and Govern (OV)
  a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
  a. Cybersecurity Defense Analysis (DA)
  b. Vulnerability Assessment and Management (VA)

5. Analyze (AN)
  a. Analyzes collected information to identify vulnerabilities and potential for exploitation.

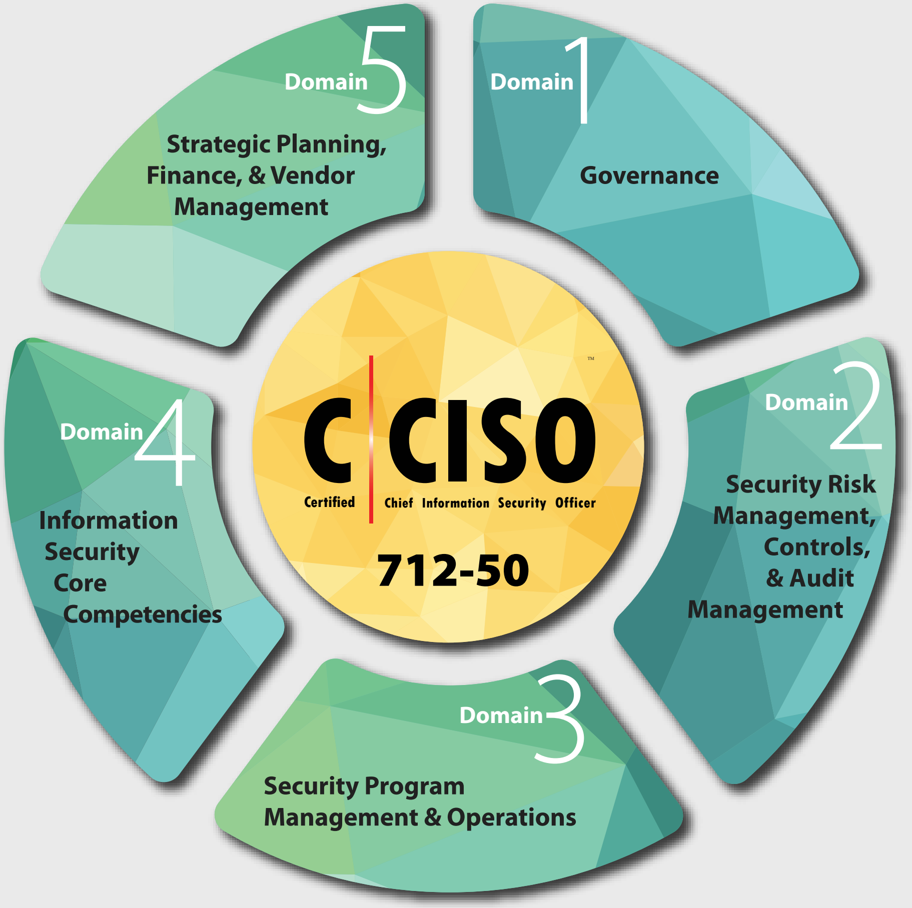
Job Roles

- Secure Software Engineer
- Security Engineer
- Software Developer
- Software Engineer/Architect
- Systems Analyst
- Web Application Developer
- Application Security Tester

Our Certified Software Security Professionals are Employed at:

WELLS FARGO, ITU, AIRBUS, TATA, axiata, BlueCross BlueShield, bol.com, alBaraka, Cognizant, Deloitte., EY Building a better working world, ecovadis, Infoblox CONTROL YOUR NETWORK, KASPERSKY lab . . .

Governance



Domain 5

Strategic Planning, Finance, & Vendor Management

Domain 1

Governance

Domain 2

Security Risk Management, Controls, & Audit Management

Domain 3

Security Program Management & Operations

Domain 4

Information Security Core Competencies

C|CISO™

Certified Chief Information Security Officer

712-50

Master of Science in Cyber Security

Graduate Certificate in:

- **Information Security Professional**
- **Information Analyst**
- **Information Technology Analyst**
- **Disaster Recovery**
- **Digital Forensics**

Job Roles

- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Information Security (IS) Director
- Information Assurance (IA) Program Manager

Our Certified CCISO Professionals are Employed at:

marta	U.S. ARMY		Akamai
MUFG Bank of Tokyo-Mitsubishi UFJ	Santander	BofI FEDERAL BANK	CHASE
CHEMICAL BANK	GENERALI	Government of South Australia	KPMG
Malwarebytes	POLICE DEPARTMENT CITY OF NEW YORK	ARROW	Polycom
Rockwell Collins	تداول Tadawul	The Bancorp	GE
HSBC	ICF	JUNIPER NETWORKS	L'ORÉAL
Rabobank	vodafone	TELSTRA	...

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
- a. Risk Management (RM)
- b. Technology R&D (RD)
- c. Systems Requirements Planning (RP)

2. Oversee and Govern (OV)
- a. Legal Advice and Advocacy (LG)
- b. Training, Education, and Awareness (ED)
- c. Cybersecurity Management (MG)
- d. Strategic Planning and Policy (PL)
- e. Executive Cybersecurity Leadership (EX)
- f. Acquisition and Program/Project Management (PM)

3. Collect and Operate (CO)
- a. Cyber Operational Planning (PL)

Certified Chief Information Security Officer (C|CISO)

Course Description

C|CISO certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security. Bringing together all the components required for a C-Level positions, the C|CISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital for leading a highly successful IS program.

The C|CISO Training Program can be the key to a successful transition to the highest ranks of information security management.

Course Outline

1. Governance
2. Security risk management, controls, and audit management
3. Security program management and operations
4. Information security core concepts
5. Strategic planning, finance, and vendor management

Key Outcomes

- Establishes the role of CISO and models for governance
- Core concepts of information security controls, risk management, and compliance
- Builds foundation for leadership through strategic planning, program management, and vendor management

Exam Information

- Exam Format : Multiple Choice
- Total number of questions : 150
- Exam duration : 2.5 Hours
- Required passing score : 72%

CCISO Course Objectives

Domain 1: Governance (Policy, Legal, & Compliance) & Risk Management

1.1. Define, implement, manage and maintain an information security governance program that includes leadership, organizational structures and processes.

1.2. Align information security governance framework with organizational goals and governance, i.e., leadership style, philosophy, values, standards and policies.

1.3. Establish information security management structure.

1.4. Establish a framework for information security governance monitoring (considering cost/benefits analyses of controls and ROI).

1.5. Understand standards, procedures, directives, policies, regulations, and legal issues that affect the information security program.

1.6. Understand the enterprise information security compliance program and manage the compliance team.

1.7. Analyze all the external laws, regulations, standards, and best practices applicable to the organization.

1.8. Understand the various provisions of the laws that affect the organizational security such as Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act [HIPAA], Federal Information Security

1.9. Management Act [FISMA], Clinger-Cohen Act, Privacy Act, Sarbanes-Oxley, etc.

1.10. Be familiar with the different standards such as ISO 27000 series, Federal Information Processing Standards [FIPS]

1.11. Understand the federal and organization specific published documents to manage operations in a computing environment

1.12. Assess the major enterprise risk factors for compliance

1.13. Coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk

1.14. Understand the importance of regulatory information security organizations and appropriate industry groups, forums, and stakeholders

1.15. Understand the information security changes, trends, and best practices

1.16. Manage enterprise compliance program controls

1.17. Understand the information security compliance process and procedures

1.18. Compile, analyze, and report compliance programs

1.19. Understand the compliance auditing and certification programs

1.20. Follow organizational ethics

Domain 2: IS Management Controls and Auditing Management

2.1. Information Security Management Controls

2.1.1. Identify the organization's operational process and objectives as well as risk tolerance level

2.1.2. Design information systems controls in alignment with the operational needs and goals and conduct testing prior to implementation to ensure e effectiveness and efficiency

2.1.3. Identify and select the resources required to effectively implement and maintain information systems controls. Such resources can include human capital, information, infrastructure, and architecture (e.g., platforms, operating systems, networks, databases, applications)

2.1.4. Design and implement information systems controls to mitigate risk. Monitor and document the information systems control performance in meeting organizational objectives by identifying and measuring metrics and key performance indicators

2.1.5. Design and conduct testing of information security controls to ensure effectiveness, discover de¬ficiencies and ensure alignment with organization's policies, standards and procedures

2.1.6. Design and implement processes to appropriately remediate de¬ficiencies and evaluate problem management practices to ensure that errors are recorded, analyzed and resolved in a timely manner

2.1.7. Assess and implement tools and techniques to automate information systems control processes.

2.1.8. Produce information systems control status reports to ensure that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives, and share with relevant stakeholders to support executive decision-making

2.2. Auditing Management

2.2.1. Understand the IT audit process and be familiar with IT audit standards

2.2.2. Apply information systems audit principles, skills and techniques in reviewing and testing information systems technology and applications to design and implement a thorough risk-based IT audit strategy

2.2.3. Execute the audit process in accordance with established standards and interpret results against defined criteria to ensure that the information systems are protected, controlled and effective in supporting organization's objectives

2.2.4. Effectively evaluate audit results, weighing the relevancy, accuracy, and perspective of conclusions against the accumulated audit evidence

2.2.5. Assess the exposures resulting from ineffective or missing control practices and formulate a practical and cost-effective plan to improve those areas

2.2.6. Develop an IT audit documentation process and share reports with relevant stakeholders as the basis for decision-making

2.2.7. Ensure that the necessary changes based on the audit findings are effectively implemented in a timely manner

Domain 3: Management – Projects and Operations (Projects, Technology & Operations)

3.1. For each information systems project develop a clear project scope statement in alignment with organizational objectives

3.2. Define activities needed to successfully execute the information systems program, estimate activity duration, and develop a schedule and staffing plan

3.3. Develop, manage and monitor the information systems program budget, estimate and control costs of individual projects

3.4. Identify, negotiate, acquire and manage the resources needed for successful design and implementation of the information systems program (e.g., people, infrastructure, and architecture)

3.5. Acquire, develop and manage information security project team

3.6. Assign clear information security personnel job functions and provide continuous training to ensure effective performance and accountability

3.7. Direct information security personnel and establish communications, and team activities, between the information systems team and other security-related personnel (e.g., technical support, incident management, security engineering)

CCISO Course Objectives

3.8. Resolve personnel and teamwork issues within time, cost, and quality constraints
3.9. Identify, negotiate and manage vendor agreement and community
3.10. Participate with vendors and stakeholders to review/assess recommended solutions; identify incompatibilities, challenges, or issues with proposed solutions
3.11. Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization
3.12. Develop a plan to continuously measure the effectiveness of the information systems projects to ensure optimal system performance
3.13. Identify stakeholders, manage stakeholders' expectations and communicate effectively to report progress and performance
3.14. Ensure that necessary changes and improvements to the information systems processes are implemented as required
Domain 4: Information Security Core Competencies
4.1. Access Control
4.1.1. Identify the criteria for mandatory and discretionary access control, understand the different factors that help in implementation of access controls and design an access control plan
4.1.2. Implement and manage an access control plan in alignment with the basic principles that govern the access control systems such as need-to-know
4.1.3. Identify different access control systems such as ID cards and biometrics
4.1.4. Understand the importance of warning banners for implementing access rules

4.1.5. Develop procedures to ensure system users are aware of their IA responsibilities before granting access to the information systems
4.2. Social Engineering, Phishing Attacks, Identity Theft
4.2.1. Understand various social engineering concepts and their role in insider attacks and develop best practices to counter social engineering attacks
4.2.2. Design a response plan to identity theft incidences
4.2.3. Identify and design a plan to overcome phishing attacks
4.3. Physical Security
4.3.1. Identify standards, procedures, directives, policies, regulations and laws for physical security
4.3.2. Determine the value of physical assets and the impact if unavailable
4.3.3. Identify resources needed to effectively implement a physical security plan
4.3.4. Design, implement and manage a coherent, coordinated, and holistic physical security plan to ensure overall organizational security
4.3.5. Establish objectives for personnel security to ensure alignment with overall security goals for the enterprise
4.3.6. Design and manage the physical security audit and update issues
4.3.7. Establish a physical security performance measurement system
4.4. Risk Management
4.4.1. Identify the risk mitigation and risk treatment processes and understand the concept of acceptable risk
4.4.2. Identify resource requirements for risk management plan implementation

CCISO Course Objectives

4.4.3. Design a systematic and structured risk assessment process and establish, in coordination with stakeholders, an IT security risk management program based on standards and procedures and ensure alignment with organizational goals and objectives

4.4.4. Develop, coordinate and manage risk management teams

4.4.5. Establish relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)

4.4.6. Develop an incident management measurement program and manage the risk management tools and techniques

4.4.7. Understand the residual risk in the information infrastructure

4.4.8. Assess threats and vulnerabilities to identify security risks, and regularly update applicable security controls

4.4.9. Identify changes to risk management policies and processes and ensure the risk management program remains current with the emerging risk and threat environment and in alignment with the organizational goals and objectives

4.4.10. Determine if security controls and processes are adequately integrated into the investment planning process based on IT portfolio and security reporting

4.5. Disaster Recovery and Business Continuity Planning

4.5.1. Develop, implement and monitor business continuity plans in case of disruptive events and ensure alignment with organizational goals and objectives

4.5.2. Define the scope of the enterprise continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery/related activities

4.5.3. Identify the resources and roles of different stakeholders in business continuity programs

4.5.4. Identify and prioritize critical business functions and consequently design emergency delegations of authority, orders of succession for key positions, the enterprise continuity of operations organizational structure and staffing model

4.5.5. Direct contingency planning, operations, and programs to manage risk

4.5.6. Understand the importance of lessons learned from test, training and exercise, and crisis events

4.5.7. Design documentation process as part of the continuity of operations program

4.5.8. Design and execute a testing and updating plan for the continuity of operations program

4.5.9. Understand the importance of integration of IA requirements into the Continuity of Operations Plan (COOP).

4.5.10. Identify the measures to increase the level of emergency preparedness such as backup and recovery solutions and design standard operating procedures for implementation during disasters

4.6. Firewall, IDS/IPS and Network Defense Systems

4.6.1. Identify the appropriate intrusion detection and prevention systems for organizational information security

4.6.2. Design and develop a program to monitor ¬firewalls and identify ¬firewall configuration issues

4.6.3. Understand perimeter defense systems such as grid sensors and access control lists on routers, ¬firewalls, and other network devices

4.6.4. Identify the basic network architecture, models, protocols and components such as routers and hubs that play a role in network security

