Communications Security Establishment

Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

The Canadian Cyber Security Skills Framework

Adapting the National Initiative for Cyber Education (NICE) Framework for the Canadian labour market

Management

Canada

Foreword

The Canadian Cyber Security Skills Framework (ITSM.00.039) is an unclassified publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email or phone our Service Coordination Centre:

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

Due to the highly dynamic nature of cyber security, this guide will be reviewed annually by the Canadian Centre for Cyber Security's Cyber Skills Development Team. All proposed changes to this publication should be sent by email to:

cyberskills-cybercompetences@cyber.gc.ca.

Effective date

This publication takes effect on April 19, 2023.

Revision history

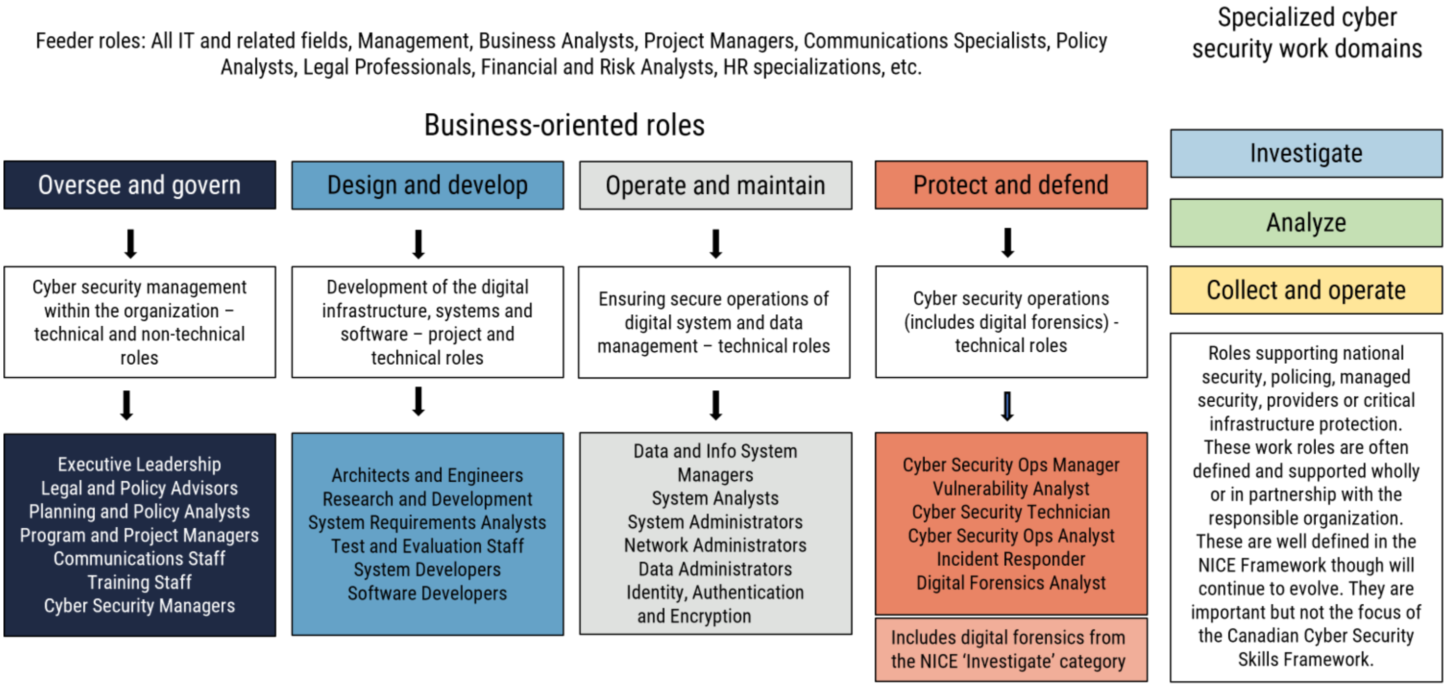
Revision	Amendments	Date
1	First release.	April 19, 2023

ISBN 978-0-660-46231-8
Cat. No. D97-4/00-039-2022E-PDF

Overview

The Canadian Cyber Security Skills Framework (Figure 1) is based on elements of the U.S. National Initiative for Cyber Education (NICE) Workforce Framework for Cybersecurity (NICE framework), contextualized for the Canadian labour market. It's a model that leverages the NICE framework while simplifying it using a business-oriented lens recognizing talent from an organizational security perspective and is a model more accessible to non-cyber security stakeholders.

Figure 1: Canadian Cyber Security Skills Framework



Feeder roles: All IT and related fields, Management, Business Analysts, Project Managers, Communications Specialists, Policy Analysts, Legal Professionals, Financial and Risk Analysts, HR specializations, etc.

Specialized cyber security work domains

Business-oriented roles

Oversee and govern

Cyber security management within the organization – technical and non-technical roles

Executive Leadership
Legal and Policy Advisors
Planning and Policy Analysts
Program and Project Managers
Communications Staff
Training Staff
Cyber Security Managers

Design and develop

Development of the digital infrastructure, systems and software – project and technical roles

Architects and Engineers
Research and Development
System Requirements Analysts
Test and Evaluation Staff
System Developers
Software Developers

Operate and maintain

Ensuring secure operations of digital system and data management – technical roles

Data and Info System Managers
System Analysts
System Administrators
Network Administrators
Data Administrators
Identity, Authentication and Encryption

Protect and defend

Cyber security operations (includes digital forensics) - technical roles

Cyber Security Ops Manager
Vulnerability Analyst
Cyber Security Technician
Cyber Security Ops Analyst
Incident Responder
Digital Forensics Analyst

Includes digital forensics from the NICE 'Investigate' category

Investigate

Analyze

Collect and operate

Roles supporting national security, policing, managed security, providers or critical infrastructure protection. These work roles are often defined and supported wholly or in partnership with the responsible organization. These are well defined in the NICE Framework though will continue to evolve. They are important but not the focus of the Canadian Cyber Security Skills Framework.

Leveraging the core elements and characteristics of the NICE framework, the Canadian Cyber Security Skills Framework will:

- help to specify the cyber security workforce gaps that exist in the Canadian labour market by applying a business lens and distinguishing between core cyber security roles and organizational roles which have some cyber security responsibilities or cyber security adjacent roles
- simplify the representation of cyber security-related work that is common within most organizations
- adapt to support broader or generalist responsibilities common within small and medium organizations (SMOs) as they aim to address foundational information technology (IT) and cyber security requirements
- maintain emphasis on cyber security responsibilities of adjacent work roles within "oversee & govern", "design & develop", and "operate & maintain"

The Canadian Cyber Security Skills Framework is a simpler presentation of cyber security work represented within many private and smaller public sector organizations. The purpose of this framework is to help better guide workforce development stakeholders in addressing the cyber security skills deficit. It can be applied across public, private, and academic sectors for career awareness and development, education and training, recruitment, or workforce planning.

Table of contents

List of figures

List of tables

List of annexes

1 Applying the NICE framework in Canada

1.1 Background

The National Occupational Standard (NOS) defines primary cyber security work as distinct from other occupations in IT, security, business management, or public administration. Cyber security is not, however, just about technical systems. It's also about people, their behaviour, and how they connect and engage with these systems.

The value of effective cyber security, and the services and products supported by cyber security professionals, cannot be understated. Cyber security work is now known across the globe as a critical and enduring career within the digital economy.

In Canada, our reliance on information and data systems has increased exponentially over the past decade as organizations digitize their operations and move to an online presence. This requires professionals who can design, build, implement, and maintain safe, secure, and reliable information systems that can support a variety of business, operational, and personal needs.

Canadian citizens have become more aware of their privacy rights and are increasingly concerned about how their personal data is protected by organizations. This requires experts in both online security and privacy who can advise on the various national and international standards, develop policies, identify requirements, and support monitoring to better protect the privacy of Canadians.

Cybercrime is an ever-increasing threat. According to the Cyber Centre's National Cyber Treat Assessment 2020, "cyber threat actors pose a threat to the Canadian economy by exacting costs on individuals and organizations, notably through the theft of intellectual property and proprietary information" [1]. Expertise is required to support detection and response to cyber threats as well as to support those who will investigate and collect digital evidence that can be used in improving protections and, when required, prosecuting offenders.

Cyber security will continue to be required across a broad range of technologies. Those employed in this field have significant and lasting career opportunities that can positively affect the lives of connected Canadians and support the future of the digital economy.

Consequently, Canadian businesses and industries struggle to meet their cyber security needs. There are four key workforce development challenges:

- Generating and retaining cyber security operations talent to meet the needs of the Canadian labour market
- Ensuring contributing technical and non-technical roles have required knowledge, skills, and abilities (KSA)
- Being responsive to the changing technology landscape
- Normalizing cyber security work and activities within the Canadian workplace

In part to help address these challenges, a group of industry, government, and academic stakeholders formed the Cyber Talent Alliance (see Annex F – available upon request). The group worked together to deliver:

- A cyber security skills framework, including taxonomy and common lexicon that describes cyber security work and workers, based on elements of the U.S. NICE framework[1] contextualized for the Canadian labour market
- NOS descriptions based on the skills framework
- Learning outcomes for relevant workforce areas
- Related resources to support workforce, career development, and learning

[1] The NICE Workforce Framework for Cyber Security, formerly the NICE Cyber Security Workforce Framework, was re-named in 2020 to recognize that cyber security is a concern across all workforces, not just the cyber security workforce.

2 A brief introduction to the NICE framework

Before the NICE framework, the diversity of ways in which cyber security work was viewed and described within the U.S. federal government posed a significant problem with recruiting, selection, training, and other workforce development activities across both the public and private sectors. Given the increasing threats to both the national and economic security, this was untenable. While conceived in the late 2000s, the first NICE working group was formed in 2011 by the U.S. National Institute of Standards and Technology (NIST) with other U.S. federal partners. Since then, over 20 U.S. federal departments, defence and security industry stakeholders, academia, and limited international participation from allies, such as Canada and Australia have contributed to the development and the evolution of the NICE framework.

The NICE framework provides an integrated view of the cyber security workforce. This means that it identifies work roles that "have an impact on an organization's ability to protect its data, systems, and operations" [2]. This includes both technical and non-technical roles intended to support organizational cyber security risk management efforts. In addition, the NICE framework includes national cyber operations capabilities including intelligence and offensive operations work roles normally housed within the federal government or partner institutions. Notably, the NICE framework includes an oversight and revision process to ensure that it meets the evolving needs of the cyber security community.

2.1 The U.S. NICE framework in the Canadian context

The NICE framework provides a comprehensive account of cyber security work. The degree to which it can be readily adopted by Canadian business and industrial organizations was a central point of investigation within this project. A few key questions are addressed:

1. **What are the key issues associated with the Canadian cyber security workforce?**

There are several issues when exploring differences and similarities between the U.S. and Canadian cyber security labour market.

Similarities:

- Both countries experience a lack of labour market information on cyber security jobs, related job titles, and roles.
- Based on the NICE framework work roles, Canada is assessed as having a similar gap as the U.S.
- In Canada, there are fewer resources dedicated to and limited attention on the cyber security workforce challenge.
- Cyber security is a highly competitive employment environment in both countries.

Differences:

- Canada and the U.S. have similar job market, but Canada has a considerably smaller and more dispersed work population.
- Resources are required in both official languages in Canada.
- A larger portion of Canada's economy is comprised of small and medium organizations (SMOs) and their needs differ from larger organizations.

- Canadian businesses and industries have limited visibility of the NICE framework and how it may apply to the Canadian labour market.

2. Is the NICE framework open for adoption?

As indicated in the NICE framework, it can be leveraged by other nations and adapted to suit their context [3]. Beyond this, there is also a long history of Five Eyes nations[2] sharing their publications and processes with partners. Canada shares its work with the U.S. and many of the Canadian federal IT security guidance publications are based on or significantly draw on NIST publications.[3]

3. What are the advantages and disadvantages of adopting the NICE framework in its current form?

Advantages:

- Can easily be accessed by the Canadian labour market and workforce development stakeholders
- Standardizes cyber security work role descriptions and provides a common lexicon for the community within the U.S. and Canada as well as other nations
- Provides a detailed description of KSAs for common cyber security roles, and recently introduced associated competencies that will aid in training, education, and career development
- Creates a known baseline to assess skilled entry candidates
- Is supported internationally by other governments
- Supports worker portability nationally and internationally
- Outlines many work roles, tasks, and KSAs that are valid within the Canadian cyber security workforce

Disadvantages:

- Lacks specificity and accuracy on the actual workforce gap to be addressed
- Is too “big” and too granular for the general Canadian market
- Can be difficult to navigate (e.g. the use of codes to cross-references KSAs versus word descriptions)
- Is “defence industry-oriented” or suited to large organizations which are heavily engaged in online activity
- Is structured with a static/horizontal perspective as it’s difficult to see career pathways, lateral or vertical progression within the cyber security work domain
- Does not scale well to smaller organizations
- Disregards cyber security generalist functions (e.g. corporate security officer) or those who support multiple cyber security roles within a typical organizational context (common in non-technical small and medium organizations)
- Minimizes important and distinct roles by incorporating them within broader roles (e.g. security engineering is part of the research and development role).

[2] The Five Eyes is an informal title of the international intelligence sharing agreement between Canada, the U.S., the U.K., Australia and New Zealand.

[3] For examples, see https://www.cyber.gc.ca/en/publications.

- Omits operational and industrial technology security roles (e.g. industrial control systems (ICS) and supervisor control and data acquisition (SCADA))
- Overlooks new and emerging roles that respond to the dynamic field of cyber security

The NICE framework does not necessarily reflect structure and employment functions that are common within the Canadian private sector or non-federal public sector organizations.

While there are several other contributing or adjacent cyber security roles noted in the NICE framework, the Canadian framework focuses on core cyber security roles and related competencies that are situated within the broader Canadian business context where most of their work is tied to organizational cyber security objectives and outcomes. Cyber security specializations that are almost solely within the intelligence, national security, or policing domain are identified and detailed within the NICE framework.

2.2 A special note on educators

The valuable role that educators play in cyber security is noted. However, as educators have their own National Occupation Classification (NOC) and an extensive network of occupational and professional standards, there is no need to reiterate that information within this publication. It's recognized that qualified educators are required who have relevant experience and the ability to facilitate and assess required learning to support industry demand according to recognized standards.

2.3 National Occupational Standards (NOS)

National Occupational Standards (NOS) describe what an individual in a particular occupation must know and be able to do to be considered "capable" in the occupation. These standards are defined in terms of competencies, including KSAs required to do the related work effectively, safely, and properly. NOS provide the benchmark for competent performance in the workplace as agreed to by a representative sample of workers, employers, and other stakeholders. NOS may also include or be driven by other external requirements, such as legal or policy compliance.

Figure 2: NOS uses

Practitioners	Employers	Educators	Workforce development stakeholders
Providing a foundation for career development Guiding their learning and development within the occupation Supporting career mobility and transitions	Identifying key tasks and roles Identifying professional development needs Facilitating objective job descriptions Providing guidance for recruitment	Identifying areas where expertise is required Providing the basis for curriculum, training development and education - private and public sector providers Providing curriculum improvements Forming the basis for certification programs and program accreditation	Creating professional development opportunities Identifying the skills required for specific occupations Providing nationally-recognized, sector-driven benchmarks of best practices Providing career development information for practitioners laddering to administration

3 Adapting the NICE framework to the Canadian labour market

3.1 Attributes of a workable skills framework for the Canadian market

By adopting and simplifying the NICE framework for the Canadian labour market and simplifying it, the Canadian framework can be more easily used by businesses and industries who may struggle with interpreting the NICE framework in its original form.

As shown in Figure 3, five key attributes have been identified to be considered when adopting the NICE framework for Canadian use. These attributes were determined based on some criticisms and structural issues of the NICE framework as well as community feedback and consultations.

Figure 3: Desired attributes for the Canadian cyber security skills framework

Specificity and accuracy

While the NICE framework describes the full spectrum of cyber security work roles, there should be a means of focusing on those that are most relevant to addressing the Canadian cyber security skills gap and the Canadian context.

Usability and accessibility

Any framework should allow for ease of use, readability, and accessibility of the content for all potential readers and users. This includes those unfamiliar with cyber security work. More specifically, the framework should not “silo” cyber security, but rather integrate concepts into the broader business/organizational context.

Clarity in constructs

Clarity is required in the constructs used to define cyber security roles and should include not only specialist roles, but generalists, non-technical and cross-disciplinary roles.

Adaptability

To address this dynamic field, there should be a means to rapidly integrate new or emerging roles as a result of technologies such as automation, cloud, artificial intelligence (AI), quantum. Related competencies/KSAs should also be developed to support the breadth of cyber security activities. The framework should be constantly evolving with the work.

Scalability

Any framework should be able to be readily scaled from large to small and medium organizations and different industry contexts. This includes the ability of organizations to identify and develop non-technical talent to support their security needs.

3.2 Adapting the Canadian framework to small and medium organizations

The Canadian framework can be adapted to SMOs. Within cyber security, most SMOs have the following characteristics:

- Lack of in-house cyber security expertise
- "Design & develop" roles are either outsourced or systems and applications are acquired "off-the-shelf"
- Individuals will often fill multiple roles that include cyber security tasks

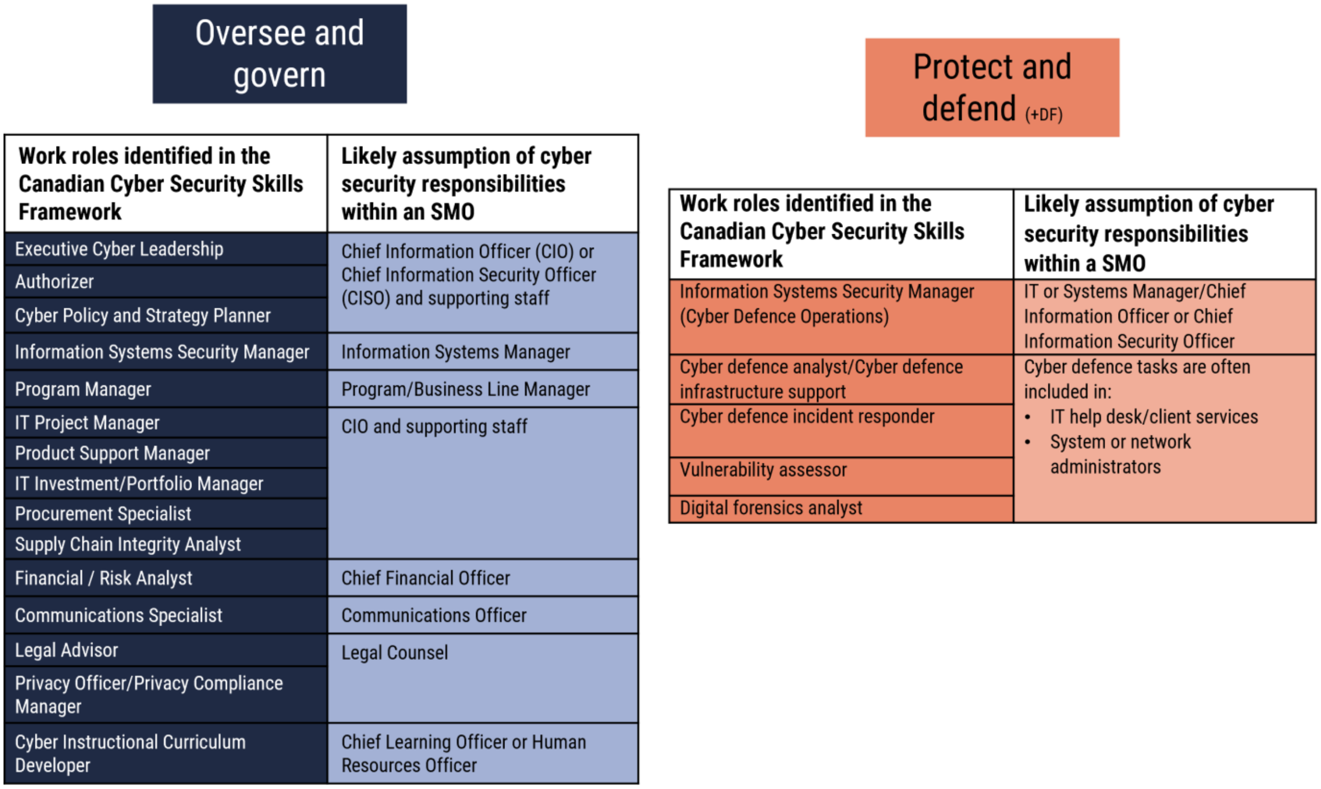
Consequently, when organizations look at the NICE framework it may be overwhelming. However, there is the potential to identify scenarios or present examples that will help SMOs scale the NICE framework using the Canadian framework. This will also help define role-based KSAs that will support cyber security within organizations.

The following section reviews two common scenarios typically found within SMOs.

1. **Medium-sized organization with some in-house IT staff**

There remains technical expertise in-house, but several cyber security roles are assumed by those who have other functions. They are not typically cyber security specialists or may have only a small IT section who will be responsible for detection and incident response. In this example, the chief information officer (CIO) would lead the small IT team and assume responsibilities for the technical aspects of the cyber security program while the executive level managers would remain responsible for defining the business priorities and risk landscape. For all "protect & defend" functions, they would likely be assumed by the IT team with specialized activities outsourced to a third party.

Figure 4: Potential technical roles in a medium organization



Oversee and govern

Work roles identified in the Canadian Cyber Security Skills Framework	Likely assumption of cyber security responsibilities within an SMO
Executive Cyber Leadership	Chief Information Officer (CIO) or Chief Information Security Officer (CISO) and supporting staff
Authorizer	
Cyber Policy and Strategy Planner	
Information Systems Security Manager	Information Systems Manager
Program Manager	Program/Business Line Manager
IT Project Manager	CIO and supporting staff
Product Support Manager	
IT Investment/Portfolio Manager	
Procurement Specialist	
Supply Chain Integrity Analyst	
Financial / Risk Analyst	Chief Financial Officer
Communications Specialist	Communications Officer
Legal Advisor	Legal Counsel
Privacy Officer/Privacy Compliance Manager	
Cyber Instructional Curriculum Developer	Chief Learning Officer or Human Resources Officer

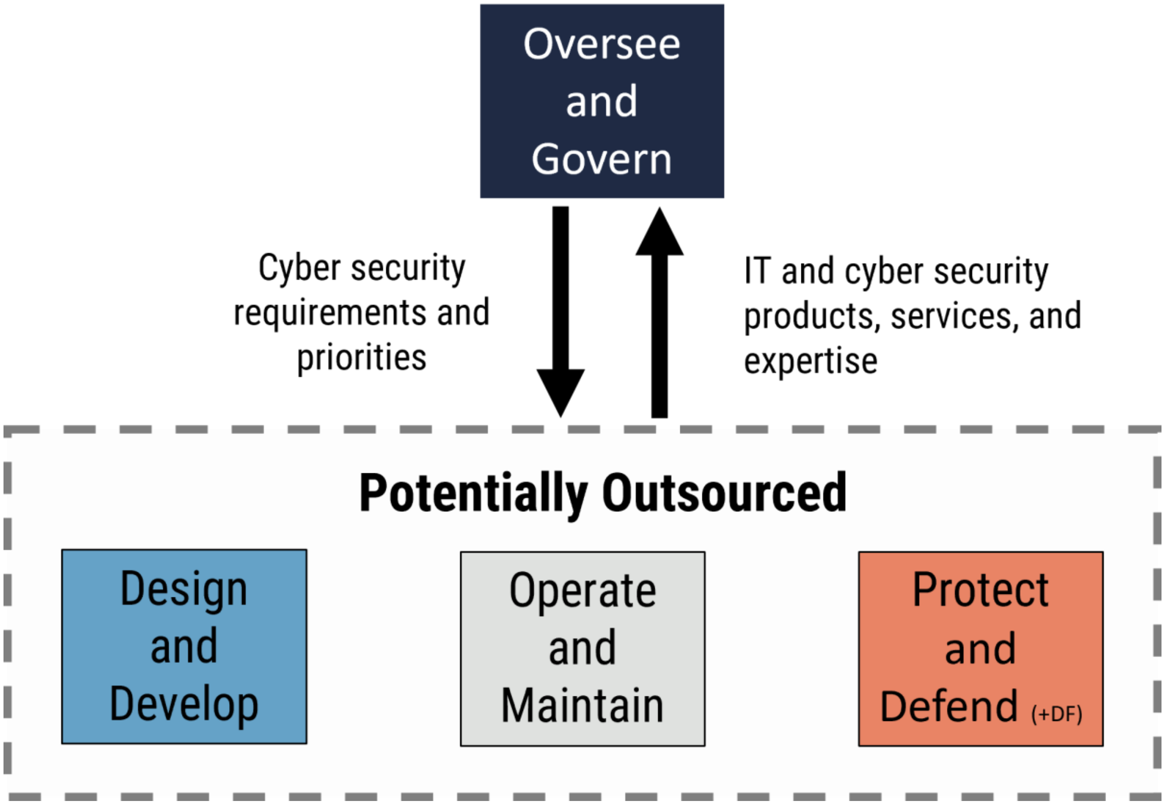
Protect and defend (+DF)

Work roles identified in the Canadian Cyber Security Skills Framework	Likely assumption of cyber security responsibilities within a SMO
Information Systems Security Manager (Cyber Defence Operations)	IT or Systems Manager/Chief Information Officer or Chief Information Security Officer
Cyber defence analyst/Cyber defence infrastructure support	Cyber defence tasks are often included in: • IT help desk/client services • System or network administrators
Cyber defence incident responder	
Vulnerability assessor	
Digital forensics analyst	

2. **Small organization with limited IT dependence and no IT staff**

Most technical work roles would be outsourced, but the primary “oversee & govern” cyber security functions would remain within the organization. This individual would effectively be fulfilling the role of the ”security generalist.”

Figure 5: Potential outsourced technical roles in a small organization



3.3 Cyber security generalist

Within many SMOs and even within larger organizations that are not heavily reliant on Internet-based activities, there are individuals tasked with cyber security responsibilities who may not have any IT or cyber security background.

Given the number of SMOs within the Canadian business landscape, this represents a very large cadre of individuals within the Canadian labour market that have primary responsibility for establishing and managing cyber security within their organizations but may not have any of the discrete roles as defined in the NICE or the Canadian framework. Typically, they:

- perform cyber security functions on a part-time basis in conjunction with other responsibilities
- only require cyber security KSAs to correspond to their business, technical, and threat context
- are not considered cyber security professionals and do not have a cyber security career trajectory

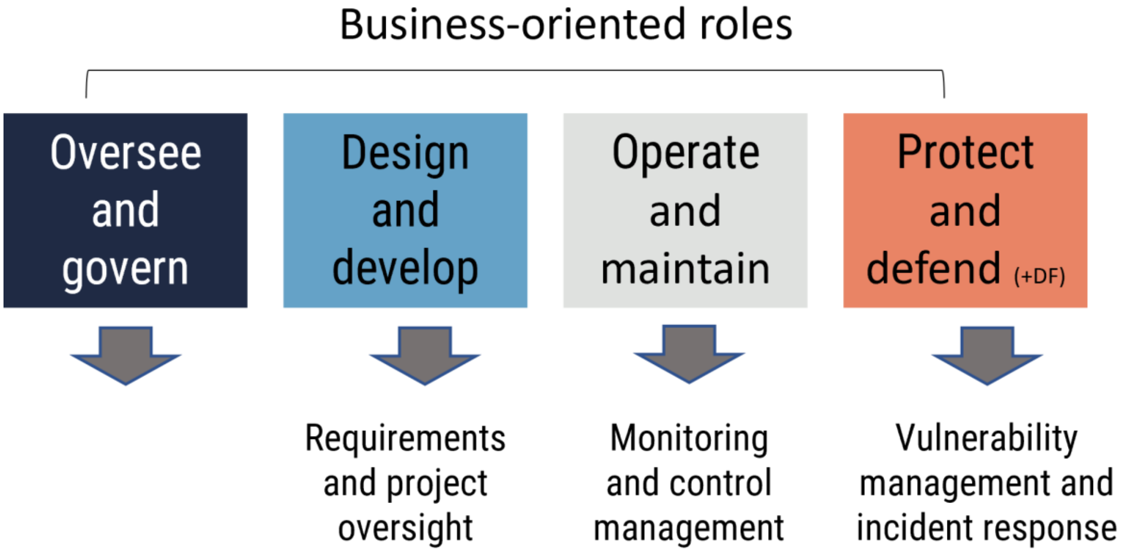
In absence of a term, this framework uses “security generalist” to differentiate them from cyber security specialists identified within the core roles. The security generalist within an organizational setting is typically not a specialist in any security area, but is often responsible for personnel, physical, contract, and loss prevention security activities as well as cyber security. It’s not uncommon, for example, for the chief executive officer (CEO), chief information officer (CIO), chief financial officer (CFO), corporate security officer, human resources manager, or senior administrative official to assume such a role.