4.6.5. Understand the concept of network segmentation

CCISO Course Objectives

4.6.6. Manage DMZs, VPN and telecommunication technologies such as PBX and VoIP

4.6.7. Identify network vulnerabilities and explore network security controls such as use of SSL and TLS for transmission security

4.6.8. Support, monitor, test, and troubleshoot issues with hardware and software

4.6.9. Manage accounts, network rights, and access to systems and equipment

4.7. Wireless Security

4.7.1. Identify vulnerability and attacks associated with wireless networks and manage different wireless network security tools

4.8. Virus, Trojans and Malware Threats

4.8.1. Assess the threat of virus, Trojan and malware to organizational security and identify sources and mediums of malware infection

4.8.2. Deploy and manage anti-virus systems

4.8.3. Develop process to counter virus, Trojan, and malware threats

4.9. Secure Coding Best Practices and Securing Web Applications

4.9.1. Develop and maintain software assurance programs in alignment with the secure coding principles and each phase of System Development Life Cycle (SDLC)

4.9.2. Understand various system-engineering practices

4.9.3. Configure and run tools that help in developing secure programs

4.9.4. Understand the software vulnerability analysis techniques

4.9.5. Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards

4.9.6. Identify web application vulnerabilities and attacks and web application security tools to counter attacks

4.10. Hardening OS

4.10.1. Identify various OS vulnerabilities and attacks and develop a plan for hardening OS systems

4.10.2. Understand system logs, patch management process and configuration management for information system security

4.11. Encryption Technologies

4.11.1. Understand the concept of encryption and decryption, digital certificates, public key infrastructure and the key differences between cryptography and steganography

4.11.2. Identify the different components of a cryptosystem

4.11.3. Develop a plan for information security encryption techniques

4.12. Vulnerability Assessment and Penetration Testing

4.12.1. Design, develop and implement a penetration testing program based on penetration testing methodology to ensure organizational security

4.12.2. Identify different vulnerabilities associated with information systems and legal issues involved in penetration testing

4.12.3. Develop pre and post testing procedures

4.12.4. Develop a plan for pen test reporting and implementation of technical vulnerability corrections

4.12.5. Develop vulnerability management systems

4.13. Computer Forensics and Incident Response

4.13.1. Develop a plan to identify a potential security violation and take appropriate action to report the incident

4.13.2. Comply with system termination procedures and incident reporting requirements related to potential security incidents or actual breaches

4.13.3. Assess potential security violations to determine if the network security policies have been breached, assess the impact, and preserve evidence

4.13.4. Diagnose and resolve IA problems in response to reported incidents

4.13.5. Design incident response procedures

4.13.6. Develop guidelines to determine whether a security incident is indicative of a violation of law that requires specific legal action

4.13.7. Identify the volatile and persistent system information

4.13.8. Set up and manage forensic labs and programs

4.13.9. Understand various digital media devices, e-discovery principles and practices and different ¬file systems

4.13.10. Develop and manage an organizational digital forensic program

4.13.11. Establish, develop and manage forensic investigation teams

4.13.12. Design investigation processes such as evidence collection, imaging, data acquisition, and analysis

4.13.13. Identify the best practices to acquire, store and process digital evidence

4.13.14. Configure and use various forensic investigation tools

4.13.15. Design anti-forensic techniques

Domain 5: Strategic Planning and Finance

5.1. Strategic Planning

5.1.1. Design, develop and maintain enterprise information security architecture (EISA) by aligning business processes, IT software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy

5.1.2. Perform external analysis of the organization (e.g., analysis of customers, competitors, markets and industry environment) and internal analysis (risk management, organizational capabilities, performance measurement etc.) and utilize them to align information security program with organization's objectives

5.1.3. Identify and consult with key stakeholders to ensure understanding of organization's objectives

5.1.4. Define a forward-looking, visionary and innovative strategic plan for the role of the information security program with clear goals, objectives and targets that support the operational needs of the organization

5.1.5. Define key performance indicators and measure effectiveness on continuous basis

5.1.6. Assess and adjust IT investments to ensure they are on track to support organization's strategic objectives

5.1.7. Monitor and update activities to ensure accountability and progress

5.2. Finance

5.2.1. Analyze, forecast and develop the operational budget of the IT department

5.2.2. Acquire and manage the necessary resources for implementation and management of information security plan

5.2.3. Allocate ¬financial resources to projects, processes and units within information security program

5.2.4. Monitor and oversee cost management of information security projects, return on investment (ROI) of key purchases related to IT infrastructure and security and ensure alignment with the strategic plan

5.2.5. Identify and report financial metrics to stakeholders

CCISO Course Objectives

5.2.6. Balance the IT security investment portfolio based on EISA considerations and enterprise security priorities

5.2.7. Understand the acquisition life cycle and determine the importance of procurement by performing Business Impact Analysis

5.2.8. Identify different procurement strategies and understand the importance of cost-benefit analysis during procurement of an information system

5.2.9. Understand the basic procurement concepts such as Statement of Objectives (SOO), Statement of Work (SOW), and Total Cost of Ownership (TCO)

5.2.10. Collaborate with various stakeholders (which may include internal client, lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others) on the procurement of IT security products and services

5.2.11. Ensure the inclusion of risk-based IT security requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents

5.2.12. Design vendor selection process and management policy

5.2.13. Develop contract administration policies that direct the evaluation and acceptance of delivered IT security products and services under a contract, as well as the security evaluation of IT and software being procured

5.2.14. Develop measures and reporting standards to measure and report on key objectives in procurements aligned with IT security policies and procedures

5.2.15. Understand the IA security requirements to be included in statements of work and other appropriate procurement documents

Mapping Methodology

Mapping Methodology

1. Identification of NICE Cybersecurity Workforce Framework (NCWF) cybersecurity work Categories, Speciality Areas and respective Job Roles
2. Analysis of Tasks, Knowledge, Skills and Abilities associated with each Job Roles
3. Analysis of Cybersecurity job roles and work role descriptions
4. Mapping NCWF Tasks and KSAs to Bloom's cognitive action verbs
5. Research on NICE proficiency description
6. Proximity search of EC-Council exam objective with relevance to each Tasks and KSAs of NCWF
7. Relationship of each Tasks and KSAs of NCWF and EC-Council certification exam objectives (with requisite knowledge & performance filters) to determine a correlation to ±5%
8. Validation of relevance of EC-Council exam objectives with reference to NCWF Tasks and KSAs based on SME reviews, student feedback, and industry acceptance of the trained workforce
9. Mapping the training proficiency level for each course with the NCWF Job Roles

Mapping References

- NCWF and United States Office of Personnel Management (OPM) Job Role Mapping
- Proficiency Descriptions
- Bloom's Taxonomy

Job Role Mapping

Categories	Specialty Areas	Work Role	NCWF ID	OPM Code
Securely Provision (SP)				
	Risk Management (RM)	Authorizing Official/Designating Representative	SP-RM-001	611
		Security Control Assessor	SP-RM-002	612
	Software Development (DEV)	Software Developer	SP-DEV-001	621
		Secure Software Assessor	SP-DEV-002	622
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	651
		Security Architect	SP-ARC-002	652
	Technology R&D (RD)	Research & Development Specialist	SP-RD-001	661
	Systems Requirements Planning (RP)	Systems Requirements Planner	SP-RP-001	641
	Test and Evaluation (TE)	System Testing and Evaluation Specialist	SP-TE-001	671
	Systems Development (SYS)	Information Systems Security Developer	SP-SYS-001	631
		Systems Developer	SP-SYS-002	632
Operate and Maintain (OM)				
	Data Administration (DA)	Database Administrator	OM-DA-001	421
		Data Analyst	OM-DA-002	422
	Knowledge Management (KM)	Knowledge Manager	OM-KM-001	431
	Customer Service and Technical Support (TS)	Technical Support Specialist	OM-TS-001	411
	Network Services (NET)	Network Operations Specialist	OM-NET-001	441
	Systems Administration (SA)	System Administrator	OM-SA-001	451
	Systems Analysis (AN)	Systems Security Analyst	OM-AN-001	461

Job Role Mapping

Categories	Specialty Areas	Work Role	NCWF ID	OPM Code
Oversee and Govern (OV)				
	Legal Advice and Advocacy (LG)	Cyber Legal Advisor	OV-LG-001	731
		Privacy Compliance Manager	OV-LG-002	732
	Training, Education, and Awareness (ED)	Cyber Instructional Curriculum Developer	OV-ED-001	711
		Cyber Instructor	OV-ED-002	712
	Cybersecurity Management (MG)	Information Systems Security Manager	OV-MG-001	722
		COMSEC Manager	OV-MG-002	723
	Strategic Planning and Policy (PL)	Cyber Workforce Developer and Manager	OV-PL-001	751
		Cyber Policy and Strategy Planner	OV-PL-002	752
	Executive Cybersecurity Leadership (EX)	Executive Cyber Leadership	OV-EX-001	901
	Acquisition and Program/Project Management (PM)	Program Manager	OV-PM-001	801
		IT Project Manager	OV-PM-002	802
		Product Support Manager	OV-PM-003	803
		IT Investment/Portfolio Manager	OV-PM-004	804
		IT Program Auditor	OV-PM-005	805
Protect and Defend (PR)				
	Cybersecurity Defense Analysis (DA)	Cyber Defense Analyst	PR-DA-001	511
	Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	PR-INF-001	521
	Incident Response (IR)	Cyber Defense Incident Responder	PR-IR-001	531
	Vulnerability Assessment and Management (VA)	Vulnerability Assessment Analyst	PR-VA-001	541

Job Role Mapping

Categories	Specialty Areas	Work Role	NCWF ID	OPM Code
Analyze (AN)				
	Threat Analysis (TA)	Warning Analyst	AN-TA-001	141
	Exploitation Analysis (XA)	Exploitation Analyst	AN-XA-001	121
	All-Source Analysis (AN)	All-Source Analyst	AN-AN-001	111
		Mission Assessment Specialist	AN-AN-002	112
	Targets (TD)	Target Developer	AN-TD-001	131
		Target Network Analyst	AN-TD-002	132
	Language Analysis (LA)	Multi-Disciplined Language Analyst	AN-LA-001	151
Collect and Operate (CO)				
	Collection Operations (CL)	All Source-Collection Manager	CO-CL-001	311
		All Source-Collection Requirements Manager	CO-CL-002	312
	Cyber Operational Planning (PL)	Cyber Intel Planner	CO-PL-001	331
		Cyber Ops Planner	CO-PL-002	332
		Partner Integration Planner	CO-PL-003	333
	Cyber Operations (OP)	Cyber Operator	CO-OP-001	321
Investigate (IN)				
	Cyber Investigation (CI)	Cyber Crime Investigator	IN-CI-001	221
	Digital Forensics (FO)	Forensics Analyst	IN-FO-001	211
		Cyber Defense Forensics Analyst	IN-FO-002	212

Proficiency Levels

Level	Proficiency Category	Description
0	No Proficiency	This training is intended for someone with insufficient knowledge, skill, or ability level necessary for use in simple or routine work situations. Knowledge, skill, or ability level provided would be similar to the knowledge of a layperson. Considered "no proficiency" for purposes of accomplishing specialized, or technical, work.
1	Basic	This training is intended for individuals who need basic knowledge, skills, or abilities necessary for use and the application in simple work situations with specific instructions and/or guidance.
2	Intermediate	This training is intended for individuals who need intermediate knowledge, skills, or abilities for independent use and application in straightforward, routine work situations with limited need for direction.
3	Advanced	This training is intended for individuals who need advanced knowledge, skills, or abilities for independent use and application in complex or novel work situations.
4	Expert	This training is intended for individuals who need expert knowledge, skills, or abilities for independent use and application in highly complex, difficult, or ambiguous work situations, or the trainee is an acknowledged authority, advisor, or key resource.

Bloom's Taxonomy

Bloom's Taxonomy

Bloom's taxonomy is a classification of learning objectives within education. It is named for Benjamin Bloom, who chaired the committee of educators that devised the taxonomy. Bloom's taxonomy is considered to be a foundational and essential element within the education community.

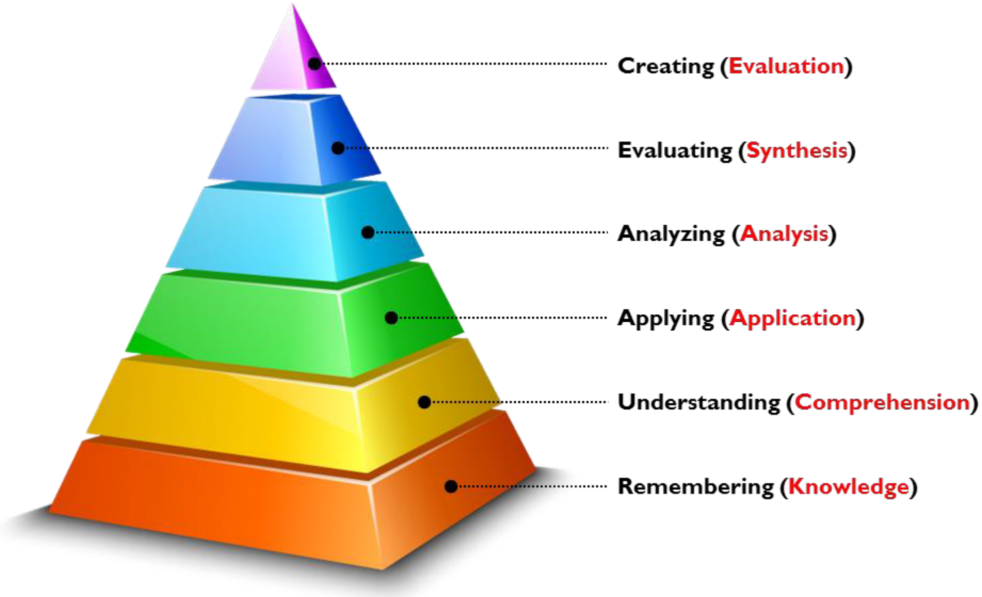
It divides educational objectives into three domains:

1. Cognitive - involves knowledge and the development of intellectual skills (Knowledge)
2. Affective - growth in feelings or emotional areas (Attitude or self)
3. Psychomotor - manual or physical skills (Skills)

Bloom's Taxonomy was revised in 2001by a group of cognitive psychologists, curriculum theorists and instructional researchers, and testing and assessment specialists led by Lorin Anderson, a former student of Bloom. This new taxonomy reflects a more active form of thinking and is considered more accurate by academicians.

The revised taxonomy points to a more dynamic conception of classification using verbs and gerunds to label their categories and subcategories (rather than the nouns of the original taxonomy). These "action words" describe the cognitive processes by which thinkers encounter and work with knowledge (Armstrong, P. Center for Teaching. Vanderbilt University. 2014).