Common tasks include:

- Assessing the organization’s cyber security posture
- Facilitating identification of organizational cyber risks
- Identifying non-technical cyber security controls
- Identifying and liaising with technical experts, internal or external, on technical controls
- Developing organizational cyber security plans and policies
- Advising leadership on security awareness and training
- Monitoring and support technical experts, whether in-house or outsourced, in their cyber security functions
- Coordinating cyber security incident response
- Monitoring and reporting on response and mitigation actions and recommend courses of action based on technical advice
- Coordinating post-mortem activities on events and incidents, integrating lessons learned into organizational policies and procedures

For many of these tasks, there are ample online resources available to guide the security generalists in their duties. Underpinning effectiveness in these tasks, however, are KSAs needed to support decision making and action. It’s unlikely that they will have any extensive cyber security training or education. Accordingly, they should be offered sufficient learning opportunities to attain the required competencies required for their roles as well as the potential threats, necessary technical skills, and business requirements. As shown in the examples in Figure 6, this typically requires competencies borrowed from some of the work roles within each major work category.

Figure 6: Security generalist functions


Business-oriented roles
Oversee and govern
Design and develop
Operate and maintain
Protect and defend (+DF)
Requirements and project oversight
Monitoring and control management
Vulnerability management and incident response

Basic knowledge

- Technical context (e.g. organizational IT infrastructure, software, devices, and policies)
- Cyber threat context (including deliberate, accidental, natural hazards)
- Business context (priorities, objectives, market, trends)
- Legal, policy, and ethical context for security
- Cyber security risk management as part of organizational risk
- Cyber security incident management (domain-specific)
- Cyber security processes, technology, trends, and emerging issues
- Sources of cyber security expertise and resources

Basic skills and abilities

- Providing business advice within the legal and policy cyber security context
- Exercising foresight and security planning to support digital business activities and growth
- Translating cyber risk to corporate risk
- Differentiating between compliance and risk
- Interpreting threat and risk assessments for the business context
- Assessing effectiveness of security controls against organizational security objectives

Common competencies

For all core cyber security roles regardless of activity area/work category, there are a number of common competencies that are applied at the basic, intermediate, or advanced level depending on the role. All cyber security professionals, regardless of role, should have a basic ability to apply the following in their work domain/context:

- IT systems and networking
- Systems architecture and models
- Internet protocols, systems and devices
- Cyber security foundations
  - Integrated security framework
  - Cyber security strategies and approaches
  - Threat landscape and common threat surfaces (personnel, physical, IT/logical, supply chain)
  - Cyber threat intelligence process and sources
  - Cyber security analytics
  - Cyber security management policies, processes, and best practices
  - Cyber security systems, tools, and applications
  - Legislation and compliance (e.g. privacy, information sharing, reporting, mandatory standards, etc.)
  - National and industry standards
- Problem-solving and complex thinking in dynamic environments
- Maintaining broader security situational awareness
- Self-awareness regarding knowledge, skills, and abilities required to respond to business, threat, and technical changes

3.4 Core cyber security roles

Recognizing that cyber security is a shared responsibility, this publication describes the cyber security occupation in terms of work that is typically conducted full-time and requires unique KSAs relative to other occupations. Moreover, as per the Canadian Cyber Security Skills Framework, the cyber security occupation is further defined in terms of titles/work roles that are relevant to the Canadian labour market and broader business community. These fall within four major cyber security activity areas or work categories: oversee & govern, design & develop, operate & maintain, and protect & defend. These activity areas/work categories and the inherent work roles are further defined in Annexes A, B, C and D (available upon request).

The core cyber security roles are divided into major work categories/occupational sub-groups similar to those established in the NICE framework[4].

- **Oversee & govern:** Overarching responsibility for this occupational sub-group is leadership and management of the cyber security program. This includes technical and non-technical roles.
- **Design & develop (securely provision in the NICE):** This occupational sub-group supports design and development of the digital infrastructure, systems and software. This includes largely technical roles.
- **Operate & maintain:** The primary responsibility of this occupational sub-group is ensuring secure operations of the digital systems and data management. All roles within this sub-group are technical roles.
- **Protect & defend:** This occupational sub-group is focused on cyber security operations. All roles within this occupational sub-group are technical roles.

Common competencies (cyber security professional foundations)

For all the core cyber security roles regardless of activity area/work category, there are a number of common competencies that are applied at the basic, intermediate, or advanced level depending on the role (as listed in Section 3.2). All cyber security professionals, regardless of role, should have a basic ability to apply the following additional competencies in their work domain/context:

- Continuous learning to support currency in knowledge of emerging threats, technological innovations in security, and the changing cyber security landscape
- Communications (oral and verbal) suited to organizational context including drafting and writing technical reports
- Strategic thinking and business acumen to include understanding the business and risk context for cyber security
- Teamwork/collaborating with others including non-cyber security professionals
- Ethics and professional responsibilities
- Cyber security training and awareness within their domain

3.5 Cyber security adjacent roles

There are also numerous roles associated with other organizational functions that typically contribute to organizational cyber security outcomes on a part-time or ad hoc basis[5]. These are cyber security adjacent roles where some cyber security KSAs are required, but they are not typically considered cyber security specialists[6]. For example, in most organizations, a business or policy analyst will likely be employed on a broad range of issues, only some of which will be in support of

[4] Of note, the work categories of Investigate, Analyze and Collect and Operate are only summarized within this document as they are fully defined within the NICE framework and typically fall within the responsibility of military and policing occupations.

[5] This is exclusive of 'users' who have ongoing cyber security responsibilities regardless of organizational role

[6] There are some professions/roles where they may be employed full-time within cyber security and are considered specialists, such as those employed in cyber-related law, privacy or ethics. As they are already part of another occupation and are not often part of an organization's workforce, they are not represented in this framework. They are, however, represented in the NICE framework.

organizational cyber security. This is not to detract from their role in supporting organizational cyber security, but only to suggest that their work involves often much more than strictly cyber security.

Similarly, executives, program managers, policy analysts, financial analysts, communications specialists, enterprise architects, IT technicians, etc., may have cyber security responsibilities but do not have full time cyber security functions and are not considered core cyber security roles in this publication. These roles are identified in Annex E (available upon request). A sampling of typical cyber security adjacent work roles is provided in Table 1 below. While they have cyber security responsibilities and require specific cyber security knowledge, skills, and abilities, their primary responsibilities are often either broader or focused on other activities that are not directed towards cyber security. Note that the “protect & defend” category is not included in the figure as that activity area or work category is exclusively employed in cyber security.

Table 1: Sampling of typical cyber security adjacent work roles

Oversee and govern	Design and develop	Operate and maintain
Chief information or technical officer	Enterprise architect	Systems manager
Corporate security officer	System requirements planner	Systems administrator
Program manager	Business analyst	Systems analyst
IT project manager	Software developer//programmer	Database administrator
Financial analyst	Control systems analyst	Data systems analyst
Learning and development specialist (e.g. security awareness & training)	Web developer	Technical support specialist

4 Summary of the Canadian Cyber Security Skills Framework and attributes

The Canadian Cyber Security Skills Framework (Figure 1) supports an organizational security lens on the NICE framework. The Canadian framework accordingly emphasizes four of the original seven work categories which represent the majority of cyber security work within the Canadian businesses and industries. Each of the work categories represent a responsibility area within cyber security and they are all interconnected.

Leveraging the core elements and characteristics of the NICE framework, the Canadian Cyber Security Skills Framework succeeds in that it:

- helps to better specify the cyber security workforce gaps that exist in the Canadian labour market by applying a business lens onto the NICE framework and distinguishing between core cyber security roles and organizational roles which have some cyber security responsibilities, or cyber security adjacent roles
- simplifies the representation of cyber security related work that is common within most organizations
- is readily adapted to support broader or generalist responsibilities common within SMOs as they aim to address foundational IT and cyber security requirements
- parses out the work categories of “analyze”, “collect & operate”, and “investigate” that focus on national security and law enforcement roles
- uses commonly understood terms familiar to the broader business and IT community, in particular using design & develop in place of “securely provision”
- maintains emphasis on cyber security responsibilities of adjacent work roles within “oversee & govern”, “design & develop”, and “operate & maintain”
- recognizes the central role within cyber security operations in “protect & defend”

5 Conclusion

The NICE framework is a comprehensive representation of the cyber security workforce though it’s primarily representative of U.S. federal government workforce structure. While it’s evolving and private sector stakeholders are becoming more engaged, some of the concerns with directly applying the NICE framework to the Canadian labour market have been discussed within this publication.

The Canadian Cyber Security Skills Framework is a simpler presentation of cyber security work represented within the majority of private and smaller public sector organizations and focuses more closely on business and industry gaps. This framework leverages an organizational security lens, rather than a national security lens, to help better translate cyber security work for businesses and industry. It also serves as a business-oriented interface to the comprehensive and detailed information in the NICE framework.

Overall, this should help to better guide workforce development stakeholders in addressing the cyber security skills deficit.

6 Supporting content

6.1 List of abbreviations

Term	Definition
AI	Artificial Intelligence
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CTA	Cyber Talent Alliance
KSA	Knowledge, skills, and abilities
ICS	Industrial Control Systems
IT	Information Technology
NICE	National Initiative for Cyber Education
NIST	National Institute of Standards and Technology
NOC	National Occupation Classification
NOS	National Occupation Standards
SCADA	Supervisor Control and Data Acquisition
SMO	Small and medium organizations

6.2 Glossary

For a detailed description of NICE categories, specialty areas and work roles, please refer to NICE framework.

Term	Definition
Ability	Ability is competence to perform an observable behaviour or a behaviour that results in an observable product.
Categories	In terms of the NICE framework, the Categories provide the overarching organizational structure of the NICE framework. There are seven Categories, and all are composed of Specialty Areas and work roles
Competency	The capability of applying or using knowledge, skills, abilities, behaviours, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position.
Cyber security	Cyber security is the protection of digital information and the infrastructure on which it resides.
Cyber threat	A cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains.
Cyber threat actor	Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The

Term	Definition
	globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information systems in Canada.
Knowledge	Knowledge is a body of information applied directly to the performance of a function.
National Institute for Standards and Technology (NIST)	A part of the U.S. Department of Commerce, U.S. NIST is the federal standards body with the mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
Offensive cyber operations (a.k.a. active cyber operations)	Within the U.S., these are cyber operations intended to project power by the application of force in and through cyberspace. Within Canada, active cyber operations are legislated though Bill C-59 and mandated by the Communications Security Establishment which under ministerial authority will carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.
Security operations centre (SOC)	A SOC provides operational and other security services to the department including the protection of people, property, assets and information. The SOC usually contains the facilities within which system operators can monitor, display and manage information (applications, video, and alarm systems) and then dispatch and respond to events. The design and development of a SOC should identify all areas to accommodate personnel, equipment and supplies associated with control, alarm and event monitoring activities.
Skill	Skill is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cyber security rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cyber security posture of an organization or individual.
Small and medium organization (SMO)	Organizations that have less than 499 employees.
Speciality area	Within the NICE framework, there are 32 specialty areas. Each specialty area represents an area of concentrated work, or function, within cyber security and related work.
Work role	Within the NICE framework, work roles are the most detailed groupings of cyber security and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSA) and tasks performed in that role.

6.3 References

Number	Reference
1	Canadian Centre for Cyber Security, National Cyber Threat Assessment 2020, November 2020.
2	National Institute of Standards and Technology, NIST Special Publication 800-181, NICE Cybersecurity Workforce Framework, August 2017.
3	National Institute of Standards and Technology, NIST Special Publication 800-181 Revision 2, Workforce Framework for Cybersecurity (NICE framework), November 2020.

Annex A Oversee & govern

Overarching responsibility for this activity area/work category is leadership and management of the cyber security program for the organization. Most of the work within this occupational sub-group is conducted by those within recognized occupational skill groups such as management (senior managers, middle managers) and business, finance, and administrative occupations (e.g. business analysts, finance analysts, risk analysts, communications). Consequently, many of the relevant work roles within this category are adjacent (non-core) roles that include policy, communications, training, and awareness, that are defined in Annex E.

For the oversee & govern activity area/work category, they will typically require advanced capabilities that relate to organizational planning, measurement, and management of cyber security.

Click on the cyber security role title to learn more about the knowledge, skills, tasks, and competency requirements for each.

Core cyber security roles

- Chief information security officer (CISO)
- Information system security officer (ISSO)
- Information security (IS) auditor

Adjacent roles

- Chief executive officer/senior leadership/owner
- Chief information officer/chief technical officer
- Cyber legal advisor
- Privacy officer/privacy compliance manager
- Communications security (COMSEC) manager
- Cyber workforce developer and manager
- Cyber instructional curriculum developer
- Cyber instructor
- Cyber policy and strategy planner
- Program manager
- IT project manager
- Product support manager
- IT investment/portfolio manager
- IT program auditor
- Business analyst
- Financial analyst
- Risk analyst
- Communications specialist
- Webmaster/online communications manager
- Learning and development specialist
- Business continuity/ resiliency planner
- Procurement specialist

A.1 Chief information security officer (CISO)

NICE framework reference	Oversee and govern, OV-EXL-001, executive cyber leadership
Functional description	An executive level role with accountability and responsibility for digital/information security activities of the organization. This includes planning, overseeing, and managing strategy development and implementation, cyber security operations, as well as budget and resources that ensure protection of the enterprise information assets throughout the supply chain. Employed throughout the public and private sectors.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in organizational decisions that can have a significant impact on the business. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	This is often considered the pinnacle of a cyber security career within a given organization. A CISO often has extensive experience (10+ years) in IT or systems, preferably with cyber security management experience. As an executive level position, the pathway also includes competency development including training, education, and experience outside of the technical field.
Other titles	▪ Chief security officer ▪ Departmental security officer ▪ Information security director Note: depending on the size of the organization and the reliance on IT, this occupational role may be subsumed within the responsibilities of the chief information security officer, chief technology officer, chief resiliency officer, or similar role.
Related National Occupational Classifications	00011 - Senior government managers and officials 00012 - Senior managers - financial, communications and other business services
Tasks	▪ Collaborate with key stakeholders to plan and establish an effective cyber security risk management program. ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement strategic plans that are aligned to the organizational objectives and security requirements ▪ Direct and approve the design of cyber security systems ▪ Identify, acquire, and oversee management of financial, technical and personnel resources required to support cyber security objectives ▪ Advise other senior management on cyber security programs, policies, processes, systems, and elements ▪ Ensure development and implementation of security controls to support organizational objectives ▪ Review, approve, oversee monitoring of cyber security policies and controls ▪ Ensure incident response, disaster recovery and business continuity plans are in place and tested ▪ Draft terms of reference, oversee and review cyber security investigations ▪ Maintain a current understanding the IT threat landscape for the business context ▪ Schedule and oversee security assessments and audits ▪ Oversee and manage vendor relations related to acquired IT security products and services ▪ Provide training and mentoring to security team members ▪ Supervise or manage protective or corrective measures when a cyber security incident or vulnerability is discovered.

Required qualifications for education	Bachelor’s degree in computer science or related discipline or equivalent training and experience.
Required training	Role-based training to support senior level management of security preferred.
Required work experience	Significant (5-10 years) experience in IT domain with 3-5 years’ experience in cyber security management roles.
Tools & technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Security event and incident management systems and/or incident reporting systems and networks ▪ Cyber security risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems
Competencies	Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework. Basic application of the following knowledge, skills, and abilities (KSA): ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Project management and security requirements throughout the project lifecycle ☐ Supply chain vulnerabilities and integrity Advanced application of the following KSAs: ☐ Organizational threats and vulnerabilities including: ○ Cyber security threat landscape ○ Vulnerability management requirements and the range of potential mitigations available when a vulnerability management protocol does not exist ○ Organizational security infrastructure including protective and defensive systems ☐ Developing, implementing, and allocating resources, personnel, and technology to address organizational security objectives. ☐ Identifying requirements and developing cyber security and cyber security risk management policies and procedures. ☐ Supplier management (if IT or security services are outsourced) ☐ Organizational communications, public communications and communicating during a crisis. ☐ Cyber security program management, measures, and monitoring
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their cyber security responsibilities relative to organizational cyber security risks. As the primary security advisor to senior management, this discussion will be led by the CISO, therefore a full appreciation of the business risks is required. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of “bring your own devices” (BYOD) and managing the associated risks. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to personnel, resources, procedures, and policies. This will need to be integrated into a security strategy and action plan for the organization. ▪ Increased use of automated tools by threat actors poses challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required.

	▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. Actions will also need to consider the organizational constraints and alternatives. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require advanced knowledge and skills related to implementing a quantum safe strategy and supporting processes within the organization.

A.2 Information system security officer (ISSO)

NICE framework reference	None
Functional description	This is an ad-hoc management role within cyber security that is primarily engaged in oversight and reporting of information system security within a department, branch, or organization. This role is primarily responsible for local planning and management of the security of system(s) over which they have been given authority. This role may report indirectly or directly to the CISO or another authority (e.g. Corporate security officer or Chief information officer or their delegate).
Consequence of error or risk	Error, neglect, outdated information, or poor judgment could result in decisions or actions that could compromise the security of the system over which the ISSO has authority. Depending on the system, this could have a significant impact on the business. A lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	This is commonly a part-time role assigned or assumed by an individual with some technical experience but is not normally a “cyber security professional”. In small and medium organizations this role may also be an IT manager or senior manager with some technical or security experience.
Other titles	▪ Chief security officer ▪ Departmental security officer ▪ Information security director **Note:** depending on the size of the organization and the reliance on IT, this occupational role may be subsumed within the responsibilities of the chief information officer, chief technology officer, chief resiliency officer or similar role.
Related National Occupational Classifications	20012 – Computer and Information Systems Managers
Tasks	▪ Collaborate with key stakeholders to plan and establish an effective cyber security risk management program. ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement strategic plans that are aligned to the organizational objectives and security requirements ▪ Direct and approve the design of cyber security systems ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support cyber security objectives ▪ Advise other senior management on cyber security programs, policies, processes, systems, and elements ▪ Ensure development and implementation of security controls to support organizational objectives ▪ Review, approve, oversee monitoring of cyber security policies and controls ▪ Ensure incident response, disaster recovery and business continuity plans are in place and tested ▪ Draft terms of reference, oversee and review cyber security investigations ▪ Maintain a current understanding the IT threat landscape for the business context ▪ Schedule and oversee security assessments and audits ▪ Oversee and manage vendor relations related to acquired IT security products and services ▪ Supervise or manage protective or corrective measures when a cyber security incident or vulnerability is discovered.

Required qualifications for education	Post-secondary education in a cyber or IT related field (e.g. Computer engineering, Computer Science, IT, Business Technology Management – Digital Security or equivalent)
Required training	As required to support the role for example cyber security team management, incident management and cyber security planning would be an asset.
Required work experience	3-5 years’ experience in IT domain with some management experience.
Tools & technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Security event and incident management systems and/or incident reporting systems and networks ▪ Cyber security risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems
Competencies	Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework. Basic application of the following knowledge, skills, and abilities (KSA): ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Project management and security requirements throughout the project lifecycle ☐ Supply chain vulnerabilities and integrity Advanced application of the following KSAs: ☐ Organizational threats and vulnerabilities including: o Cyber security threat landscape o Vulnerability management requirements and the range of potential mitigations available when a vulnerability management protocol does not exist o Organizational security infrastructure including protective and defensive systems ☐ Cyber security team management ☐ Developing, implementing and allocating resources, personnel and technology to address organizational security objectives ☐ Identifying requirements and developing cyber security and cyber security risk management policies and procedures ☐ Supplier management (if IT or security services are outsourced) ☐ Organizational communications, public communications and communicating during a crisis. ☐ Cyber security program management, measures, and monitoring
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their cyber security responsibilities relative to organizational cyber security risks. As a senior security advisor to management, this role will need a full appreciation of the business risks is required. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of ‘bring your own devices’ (BYOD) and managing the associated risks ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to personnel, resources, procedures, and policies. This will need to be integrated into a security strategy and action plan for the organization.

	▪ Increased use of automated tools by threat actors poses challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. Actions will also need to consider the organizational constraints and alternatives. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require advanced knowledge and skills related to implementing a quantum safe strategy and supporting processes within the organization.

A.3 Information security (IS) auditor

NICE framework reference	None. Associated with OV-PMA-005 IT program auditor
Functional description	A specialized auditor role, an information security auditor is responsible for evaluating and reporting on the security and effectiveness of IT systems and related controls in support of organizational information//data security, IT systems and their components. The audit conducted is often reported to a senior manager with recommendations for changes or improvements.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in an incomplete or inaccurate audit that does not identify critical system or process issues and fails to address organizational security requirements and increasing the potential risks of a compromise or security system failure.
Development pathway	Employment in this role is often preceded by formal education with a degree or diploma in an IT field as well as experience in an organizational cyber security role. There is also a requirement for specialized training and education in information system and information security audit practices.
Other titles	Cyber security auditor Security control assessor IT security auditor
Related National Occupational Classifications	21222 – Information specialists 21311 – Computer engineers (except software engineers and designers)
Tasks	▪ Collaborate with key stakeholders to establish an effective information security audit strategy which defines both internal and external audit requirements ▪ Liaise with external auditors as required to support organizational requirements ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement detailed internal audit plans that are aligned to the organizational objectives and security requirements ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support IS audit activities ▪ Develop and deploy policy testing on IS systems ▪ Review security assessment and authorization activities ▪ Advise other senior management on cyber security programs, policies, processes, systems, and elements ▪ Review and interpret cyber security/information security policies and controls ▪ Maintain a current understanding the IT threat landscape for the business context ▪ Schedule and conduct internal IS audits ▪ Analyze and interpret and external IS audit results ▪ Report results and provide recommendations to leadership and system owner(s)
Required qualifications for education	Post-secondary education in a cyber or IT related field (e.g., Computer engineering, Computer Science, IT, Business Technology Management – Digital Security or equivalent)
Required training	Specialized training in IT or information system audit and security audit.

Required work experience	Experience (3-5 years) in cyber security with preference in systems analytics (e.g. cyber security operations analyst, vulnerability analyst, IT systems security analyst)
Tools & technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Cyber security risk management processes & policies ▪ Compliance requirements including privacy and security legislation ▪ Organizational security infrastructure and reporting systems ▪ IS audit tools and systems ▪ Vulnerability assessments ▪ Penetration testing results ▪ IT systems performance measures
Competencies	Basic application of the following knowledge, skills, and abilities (KSA): ☐ Project and program management ☐ IT audit policies, practices, and procedures Advanced application of the following KSAs: ☐ Legal, policy and compliance requirements ☐ Business objectives and how IT/data/systems enable the business ☐ Information security audit polices, practices and procedures ☐ Integrated/organizational security concepts, principles, and practice (software, system, data, physical and personnel) ☐ External audit resources, competencies, and capabilities ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Organizational security responsibilities, accountabilities, and performance measures ☐ Cyber security program management, measures, and monitoring ☐ Organizational cyber security controls and responsible agents ☐ Organizational threats and vulnerabilities including: ○ Cyber security threat landscape ○ Vulnerability assessments and application of mitigations ○ Organizational security infrastructure including protective and defensive systems ☐ Security throughout the system/software development lifecycle ☐ Supply chain security ☐ System integration, testing and deployment ☐ Supplier management (if IT or security services are outsourced) and supply arrangements
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider and linkages with organizational systems ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of ‘bring your own devices’ (BYOD) and managing the associated risks ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools are integrated into the organizational security infrastructure, the implications to security controls and how they will be measured and assessed against security goals ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Therefore, audits of defensive tools and systems will evolve. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand how those tools operate, how their performance can be measured and what audit activities may be necessary. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization.

Annex B Design & develop

This activity area/work category is involved with developing secure infrastructure, systems and software. This is a highly technical branch of cyber security work. The majority of this work falls within the responsibilities of computer engineers (NOC 21311), computer systems developers and programmers (NOC 21230), information systems specialists (NOC 21222), and cyber security specialists (NOC 21220). As these are common occupations, which are also defined within the NICE, they have not been included within this framework.

Given the focus of this activity area, the emphasis is on applying deep technical understanding within a business context to better support organizational cyber security outcomes.

Click on the Cyber Security Role title to learn more about the knowledge, skills, tasks and competency requirements for each.

Core cyber security roles

- Security architect
- Security engineer/technologist
- Encryption engineer/technologist
- Operational technology engineer/technologist
- Secure software assessor
- Security testing and evaluation specialist
- Operational technology systems analyst
- Supply chain security analyst
- Information systems security developer
- Security automation engineer/analyst
- Cryptographer/cryptanalyst

Adjacent roles

- Authorizer (often CIO or system owner)
- Enterprise architect
- Software developer
- Systems requirements planner
- System testing and evaluation specialist
- Systems developer
- Web developer

B.1 Security architect

NICE framework reference	Securely provision, SP-ARC 002, security architect
Functional description	Designs, develops and oversees the implementation of network and computer security structures for an organization, ensuring security requirements are adequately addressed in all aspects of the infrastructure, and the system supports an organization's processes
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in flawed designs or architectures that could fail or experience exploitable vulnerabilities which could place IT systems upon which the organization relies in jeopardy. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	Primarily following education and a career pathway from an existing enterprise architect role, this is an emerging specialist role primarily employed in large tech-enabled organizations, shared services or systems or security providers.
Other title	Enterprise security architect
Related National Occupational Classifications	21311 – Computer engineers (except software engineers and designers) 21220 – Cyber security specialists
Tasks	▪ Collaborate with key stakeholders to establish an effective cyber security risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Define and review an organization's technology and information systems, and ensure security requirements ▪ Recognize appropriate disaster recovery plans and business continuity functions, including any failover or backup requirements for system restoration ▪ Plan, research, and develop robust security architectures for systems and networks ▪ Research current and emerging technologies to understand capabilities of required networks or systems ▪ Prepare cost estimates and identify integration issues ▪ Conduct vulnerability testing, risk analyses and security assessments ▪ Research and develop a system security context, and define security assurance requirements based on industry standards and cyber security policies and practices ▪ Ensure the acquired or developed systems and architectures are consistent with an organization's cyber security policies and practices ▪ Perform security reviews and identify gaps or determine the capability of security architectures and designs (e.g. firewall, virtual private networks, routers, servers, etc.), and develop a security risk management plan ▪ Prepare technical reports that document the architecture development process ▪ Document and address an organization's information security, cyber security architecture, and systems security engineering requirements throughout a system life cycle ▪ Advise on security requirements and risk management process activities ▪ Support incident management and post-analysis advising on recovery operations ▪ Develop, deliver, and oversee related cyber security training material and educational efforts related to role
Required qualifications for education	Post-secondary education in IT infrastructure and architecture (e.g. computer engineering, IT systems architecture)

Required training	Specialized training in security architecture concepts, principles, and practices. Training to support security tools needed to support role.
Required work experience	Previous training and experience in IT security infrastructure, requirements analysis or program management is preferred – 5-10 years of relevant IT experience for advanced-level.
Tools & technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Systems architectures ▪ IT mapping tools and applications ▪ Incident management processes and procedures ▪ Security event and incident management systems and/or incident reporting systems and networks, ▪ Cyber security risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems
Competencies	Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework. Advanced application of the following knowledge, skills, and abilities (KSA): ☐ Business needs for security ☐ Legal, policy and compliance requirements ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Project management and security requirements throughout the project lifecycle ☐ Cryptography and cryptographic key management concepts ☐ Virtual Private Network devices and encryption ☐ Engineering concepts and practices as applied to systems security and systems architecture ☐ Security architecture concepts and enterprise architecture reference models ☐ Security assessment and authorization processes ☐ Authentication, authorization, and access control methods ☐ System testing and evaluation methodologies and processes ☐ Application security system concepts and functions ☐ System life cycle management principles, including software security and usability ☐ Industry standards and organizationally accepted analysis principles and methods ☐ Configuring and using software-based computer protection tools ☐ Designing hardware and software solutions ☐ Cyber security program management, measures and monitoring ☐ Incident management and system recovery planning and operations
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require deep knowledge at the intersection between organizational and service providers architectures to determine and manage cyber security risks ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of ‘bring your own devices’ (BYOD) and how security controls are integrated into the organizational infrastructure. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the overall security architecture and infrastructure and the implications to personnel, resources, procedures, and policies ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required that will need to be integrated into the security architecture. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand

	organizational risks posed, measures of security and what policies, processes, or procedures need to be in place to support an integrated security architecture. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization and integrating it across the architecture.