Revised Bloom's Taxonomy for Cognitive Learning



Creating (Evaluation)
Evaluating (Synthesis)
Analyzing (Analysis)
Applying (Application)
Understanding (Comprehension)
Remembering (Knowledge)

Note: Parentheses contain the original taxonomy domains.

Bloom’s Taxonomy

Revised Bloom’s Taxonomy Categories, Definitions and Action Verbs

Bloom’s Category	Definition	Action Verbs
Remembering	Recall previous learned information.	Arrange, Choose, Cite, Define, Describe, Duplicate, Enumerate, Group, Identify, Label, List, Listen, Locate, Match, Memorize, Name, Order, Outline, Quote, Recognize, Relate, Recall, Repeat, Reproduce, Read, Recite, Record, Review, Select, Show, Sort, State, Underline, Write
Understanding	Comprehend the meaning, translation, interpolation, and interpretation of instructions and problems. State a problem in one’s own words.	Account for, Annotate, Associate, Classify, Convert, Defend, Define, Describe, Discuss, Distinguish, Estimate, Explain, Express, Extend, Generalized, Give example(s),Identify, Indicate, Infer, Interpret, Locate, Observe, Outline, Paraphrase, Predict, Recognize, Rewrite, Review, Reorganize, Report, Research, Restate, Retell, Select, Summarize, Translate
Applying	Apply rules, facts, concepts and ideas.	Adapt, Apply, Calculate, Change, Choose, Collect, Compute, Construct, Demonstrate, Discover, Dramatize, Draw, Employ, Exhibit, Generalize, Illustrate, Interpret, Interview, Make, Manipulate, Modify, Operate, Paint, Practice, Predict, Prepare, Produce, Relate, Schedule, Sequence, Show, Sketch, Solve, Translate, Use, Write
Analyzing	Separate material or concepts into component parts so that its organizational structure may be understood. Distinguish between facts and inferences.	Analyze, Appraise, Arrange, Breakdown, Calculate, Categorize, Compare, Contrast, Criticize, Debate, Detect, Diagram, Differentiate, Discriminate, Dissect, Distinguish, Examine, Experiment, Group, Identify, Illustrate, Infer, Inquire, Inspect, Investigate, Model, Order, Outline, Point out, Probe, Question, Relate, Research, Scrutinize, Select, Separate, Sequence, Sift, Subdivide, Summarize, Survey, Test
Evaluating	Make judgments about the value of ideas or materials.	Appraise, Argue, Assess, Choose, Compare, Conclude, Criticize, Critique, Debate, Decide, Deduce, Defend, Determine, Differentiate, Discriminate, Evaluate, Infer, Judge, Justify, Measure, Predict, Prioritize, Probe, Rank, Rate, Recommend, Revise, Score, Select, Validate, Value
Creating	Build a structure or pattern from diverse elements. Put parts together to form a whole, with emphasis on creating a new meaning or structure.	Act, Assemble, Blend, Combine, Compile, Compose, Concoct, Construct, Create, Design, Develop, Devise, Formulate, Forecast, Generate, Hypothesize, Imagine, Invent, Organize, Originate, Predict, Plan, Prepare, Propose, Produce, Set up

Mapping Summary

NCWF Categories	Specialty Areas	Work Role	NCWF ID	EC-Council Certification	Proficiency Match (0-4)
Securely Provision (SP)					
	Risk Management (RM)	Authorizing Official/Designating Representative	SP-RM-001	CCISO	4
		Security Control Assessor	SP-RM-002	CCISO	3
	Software Development (DEV)	Software Developer	SP-DEV-001	CASE	3
		Secure Software Assessor	SP-DEV-002	CASE	3
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	CND	3
		Security Architect	SP-ARC-002	CND	3
	Technology R&D (RD)	Research & Development Specialist	SP-RD-001	CEH	3
	Systems Requirements Planning (RP)	Systems Requirements Planner	SP-RP-001	CND	3
	Test and Evaluation (TE)	System Testing and Evaluation Specialist	SP-TE-001	CND	3
	Systems Development (SYS)	Information Systems Security Developer	SP-SYS-001	CND	3
		Systems Developer	SP-SYS-002	CND	3
Operate and Maintain (OM)					
	Data Administration (DA)	Database Administrator	OM-DA-001	N/A	
		Data Analyst	OM-DA-002	N/A	
	Knowledge Management (KM)	Knowledge Manager	OM-KM-001	N/A	
	Customer Service and Technical Support (TS)	Technical Support Specialist	OM-TS-001	CND	3
	Network Services (NET)	Network Operations Specialist	OM-NET-001	CND	3
	Systems Administration (SA)	System Administrator	OM-SA-001	CND	3
	Systems Analysis (AN)	Systems Security Analyst	OM-AN-001	CND	3

Mapping Summary

NCWF Categories	Specialty Areas	Work Role	NCWF ID	EC-Council Certification	Proficiency Match (0-4)
Oversee and Govern (OV)					
	Legal Advice and Advocacy (LG)	Cyber Legal Advisor	OV-LG-001	CCISO	3
		Privacy Compliance Manager	OV-LG-002	CCISO	4
	Training, Education, and Awareness (ED)	Cyber Instructional Curriculum Developer	OV-ED-001	CEI	4
		Cyber Instructor	OV-ED-002	CEI	4
	Cybersecurity Management (MG)	Information Systems Security Manager	OV-MG-001	CCISO	4
		COMSEC Manager	OV-MG-002	CCISO	4
	Strategic Planning and Policy (PL)	Cyber Workforce Developer and Manager	OV-PL-001	CCISO	3
		Cyber Policy and Strategy Planner	OV-PL-002	CCISO	4
	Executive Cybersecurity Leadership (EX)	Executive Cyber Leadership	OV-EX-001	CCISO	4
	Acquisition and Program/Project Management (PM)	Program Manager	OV-PM-001	CCISO	3
		IT Project Manager	OV-PM-002	CCISO	3
		Product Support Manager	OV-PM-003	CCISO	3
		IT Investment/Portfolio Manager	OV-PM-004	CCISO	3
		IT Program Auditor	OV-PM-005	CCISO	4
Protect and Defend (PR)					
	Cybersecurity Defense Analysis (DA)	Cyber Defense Analyst	PR-DA-001	CEH	3
	Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	PR-INF-001	CND	3
	Incident Response (IR)	Cyber Defense Incident Responder	PR-IR-001	ECIH	3

Mapping Summary

NCWF Categories	Specialty Areas	Work Role	NCWF ID	EC-Council Certification	Proficiency Match (0-4)
	Vulnerability Assessment and Management (VA)	Vulnerability Assessment Analyst	PR-VA-001	CEH	3
Analyze (AN)					
	Threat Analysis (TA)	Warning Analyst	AN-TA-001	CEH	3
	Exploitation Analysis (XA)	Exploitation Analyst	AN-XA-001	ECSA	4
	All-Source Analysis (AN)	All-Source Analyst	AN-AN-001	ECSA	3
		Mission Assessment Specialist	AN-AN-002	ECSA	3
	Targets (TD)	Target Developer	AN-TD-001	ECSA	4
		Target Network Analyst	AN-TD-002	ECSA	4
	Language Analysis (LA)	Multi-Disciplined Language Analyst	AN-LA-001	ECSA	4
Collect and Operate (CO)					
	Collection Operations (CL)	All Source-Collection Manager	CO-CL-001	ECSA	3
		All Source-Collection Requirements Manager	CO-CL-002	ECSA	3
	Cyber Operational Planning (PL)	Cyber Intel Planner	CO-PL-001	ECSA	3
		Cyber Ops Planner	CO-PL-002	ECSA	3
		Partner Integration Planner	CO-PL-003	ECSA	3
	Cyber Operations (OP)	Cyber Operator	CO-OP-001	ECSA	4
Investigate (IN)					
	Cyber Investigation (CI)	Cyber Crime Investigator	IN-CI-001	CHFI	4
	Digital Forensics (FO)	Forensics Analyst	IN-FO-001	CHFI	3
		Cyber Defense Forensics Analyst	IN-FO-002	CHFI	3

SECURELY PROVISION (SP)

Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.

Risk Management (RM)

Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new IT systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

Software Development (DEV)

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Systems Architecture (ARC)

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

Technology Research and Development (RD)

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

Systems Requirements Planning (RP)

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

Test and Evaluation (TE)

Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).

Systems Development (SYS)

Works on the development phases of the systems development lifecycle.

NCWF JOB ROLE

Authorizing Official/Designating Representative

Job Role Description: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an Authorizing Official. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .6 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0145	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Synthesis, Evaluation	1.5 to 1.10	4	60% or .6
T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Synthesis, Evaluation	2.1, 4.4	4	70% or .7
T0371	Establish acceptable limits for the software application, network, or system.	Analyze, Synthesis	2.1	3	50% or .5
T0495	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Synthesis, Evaluation	1.5 to 1.10	4	60% or .6
	Summary			**4**	**60% or .6**

NCWF JOB ROLE

Authorizing Official/Designating Representative

Job Role Description: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an Authorizing Official. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .6 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	2.1.7, 4.1.2, 4.7.1, 4.9.6	4	95% or .95
K0019	Knowledge of cryptography and cryptographic key management concepts.	4.11	4	60% or .60
K0027	Knowledge of organization’s enterprise information security architecture system.	2.1	3	65% or .65
K0028	Knowledge of organization’s evaluation and validation requirements.	3.11	3	60% or .60
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	4.4	3	65% or .65
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	4.12	3	95% or .95
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	4.1 to 4.12	4	95% or .95
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	4	95% or .95
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	4.6	4	90% or .9
K0054	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.	2.1,2.2	3	65% or .65

Authorizing Official/Designating Representative

Job Role Description: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an Authorizing Official. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .6 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	5.1		
K0084	Knowledge of structured analysis principles and methods.	1.1, 1.3,5.1	3	60% or .60
K0085	Knowledge of system and application security threats and vulnerabilities.	4.9	3	60% or .60
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	4.10, 4.13.4	3	60% or .60
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	5.1	4	100% or 1
K0146	Knowledge of the organization's core business/mission processes.	3.1 to 3.14	4	100% or 1
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy 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 relevant to work performed.	1.7 to 1.10	4	100% or 1
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	4	100% or 1
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	3.12	3	60% or .60
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	4.6	3	100% or 1
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	5.1	4	100% or 1
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	5.1	4	100% or 1
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	1.7 to 1.10	4	100% or 1
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	1.7 to 1.10	4	100% or 1
K0262	Knowledge of Personal Health Information (PHI) data security standards.	1.7 to 1.10	4	100% or 1

Authorizing Official/Designating Representative

Job Role Description: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an Authorizing Official. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .6 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.7 to 1.10	4	100% or 1
K0295	Knowledge of confidentiality, integrity, and availability principles.	4.1	4	100% or 1
K0322	Knowledge of embedded systems.	NA		
K0342	Knowledge of penetration testing principles, tools, and techniques.	4.12	3	80% or .80
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	2.1.3	3	80% or .80
	Summary		**4**	**90% or .9**

NCWF JOB ROLE

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0032	Conduct Privacy Impact Assessments (PIA) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Synthesis, Evaluation	2.2.2	4	80% or .80
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	4.4.3	**3**	60% or .60
T0079	Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.	Synthesis, Evaluation	4.4.1 to 4.4.10	4	80% or .80
T0083	Draft statements of preliminary or residual security risks for system operation.	Synthesis, Evaluation	4.4.7	4	80% or .80
T0141	Maintain information systems assurance and accreditation materials.	Application, Evaluation	5.1.1	4	80% or .80
T0150	Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.	Synthesis, Evaluation	1.4	**3**	60% or .60
T0183	Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks.	Synthesis, Evaluation	2.2.3,2.2.4	4	80% or .80
T0184	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.	Synthesis, Evaluation	4.1.1 to 4.1.5	3	60% or .60
T0197	Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant cybersecurity compliances.	Synthesis, Evaluation	2.2.4	3	60% or .60
T0218	Recommend new or revised security, resilience, and dependability measures based on the results of reviews.	Application, Analysis	2.2.7	3	60% or .60
T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Application, Analysis	2.1.5	2	40% or .40

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0244	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Application, Analysis	2.2.3,2.2.4	3	60% or .60
T0245	Verify that the software application/network/system accreditation and assurance documentation is current.	Application, Analysis	2.2.2,2.2.3	3	60% or .60
T0251	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).	Synthesis, Evaluation	2.2.1 to 2.2.7	3	60% or .60
T0301	Develop and Implement cybersecurity independent audit processes for application software/networks/systems and oversee ongoing independent audits to ensure that operational and Research and Design (R&D) processes and procedures are in compliance with organizational and mandatory cybersecurity requirements and accurately followed by Systems Administrators and other cybersecurity staff when performing their day-to-day activities.	Application, Analysis, Synthesis, Evaluation	2.2.1 to 2.2.7	3	60% or .60
	Summary			**3**	**65% or .65**

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	2.1.7, 4.1.2, 4.7.1, 4.9.6	4	95% or .95
K0019	Knowledge of cryptography and cryptographic key management concepts.	4.11	4	60% or .60
K0027	Knowledge of organization's enterprise information security architecture system.	2.1	3	65% or .65
K0028	Knowledge of organization's evaluation and validation requirements.	3.11	3	60% or .60
K0037	Knowledge of the Security Assessment and Authorization process.	4.1, 4.12	3	60% or .60
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	4.4	3	65% or .65
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	4.12	3	95% or .95
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	4.1 to 4.12	4	95% or .95
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	4	95% or .95
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	4.6	4	90% or .9

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0054	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.	2.1,2.2	3	65% or .65
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	5.1		
K0084	Knowledge of structured analysis principles and methods.	1.1, 1.3,5.1	3	60% or .60
K0085	Knowledge of system and application security threats and vulnerabilities.	4.9	3	60% or .60
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	4.10, 4.13.4	3	60% or .60
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	5.1	4	100% or 1
K0146	Knowledge of the organization's core business/mission processes.	3.1 to 3.14	4	100% or 1
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy 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 relevant to work performed.	1.7 to 1.10	4	100% or 1
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	4	100% or 1
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	3.12	3	60% or .60
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	4.6	3	100% or 1
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	5.1	4	100% or 1
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	5.1	4	100% or 1
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	1.7 to 1.10	4	100% or 1

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	1.7 to 1.10	4	100% or 1
K0262	Knowledge of Personal Health Information (PHI) data security standards.	1.7 to 1.10	4	100% or 1
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.7 to 1.10	4	100% or 1
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.1	4	100% or 1
K0322	Knowledge of embedded systems.	NA		
K0342	Knowledge of penetration testing principles, tools, and techniques.	4.12	3	80% or .80
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	4.4.8, 4.6.7, 4.7.1, 4.9.6, 4.10.1, 4.12.4, 4.12.5	4	100% or 1
S0006	Skill in applying confidentiality, integrity, and availability principles.	4.1 - 4.13	4	100% or 1
S0027	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.	5.1.2	3	80% or .80
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	2.1.3	3	80% or .80
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	2.1.4	4	80% or .80
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.	5.2.10	4	80% or .80
	Summary		**4**	**90% or .9**

OPERATE AND MAINTAIN (OM)

Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Data Administration (DA)
Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

Knowledge Management (KM)
Manages and administers processes and tools that enable the organization to identify, document, and access Intellectual capital and information content.

Customer Service and Technical Support (TS)
Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

Network Services (NET)
Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

System Administration (SA)
Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Systems Security Analysis (AN)
Conducts the integration/testing, operations, and maintenance of systems security.

Data Administration (DA) | Knowledge Management (KM) | Customer Service and Technical Support (TS) | Network Services (NET) | Systems Administration (SA) | Systems Analysis (AN)
About NICE, NCWF and EC-Council | Methodology and Mapping Summary | Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV) | Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO) | Investigate (IN)

OVERSEE AND GOVERN (OV)

Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

Legal Advice and Advocacy

Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

Strategic Planning and Policy (PL)

Develops policies and plans and/or advocates for changes in policy that supports organizational cyberspace initiatives or required changes/enhancements.

Executive Cybersecurity Leadership (EX)

Supervises, manages, and/or leads work and workers performing cybersecurity work.

Training, Education, and Awareness (ED)

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

Acquisition and Program/Project Management (PM)

Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use IT (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life-cycle.

Cybersecurity Management (MG)

Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

Cyber Legal Advisor

Job Role Description: A Cyber Legal Advisor provides legal advice and recommendations on relevant topics related to cyber law.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Legal Advisor. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .5 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0006	Advocate organization's official position in legal and legislative proceedings.	Synthesis, Evaluation	1.5	4	60% or .6
T0098	Evaluate contracts to ensure compliance with funding, legal, and program requirements.	Synthesis, Evaluation	5.2.11	3	80% or .8
T0102	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.	Synthesis, Evaluation	2.1.5	4	80% or .8
T0131	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	Analysis, Evaluation	1.5 to 1.10	3	60% or .6
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis, Evaluation	1.5 to 1.12	3	60% or .6
T0419	Acquire and maintain a working knowledge of constitutional issues relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.	Synthesis, Evaluation	1.5 to 1.10	4	80% or .8
T0434	Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.	Analysis, Evaluation	1.12	3	30% or .3
T0465	Develop guidelines for implementation.	Analysis, Evaluation	1.17,1.18	3	30% or .3
T0474	Provide legal analysis and decisions to inspector generals, privacy officers, oversight and compliance personnel with regard to compliance with cybersecurity policies and relevant legal and regulatory requirements.	Analysis, Evaluation	1.13,1.14	3	30% or .3
T0476	Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.	Analysis, Evaluation	**2.1.5**	**3**	30% or .3
T0478	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	Analysis, Evaluation	1.14,1.19	3	30% or .3
T0487	Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.	Analysis, Evaluation	1.13	**3**	30% or .3

Cyber Legal Advisor

Job Role Description: A Cyber Legal Advisor provides legal advice and recommendations on relevant topics related to cyber law.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Legal Advisor. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .5 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0522	Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).	Analysis, Evaluation	1.18	3	60% or .6
	Summary			**3**	**50% or .5**

Cyber Legal Advisor

Job Role Description: A Cyber Legal Advisor provides legal advice and recommendations on relevant topics related to cyber law.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Legal Advisor. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .5 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0017	Knowledge of concepts and practices of processing digital forensic data.	4.13	3	90% or .9
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	5.1	3	60% or .6
K0107	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/ regulations.	4.13	3	90% or .9
K0157	Knowledge of cyber defense policies, procedures, and regulations.	1.5 to 1.10	3	95% or .95
K0312	Knowledge of intelligence principles, policies, and procedures including legal authorities and restrictions.	1.5 to 1.10	3	95% or .95
K0316	Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.	5.1	3	70% or .7
K0341	Knowledge of foreign disclosure policies and import/export control regulations as related to cybersecurity.	5.2	3	70% or .7
	Summary		**3**	**90% or .9**

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Synthesis, Evaluation	4.4	4	90% or .9
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, and systems, and elements.	Synthesis, Evaluation	5.2	4	90% or .9
T0032	Conduct Privacy Impact Assessments (PIA) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Analysis	4.9.1	3	90% or .9
T0066	Develop and maintain strategic plans.	Analysis, Evaluation	5.1	4	100% or 1
T0098	Evaluate contracts to ensure compliance with funding, legal, and program requirements.	Analysis, Evaluation	5.2.11	3	90% or .9
T0099	Evaluate cost benefit, economic, and risk analysis in decision making process.	Synthesis, Evaluation	5.2.8	4	90% or .9
T0131	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	Analysis, Evaluation	1.1 to 1.19	4	80% or .8
T0133	Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	Analysis, Evaluation	1.1 to 1.19	4	80% or .8
T0188	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Analysis, Evaluation	2.2.3 to 2.2.6	4	80% or .8
T0381	Present technical information to technical and non-technical audiences.	Analysis	5.1	3	90% or .9
T0384	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Analysis, Evaluation	5.1	3	90% or .9
T0478	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	Synthesis, Evaluation	1.1 to 1.19	4	90% or .9
T0861	Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.	Analysis	1.8, 1.9	3	90% or .9

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0862	Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.	Analysis	1.8, 1.10	3	90% or .9
T0863	Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.	Analysis	1.1 to 1.19	3	90% or .9
T0864	Liaise with regulatory and accrediting bodies.	Analysis	1.1 to 1.19		90% or .9
T0865	Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.	Analysis	1.7 - 1.14	3	90% or .9
T0866	Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.	Analysis	1.1 to 1.19	3	80% or .8
T0867	Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.	Analysis	1.7 - 1.14	3	80% or .9
T0868	Work with business teams and senior management to ensure awareness of "best practices" on privacy and data security issues.	Analysis	1.7	3	90% or .9
T0869	Work with organization senior management to establish an organization-wide Privacy Oversight Committee	Analysis	5.1	3	90% or .9
T0870	Serve in a leadership role for Privacy Oversight Committee activities	Analysis	5.1	3	90% or .9
T0871	Collaborate on cyber privacy and security policies and procedures	Analysis	5.1	3	90% or .9
T0872	Collaborate with cyber security personnel on the security risk assessment process to address privacy compliance and risk mitigation	Analysis	4.4	3	80% or .8

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0873	Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations	Synthesis, Evaluation	5.1	4	80% or .8
T0874	Provide strategic guidance to corporate officers regarding information resources and technology	Synthesis, Evaluation	5.1	4	80% or .8
T0875	Assist the Security Officer with the development and implementation of an information infrastructure	Analysis	2.1	3	90% or .9
T0876	Coordinate with the Corporate Compliance Officer re: procedures for documenting and reporting self-disclosures of any evidence of privacy violations.	Analysis	1.1 to 1.19	3	90% or .9
T0877	Work cooperatively with applicable organization units in overseeing consumer information access rights	Analysis	4.1	3	90% or .9
T0878	Serve as the information privacy liaison for users of technology systems	Analysis	3.1 to 3.14	3	90% or .9
T0879	Act as a liaison to the information systems department	Analysis	3.1 to 3.14	3	90% or .9
T0880	Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	Synthesis, Evaluation	3.6	4	90% or .9
T0881	Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties	Synthesis, Evaluation	3.6	4	90% or .9
T0882	Conduct on-going privacy training and awareness activities	Analysis	3.6	3	90% or .9
T0883	Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security	Analysis	1.14	3	90% or .10

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0884	Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.	Analysis	1.14	3	90% or .11
T0885	Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee	Analysis, Evaluation	2.1.8	4	80% or .80
T0886	Work with External Affairs to respond to press and other inquiries with regard to concern over consumer and employee data	Analysis, Evaluation	1.14	3	90% or .11
T0887	Provide leadership for the organization's privacy program	Analysis, Evaluation	1.1	4	80% or .80
T0888	Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization	Analysis	3.7	3	80% or .80
T0889	Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable	Analysis	1.1 to 1.19	3	90% or .9
T0890	Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures	Synthesis, Evaluation	1.1 to 1.19	4	90% or .9
T0891	Resolve allegations of non-compliance with the corporate privacy policies or notice of information practices	Analysis, Evaluation	1.1 to 1.19	3	90% or .9
T0892	Develop and coordinate a risk management and compliance framework for privacy	Synthesis, Evaluation	4.4	4	80% or .80

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0893	Undertake a comprehensive review of the company's data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.	Analysis, Evaluation	5.1.2	3	90% or .9
T0894	Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations	Synthesis, Evaluation	3.1 to 3.14	4	90% or .9
T0895	Establish a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the organization's privacy policies and procedures	Synthesis, Evaluation	3.1 to 3.14	4	90% or .9
T0896	Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity	Synthesis, Evaluation	3.1 to 3.14	4	90% or .9
T0897	Provide leadership in the planning, design and evaluation of privacy and security related projects	Analysis, Evaluation	2.1.1 to 2.1.8	3	90% or .9
T0898	Establish an internal privacy audit program	Synthesis, Evaluation	2.2	4	90% or .9
T0899	Periodically revise the privacy program in light of changes in laws, regulatory or company policy	Analysis, Evaluation	1.1 to 1.19	3	90% or .9
T0900	Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel	Analysis, Evaluation	1.1 to 1.19	3	90% or .9
T0901	Assure that the use of technologies maintain, and do not erode, privacy protections on use, collection and disclosure of personal information	Analysis, Evaluation	2.1	3	90% or .9

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0902	Monitor systems development and operations for security and privacy compliance	Analysis, Evaluation	1.1 to 1.19	3	90% or .9
T0903	Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected	Analysis, Evaluation	4.13.3	3	90% or .9
T0904	Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions	Analysis, Evaluation	4.5.5	3	90% or .9
T0905	Review all system-related information security plans to ensure alignment between security and privacy practices	Analysis, Evaluation	3.12	4	80% or .80
T0906	Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements	Analysis, Evaluation	2.1.5	4	80% or .80
T0907	Account for and administer individual requests for release or disclosure of personal and/or protected information	Analysis	NA		
T0908	Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements	Synthesis, Evaluation	1.1 to 1.19	4	90% or .9
T0909	Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed	Analysis	1.1 to 1.19	3	90% or .9
T0910	Act as, or work with, counsel relating to business partner contracts	Analysis	NA	3	90% or .9
T0911	Mitigate effects of a use or disclosure of personal information by employees or business partners	Analysis	2.1.6	3	90% or .9
T0912	Develop and apply corrective action procedures	Synthesis, Evaluation	2.1	4	90% or .9

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0913	Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel	Analysis	NA		
T0914	Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations	Analysis	1.16 to 1.19	3	90% or .9
T0915	Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations	Analysis, Evaluation	1.12	3	90% or .9
T0916	Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units	Analysis, Evaluation	4.4.6	3	90% or .9
T0917	Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices	Analysis, Evaluation	1.15	3	90% or .9
T0918	Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations	Synthesis, Evaluation	1.1 to 1.19	4	90% or .9
T0919	Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials	Analysis, Evaluation	1.11, 2.1	3	80% or .8
	Summary			4	**90% or .9**

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0008	Knowledge of applicable business processes and operations of customer organizations.	3.1 to 3.14	4	95% or .95
K0066	Knowledge of Privacy Impact Assessments.	4.13.3	3	95% or .95
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy 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 relevant to work performed.	1.1 to 1.19	3	95% or .95
K0606	Knowledge of transcript development processes and techniques (e.g., verbatim, gists, summaries).	NA		
K0607	Knowledge of translation processes and techniques.	NA		
K0608	Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).	4.1	3	40% or .4
K0609	Knowledge of virtual machine technologies.	NA		
K0610	Knowledge of virtualization products (VMware, Virtual PC).	NA		
K0611	Withdrawn – Integrated into K0131	NA		
K0612	Knowledge of what constitutes a "threat" to a network.	NA		
K0613	Knowledge of who the organization's operational planners are, how and where they can be contacted, and what are their expectations.	3.1 to 3.14	4	95% or .95

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	4.7	3	95% or .95
S0354	Skill in creating policies that reflect the business's core privacy objectives.	1.1 to 1.19	3	95% or .95
S0355	Skill in negotiating vendor agreements and evaluating vendor privacy practices.	3.9	4	95% or .95
S0356	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).	3.13	3	40% or .40
A0024	Ability to develop clear directions and instructional materials.	3.7, 4.5.5	3	40% or .40
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	1.1 to 1.19	3	95% or .95
A0034	Ability to develop, update, and/or maintain standard operating procedures (SOPs).	4.15	3	95% or .95
A0104	Ability to select the appropriate implant to achieve operational goals.	3.1 to 3.14	4	95% or .95
A0105	Ability to tailor technical and planning information to a customer's level of understanding.	1.18, 2.1.8, 2.2.6, 3.13		95% or .95
A0110	Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance.	4.4.9	3	95% or .95
A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	4.4.3	3	95% or .95
A0112	Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.	1.15, 1.16	3	95% or .95
A0113	Ability to determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.	4.13.3	3	95% or .95
A0114	Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.	3.6	3	95% or .95
A0115	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	4.4.3	3	95% or .95
	Summary		**3**	**95% or .95**

NCWF JOB ROLE

Cyber Instructional Curriculum Developer

Job Role Description: A Cyber Instructional Curriculum Developer develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs..

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructional Curriculum Developer. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0230	Support the design and execution of exercise scenarios.	Analysis	6.1, 6.2	3	90% or .9
T0247	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Write, Synthesis	5.2, 8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0345	Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.	Assess, Evaluation	NA		
T0352	Conduct learning needs assessments and identify requirements.	Conduct, Analysis	14.4	3	90% or .9
T0357	Create interactive learning exercises to create an effective learning environment.	Create, Synthesis	16.1, 16.2, 16.3	4	100% or 1
T0365	Develop or assist in the development of training policies and protocols for cyber training.	Develop, Analysis	17.6	3	90% or .9
T0367	Develop the goals and objectives for cyber curriculum.	Develop, Analysis	8.1	3	90% or .9
T0380	Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.	Plan, Synthesis	6.1, 6.2, 13.1, 13.2, 13.3	4	100% or 1
T0437	Correlates training and learning to business or mission requirements.	Correlate, Evaluation	16.1, 16.2, 16.3	4	100% or 1
T0442	Create training courses tailored to the audience and physical environment.	Create, Synthesis	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0450	Design training curriculum and course content based on requirements.	Design, Synthesis	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0534	Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions).	Conduct	15.1, 15.2	3	90% or .9
T0536	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Serve	3.1, 3.2, 3.3	3	90% or .9

Cyber Instructional Curriculum Developer

Job Role Description: A Cyber Instructional Curriculum Developer develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs..