B.2 Security engineer/technologist

This includes encryption engineer/technologies and operational technology engineer/technologist.

NICE framework reference	Securely provision, R&D specialist, SP-TRD-001
Functional Description	Given references, organizational security documentation, IT security guidance and required tools and resources, researches and defines the business needs for security and ensures that they are addressed throughout all aspects of system engineering and throughout all phases of the System Development Lifecycle (SDLC).
Consequence of error or risk	Error, neglect, outdated information or failure to account for organizational requirements, business needs and threats could result in poor systems design and/or integration of systems/devices that create exploitable vulnerabilities which can have significant implications to organizational objectives including the potential for catastrophic systems failure.
Development pathway	Typically follows formal education and 5-10 years' experience in related IT engineering, systems design, or systems integration functions. This role often requires advanced training, education or experience related to system capabilities. May be employed in general or specialized contexts such as Cryptography/Encryption, security testing and evaluation, or Operational Technology (ICS/OCS/SCADA).
Other titles	▪ Security designer ▪ Security requirements analyst ▪ Network security engineer ▪ Security engineering technologist ▪ Operational technology engineer ▪ Encryption engineer
Related National Occupational Classifications	21310 – Electrical and electronical engineers 21311 – Computer engineers (except software engineers and designers) 21222 – Information systems specialists 22310 – Electrical and electronics engineering technologists and technicians
Tasks	▪ Define/validate business needs for security & security requirements ▪ Review and analyze security IT/OT architectures & design documents, as well as related systems, protocols, services, controls, appliances, applications, encryption and crypto algorithms relative to security requirements and industry standards ▪ Develop and review system use cases ▪ Identify the technical threats to, and vulnerabilities of, systems ▪ Manage the IT /OT security configuration ▪ Analyze IT/OT security tools and techniques ▪ Analyze the security data and provide advisories and reports ▪ Analyze IT/OT security statistics ▪ Prepare technical reports such as IT security solutions option analysis and implementation plans ▪ Provide Independent Verification and Validation (IV&V) on IT/OT Security Projects ▪ Oversee IT/OT security audits ▪ Advise on security of IT /OT projects ▪ Advise on IT/OT security policies, plans and practices ▪ Review system plans, contingency plans, Business Continuity Plans (BCP) and Disaster Response Plans (DRP) ▪ Design/development and conduct IT/OT security protocols tests and exercises ▪ Review, develop and deliver training materials

Required qualifications for education	Relevant engineering degree or technologist diploma (depending on organizational requirements).
Required training	Valid industry level certification in related cyber security specialization (e.g. network security, cryptography, systems integration, etc.).
Required work experience	Moderate experience (3-5 years) in security and associated systems design, integration, testing and support.
Tools & technology	▪ Threat and risk assessment tools and methodologies ▪ Protective and defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms ▪ Security event and incident management systems and/or incident reporting systems and networks ▪ Authentication software and systems ▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used ▪ Security services provided if applicable ▪ Security testing and evaluation tools and techniques
Competencies	The security engineer/engineering technologist requires a basic level of application of the following KSAs while the security engineer requires an advanced level of application of the following knowledge, skills, and abilities (KSA): ☐ Security engineering models ☐ Defining and communicating security approaches that support organizational requirements ☐ International security standards and compliance ☐ Security architecture concepts and enterprise architecture reference models ☐ SDN, NFV, and VNF functions ☐ Systems security during integration and configuration ☐ Security assessment and authorization processes ☐ Security testing and evaluation methodologies and processes ☐ Security across the system/software development lifecycle ☐ Vulnerability assessment and penetration testing methodologies and applications ☐ Systems and software testing and evaluation methodologies ☐ Evidence-based security design ☐ Developing and testing threat models ☐ Project management and security assessment throughout the project lifecycle ☐ Procurement processes and supply chain integrity assessments ☐ Advising on security requirements, policies, plans and activities ☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives) In addition, in High Assurance, Encryption, and Cryptographic environments: ☐ Security governance in high assurance, encryption and cryptographic environments ☐ Advanced threat modeling and risk management in sensitive information environments ☐ Key management policies and practices (including Communications Security [COMSEC]) ☐ Emissions security standards ☐ Physical and IT security zoning ☐ Cryptography and encryption including algorithms and cyphers ☐ Stenography ☐ Testing and implementing Cross-domain solutions ☐ Key management, key management products and certification lifecycle ☐ Advanced persistent and sophisticated threat actor tactics, techniques and procedures ☐ Quantum safe/resistant technology ☐ Assessment and auditing encryption/cryptographic networks and systems In addition, within Operational Technology (ICS/OCS/SCADA) environments:

	☐ Industry standards and organizationally accepted analysis principles and methods ☐ Control system: ○ architecture and system defenses ○ governance and management in various environments ○ attack surfaces, threats and vulnerabilities ○ security monitoring, tools and techniques ☐ IT systems and protocols within control systems configurations ☐ Integration of IT and OT control systems ☐ Hardening and monitoring OT control systems ☐ Security assessment and authorization process of OT systems ☐ Incident response planning and activities in control system environments ☐ Business continuity planning and disaster recovery plans and activities in a control system environment
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services to be provided and how they are integrated into the organizational networks ▪ If practiced within the organization, there will be a requirement to fully understand the implications of “bring your own device” (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization and mitigations implemented to the level of acceptable risk. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organization and the potential security implications. If automated security tools will be used, testing, integration and monitoring requirements will need to be defined and those responsible for these activities will need to be advised/trained on the resulting process and procedural changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need for increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization.

B.3 Secure software assessor

NICE framework reference	Security provision, SP Dev-001, secure software assessor
Functional description	Given references, organizational security documentation, cyber security guidance and required tools and resources, analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
Consequence of error or risk	Error, neglect, outdated information could result in vulnerabilities in software and web-based tools can place organizational systems and services at risk.
Development pathway	Typically follows formal education and 5-10 years' experience in the software development field. This role often requires advanced training, education or experience related to secure software and vulnerability assessment activities for software/application security.
Other titles	▪ Secure software developer/programmer ▪ Software testing and evaluation specialists ▪ Vulnerability analyst/assessor
Related National Occupational Classifications	21222 – Information systems specialists 21231 – Software engineers and designers 21232 – Software developers and programmers
Tasks	▪ Define/validate business needs for security & security requirements ▪ Review and analyze security IT architectures & design documents, as well as related systems, protocols, services, controls, appliances, applications, encryption and crypto algorithms relative to security requirements and industry standards ▪ Research, analyze and implement secure application development processes and techniques ▪ Analyze the security data and provide advisories and reports ▪ Develop and conduct software system or application testing and validation procedures, programming, and secure coding, and report on functionality and resiliency ▪ Develop and review system use cases ▪ Conduct vulnerability scans and reviews on software systems or applications, and examine controls and measures required to protect software systems or applications ▪ Prepare reports on software systems, development and applications, patches or releases that would leave systems vulnerable ▪ Develop countermeasures against potential exploitations of vulnerabilities in systems ▪ Perform risk analysis whenever an application or system undergoes a change ▪ Prepare technical reports such as IT security solutions option analysis and implementation plans ▪ Provide Independent Verification and Validation (IV&V) on software projects ▪ Advise on software security policies, plans and practices ▪ Review, develop and deliver training materials
Required qualifications for education	Relevant computer science degree or diploma related to programming, software design or software development
Required training	Valid industry level certification in related secure software development and software security testing

Required work experience	Moderate experience (3-5 years) in software development followed by moderate experience (3-5 years) in secure software development activities.
Tools & technology	▪ Software development tools, processes, and protocols ▪ Threat and risk assessment tools and methodologies ▪ Protective and defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners, and alarms ▪ Open source software and application security information (e.g. OWASP) ▪ Security event and incident management systems and/or incident reporting systems and networks ▪ Software security testing and evaluation tools and techniques ▪ Authentication software and systems, ▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used ▪ Common vulnerability data bases ▪ Software development social collaboration sites (e.g. GITHUB) ▪ Security services provided if applicable
Competencies	Basic application of the following knowledge, skills, and abilities (KSA): ☐ Security architecture concepts and enterprise information security architecture model ☐ Security assessment and authorization processes ☐ Software procurement processes and supply chain integrity assessments ☐ IT security systems testing and evaluations tools, procedures, and practices Advanced application of the following KSAs: ☐ Software engineering models, processes, and principles ☐ Software development lifecycle and software project management ☐ Secure coding/software development operations processes, procedures, practices, tools, and techniques ☐ Business needs for security including compliance requirements ☐ Data security characteristics and requirements ☐ Security controls for software development ☐ Software development standards ☐ Secure software standards ☐ Secure software testing and evaluation methodologies and processes ☐ Vulnerability assessment and penetration testing methodologies and applications ☐ Developing and testing threat models ☐ Vulnerability scanning, assessment, and analysis ☐ Penetration testing activities and techniques ☐ Investigating and analyzing software vulnerabilities and breaches ☐ Establishing and managing a secure software/ web application testing environment ☐ Advising on security requirements, policies, plans and activities ☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives)
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-base” services will require knowledge of responsibilities of the services to be provided, software systems and applications used and how they are integrated into the organizational networks ▪ If practiced within the organization, there will be a requirement to fully understand the implications of “bring your own device” (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization and mitigations implemented to the level of acceptable risk. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools that may support software development, testing and integration will be used as well as the potential security implications. If automated security tools in software development and assessment, responsibilities for testing, integration and monitoring requirements will need to be defined and those responsible for these activities will need to be advised/trained on the resulting process and procedural changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant assessments of the robustness of software/applications security and potential mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities.

	▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need for increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as it applies to the software/application environment.

B.4 Security testing and evaluation specialist

NICE framework reference	Securely provision, security testing and evaluation, SP-TST-001
Functional description	Plans, prepares, and executes tests of security devices, operating systems, software, and hardware to evaluate results against defined specifications, policies, and requirements, and documents results and makes recommendations that can improve information confidentiality, integrity, and availability.
Consequence of error or risk	Error, neglect, outdated information, or poor judgment could result in IT systems, software or services being integrated and deployed with vulnerabilities that increase threat exposure and organizational risk. Resulting compromises could have a significant impact on the business.
Development pathway	Typically follows formal education and 5-10 years' experience in IT security. This role often requires specialized training, education or experience related to systems testing and measurement.
Other title	Systems security assessor
Related National Occupational Classifications	21222 – Information systems specialists 21311 – Computer engineers (except software engineers and designers)
Tasks	▪ Tests, evaluates, and verifies systems under development; systems exchanging electronic information with other systems; related operating system software and hardware; and security controls and devices used within an organization to determine level of compliance with defined specifications, policies, and requirements ▪ Analyze test results of operating systems, software, and hardware and make recommendations based on finding ▪ Develop test plans to address specifications, policies, and requirements ▪ Validate specifications, policies, and requirements for testability ▪ Create verifiable evidence of security measure ▪ Prepare assessments that document the test results and any security vulnerabilities present ▪ Deploy, validate, and verify network infrastructure device operation ▪ Develop, deliver, and oversee training material and educational efforts ▪ Provide training and mentoring to security team members
Required qualifications for education	Bachelor's degree in computer science or related discipline or equivalent training and experience.
Required training	Training in system security measurement, assessment, and testing.
Required work experience	Significant (5-10 years) experience in IT domain with 3-5 years' experience in systems security role supporting security assessments and IT audits preferred. Experience working in secured testing environments.
Tools & technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Security event and incident management systems and/or incident reporting systems and networks, ▪ System architecture ▪ Cyber security risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems ▪ System testing and evaluation policies tools, techniques, procedures and protocols

	▪ Legislation and compliance requirements
Competencies	Basic application of the following knowledge, skills, and abilities (KSA): □ Security procurement processes and supply chain integrity assessments □ Systems engineering process Advanced application of the following KSAs: □ Security assessment and authorization processes □ IT systems testing and evaluation strategies □ IT systems testing and evaluation infrastructure and resources □ IT security systems testing and evaluations tools, procedures, and practices □ Technical knowledge of networks, computer components, power supply technology, system protocols, cyber security-enabled software □ Network security architecture and models □ Conducting independent validation and verification security testing □ Systems testing and evaluation methods and techniques □ Test design, scenario development, and readiness review □ Systems integration testing □ Security assessment and authorization processes □ Security architecture concepts and enterprise information security architecture model □ Identifying test and evaluation policies and requirements □ Collect, analyze, verify and validate test data and translate data and test results into conclusion □ Designing and document test and evaluation strategies □ Writing technical and test and evaluation reports.
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their cyber security responsibilities relative to organizational systems, how those systems are integrated and how they can be tested and evaluated ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of “bring your own devices” (BYOD) and managing the associated risks to organizational systems ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to testing and evaluation practices ▪ Increased use of automated tools by threat actors pose challenges that will require continuous assessment of testing and evaluation practices and required tools ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place and any implications on security testing and evaluation. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy relevant to testing and evaluating encryption and degree of quantum resistance.