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructional Curriculum Developer. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0926	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	Develop, Synthesis	2.1, 2.2, 5.1, 6.1, 6.2, 8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
	Summary			**4**	**95% or .95**

Cyber Instructional Curriculum Developer

Job Role Description: A Cyber Instructional Curriculum Developer develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs..

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructional Curriculum Developer. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	NA		
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	NA		
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	18.2	2	50% or .5
K0004	* Knowledge of cybersecurity principles.	18.2	2	50% or .5
K0005	* Knowledge of cyber threats and vulnerabilities.	18.2	2	50% or .5
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	18.2	2	50% or .5
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	18.2	2	50% or .5
K0124	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain.	18.2, 18.4, 18.6	3	60% or .6
K0146	Knowledge of the organization's core business/mission processes.	1.1 to 1.9	3	100% or 1
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	18.2, 18.4, 18.6	3	60% or .6
K0239	Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.	13.1, 13.2, 13.3	4	100% or 1
K0245	Knowledge of principles and processes for conducting training and education needs assessment.	2.1, 2.2, 3.1, 3.2, 3.3, 6.1, 6.2, 10.1, 10.2, 12.1, 13.1, 13.2, 13.3, 14.1, 16.1, 16.2, 16.3	4	100% or 1
K0246	Knowledge of relevant concepts, procedures, software, equipment, and technology applications.	17.1, 17.2, 17.3, 17.4, 17.5, 18.1, 18.2, 18.3, 18.4, 18.5, 18.6	4	100% or 1

Cyber Instructional Curriculum Developer

Job Role Description: A Cyber Instructional Curriculum Developer develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs..

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructional Curriculum Developer. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0252	Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects.	2.1, 2.2, 3.1, 3.2, 3.3, 6.1, 6.2, 10.1, 10.2, 12.1, 13.1, 13.2, 13.3, 14.1, 16.1, 16.2, 16.3	4	100% or 1
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	2.1, 2.2, 4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 6.1, 6.2	4	100% or 1
S0064	Skill in developing and executing technical training programs and curricula.	8.1, 8.2, 8.3, 8.4, 8.5, 13.1, 13.2, 13.3	4	100% or 1
S0066	Skill in identifying gaps in technical capabilities.	6.1, 6.2, 7.1, 8.1, 8.2, 8.3, 8.4, 8.5, 10.1, 10.2, 11.1, 11.2	4	100% or 1
S0070	Skill in talking to others to convey information effectively.	12.1	3	90% or .9
S0102	Skill in applying technical delivery capabilities.	8.1, 8.2, 8.3, 8.4, 8.5, 13.,1, 13.2, 13.3	3	90% or .9
S0166	Skill in identifying gaps in technical delivery capabilities.	8.1, 8.2, 8.3, 8.4, 8.5, 13.,1, 13.2, 13.3	3	90% or .9
A0004	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.	8.1, 8.2, 8.3, 8.4, 8.5	3	90% or .9
A0032	Ability to develop curriculum for use within a virtual environment.	8.1, 8.2, 8.3, 8.4, 8.5	3	90% or .9
A0054	Ability to apply the Instructional System Design (ISD) methodology.	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
	Summary		**3**	**80% or .8**

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0030	Conduct interactive training exercises to create an effective learning environment.	Conduct, Synthesis	6.1, 14.1	4	100% or 1
T0073	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	Develop, Synthesis	8.1, 8.2, 8.3, 8.4	4	100% or 1
T0101	Evaluate the effectiveness and comprehensiveness of existing training programs.	Evaluate	14.1, 15.1, 15.2	3	90% or .9
T0224	Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions).	Review	16.1, 16.2, 16.3	3	90% or .9
T0230	Support the design and execution of exercise scenarios.	Design	6.1, 6.2	3	90% or .9
T0247	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Write, Synthesis	5.2, 8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0316	Develop or assist in the development of computer based training modules or classes.	Analysis, Synthesis	5.1, 5.2, 5.3	3	90% or .9
T0317	Develop or assist in the development of course assignments.	Analysis, Synthesis	14.1	3	90% or .9
T0318	Develop or assist in the development of course evaluations.	Analysis, Synthesis	14.1	3	90% or .9
T0319	Develop or assist in the development of grading and proficiency standards.	Analysis, Synthesis	16.1, 16.2, 16.3	3	90% or .9
T0320	Assist in the development of individual/collective development, training, and/or remediation plans.	Assist	3, 4, 2005	4	100% or 1
T0321	Develop or assist in the development of learning objectives and goals.	Analysis, Synthesis	8.1	3	90% or .9
T0322	Develop or assist in the development of on-the-job training materials or programs.	Analysis, Synthesis	8.1, 8.2, 8.3., 8.4, 8.5	4	100% or 1
T0323	Develop or assist in the development of written tests for measuring and assessing learner proficiency.	Analysis, Synthesis	10.1, 10.2, 12.1	4	100% or 1
T0443	Deliver training courses tailored to the audience and physical/virtual environments.	Deliver	13.1, 13.2, 13.3	3	90% or .9

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0444	Apply concepts, procedures, software, equipment, and/or technology applications to students.	Apply	1 - 16	3	90% or .9
T0450	Design training curriculum and course content based on requirements.	Design, Analysis, Synthesis	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0467	Ensure training meets the goals and objectives for cybersecurity training, education, or awareness.	Analysis, Evaluation	14.1, 15.1, 15.2	4	100% or 1
T0519	Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for most effective learning environment.	Analysis, Evaluation	8.4, 8.5, 13.1, 13.2, 13.3	3	90% or .9
T0520	Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses).	Analysis	13.2, 13.3	3	90% or .9
T0535	Recommend revisions to curriculum end course content based on feedback from previous training sessions.	Analysis	11.1, 11.2	3	90% or .9
T0536	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Analysis	3.1, 3.2, 3.3	3	90% or .9
T0926	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	Develop, Analysis, Synthesis	2.1, 2.2, 5.1, 6.1, 6.2, 8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
	Summary			**4**	**95% or .95**

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	NA		
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	NA		
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	18.2	2	50% or .5
K0004	* Knowledge of cybersecurity principles.	18.2	2	50% or .5
K0005	* Knowledge of cyber threats and vulnerabilities.	18.2	2	50% or .5
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	18.2	2	50% or .5
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	18.2	2	50% or .5
K0115	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries.	18.2	3	60% or .6
K0124	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain.	18.2, 18.4, 18.6	3	60% or .6
K0130	Knowledge of virtualization technologies and virtual machine development and maintenance.	All Labs	3	60% or .6
K0146	Knowledge of the organization's core business/mission processes.	1.1 to 1.9	3	100% or 1
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	18.2, 18.4, 18.6	3	60% or .6
K0204	Knowledge of assessment techniques (rubrics, evaluation plans, tests, quizzes).	14.1	3	60% or .6
K0208	Knowledge of computer based training and e-learning services.	3.1, 3.2, 3.3	3	70% or .7
K0213	Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne's Events of Instruction, Kirkpatrick's model of evaluation).	14.1, 15.1, 15.2	4	100% or 1
K0215	Knowledge of organizational training policies.	17.5	3	90% or .9
K0216	Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).	10.1	3	90% or .9
K0217	Knowledge of Learning Management Systems and their use in managing learning.	10.1, 12.1, 16.1, 16.2, 16.3	4	100% or 1
K0218	Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic).	3.2, 8.4, 16.1, 16.2, 16.3	3	85% or .85
K0220	Knowledge of modes of learning (e.g., rote learning, observation).	12.1	3	80% or .8

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0226	Knowledge of organizational training systems.	16.1, 16.2, 16.3	3	90% or .9
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.1, 4.2, 4.3	3	90% or .9
K0319	Knowledge of technical delivery capabilities and their limitations.	6.1, 6.2	4	100% or 1
S0064	Skill in developing and executing technical training programs and curricula.	8.1, 8.2, 8.3, 8.4, 8.5, 13.1, 13.2, 13.3	4	100% or 1
S0070	Skill in talking to others to convey information effectively.	12.1	3	90% or .9
S0100	Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises).	6.1, 6.2, 8.1, 8.2, 8.3, 8.4, 8.5, 10.1, 10.2, 13.1, 13.2, 13.3, 14.1, 15.1, 15.2, 16.1, 16.2, 16.3	4	100% or 1
S0101	Skill in utilizing technologies (e.g., SmartBoards, websites, computers, projectors) for instructional purposes.	6.1, 6.2	3	90% or .9
A0006	Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures.	Module 01	4	100% or 1
A0011	Ability to answer questions in a clear and concise manner.	10.1, 10.2	4	100% or 1
A0012	Ability to ask clarifying questions.	10.1, 10.2	4	100% or 1
A0013	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	3.1, 3.2, 3.3	4	100% or 1
A0014	Ability to communicate effectively when writing.	3.3	4	100% or 1
A0016	Ability to facilitate small group discussions.	9.3, 11.2	3	90% or .9
A0017	Ability to gauge learner understanding and knowledge level.	12.1	3	90% or .9
A0020	Ability to provide effective feedback to students for improving learning.	11.1	3	90% or .9
A0022	Ability to apply principles of adult learning.	10.1, 12.1, 13.1, 16.1, 16.2, 16.3	3	90% or .9

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
A0023	Ability to design valid and reliable assessments.	14.1	4	100% or 1
A0024	Ability to develop clear directions and instructional materials.	8.1, 8.2, 8.3, 8.4, 8.5	3	90% or .9
A0057	Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
	Summary		**3**	**90% or .9**

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0001	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.	Synthesis, Evaluation	2.1.3, 3.4, 4.33, 4.4.2, 5.2.2,5.2.3	4	100% or 1
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Synthesis, Evaluation	5.2.2,5.2.3	4	100% or 1
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Synthesis, Evaluation	2.1.1, 4.4	4	100% or 1
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, and systems, and elements.	Synthesis, Evaluation	1.4, 3.3, 5.2.4, 5.2.8	4	100% or 1
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	Synthesis, Evaluation	4.4.9	4	100% or 1
T0024	Collect and maintain data needed to meet system cybersecurity reporting.	Analysis, Evaluation	2.1.8	**3**	40% or .40
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Analysis, Evaluation	1.13, 1.14, 3.13	3	90% or .9
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Synthesis, Evaluation	4.5.1,4.5.2	4	100% or 1
T0089	Ensure security improvement actions are evaluated, validated, and implemented as required.	Synthesis, Evaluation	3.14	4	100% or 1
T0091	Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.	Analysis, Evaluation	1.13	**3**	40% or .40
T0092	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	Synthesis, Evaluation	4.5.9	4	100% or 1

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0093	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.	Synthesis, Evaluation	4.6.1	4	100% or 1
T0095	Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	Synthesis, Evaluation	5.1.1	4	100% or 1
T0097	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.	Analysis, Evaluation	3.1	3	60% or .60
T0099	Evaluate cost benefit, economic, and risk analysis in decision making process.	Analysis, Evaluation	3.11	3	60% or .60
T0106	Identify alternative information security strategies to address organizational security objective.	Analysis, Evaluation	5.14	3	40% or .40
T0115	Identify information technology (IT) security program implications of new technologies or technology upgrades.	Analysis, Evaluation	3.14	3	40% or .40
T0130	Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.	Analysis, Evaluation	1.7, 1.13, 1.14, 4.4.5, 5.1.2	3	90% or .9
T0132	Interpret and/or approve security requirements relative to the capabilities of new information technologies.	Analysis, Evaluation	5.2.11	3	40% or .40
T0133	Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	Synthesis, Evaluation	1.6, 1.12, 1.16, 1.17, 1.19, 4.4	4	100% or 1
T0134	Lead and align information technology (IT) security priorities with the security strategy.	Analysis, Evaluation	5.1.1	3	40% or .40
T0135	Lead and oversee information security budget, staffing, and contracting.	Synthesis, Evaluation	3.3	4	60% or .60
T0147	Manage the monitoring of information security data sources to maintain organizational situational awareness.	Synthesis, Evaluation	5.1.7	4	60% or .60

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0148	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Analysis, Evaluation	1.11, 3.7, 5.1.1	3	60% or .60
T0149	Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.	Analysis, Evaluation	4.4.8	3	60% or .60
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure they provide the intended level of protection.	Synthesis, Evaluation	3.12,5.1.5	4	100% or 1
T0157	Oversee the information security training and awareness program.	Analysis, Evaluation	3.6	3	60% or .60
T0158	Participate in an information security risk assessment during the Security Assessment and Authorization process.	Synthesis, Evaluation	4.4.3	4	60% or .60
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	Synthesis, Evaluation	5.1.4	4	60% or .60
T0192	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.	Application, Analysis	1.13	3	60% or .60
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Synthesis, Evaluation	4.5.5., 4.5.8	4	60% or .60
T0206	Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.	Synthesis, Evaluation	3.7	4	60% or .60
T0211	Provide system related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	Synthesis, Evaluation	5.2.15	4	100% or 1
T0213	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.	Synthesis, Evaluation	2.1.8	4	100% or 1

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0215	Recognize a possible security violation and take appropriate action to report the incident, as required.	Synthesis, Evaluation	4.13.1, 4.13.6	4	100% or 1
T0219	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.	Synthesis, Evaluation	2.13	4	100% or 1
T0227	Recommend policy and coordinate review and approval.	Synthesis, Evaluation	1.13	4	100% or 1
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Synthesis, Evaluation	4.12.5,4.13.5	4	100% or 1
T0234	Track audit findings and recommendations to ensure appropriate mitigation actions are taken.	Synthesis, Evaluation	2.2.7	4	100% or 1
T0239	Use federal and organization-specific published documents to manage operations of their computing environment system(s).	Analysis	3.1	3	40% or .40
T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Analysis	3.1	3	40% or .40
T0254	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	Synthesis, Evaluation	1.1 to 1.18	4	40% or .40
T0255	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	Synthesis, Evaluation	1.1	4	100% or 1
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Synthesis, Evaluation	5.2.8,5.2.14	4	100% or 1
T0263	Identify security requirements specific to an information technology (IT) system in all phases of the System Life Cycle.	Synthesis, Evaluation	4.9.1	4	100% or 1
T0264	Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Synthesis, Evaluation	4.4.9	4	60% or .60