B.5 Operational technology systems analyst

NICE framework reference	None.
Functional description	Responsible for providing advice and ensuring effective cyber security within operations technology (OT) contexts (ICS/OCS/SCADA). Works in concert with systems engineers/technologists from different disciplines that are associated to the systems that are managed through OT (e.g. fluid, power, mechanical systems engineers).
Consequence of error or risk	Error, neglect, outdated information, or poor judgment could result in catastrophic failure of OT and related systems that they are used for management. In many cases, this can have a significant impact on the organizational operations and in some cases can directly result in significant human harm (e.g. in critical infrastructure systems).
Development pathway	Following technical education, often employed in IT or OT systems activities which provide the foundation for more specialized cyber security work in the OT environment. Similarly, cyber security professionals that normally work in an IT environment, may cross over to OT systems with the benefit of specialized training and education in OT and systems integration.
Other titles	OT security advisor OT security technician Security analyst - ICS/OCS/SCADA
Related National Occupational Classifications	21310 – Electrical and electronics engineers 21311 – Computer engineers (except software engineers and designers) 21220 – Cyber security specialists 21222 – Information systems specialists 22310 – Electrical and electronics engineering technologies and technicians
Tasks	▪ Collaborate with key stakeholders to establish an effective cyber security risk management program across the OT environment. ▪ Research and support design of cyber security solutions within OT context ▪ Ensure compliance with the changing laws and applicable regulations ▪ Draft, implement, and maintain IT/OT security policies, standards, and procedures. ▪ Monitor and manage cyber security requirements and controls across the OT environment ▪ Assess and analyze cyber security posture across OT systems and recommend remediation/risk management for vulnerabilities. ▪ Working with other stakeholders, support design and development of security solutions to enable business and technical requirements within the OT environment ▪ Manage the technical integration between IT and OT ▪ Define and maintain tool sets and procedures that support monitoring and management of OT ▪ In concert with other stakeholders, develop cyber security incident response plans clearly defining the role of those engaged in management and maintenance of OT systems ▪ Prepare technical reports ▪ Develop, deliver, and oversee related cyber security training material and educational efforts related to OT

Required qualifications for education	Bachelor's degree in computer science, computer engineering or related discipline or equivalent training and experience.
Required training	Specialized training associated with OT cyber security as well as system specific tools and techniques required.
Required work experience	Preferred experience for entry level role requires moderate experience 2-3 years working in the OT environment.
Tools & technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ OT Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Security event and incident management systems and/or incident reporting systems and networks that may be used for OT cyber security incidents, ▪ Cyber security risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems ▪ OT security tools, techniques and procedures
Competencies	Appreciating that not all OT analysts will necessarily have an IT background, the following basic application of the following knowledge, skills, and abilities (KSA): are relevant: ☐ Telemetry systems, data communications, data acquisition and process control ☐ Operating systems, networking, and communications systems concepts ☐ Electrical distribution networks, power system equipment, transformer station operation and electrical theory ☐ Computer and networking troubleshooting and maintenance procedures ☐ Network administration principles and practices ☐ System life cycle management principles, including software security and usability ☐ Database management systems and applications ☐ Database administration and optimization ☐ System testing and evaluation methodologies and processes ☐ Measures or indicators of system performance, availability, capacity, or configuration problems ☐ Analysis tools and network protocols ☐ Diagnostic tools and fault identification techniques Advanced application of the following KSAs: ☐ OT systems software and hardware, programmable logic controllers, and digital and analog relaying ☐ Threat and risk assessment to Internet connected OT (including implications and assessment of IoT devices) ☐ Legal and compliance requirements including organizational responsibilities for workplace and public safety related to OT/ production ☐ Industry standards and best practices, especially related to industrial environments in the cyber security space ☐ Cyber security program management, measures, and monitoring Control systems – applicable to industry/production environments ☐ IT/OT integration and convergence ☐ Process safety and hazard analysis ☐ Systems analysis and integration ☐ Problem-solving in complex systems environments ☐ Technical communications including report writing to address cross- disciplinary technical issues
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or "cloud-based" services will require knowledge of responsibilities of the services provider including their cyber security responsibilities relative to organizational cyber security risks and specifically those that relate to OT and remote operation and access.

	▪ If practiced within the organization, there will be a requirement to fully understand the security implications of “bring your own devices” (BYOD) and remote monitoring and operations through IoT and devices ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to OT requirements, procedures, and policies ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. For encryption within OT systems, this will require knowledge and skills related to implementing a quantum safe strategy within the organization.

B.6 Supply chain security analyst

NICE framework reference	None.
Functional description	Has the primary responsibility to collect and analyze data to identify cyber security flaws and vulnerabilities in an organization's supply chain operations, and to provide advice and guidance to help reduce these supply chain risks.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in organizational decisions that can have a significant impact on the business. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	Typically drawn from cyber security analysis roles (e.g. Cyber security operations analyst, vulnerability analyst, etc.) this role can nonetheless be assumed by a broad cross-section of professionals who can assess and provide insights on the potential supply chain threats. This includes those who may specialize in human factors aspects of supply chain (e.g. close access, insider threat).
Other titles	Cyber security analyst Supply chain integrity analyst
Related National Occupational Classifications	21220 - Cyber security specialists 21230 – Computer systems developers and programmers
Tasks	▪ Collaborate with key stakeholders to establish an effective cyber security risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement plans that are aligned to the organizational objectives and security requirements ▪ Collect and analyze supply chain relevant information to identify and mitigate flaws and vulnerabilities, including component integrity, in an organization's computer networks or systems ▪ Analyze system hardware and software configurations ▪ Recommend hardware, software, and countermeasures to install or update based on cyber threats and security vulnerabilities ▪ Coordinate with colleagues to implement changes and new systems ▪ Track and report on cyber threats and security vulnerabilities that impact supply chain performance ▪ Define, develop, implement, and maintain cyber security plans, policies and procedures ▪ Ensure compliance with cyber security policies, regulations, and procedures of the organization ▪ Ensure compliance with security requirements of organization networks and systems ▪ Develop and maintain risk assessments and related reports on vendors, products and services ▪ Define and maintain tool sets and procedures that support supply chain integrity ▪ Prepare technical reports ▪ Develop, deliver, and oversee related cyber security training material and educational efforts related to cyber security and supply chain integrity
Required qualifications for education	Post-secondary education in a cyber or IT related field (e.g. computer engineering, computer science, IT, business technology management – digital security or equivalent)
Required training	In addition to formal training in cyber security analysis, specialized training and skills in vulnerability analysis and supply chain threats required.

Required work experience	Individuals employed in this role can have diverse levels of cyber security expertise. Requested experience will depend on the organizational need and complexity of systems to be analyzed.
Tools & technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessment tools and applications ▪ Incident management processes and procedures ▪ Organizational security infrastructure and reporting systems Security event and incident management systems and/or incident reporting systems and networks ▪ Cyber security risk management processes & policies across the supply chain ▪ Third party and service level agreements and contracts
Competencies	Basic application of the following knowledge, skills, and abilities (KSA): ☐ Integrated/organizational security concepts, principles, and practice (software, system, data, physical and personnel) ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Project management and security requirements throughout the project lifecycle ☐ Procurement processes and security requirements Advanced application of the following KSAs: ☐ Organizational security infrastructure including protective and defensive systems across the supply chain ☐ Cyber security threat landscape and threat intelligence sources for supply chain threats ☐ Legal and compliance requirements as they extend to organizational third-party arrangements ☐ Vulnerability analysis and tools ☐ Advanced security information and data security analysis and techniques ☐ Functional and technical design of networks and system, and cyber security solutions ☐ Risk management processes, responsibilities, and authorities within the organization and across the supply chain ☐ Third party risk management and liability ☐ System life cycle management principles, including software security and usability ☐ Current national supply chain processes
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their cyber security responsibilities relative to organizational cyber security risks ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of “bring your own devices” (BYOD) and managing the associated risks ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to personnel, resources, procedures, and policies ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization.

B.7 Information Systems Security Developer

NICE framework reference	Securely provision, SP-SYS-001, information systems security developer
Functional description	Develops, creates, integrates, tests, and maintains information system security throughout the systems life cycle, and reports on information system performance in providing confidentiality, integrity, and availability and recommends corrective action to address deficiencies.
Consequence of error or risk	Error, neglect, outdated information, or poor judgment could result in organizational decisions that can have a significant impact on the business. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	This is an entry level role in cyber security that leverages previous IT and systems experience, following cyber security technical training, this work can lead to increased responsibilities in cyber security infrastructure roles and technical expertise.
Other titles	IT security systems administrator Cyber security systems technician
Related National Occupational Classifications	21220 - Cyber security specialists 21230 – Computer systems developers and programmers
Tasks	▪ Collaborate with key stakeholders to establish an effective cyber security risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Define and review an organization's information systems, and ensure security requirements recognize appropriate disaster recovery plans and business continuity functions, including any failover or backup requirements for system restoration ▪ Analyze existing security systems and make recommendations for changes or improvements ▪ Prepare cost estimates and constraints, and identify integration issues or risks to organization ▪ Research and develop a system security context, and define security assurance requirements based on industry standards and cyber security policies and practices ▪ Ensure the acquired or developed systems are consistent with an organization's cyber security policies and practices ▪ Develop and conduct information system testing and validation procedures and report on functionality and resiliency ▪ Plan and support vulnerability testing and security reviews on information systems or networks to identify gaps, and examine controls and measures required to protect the confidentiality and integrity of information under different operating conditions ▪ Conduct trial runs of information systems to ensure security levels and procedures are correct and develop a security risk management plan ▪ Support development of disaster recovery and continuity of operations plans for information systems under development ▪ Prepare technical reports that document system development process and subsequent revisions ▪ Document and address security throughout a system life cycle ▪ Update and upgrade information systems as needed to correct errors, and to improve performance and interfaces ▪ Prepare reports on information systems patches or releases that would leave networks or systems vulnerable

	▪ Develop countermeasures and risk mitigation strategies against potential exploitations of vulnerabilities in networks or systems ▪ Perform risk analysis whenever a system undergoes a change ▪ Develop, deliver, and oversee related cyber security training material and educational efforts related to role
Required qualifications for education	Post-secondary education in a cyber or IT related field (e.g. Computer Science, IT systems administration, Computer Engineering or equivalent).
Required training	Supporting training can include cyber security systems development tools, techniques and practices as well as Security throughout the system development lifecycle
Required work experience	Previous training and experience in system development.
Tools & technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Security event and incident management systems and/or incident reporting systems and networks, ▪ Cyber security risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems
Competencies	Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework. Basic application of the following knowledge, skills, and abilities (KSA): ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Risk management policies, requirements, and practices ☐ Business continuity and disaster response planning ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Project management ☐ Costing models and cost benefit analysis ☐ Cryptography and cryptographic key management concepts ☐ Identity and access management ☐ Vulnerability management and penetration testing planning and processes ☐ Data security conceptions and functions, analysis methodologies, testing, and protocols ☐ Secure coding and configuration techniques ☐ Cyber security program management, measures, and monitoring Advanced application of the following KSAs: ☐ Industry standards and organizationally accepted system analysis principles and methods ☐ System design tools, methods, and techniques ☐ Computer architecture, data structures, and algorithms ☐ System life cycle management principles, including software security and usability ☐ System testing and evaluation methodologies and processes ☐ System, application and data security threats, risks and vulnerabilities ☐ Designing countermeasures to identified security risks ☐ Configuring and using software-based computer protection tools ☐ Considerations for designing and hardware and software solutions ☐ Incident management and system recovery

Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their cyber security responsibilities and system to system interactions, access and accountabilities. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of “bring your own devices” (BYOD) and managing the associated risks throughout the system development life-cycle ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required, and system security responses developed and exercised. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization and across all systems that handle sensitive data.

B.8 Security automation engineer/analyst

NOTE: This is an emerging work role. There are limited samples of this work role and subject matter expert tasks and activities vary based on organizational requirements. Accordingly, the information below is based upon current representations based on demand driven requirements and an understanding of artificial intelligence, machine learning and data science requirements to support automated process engineering and analysis. It's anticipated that this will evolve significantly over the next years.

NICE framework Reference	None.
Functional description	Given references, organizational security documentation, IT security guidance and required tools and resources researches and defines the business needs for security, identifies requirements for and engineers automated solutions that support organizational security.
Consequence of error or risk	Error, neglect, outdated information, or failure to account for organizational requirements, business needs and threats could result in poor systems design and/or integration of systems/devices that create exploitable vulnerabilities which can have significant implications to organizational objectives including the potential for catastrophic systems failure.
Development pathway	Typically follows formal education and 5-10 years' experience in related IT engineering, systems design, or systems integration functions. Additional training, education and/or experience in process automation and related artificial intelligence/machine learning engineering activities.
Other titles	▪ Systems automation engineer ▪ Automated systems designer ▪ Security automation and controls engineer
Related National Occupational Classifications	21310 – Electrical and electronics engineers 21311 – Computer engineers (except software engineers and designers) 21231 – Software engineers and designers 22310 – Electrical and electronics engineering technologies and technicians
Tasks	▪ Research, develop, integrate, test, and implement security automation solutions for cloud or systems ▪ Scope and plan out automation work to meet timelines ▪ Manage/monitor automated security solution activities including fixes, updates, and related processes ▪ Develop and maintain tools and processes to support security automation activities ▪ Review and test security automation scripting prior to implementation ▪ Troubleshoot any issues that arise during testing, production, or use ▪ Create, use, and maintain resource documentation for reference ▪ Identify, acquire, and oversee management of financial, technical and personnel resources required to support security automation activities ▪ Review, approve, and oversee changes on cyber security policies and controls and their implication for automated activities ▪ Schedule and oversee security assessments and audits ▪ Oversee and manage vendor relations related to acquired IT security products and services ▪ Ensure security requirements are identified for all IT systems throughout their life cycle ▪ Supervise or manage protective or corrective measures when a cyber security incident or vulnerability is discovered ▪ Assess threats and develop countermeasures and risk mitigation strategies against automated system vulnerabilities

	▪ Perform risk analysis and testing whenever an automated system undergoes a change ▪ Develop, deliver, and oversee related cyber security training material and educational efforts related to role
Required qualifications for education	Relevant engineering or computer science degree with post graduate training or equivalent in systems automation, artificial learning or machine learning.
Required training	Relevant cyber security training to support functions as a security engineer.
Required work experience	Moderate experience (3-5 years) in security and associated systems design, integration, testing and support. Experience in programming and application testing. 2-3 years practical experience in automating system processes.
Tools & technology	▪ Threat and risk assessment tools and methodologies ▪ Protective and defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners, and alarms ▪ Security event and incident management systems and/or incident reporting systems and networks ▪ Authentication software and systems ▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used ▪ Security services provided if applicable ▪ Security testing and evaluation tools and techniques ▪ Process automation tools, techniques, and procedures ▪ Applicable programming languages
Competencies	Advanced level of application of the following knowledge, skills, and abilities (KSA): ☐ Process automation within a security setting ☐ API, automation, and scripting languages ☐ SDN, NFV, and VNF functions ☐ Security engineering models ☐ Defining and communicating security approaches that support organizational requirements ☐ International security standards and compliance ☐ Security architecture concepts and enterprise architecture reference models ☐ Systems security during integration and configuration ☐ Security assessment and authorization processes ☐ Security testing and evaluation methodologies and processes ☐ Security across the system/software development lifecycle ☐ Vulnerability assessment and penetration testing methodologies and applications ☐ Systems and software testing and evaluation methodologies ☐ Evidence-based security design ☐ Developing and testing threat models ☐ Project management and security assessment throughout the project lifecycle ☐ Procurement processes and supply chain integrity assessments ☐ Advising on security requirements, policies, plans and activities ☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives)
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their cyber security responsibilities relative to organizational cyber security risks ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of “bring your own devices” (BYOD) and managing the associated risks ▪ If automated security tools will be used, testing, integration and monitoring requirements will need to be defined and those responsible for these activities will need to be advised/trained on the resulting process and procedural changes. Additionally, as the potential technical lead for security automation, there may be a requirement to educate organizational leaders on the benefits and risks of automation and any change management required. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be

	required. This will require a significantly better appreciation of threat actor capabilities and potential countermeasures. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need for increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy and understanding of the implications on AI-enabled security mechanisms.