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0265	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.	Synthesis, Evaluation	1.1 to 1.18	4	100% or 1
T0275	Support necessary compliance activities (e.g., ensure system security configuration guidelines are followed, compliance monitoring occurs).	Synthesis, Evaluation	1.1 to 1.18	4	100% or 1
T0276	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.	Analysis, Evaluation	4.4.9	3	60% or .60
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Synthesis, Evaluation	5.2.11	4	60% or .60
T0280	Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.	Synthesis, Evaluation	1.1 to 1.18	4	60% or .60
T0281	Forecast ongoing service demands and ensure security assumptions are reviewed as necessary.	Synthesis, Evaluation	5.2.1	4	60% or .60
T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Application, Analysis	1.1 to 1.18	3	60% or .60
	Summary			**4**	**90% or .9**

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0008	Knowledge of applicable business processes and operations of customer organizations.	5.11	3	40% or .40
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	4.11	3	60% or .6
K0021	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	4.5.10	3	60% or .6
K0026	Knowledge of disaster recovery continuity of operations plans.	4.5.1 to 4.5.10	3	100% or 1
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	4.1, 4.6.3, 4.6.9	3	100% or 1
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	4.5.9	3	100% or 1
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	4.4.8, 4.6.7, 4.7.1, 4.9.4, 4.9.6, 4.10.1, 4.12	3	90% or .9
K0042	Knowledge of incident response and handling methodologies.	4.4.5, 4.4.6, 4.13	3	90% or .9
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1.1 to 1.18	3	90% or .9
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	4.6	3	90% or .9

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4.9	4	100% or 1
K0053	Knowledge of measures or indicators of system performance and availability.	NA		
K0054	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.	2.2.1 to 2.2.7	3	90% or .9
K0058	Knowledge of network traffic analysis methods.	NA		
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	2.1.3	4	90% or .9
K0061	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]).	NA		
K0070	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).	4.2, 4.9,4.10,	3	60% or .60
K0072	Knowledge of resource management principles and techniques.	3.4	4	100% or 1
K0076	Knowledge of server administration and systems engineering theories, concepts, and methods.	NA		
K0077	Knowledge of server and client operating systems.	NA		
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	1.1 to 1.10	4	100% or 1
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1 to 4.9.6	3	60% or .60
K0092	Knowledge of technology integration processes.	2.1.4	3	60% or .60
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	2.1.1	4	60% or .60
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	4.6	3	60% or .60

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0121	Knowledge of information security program management and project management principles and techniques.	3.1 to 3.14	4	100% or 1
K0126	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	5.2.11	4	100% or 1
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	2.1.1,4.4.1	4	100% or 1
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	4.4.5, 4.4.6, 4.13	3	90% or .9
K0151	Knowledge of current and emerging threats/threat vectors.	1.15	3	90% or .9
K0163	Knowledge of critical information technology (IT) procurement requirements.	5.2.15	3	90% or .9
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	4.10	3	90% or .9
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy 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 relevant to work performed.	1.1 to 1.19	**3**	95% or .95
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4.9	3	95% or .95
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	2.1.3, 5.1.1	3	90% or .9
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	4.6.4	3	60% or .60
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	4.6	3	60% or .60
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	5.1.1	3	60% or .60

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	1.1 to 1.19	**3**	95% or .95
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	1.1 to 1.19	**3**	95% or .95
K0262	Knowledge of Personal Health Information (PHI) data security standards.	1.1 to 1.19	**3**	95% or .95
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.1 to 1.19	**3**	95% or .95
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.1	2	40% or .4
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	4.6.4	2	40% or .4
K0342	Knowledge of penetration testing principles, tools, and techniques.	4.12	3	60% or .60
S0018	Skill in creating policies that reflect system security objectives.	1.1 to 1.19	**3**	95% or .95
S0027	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.	4.1 - 4.13	3	90% or .9
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.	5.2.10 - 5.2.14	3	90% or .9
	Summary		**3**	**90% or .9**

COMSEC Manager

Job Role Description: A COMSEC Manager Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a COMSEC Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Synthesis, Evaluation	2.1.1, 4.4	4	100% or 1
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, and systems, and elements.	Synthesis, Evaluation	1.4, 3.3, 5.2.4, 5.2.8	4	100% or 1
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Synthesis, Evaluation	NA		
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Synthesis, Evaluation	4.5.1,4.5.2	4	100% or 1
T0089	Ensure security improvement actions are evaluated, validated, and implemented as required.	Synthesis, Evaluation	3.14	4	100% or 1
T0095	Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	Synthesis, Evaluation	5.1.1	4	100% or 1
T0099	Evaluate cost benefit, economic, and risk analysis in decision making process.	Synthesis, Evaluation	3.11	3	60% or .60
T0215	Recognize a possible security violation and take appropriate action to report the incident, as required.	Synthesis, Evaluation	4.13.1, 4.13.6	4	100% or 1
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Synthesis, Evaluation	4.12.5,4.13.5	4	100% or 1
	Summary			**4**	**100% or 1**

COMSEC Manager

Job Role Description: A COMSEC Manager Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a COMSEC Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	4.11	3	60% or .6
K0026	Knowledge of disaster recovery continuity of operations plans.	4.5.1 to 4.5.10	4	100% or 1
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	4.5.9	4	100% or 1
K0042	Knowledge of incident response and handling methodologies.	4.4.5, 4.4.6, 4.13	3	60% or .6
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1 to 4.9.6	3	60% or .60
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	2.1.1	4	60% or .60
K0121	Knowledge of information security program management and project management principles and techniques.	3.1 to 3.14	4	100% or 1
K0126	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	5.2.11	4	100% or 1
K0163	Knowledge of critical information technology (IT) procurement requirements.	5.2.15	3	60% or .60
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.1 to 1.19	**3**	95% or .95

COMSEC Manager

Job Role Description: A COMSEC Manager Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a COMSEC Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.1	2	40% or .4
S0027	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.	4.1 - 4.13	3	60% or .60
	Summary		**3**	**80% or .8**

NCWF JOB ROLE

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0074	Develop policy, programs, and guidelines for implementation.	Synthesis, Evaluation	1.1	4	60% or .6
T0094	Establish and maintain communication channels with stakeholders.	Application, Analysis	3.13	**3**	80% or .8
T0116	Identify organizational policy stakeholders.	Analysis	1.14	3	60% or .6
T0222	Review existing and proposed policies with stakeholders.	Analysis	1.7	3	40% or .4
T0226	Serve on agency and interagency policy boards.	Analysis	1.1 to 1.20	3	40% or .4
T0341	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Analysis	3.8	**3**	40% or .4
T0355	Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.	Analysis	NA		
T0356	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Analysis	2.1.3	3	40% or .4
T0362	Develop and implement standardized position descriptions based on established cyber work roles.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0363	Develop and review recruiting, hiring, and retention procedures in accordance with current Human Resource (HR) policies.	Application, Analysis	NA		
T0364	Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0368	Ensure cyber career fields are managed in accordance with organizational Human Resource (HR) policies and directives.	Analysis	NA		
T0369	Ensure cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/ employment practices.	Analysis	NA		

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0372	Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0373	Establish and oversee waiver processes for cyber career field entry and training qualification requirements.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0374	Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0375	Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0376	Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0384	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Application, Analysis	1.1 to 1.20	3	40% or .4
T0387	Review and apply cyber career field qualification standards.	Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0388	Review and apply organizational policies related to or having an effect on the cyber workforce.	Analysis	1.1 to 1.20	3	40% or .4
T0390	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0391	Support integration of qualified cyber workforce personnel into information systems lifecycle development processes.	Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	3	40% or .4
T0408	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Analysis	1.1 to 1.20	4	100% or 1
T0425	Analyze organizational cyber policy.	Synthesis, Evaluation	1.1 to 1.20	4	100% or 1

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Analysis, Evaluation	1.1 to 1.20	3	100% or 1
T0441	Define and integrate current and future mission environments.	Application, Analysis	5.1.1 to 5.1.7	4	100% or 1
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Synthesis, Evaluation	5.1.1 to 5.1.7	4	100% or 1
T0472	Draft, staff, and publish cyber policy.	Analysis	1.1 to 1.20	3	40% or .4
T0481	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0505	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Analysis	1.1 to 1.20	3	40% or .4
T0506	Seek consensus on proposed policy changes from stakeholders.	Analysis	1.1 to 1.20	3	40% or .4
T0529	Provide policy guidance to cyber management, staff, and users.	Analysis	1.1 to 1.20	3	40% or .4
T0533	Review, conduct, or participate in audits of cyber programs and projects.	Analysis, Evaluation	2.2.1 to 2.2.7	3	40% or .4
T0537	Support the CIO in the formulation of cyber-related policies.	Analysis	1.1 to 1.20	3	40% or .4
T0552	Review and approve a supply chain security/risk management policy.	Analysis, Evaluation	1.1 to 1.20	3	40% or .4
	Summary			**3**	**50% or .5**

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0070	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).	4.2, 4.9,4.10,	3	60% or .60
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	NA		
K0146	Knowledge of the organization's core business/mission processes.	3.1	3	40% or .40
K0166	Knowledge of the nature and function of the relevant information structure.	NA		
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy 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 relevant to work performed.	1.1 to 1.20	3	40% or .40
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	NA		
K0234	Knowledge of full spectrum cyber capabilities.	NA		
K0241	Knowledge of organizational human resource policies, processes, and procedures.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0243	Knowledge of organizational training and education policies, processes, and procedures.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40
K0309	Knowledge of emerging technologies that have potential for exploitation by adversaries.	1.15	2	40% or .40
K0311	Knowledge of industry indicators useful for identifying technology trends.	1.15	2	40% or .40
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/ training and Research & Development).	NA		
K0335	Knowledge of current and emerging cyber technologies.	1.15	2	40% or .40
S0108	Skill in developing workforce and position qualification standards.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40
S0128	Skill in using manpower and personnel IT systems.	3.1 to 3.14	2	40% or .40
A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.	5.1.4, 5.2.1	2	40% or .40
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	1.1 to 1.20	3	40% or .40
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	NA		
A0042	Ability to develop career path opportunities.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40
A0053	Ability to determine the validity of workforce trend data.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40
	Summary		**3**	**50% or .5**

Cyber Policy and Strategy Planner

Job Role Description: A Cyber Policy and Strategy Planner develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Policy and Strategy Planner. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .6 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0074	Develop policy, programs, and guidelines for implementation.	Synthesis, Evaluation	1.1	4	95% or .95
T0094	Establish and maintain communication channels with stakeholders.	Synthesis, Evaluation	**3.13**	**4**	95% or .95
T0222	Review existing and proposed policies with stakeholders.	Evaluation	1.7	4	95% or .95
T0226	Serve on agency and interagency policy boards.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0341	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Analysis	**3.8**	3	80% or .8
T0369	Ensure cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/ employment practices.	Analysis, Evaluation	NA		95% or .95
T0384	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Evaluation	1.1 to 1.20	4	95% or .95
T0390	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Analysis, Evaluation	1.6, 3.5, 3.7, 4.4.4, 4.13.11	3	80% or .8
T0408	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Evaluation	1.1 to 1.20	3	95% or .95
T0425	Analyze organizational cyber policy.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Evaluation	1.1 to 1.20	4	95% or .95
T0441	Define and integrate current and future mission environments.	Synthesis, Evaluation	**5.1.1 to 5.1.7**	**3**	95% or .95
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Synthesis, Evaluation	**5.1.1 to 5.1.7**	**3**	95% or .95
T0472	Draft, staff, and publish cyber policy.	Synthesis, Evaluation	1.1 to 1.20	4	95% or .95

Cyber Policy and Strategy Planner

Job Role Description: A Cyber Policy and Strategy Planner develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Policy and Strategy Planner. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .6 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0505	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0506	Seek consensus on proposed policy changes from stakeholders.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0529	Provide policy guidance to cyber management, staff, and users.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0533	Review, conduct, or participate in audits of cyber programs and projects.	Analysis, Evaluation	2.2.1 to 2.2.7	4	95% or .95
T0537	Support the CIO in the formulation of cyber-related policies.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
	Summary			**4**	**95% or .95**

Cyber Policy and Strategy Planner

Job Role Description: A Cyber Policy and Strategy Planner develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Policy and Strategy Planner. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0070	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).	4.2, 4.9,4.10,	3	60% or .6
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	NA		
K0146	Knowledge of the organization's core business/mission processes.	3.1	3	40% or .4
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy 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 relevant to work performed.	1.1 to 1.20	3	40% or .4
K0234	Knowledge of full spectrum cyber capabilities.	NA		
K0248	Knowledge of strategic theory and practice.	5.1	2	40% or .4
K0309	Knowledge of emerging technologies that have potential for exploitation by adversaries.	1.15	2	40% or .4
K0311	Knowledge of industry indicators useful for identifying technology trends.	1.15	2	40% or .4
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).	NA		
K0335	Knowledge of current and emerging cyber technologies.	1.15	2	40% or .4

Cyber Policy and Strategy Planner

Job Role Description: A Cyber Policy and Strategy Planner develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Policy and Strategy Planner. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
A0003	Ability to determine the validity of technology trend data.	PM	2	40% or .4
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	1.1 to 1.20	3	40% or .4
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	NA		
	Summary		**3**	**60% or .6**

Executive Cyber Leadership

Job Role Description: A Executive Cyber Leadership executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0001	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.	Evaluation	5.2.2	4	100% or 1
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Evaluation	**5.2.3**	**4**	100% or 1
T0006	Advocate organization's official position in legal and legislative proceedings.	Evaluation	1.5	4	60% or .6
T0066	Develop and maintain strategic plans.	Synthesis, Evaluation	5.1	4	100% or 1
T0157	Oversee the information security training and awareness program.	Evaluation	**3.6**	**4**	90% or .9
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Evaluation	4.12.4	4	90% or .9
T0264	Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Analysis, Evaluation	2.2.7	3	90% or .9
T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Synthesis, Evaluation	2.1.5	4	90% or .9
T0337	Supervise and assign work to programmers, designers, technologists and technicians and other engineering and scientific personnel.	Evaluation	3.6	3	60% or .6
T0356	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Analysis	2.1.3	3	40% or .4
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Evaluation	1.5	3	60% or .6
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Synthesis, Evaluation	5.1.4	4	90% or .9
T0509	Perform an information security risk assessment.	Evaluation	4.4.3	4	90% or .9