B.9 Cryptographer/cryptanalyst

NICE framework reference	None.
Functional description	Develops algorithms, ciphers, and security systems to encrypt information/Analyzes and decodes secret messages and coding systems.
Consequence of error or risk	Error, neglect, outdated information, or poor judgment could result in poor cryptologic artefacts, protocols, and systems that will jeopardize intended security of the systems/information they are protecting. Failure to keep up to date on related science and emerging technology carries equal risk.
Development pathway	A highly specialized cyber security activity, this role is filled by experienced and educated professionals who are interested in this field. Opportunities exist for increased specialization and advanced research and studies in the field.
Other titles	None.
Related National Occupational Classifications	21311 – Computer engineers (except software engineers and designers) 21210 – Mathematicians, statisticians and actuaries 21220 – Cyber security specialists 21222 – Information systems specialists
Tasks	▪ Collaborate with key stakeholders to establish an effective cyber security risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop systems for protection of important/sensitive information from interception, copying, modification and/or deletion ▪ Evaluate, analyze, and target weaknesses and vulnerabilities in security systems and algorithms ▪ Develop statistical and mathematical models to analyze data and troubleshoot security problems ▪ Develop and test computational models for reliability and accuracy ▪ Identify, research and test new cryptology theories and applications ▪ Decode cryptic messages and coding systems for the organization ▪ Develop and update methods for efficient handling of cryptic processes ▪ Prepare technical reports that document security processes or vulnerabilities ▪ Provide guidance to management and personnel on cryptical or mathematical methods and applications ▪ Support countermeasures and risk mitigation strategies against potential exploitations of vulnerabilities related to cryptographic systems and, algorithms ▪ Provide insights and guidance related to quantum safety and quantum resistant strategies ▪ Support incident management and post-analysis in the event of a compromise to encryption/cryptographic processes or systems ▪ Develop, deliver, and oversee related cyber security training material and educational efforts related to role ▪ Guide and support encryption specialists as required
Required qualifications for education	Post-secondary university degree in Computer Engineering, Computer Science, or Mathematics. A Master of Science or Doctorate is preferred.
Required training	As required to support organizational technical context (e.g. local tools, processes and procedures)

Required work experience	In addition to academic credentials, entry level roles normally require 3-5 years' experience in an IT/systems domain with familiarity of encryption and key management activities.
Tools & technology	▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures (crypto/encryption related) ▪ Cyber security risk management processes & policies ▪ Privacy and security legislation ▪ Cryptographic algorithms, ciphers and systems ▪ Key management policies and plans ▪ Organizational security infrastructure and reporting systems
Competencies	Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework. Basic application of the following knowledge, skills, and abilities (KSA): ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Information and data requirements including sensitivity, integrity and lifecycle ☐ Applicable computer programming languages ☐ Cyber security program management, measures, and monitoring Advanced application of the following KSAs: ☐ Advanced threats and crypto breaking /decryption capabilities ☐ Applicable laws, legal codes, regulations, policies, and ethics as they relate to cyber security; and ☐ Computer architecture, data structures, and algorithms ☐ Linear/matrix algebra and/or discrete mathematics ☐ Probability theory, information theory, complexity theory and number theory ☐ Cryptography and cryptographic key management concepts ☐ Principles of symmetric cryptography (e.g. symmetric encryption, hash functions, message authentication codes, etc.) ☐ Principles of asymmetric cryptography (asymmetric encryption, key exchange, digital signatures, etc.) ☐ Incident response requirements for cryptographic compromise ☐ Technical report writing
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or "cloud-based" services will require knowledge of responsibilities of the services provider including their cyber security responsibilities relative to organizational cyber security risks particularly as they pertain to data encryption requirements. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the cryptographic tools are affected and automated to support organizational requirements. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools to ensure robust cryptographic systems, ciphers and algorithms. If there are known disparities between the threat and the ability to defend, mitigations should be defined and implemented ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization. The cryptographer/cryptanalyst will play a key role in ensuring quantum safe/resistant design and may be involved in testing of algorithms, encryption protocols and equipment.

Annex C Operate & maintain

This activity area/work category is involved in operating and maintaining system and data security as prescribed within the security architecture and design specifications. All these functions are performed within existing occupations within the Canadian labour market except for those identified below which have become established as occupations with the increasing reliance on Internet connected systems and associated threats.

For the cyber security specialist working in this activity area, not only do they need to bring their technical expertise, they are also required to closely integrate with day-to-day organizational IT operational requirements. This typically involves enhanced client-services and communication skills in addition to the technical competencies.

Click on the Cyber Security Role title to learn more about the knowledge, skills, tasks and competency requirements for each.

Core cyber security roles

- Identity management & authentication support specialist
- Encryption/key management support specialist
- Data privacy specialist/privacy officer

Adjacent roles

- Database administrator
- Data analyst
- Information manager (nice knowledge manager)
- Technical support specialist
- Network operations specialist
- System administrator
- Data systems analyst
- Systems manager (includes system, software and data systems manager roles)

C.1 Identity management & authentication support specialist

NICE framework role	None.
Functional description	Provides ongoing support to identity, credentials, access, and authentication management in support of organizational IT security.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in compromise of the system which, depending on the type of compromise, may have a significant impact on organizational IT systems, capabilities, or functions.
Development pathway	This is an often an entry-level job to the security domain after gained experience with network or system administration access management and credentials. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.
Other titles	▪ Access management analyst ▪ System analyst ▪ Identity, credentials, and access management (ICAM) specialist
Related National Occupational Classifications	21222 – Information systems specialists 22220 – Computer network and web technicians 22221 – User support technicians
Tasks	▪ Identify client requirements and propose technical solutions ▪ Model and map users to resources (e.g. role based) ▪ Install, configure, operate, maintain, and monitor related applications ▪ Deploy, configure and manage user provisioning including identity synchronization, auto-provisioning and automatic access deactivation, self-service security request approvals workflow and consolidated reporting ▪ Configure and manage enterprise and web-based access management solutions (single sign on, password management, authentication & authorization, delegated administration) ▪ Analyze patterns or trends in incidents for further resolution ▪ Manage identity change-request approval processes ▪ Audit, log and report user life-cycle management steps against access control list on managed platforms ▪ Configure and manage federated identity, credentials, access management tools in compliance with security policy, standards, and procedures ▪ Complete tasks related to authorization and authentication in physical and logical environments ▪ Develop, deliver, and oversee related cyber security training material and educational efforts related to role
Required qualifications for education	College diploma in IT field.
Required training	Training in relevant identity, credentials, access management and authentication policies, protocols, tools, and procedures. Developing and applying user credential management system.
Required work experience	Experience in managing directory services and working in a security environment.
Tools & technology	▪ Identity and access management systems ▪ Directory services ▪ Authentication tools and services

	▪ Security event and incident management systems and/or incident reporting systems and networks
Competencies	Knowledge, skills, and abilities (KSA) applied at the basic level: ☐ Identity, credential and access management architectures and standards ☐ Related application life-cycle processes ☐ Mapping and modeling credentials ☐ Policy-based and risk-adaptive access controls ☐ Developing and applying user credential management system ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution KSAs applied at an advanced level: ☐ Network access, identity, and access management protocols, tools and procedures ☐ Authentication, authorization, and access control methods ☐ Install, configure, operate, maintain, and monitor related applications ☐ Developing and applying security system access controls. ☐ Maintaining directory services ☐ Organizational IT user security policies (e.g. account creation, password rules, access control)
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their responsibilities for cyber security systems management ▪ If practiced within the organization, there will be a requirement to fully understand the implications of “bring your own device” (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into identity and access management processes and the related technical and process changes ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as a deep understanding of the implications to authentication protocols and how to defend against potential quantum computing threats.

C.2 Encryption/key management support specialist

NICE framework reference	None.
Functional description	Provides ongoing support to management and maintenance of virtual private networks, encryption, public key infrastructure, and, in some cases, Communications Security (COMSEC) in support of organizational IT security.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in compromise of the system which, depending on the type of compromise, may have a significant impact on organizational IT systems, capabilities, or functions.
Development pathway	This is an often an entry-level job to the security domain after gained experience with network or system administration access management and credentials. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.
Other titles	▪ Access management analyst ▪ System analyst ▪ Identity, credentials, and access management (ICAM) specialist
Related National Occupational Classifications	21222 – Information systems specialists 22220 – Computer network and web technicians 22221 – User support technicians
Tasks	▪ Identify client requirements and propose technical solutions ▪ Install, configure, operate, maintain and monitor related applications ▪ Developing and applying security system access controls ▪ Deploy, configure, and manage encryption/key management services ▪ Establish VPNs ▪ Analyze patterns or trends for further resolution ▪ Manage identity change-request approval processes ▪ Audit, log and report user life-cycle management steps against access control list on managed platforms ▪ Configure and manage federated identity, credentials, access management tools in compliance with security policy, standards, and procedures ▪ Complete tasks related to authorization and authentication in physical and logical environments ▪ Develop, deliver, and oversee related cyber security training material and educational efforts related to role
Required qualifications for education	College diploma in IT field.
Required training	Training in relevant encryption and key management technologies at the applied level.
Required work experience	Experience in managing directory services and working in a security environment.
Tools & Technology	▪ Identity and access management systems ▪ Encryption and key management tools, processes, and procedures ▪ VPN and Wi-fi encryption tools and procedures ▪ Authentication tools and services ▪ Security event and incident management systems and/or incident reporting systems and networks
Competencies	Knowledge, skills, and abilities (KSA) applied at the basic level:

	☐ Cryptanalysis ☐ Cryptography and encryption concepts and methodologies ☐ Symmetric and asymmetric cryptography ☐ Steganography and Steganalysis ☐ National cryptologic authorities (Communications Security Establishment) ☐ Public key infrastructure providers KSAs applied at the advanced level: ☐ Organizational IT user security policies (e.g., account creation, password rules, access control) ☐ Network access, identity, and access management protocols, tools, and procedures ☐ National and international standards ☐ Authentication, authorization, and access control methods ☐ PKI (Public Key Infrastructure), HSM (Hardware Security Module), Digital Certificate, SSL/TLS (Secure Sockets Layer/Transport Layer Security), SSH (Secure Shell), current encryption technologies ☐ Related application life-cycle processes ☐ Digital signatures, digital certificates, and digital certificate management ☐ Authentication protocols ☐ VPN and Protocols ☐ File and Disk Encryption ☐ Encryption Algorithms ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their cyber security responsibilities relative to organizational cyber security risks particularly as they pertain to data encryption requirements ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the cryptographic tools are affected and automated to support organizational requirements ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools to ensure robust cryptographic systems, ciphers and algorithms. If there are known disparities between the threat and the ability to defend, mitigations should be defined and implemented ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization. This includes knowledge and skill of quantum safe algorithms being used, integration and implementation of quantum safe technologies within the organization and testing and evaluation protocols for quantum safe/quantum resistant hardware, software, and protocols.

C.3 Data privacy specialist/privacy officer

NICE framework reference	Oversee and govern, OV-LGA-002, privacy officer/privacy compliance manager
Functional description	Develops, implements, advises on and administers organization privacy compliance program which supports requirements to safeguard personal private information (PPI).
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in a compromise or breach of PPI, which, in addition to the potential individual consequences and liability, may result in significant fines levied for the breach, and loss of reputation and trust.
Development pathway	This role may be supported through technical or non-technical pathways that lead to an entry level role related to privacy/sensitive data management and progress to the policy advisor level. Individuals can further specialize in data security or policy analyst, or senior advisor.
Other titles	▪ Privacy officer ▪ Privacy compliance officer/manager
Related National Occupational Classifications	21222 – Information systems specialists 41400 – Natural and applied science policy researchers, consultants and program officers
Tasks	▪ Interpret and apply laws, regulations, policies, standards, or procedures to specific privacy issues ▪ Conduct periodic impact assessments and ongoing compliance monitoring activities to identify compliance gaps and/or areas of risk to ensure privacy concerns, requirements and responsibilities are addressed ▪ Establish and maintain a mechanism to track access to information within the purview of the organization and as required by law to allow qualified personnel to review or receive such information ▪ Establish and implement an internal privacy audit program, and prepare audit reports that identify technical and procedural findings, and privacy violations, and recommend remedial solutions ▪ Provide advice and guidance on laws, regulations, policies, standards, or procedures to management, personnel, or key departments ▪ Ensure compliance with privacy and cyber security laws, regulations, and policies, and consistent application of sanctions for failure to comply with stated measures for all personnel in the organization ▪ Initiate, facilitate and promote activities to foster privacy awareness within the organization that include the collection, use and sharing of information ▪ Monitor advancements in privacy enhancing technology and ensure the use of technologies complies with privacy and cyber security requirements, including the collection, use and disclosure of information ▪ Review the organization's network security plans and projects to ensure that they are consistent with privacy and cyber security goals and policies ▪ Collaborate with legal counsel and management to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and relevant materials are compliant with legal practices and requirements ▪ Develop, deliver, and oversee privacy training material and awareness activities
Required qualifications for education	Post-secondary education in an applicable field (e.g. Business Administration, Law, Political Science, Social Sciences or equivalent)
Required training	Specialized training in data privacy and security, cyber security foundations, privacy impact analysis, privacy legislation and compliance

Required work experience	Previous training and experience (2-3 years) in policy analysis role related to security or privacy typically required for entry level role
Tools & technology	▪ Privacy and information legislation and policies ▪ Compliance requirements ▪ Reporting mechanisms and templates ▪ Privacy impact assessments/statements of sensitivity ▪ Threat and risk assessments ▪ Data and information requirements ▪ Privacy assessment tools and methodologies
Competencies	Knowledge, skills, and abilities (KSA) applied at the basic level: ☐ A working knowledge of cyber security principles and elements ☐ Technical knowledge to understand data security and integrity, security requirements, and the functional and technical design of networks and system, and cyber security solutions ☐ Data security conceptions and functions, analysis methodologies, testing, and protocols ☐ Cyber security program management, measures and monitoring KSAs applied at an advanced level: ☐ Threat and risk assessment (focused on privacy/data privacy security) ☐ Domestic and international laws, regulations, policies, and procedures ☐ Information security policies, procedures, and regulations ☐ Specific impacts of cyber security gaps and breaches ☐ Monitor advancements in privacy laws and policies ☐ Privacy impact assessments ☐ Privacy disclosure statements based on laws and regulations ☐ Breach reporting
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their responsibilities for protecting sensitive data and responding/reporting potential breaches ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into protection of PPI within the organization and how that needs to be translated into policies, procedures and practices. ▪ Increased use of automated tools by threat actors will likely challenge existing technologies and resources intended to manage protection of PPI. Accordingly, additional tools, processes or training will be required to stay ahead of the threats. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed to PPI/data, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. Encryption used to protect PPI will require knowledge and skills related to ensuring that the PPI remains protected under quantum threat.