Executive Cyber Leadership

Job Role Description: A Executive Cyber Leadership executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Analysis, Evaluation	5.1.2	4	90% or .9
T0871	Collaborate on cyber privacy and security policies and procedures	Analysis, Evaluation	1.13	4	90% or .9
T0872	Collaborate with cyber security personnel on the security risk assessment process to address privacy compliance and risk mitigation	Analysis, Evaluation	1.12	4	90% or .9
T0927	Appoint and guide a team of IT security experts	Analysis, Evaluation	2.1.3,3.7	4	90% or .9
T0928	Collaborate with key stakeholders to establish a cybersecurity risk management program	Analysis, Evaluation	4.4.3	4	90% or .9
	Summary			**4**	**90% or .9**

Executive Cyber Leadership

Job Role Description: A Executive Cyber Leadership executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0009	Knowledge of application vulnerabilities.	4.9	3	60% or .6
K0085	Knowledge of system and application security threats and vulnerabilities.	4.9	3	60% or .6
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	4.2, 4.4.8, 4.4.9, 4.6.7, 4.7.1, 4.8, 4.9.6, 4.10.1, 4.12.2	4	90% or .9
K0314	Knowledge of industry technologies and how differences affect exploitation/vulnerabilities.	4.2, 4.4.8, 4.4.9, 4.6.7, 4.7.1, 4.8, 4.9.6, 4.10.1, 4.12.3	3	90% or .9
K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	4.2, 4.4.8, 4.4.9, 4.6.7, 4.7.1, 4.8, 4.9.6, 4.10.1, 4.12.4	4	90% or .9
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	4.2, 4.4.8, 4.4.9, 4.6.7, 4.7.1, 4.8, 4.9.6, 4.10.1, 4.12.5	4	90% or .9
S0356	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).	3.7	3	95% or .95
S0357	Skill to anticipate new security threats.	1.15	3	95% or .95

Executive Cyber Leadership

Job Role Description: A Executive Cyber Leadership executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
S0358	Skill to remain aware of evolving technical infrastructures.	1.15	3	95% or .95
S0359	Skill to use critical thinking to analyze organizational patterns and relationships.	5.1.2	3	95% or .95
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	1.5	3	95% or .95
A0070	Ability to apply critical reading/thinking skills.	5.1	2	60% or .6
A0085	Ability to exercise judgment when policies are not well-defined.	1.16	2	60% or .6
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	1.15	3	95% or .95
A0105	Ability to tailor technical and planning information to a customer's level of understanding.	5.13	2	60% or .6
A0106	Ability to think critically.	5.1	2	60% or .6
A0116	Ability to prioritize and allocate cybersecurity resources correctly and efficiently.	4.5.4	2	60% or .6
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.	5.1	3	95% or .95
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.	3.1 to 3.14	2	95% or .95
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	4.13.3	2	60% or .6
	Summary		**3**	**90% or .9**

Program Manager

Job Role Description: A Program Manager leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0066	Develop and maintain strategic plans.	Synthesis, Evaluation	5.1	4	95% or .95
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	1.12	4	95% or .95
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.	Analysis, Evaluation	5.1.1,5.1.2	4	95% or .95
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Synthesis, Evaluation	4.4.2,4.4.3	4	95% or .95
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis, Evaluation	1.5,1.7	3	90% or .9
T0223	Review or conduct audits of information technology (IT) programs and projects.	Evaluation	2.2	4	90% or .9
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Evaluation	5.2.4	3	90% or .9
T0273	Develop and document supply chain risks for critical system elements, as appropriate.	Application, Analysis	5.2.11	3	90% or .9
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Application, Analysis	5.2.11	3	90% or .9
T0302	Develop contract language to ensure supply chain, system, network, and operational security are met.	Application, Analysis	5.2.11	3	90% or .9
T0340	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Application, Analysis	3.1	3	90% or .9
T0354	Coordinate and manage the overall service provided to a customer end-to-end.	Application, Analysis	3.7	3	90% or .9
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Application, Analysis	3.11	3	80% or .8

Program Manager

Job Role Description: A Program Manager leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0379	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	Application, Analysis	NA		
T0407	Participate in the acquisition process as necessary.	Application, Analysis	5.2.11	3	90% or .9
T0412	Conduct import/export reviews for acquiring systems and software.	Analysis, Evaluation	3.4	4	90% or .9
T0414	Develop supply chain, system, network, performance, and cyber security requirements.	Application, Analysis	5.2.11	3	90% or .9
T0415	Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.	Application, Analysis	5.2.11	3	90% or .9
T0481	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Analysis	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.1	3	80% or .8
T0493	Lead and oversee budget, staffing, and contracting.	Analysis	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.2	3	80% or .8
T0551	Draft and publish supply chain security and risk management documents.	Application, Analysis	4.4	3	60% or .6
	Summary			**3**	**90% or .9**

Program Manager

Job Role Description: A Program Manager leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.	5.1.1	3	90% or .9
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	90% or .9
K0072	Knowledge of resource management principles and techniques.	3.4	3	90% or .9
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1	3	90% or .9
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	2.1.1	3	90% or .9
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	60% or .6
K0146	Knowledge of the organization's core business/mission processes.	2.1.1	3	95% or .95
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	NA		
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	NA		
K0165	Knowledge of risk threat assessment.	4.4		95% or .95

Program Manager

Job Role Description: A Program Manager leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	90% or .9
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.	5.1.1	3	90% or .9
K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.	4.11	3	90% or .9
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	1.1,12	3	90% or .9
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	NA		
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	90% or .9
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	90% or .9
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	5.5	4	90% or .9
A0009	Ability to apply supply chain risk management standards.	NA		
A0039	Ability to oversee the development and update of the lifecycle cost estimate.	5.2.11	3	90% or .9
A0045	Ability to evaluate/ensure the trustworthiness of the supplier and/or product.	5.2.11	3	90% or .9
A0056	Ability to ensure security practices are followed throughout the acquisition process.	4.13.13	3	90% or .9
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

IT Project Manager

Job Role Description: An IT Project Manager directly manages information technology projects to provide a unique service or product.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Project Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	1.12	4	95% or .95
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.	Analysis	5.1.1,5.1.2	4	95% or .95
T0196	Provide advice on project costs, design concepts, or design changes.	Analysis	3.3	3	60% or .60
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Analysis	4.4.2,4.4.3	4	95% or .95
T0207	Provide ongoing optimization and problem solving support.	Analysis	2.1.8	4	95% or .95
T0208	Provide recommendations for possible improvements and upgrades.	Analysis	3.14	4	95% or .95
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis	1.5,1.7	3	90% or .9
T0223	Review or conduct audits of information technology (IT) programs and projects.	Analysis	2.2	4	90% or .9
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Analysis	5.2.4	3	90% or .9
T0273	Develop and document supply chain risks for critical system elements, as appropriate.	Analysis	5.2.11	3	90% or .9
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Analysis	5.2.11	3	90% or .9
T0340	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Analysis	3.1	3	90% or .9
T0354	Coordinate and manage the overall service provided to a customer end-to-end.	Analysis	3.7	3	90% or .9
T0370	Ensure that appropriate Service Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	Analysis	5.2.11	3	90% or .9

IT Project Manager

Job Role Description: An IT Project Manager directly manages information technology projects to provide a unique service or product.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Project Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Analysis	3.11	3	90% or .9
T0379	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	Analysis	NA		
T0389	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Analysis	5.1.5	3	90% or .9
T0394	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	Analysis	4.5.4	3	90% or .9
T0407	Participate in the acquisition process as necessary.	Analysis	5.2.11	3	90% or .9
T0412	Conduct import/export reviews for acquiring systems and software.	Analysis	3.4	3	90% or .9
T0414	Develop supply chain, system, network, performance, and cyber security requirements.	Analysis	5.2.11	3	90% or .9
T0415	Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.	Analysis	5.2.11	3	90% or .9
T0481	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Analysis	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.1	2	90% or .9
T0493	Lead and oversee budget, staffing, and contracting.	Analysis	4.4	3	90% or .9
T0551	Draft and publish supply chain security and risk management documents.	Application, Analysis	4.4	3	60% or .6
	Summary			**3**	**90% or .9**

IT Project Manager

Job Role Description: An IT Project Manager directly manages information technology projects to provide a unique service or product.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Project Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0012	Knowledge of capabilities and requirements analysis.	3.11	3	90% or .9
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1.7	3	90% or .9
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.	5.1.1	3	90% or .9
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	90% or .9
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	2.1.3	3	90% or .9
K0072	Knowledge of resource management principles and techniques.	3.4	3	90% or .9
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1	3	90% or .9
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	2.1.1	3	90% or .9
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	90% or .9
K0146	Knowledge of the organization's core business/mission processes.	2.1.1	3	95% or .95
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	NA		
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	NA		

IT Project Manager

Job Role Description: An IT Project Manager directly manages information technology projects to provide a unique service or product.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Project Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0165	Knowledge of risk threat assessment.	4.4	4	95% or .95
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	90% or .9
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.	5.1.1	3	90% or .9
K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.	4.11	3	90% or .9
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	1.1,12	3	90% or .9
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	NA		
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		90% or .9
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	90% or .9
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	90% or .9
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	5.5	4	90% or .9
A0009	Ability to apply supply chain risk management standards.	NA		
A0039	Ability to oversee the development and update of the lifecycle cost estimate.	5.2.11	3	90% or .9
A0045	Ability to evaluate/ensure the trustworthiness of the supplier and/or product.	5.2.11	3	90% or .9
A0056	Ability to ensure security practices are followed throughout the acquisition process.	4.13.13	3	90% or .9
	Summary		**3**	**90% or .9**

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	1.12	4	95% or .95
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.	Analysis, Evaluation	5.1.1,5.1.2	4	95% or .95
T0196	Provide advice on project costs, design concepts, or design changes.	Analysis	3.3	3	90% or .9
T0204	Provide input to implementation plans and standard operating procedures.	Analysis	4.5.10	3	90% or .9
T0207	Provide ongoing optimization and problem solving support.	Analysis	2.1.8	4	95% or .95
T0208	Provide recommendations for possible improvements and upgrades.	Analysis, Evaluation	3.14	4	95% or .95
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis	1.5,1.7	3	90% or .9
T0223	Review or conduct audits of information technology (IT) programs and projects.	Analysis, Evaluation	2.2	4	90% or .9
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Analysis, Evaluation	5.2.4	3	90% or .9
T0273	Develop and document supply chain risks for critical system elements, as appropriate.	Application, Analysis	5.2.11	3	90% or .9
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Analysis	5.2.11	3	90% or .9
T0302	Develop contract language to ensure supply chain, system, network, and operational security are met.	Application, Analysis	2.1.3	3	90% or .9
T0340	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Analysis	3.1	3	90% or .9
T0354	Coordinate and manage the overall service provided to a customer end-to-end.	Analysis	3.7	3	90% or .9

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0370	Ensure that appropriate Service Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	Analysis	5.2.11	3	90% or .9
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Analysis	3.11	3	80% or .8
T0389	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Analysis	5.1.5	3	80% or .8
T0394	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	Analysis	4.5.4	3	80% or .8
T0412	Conduct import/export reviews for acquiring systems and software.	Application, Analysis	3.4	3	90% or .9
T0414	Develop supply chain, system, network, performance, and cyber security requirements.	Application, Analysis	5.2.11	3	90% or .9
T0493	Lead and oversee budget, staffing, and contracting.	Analysis	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.1	3	90% or .9
T0525	Provide enterprise cybersecurity and supply chain risk management guidance.	Analysis	5.1.1	3	90% or .9
T0551	Draft and publish supply chain security and risk management documents.	Analysis	4.4	3	90% or .9
T0553	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Analysis	4.1, 4.11	3	90% or .9
	Summary			**3**	**90% or .9**

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1.7	3	80% or .8
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	80% or .8
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	2.1.3	3	80% or .8
K0072	Knowledge of resource management principles and techniques.	3.4	3	80% or .8
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1	3	80% or .8
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	80% or .8
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	NA		
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	4.13	3	95% or .95
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	NA		
K0165	Knowledge of risk threat assessment.	4.4	4	95% or .95

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	80% or .8
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.	5.1.1	3	80% or .8
K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.	4.11	3	80% or .8
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	1.1,1.2	3	80% or .8
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	NA		
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		
K0249	Knowledge of sustainment technologies, processes and strategies.	5.1.1	3	80% or .8
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	80% or .8
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	80% or .8
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	5.5	4	80% or .8
A0009	Ability to apply supply chain risk management standards.	NA		
A0031	Ability to conduct and implement market research to understand government and industry capabilities and appropriate pricing.	5.2.8	3	90% or .9
A0039	Ability to oversee the development and update of the lifecycle cost estimate.	5.2.11	3	90% or .9

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
A0045	Ability to evaluate/ensure the trustworthiness of the supplier and/or product.	5.2.11	3	90% or .9
A0056	Ability to ensure security practices are followed throughout the acquisition process.	4.13.13	3	90% or .9
	Summary		**3**	**90% or .9**

IT Investment/Portfolio Manager

Job Role Description: An IT Investment/Portfolio Manager Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Investment/Portfolio Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis, Evaluation	1.5,1.7	3	90% or .9
T0223	Review or conduct audits of information technology (IT) programs and projects.	Analysis, Evaluation	2.2	4	90% or .9
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Analysis	5.2.11	4	90% or .9
T0302	Develop contract language to ensure supply chain, system, network, and operational security are met.	Analysis	2.1.3	3	90% or .9
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Analysis	3.11	3	60% or .6
T0415	Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.	Analysis	5.2.11	3	90% or .9
T0493	Lead and oversee budget, staffing, and contracting.	Analysis, Evaluation	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.1	3	90% or .9
T0551	Draft and publish supply chain security and risk management documents.	Application, Analysis	4.4	3	90% or .9
	Summary			**3**	**90% or .9**

IT Investment/Portfolio Manager

Job Role Description: An IT Investment/Portfolio Manager Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Investment/Portfolio Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	60% or .60
K0072	Knowledge of resource management principles and techniques.	3.4	3	60% or .60
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	60% or .60
K0126	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	5.2.11	4	100% or 1
K0146	Knowledge of the organization's core business/mission processes.	2.1.1	3	95% or .95
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0165	Knowledge of risk threat assessment.	4.4	4	95% or .95
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	60% or .60
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	60% or .60
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	60% or .60

IT Investment/Portfolio Manager

Job Role Description: An IT Investment/Portfolio Manager Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Investment/Portfolio Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
A0039	Ability to oversee the development and update of the lifecycle cost estimate.	5.2.11	3	60% or .60
	Summary		**3**	**80% or .8**

IT Program Auditor

Job Role Description: An IT Program Auditor conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Program Auditor. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	1.12	4	95% or .95
T0207	Provide ongoing optimization and problem solving support.	Analysis, Evaluation	2.1.8	4	95% or .95
T0208	Provide recommendations for possible improvements and upgrades.	Analysis, Evaluation	3.14	4	95% or .95
T0223	Review or conduct audits of information technology (IT) programs and projects.	Analysis, Evaluation	2.2	4	95% or .95
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Analysis, Evaluation	5.2.4	4	95% or .95
T0389	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Analysis, Evaluation	5.1.5	4	95% or .95
T0412	Conduct import/export reviews for acquiring systems and software.	Analysis, Evaluation	3.4	4	95% or .95
T0415	Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.	Analysis	5.2.11	4	95% or .95
	Summary			**4**	**95% or .95**

IT Program Auditor

Job Role Description: An IT Program Auditor conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Program Auditor. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1.7	3	90% or .9
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.	5.1.1	3	90% or .9
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	90% or .9
K0072	Knowledge of resource management principles and techniques.	3.4	3	90% or .9
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1	3	90% or .9
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	90% or .9
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	NA		
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0165	Knowledge of risk threat assessment.	4.4	4	95% or .95
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	90% or .9
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	1.1,1.2	3	90% or .9

IT Program Auditor

Job Role Description: An IT Program Auditor conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Program Auditor. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	NA		90% or .9
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		90% or .9
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	90% or .9
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	90% or .9
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	5.5	4	90% or .9
S0085	Skill in conducting audits or reviews of technical systems.	2.2	4	90% or .9
A0056	Ability to ensure security practices are followed throughout the acquisition process.	4.13.13	3	90% or .9
	Summary		**3**	**90% or .9**

PROTECT AND DEFEND (PR)

Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

Cybersecurity Defense Analysis (DA)

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Cybersecurity Defense Infrastructure Support (INF)

Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

Vulnerability Assessment and Management (VA)

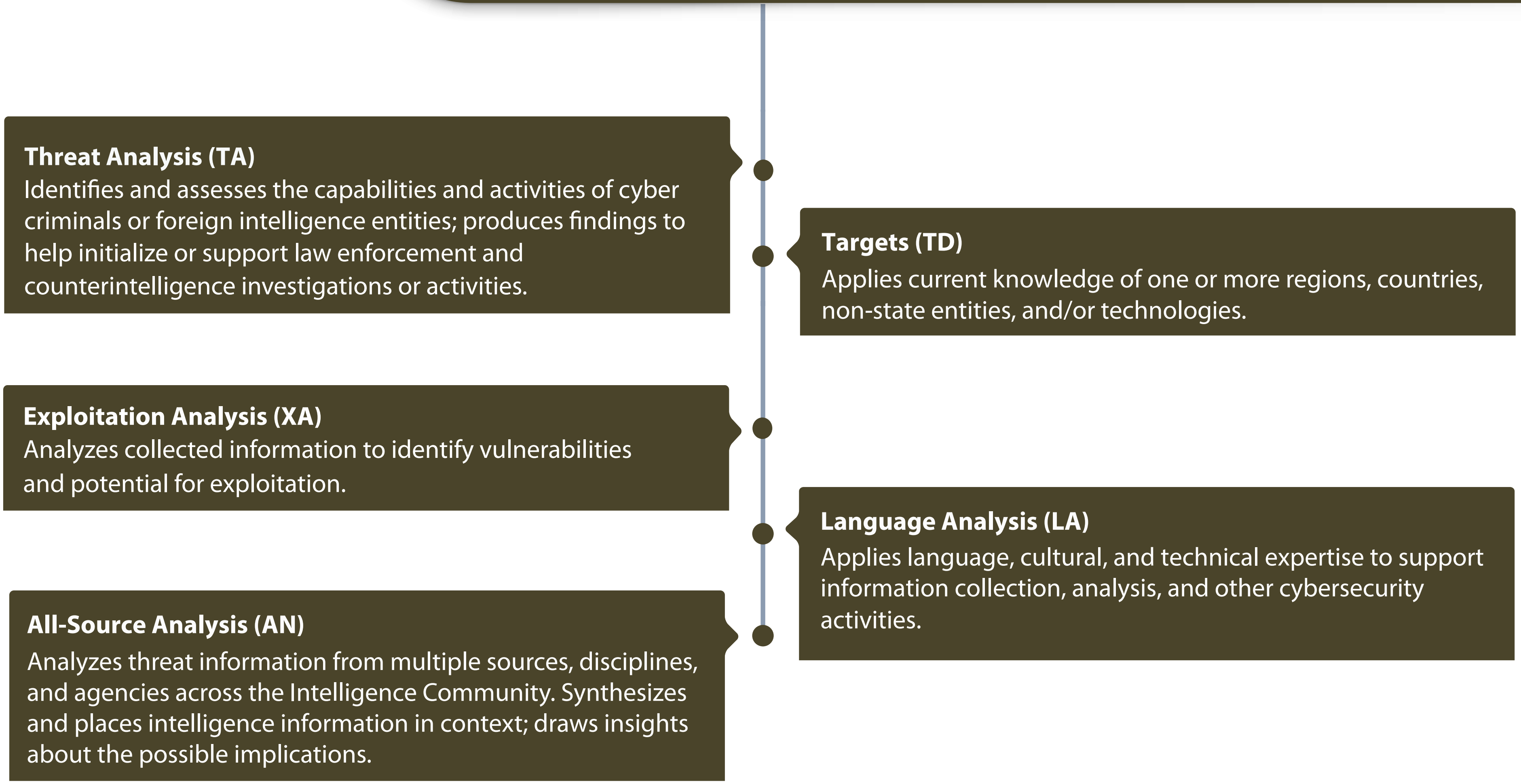
Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Incident Response (IR)

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.
Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

ANALYZE (AN)

Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.



Threat Analysis (TA)
Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Targets (TD)
Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

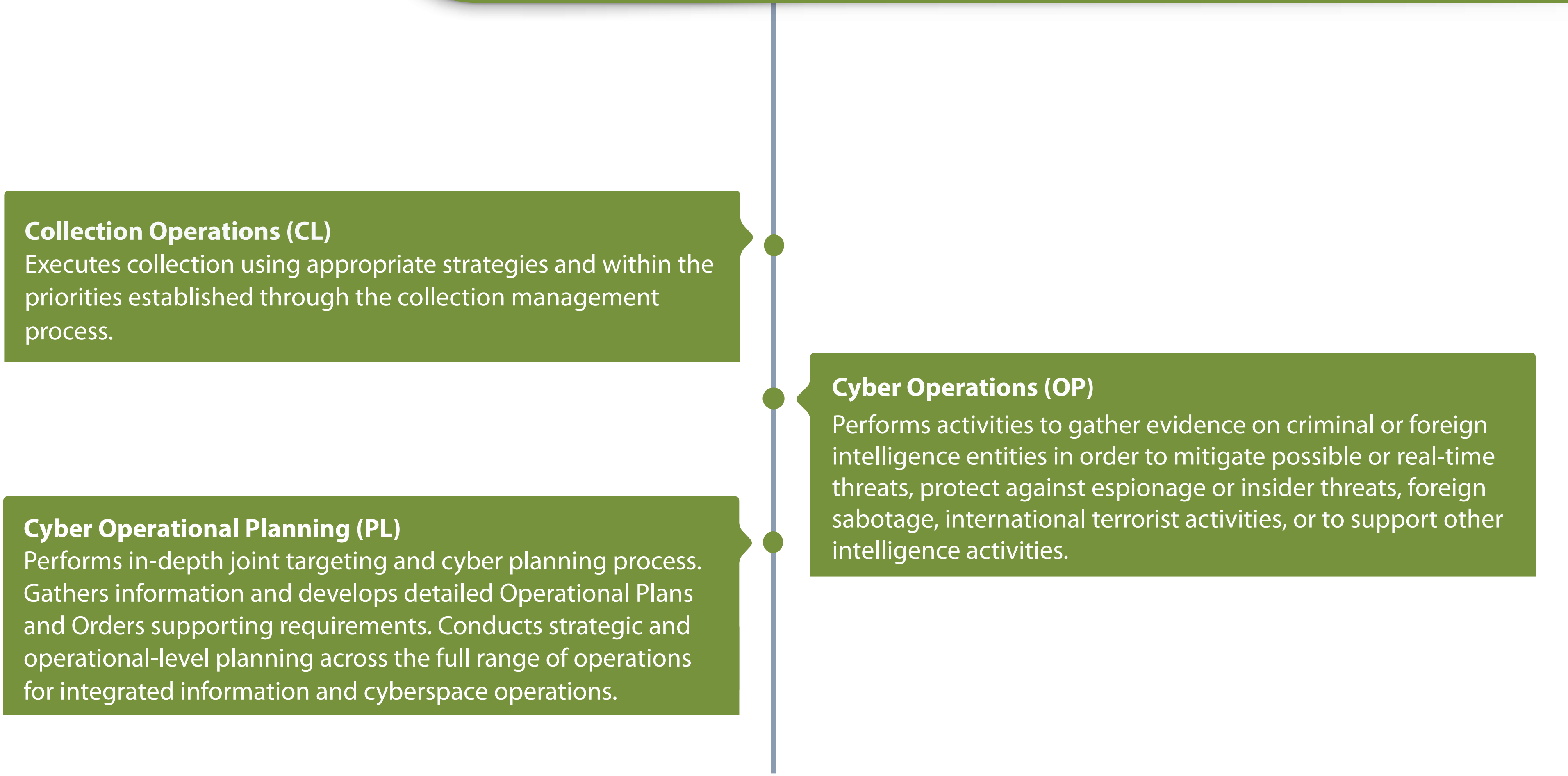
Exploitation Analysis (XA)
Analyzes collected information to identify vulnerabilities and potential for exploitation.

Language Analysis (LA)
Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.

All-Source Analysis (AN)
Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

COLLECT AND OPERATE (CO)

Specialty areas responsible for specialized denial and deception operations and Collection of cybersecurity information that may be used to develop intelligence.



Collection Operations (CL)
Executes collection using appropriate strategies and within the priorities established through the collection management process.

Cyber Operations (OP)
Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Cyber Operational Planning (PL)
Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Collection Operations (CL) | Cyber Operational Planning (PL) | Cyber Operations (OP)

About NICE, NCWF and EC-Council | Methodology and Mapping Summary | Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV) | Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO) | Investigate (IN)

INVESTIGATE (IN)

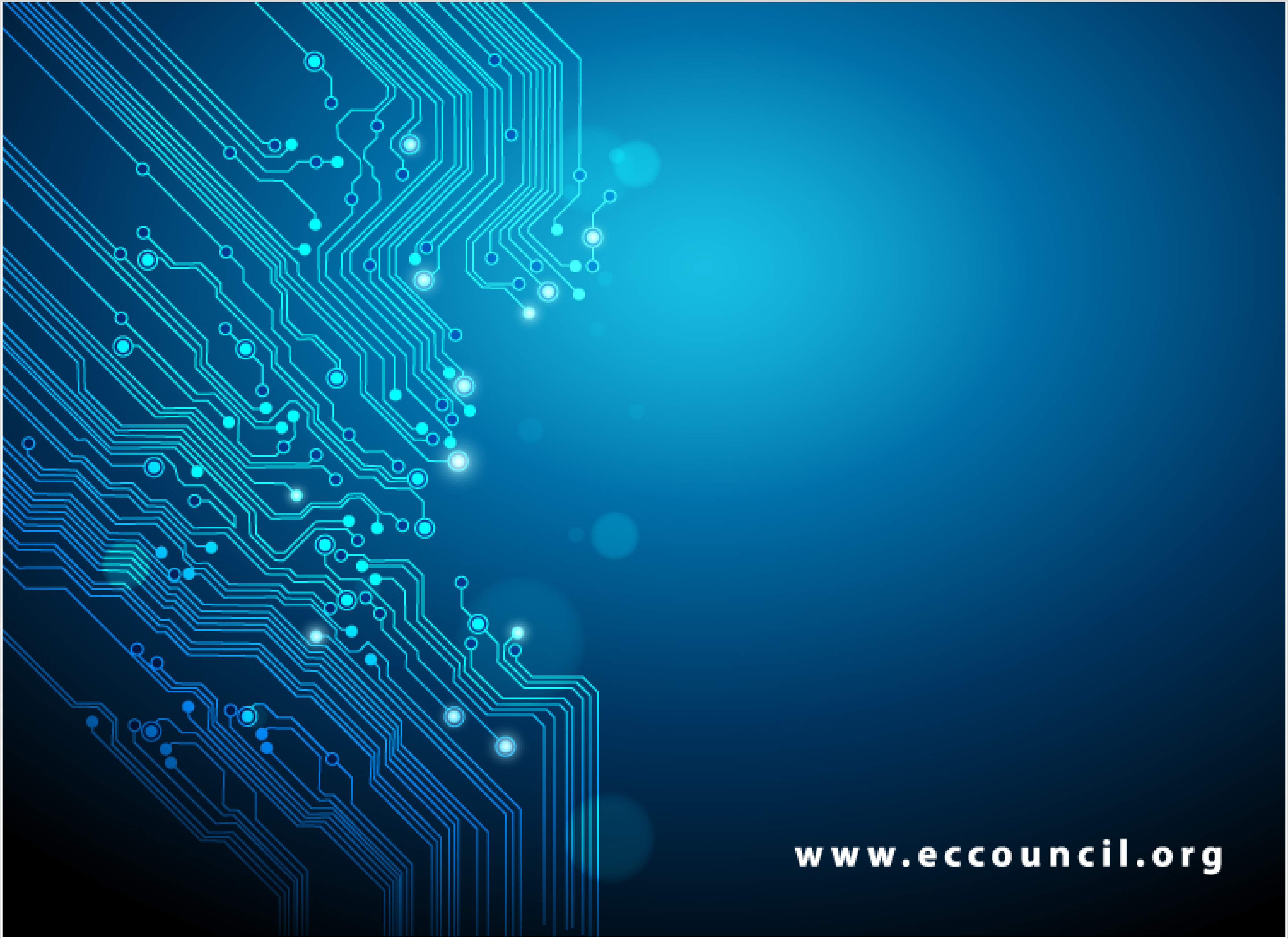
Specialty areas responsible for investigating cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Cyber Investigation (CI)

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Digital Forensics (FO)

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.



www.eccouncil.org