Annex D Protect & defend

This occupational sub-group area is involved with cyber security operations that encompass active protection, event detection, incident response and recovery of organizational digital systems. While individuals have been doing related jobs for decades, the key work roles have not been identified as occupations but rather have been typically associated with occupational groups: computer and information systems managers (NOC 20012); cyber security specialists (NOC 21220); and information systems specialists (NOC 21222). Individuals in this, the Protect & Defend work area, are therefore focused on managing cyber security technologies, processes and personnel, that requires unique experience and distinct knowledge, skills and abilities that differentiate them from their other technical colleagues.

Click on the cyber security role title to learn more about the knowledge, skills, tasks and competency requirements for each.

Core cyber security roles

- Information systems security manager – cyber security operations
- Cyber security operations analyst
    - Tier 1 analyst – cyber security operations analysis
    - Tier 2 analyst – malware specialist
    - Tier 3 analyst – threat hunter: management and active defence
- Cyber security incident responder
- OT incident responder
- Cyber security operations technician
- Vulnerability assessment analyst
- Penetration tester
- Digital forensics analyst

Adjacent roles

None

D.1 Information systems security manager – cyber security operations

NICE framework reference	Oversee & govern, OV-MGT-001, information systems security manager,
Functional description	Plans, organizes, directs, controls and evaluates the activities of the cyber security operations centre within an organization. Employed throughout the public and private sectors.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in catastrophic failure of organizational IT and data systems and associated implications to the organizational functions which rely on those systems.
Development pathway	Typically follows 5 to 10 years in related roles in IT operations or cyber security operations or similar employment. This role supports increasing management level responsibilities based on a solid technical foundation in cyber security operations or a related work role (e.g. vulnerability assessment & management, digital forensics, cyber security analysis).
Other titles	▪ Cyber security operations manager (CSOC) ▪ Security operations (SOC) manager ▪ Cyber security manager ▪ Information systems security manager (cyber security operations)
Related National Occupational Classifications	20012 – Computer and information systems managers
Tasks	▪ Lead and manage SOC personnel including hiring, training, staff development, performance management and conducting annual performance reviews ▪ Maintain currency in cyber security threat landscape and security technologies ▪ Develop and implement an integrated SOC program that meets legislative and organizational requirements ▪ Develop and publish SOC governance mechanisms (policies, procedures and guidance) ▪ Develop and implement a measurement and quality assurance program ▪ Monitor and report on SOC program effectiveness to senior management ▪ Monitor and manage relationships with security services and technologies providers ▪ Provide strategic assessments on threat landscape, SOC technology trends, and emerging security technologies ▪ Seek and interpret threat intelligence based on organizational risks ▪ Manage cyber security events and incidents within the SOC ▪ Provide reports, briefings and risk-based recommendations on routine and non-routine cyber security events and incidents including responding to organizational crises (e.g. business systems shut-downs) ▪ Lead and facilitate lessons learned, post-mortem and best practices activities on cyber security events and incidents ▪ Develop and oversee implementation of action plans in support of continuous improvement of cyber security posture
Required qualifications for education	Bachelor's degree in computer science or related discipline or college diploma in IT field.
Required training	Cyber security operations training with industry-level certification in related field (e.g. network security, incident handling, threat detection and mitigation, digital forensics). Security operations team management training or equivalent development and experience.

	Training on organization relevant tools and technology that support cyber security operations
Required work experience	Significant (5-10 years) experience in IT domain with 3-5 years' experience in cyber security operations or related domain.
Tools & technology	▪ Incident management processes and procedures ▪ Defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms ▪ Security event and incident management systems and/or incident reporting systems and networks, ▪ Authentication software and systems, ▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used ▪ Security services provided if applicable
Competencies	Underpinning this occupation are those competencies demonstrated for an activity manager as well as the Information Systems Security Manager within the NICE framework. Specifically, this work requires: Basic level of application of the following knowledge, skills, and abilities (KSA): □ Preventative technical, operational and management controls available and organizational responsibilities for those controls Advanced level of application of the following KSAs □ Organizational threats and vulnerabilities including: ○ Cyber security threat landscape and adapting SOC processes to meet the evolving threat ○ Vulnerability management requirements and the range of potential mitigations available when a vulnerability management protocol does not exist □ Defensive systems management including: ○ Firewalls, anti-virus, intrusion detection and protection systems ○ Required manual and automated settings ○ Monitoring, testing and maintenance requirements □ Developing, implementing, and managing: ○ Incident management processes and policies ○ Incident management responsibilities ○ Incident monitoring and reporting practices in accordance with legislative requirements and organizational policies ○ Post-incident analyses and reports ○ Organizational lessons learned in support of continuous improvement □ Supplier management (if IT or security services are outsourced): ○ Roles and responsibilities of security controls of supplied services ○ Roles and responsibilities of supplier in incident management and reporting ○ Incident monitoring, assessment and reporting requirements during the lifecycle of the contract ○ Organizational responsibilities in response to a compromise/breach on the part of the supplier ○ Managing supplier communications and relations during a crisis □ Advising on security requirements, policies, plans and activities □ Drafting and providing briefings and reports to different audience levels (users, managers, executives) □ Maintaining broader security situational awareness □ Self-awareness regarding knowledge, skills and abilities required to respond to business, threat and technical changes □ Continuous learning to support currency in knowledge of emerging threats, technological innovations in security, and the changing cyber security landscape.
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or "cloud-based" services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cyber security incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of "bring your own device" (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential

	compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. Understanding quantum threat capabilities and knowledge and skills related to implementing a quantum safe strategy will be required.

D.2 Cyber security operations analyst

Note: This role includes the following:

- Cyber security operations analyst
- Malware specialist
- Threat hunter: management and active defense

NICE framework reference	Protect and defend, cyber defence analyst, PR-CDA-001
Functional description	Front-line cyber security operations center operator responsible for monitoring and maintaining IT security devices and is often responsible for initial detection, incident response and mitigation.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in catastrophic failure of organizational IT and data systems and associated implications to the organizational functions which rely on those systems.
Development pathway	This is a common entry-level job within the security operations centre (SOC). With additional training and experience there is potential for more technically or operationally focused roles in cyber security operations (e.g. vulnerability assessment & management, digital forensics, threat analytics and malware analysis) as well as management opportunities. Note that Tier 2 and Tier 3 roles may require more extensive training and education in addition to relevant experience. Often a computer science or computer engineering degree is a pre-requisite given the level of knowledge and skill required in more complex tasks. However, there are many that have progressed from cyber security analyst positions to advanced cyber security roles without a related degree.
Other titles	▪ SOC operator ▪ Cyber security Operator ▪ Infrastructure security analyst ▪ Network security analyst ▪ Network security administrator ▪ Data security analyst
Related National Occupational Classifications	21222 – Information systems specialists 21311 – Computer engineers (except software engineers and designers) 21231 – Software engineers and designers
Tasks	▪ Identify and analyze technical threats to, and vulnerabilities of, networks ▪ Identify, contain, conduct initial mitigations and report system compromises ▪ Review, analyze, and/or apply Internet security protocols, cryptographic algorithms, directory standards, networking protocols, network hardening, technical IT security controls, IT security tools and techniques, OS, intrusion detection/protection systems, firewalls, routers, multiplexers and switches, and wireless devices ▪ Analyze security data and provide alerts, advisories and reports ▪ Install, configure, integrate, adjust, operate, monitor performance, and detect faults on security devices and systems ▪ Conduct impact analysis for new software implementations, major configuration changes and patch management ▪ Develop proof-of-concept models and trials for IT security products and services ▪ Troubleshoot security products and incidents

	▪ Design/develop IT security protocols ▪ Complete tasks related to authorization and authentication in physical and logical environments ▪ Develop options and solutions to meet the security-related project objectives ▪ Identify the security products and its configuration to meet security-related project objectives ▪ Implement and test configuration specifications ▪ Develop configuration and operational build books ▪ Review, develop and deliver relevant training material
Required qualifications for education	College diploma in IT field with specialization in IT/cyber security, network security or similar.
Required training	Cyber security operations training with industry-level certification in related field (e.g. security operations, network security, threat detection and mitigation, security appliance operations). More advanced training required for Tier 2 and III analysts.
Required work experience	Initial experiential requirement is to have been successful working in an IT environment and technical team setting.
Tools & technology	▪ Incident management processes and procedures ▪ Defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms ▪ Security event and incident management systems and/or incident reporting systems and networks
Competencies	In larger SOCs there may be the opportunity to progress from Tier 1 to Tier 2 analyst. Tier 3 analysts are rare and almost exclusively employed in national security and military contexts. The required competencies for Tier 1 and 2 are provided below. **For Tier 1 - Cyber security operations analyst** The following knowledge, skills, and abilities (KSA) are applied at a basic level: ☐ Network security administration and management ☐ Network security architecture ☐ Hardware and firmware security ☐ Software defined security and application security ☐ Virtualization and Virtual Private Network (VPN) security ☐ Cloud-based security ☐ Wireless/mobile device security ☐ IT security zoning ☐ Encryption and cryptography including key management concepts and principles ☐ Vulnerability scanning and analysis ☐ Vulnerability management tools, processes and procedures ☐ Web application security ☐ Configuration and operational build books ☐ System acquisitions and projects ☐ Legal and ethical responsibilities associated with cyber security operations including conduct of investigations, privacy, and preservation of evidence ☐ Writing and briefing on technical matters (e.g. incident reports, technical reports, etc.) for managerial level understanding The following KSA are applied at an advanced level: ☐ Network security appliance concepts, operation and configuration (equipment specific based on role - network, server and desktop cyber defence systems and/or appliances) ☐ Types of intrusions and indicators of compromise (IoCs) ☐ Sources of threat information ☐ Common threat actor tactics, techniques, and procedures (TTPs) ☐ Incident management processes, responsibilities and authorities

	□ Intrusion detection and prevention methodologies, tools and systems □ Intrusion analysis and mitigation techniques □ Basic malware analysis **For Tier 2 analyst - malware specialist** The following KSA are applied at an advanced level. All of the above plus: □ Persistent and sophisticated threat TTPs □ Cyber defence tools, techniques and procedures □ Development and testing of network security appliances (including scripts and coding). □ Advanced malware analysis and reverse malware engineering □ Implementing advance security controls in response to advanced persistent threats □ Advanced incident response and recovery activities **For Tier 3 analyst - threat hunter: management and active defence** The following KSA are applied at an advanced level: □ Advanced threat management □ Advanced threat actor TTPs including specialization of persistent threat actors (e.g. nation state, organized crime) □ Interpreting/synthesizing classified/sensitive threat intelligence from multiple sources □ Legal and ethical responsibilities associated with active defence techniques □ Exploitation analysis □ Threat hunting and active defence frameworks □ Developing complex courses of action including risk assessment and mitigation plan □ Active defence tactics, tools and procedures including advanced threat countermeasures and counter-countermeasures □ Adversarial thinking □ Developing, testing and deploying technical tools within an active defence framework to protect organizational information and systems at risk
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cyber security incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of “bring your own device” (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.

D.3 Cyber incident responder

Operational technology (OT) incident responder

NICE framework reference	Protect and defend, cyber defence incident responder, PR-CIR-001
Functional description	Provides immediate and detailed response activities to mitigate or limit unauthorized cyber security threats and incidents within an organization. This includes planning and developing courses of action; prioritizing activities; and supporting recovery operations and post-incident analysis.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in catastrophic failure of organizational IT and data systems and associated implications to the organizational functions which rely on those systems.
Development pathway	This is a common entry-level job within the security operations centre (SOC). With additional training and experience there is potential for more technically or operationally focused roles in cyber security operations such as vulnerability assessment & management, digital forensics, threat analytics and malware analysis.) as well as management opportunities.
Other titles	▪ Cyber security incident responder ▪ Security operations centre - incident handler ▪ Cyber security first responder ▪ Operational technology security incident responder
Related National Occupational Classifications	21220 – Cyber security specialists 21311 – Computer engineers (except software engineers and designers) 21231 – Software engineers and designers
Tasks	These tasks apply equally to IT and OT systems. ▪ Perform real-time cyber defense incident handling tasks (e.g. forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) ▪ Conduct security triage to identify and analyze cyber incidents and threats ▪ Actively monitor networks and systems for cyber incidents and threats ▪ Conduct risk analysis and security reviews of system logs to identify possible cyber threats ▪ Conduct analysis and review, and/or apply network scanners, vulnerability assessment tools, network protocols, Internet security protocols, intrusion detection systems, firewalls, content checkers and endpoint software ▪ Collect and analyze data to identify cyber security flaws and vulnerabilities and make recommendations that enable prompt remediation ▪ Develop and prepare cyber defence incident analysis and reporting ▪ Define and maintain tool sets and procedures ▪ Develop, implement, and evaluate prevention and incident response plans and activities, and adapt to contain, mitigate or eradicate effects of cyber security incident ▪ Provide incident analysis support on response plans and activities ▪ Conduct research and development on cyber security incidents and mitigations ▪ Create a program development plan that includes security gap assessments, policies, procedures, playbooks, and training manuals ▪ Review, develop and deliver relevant training material
Required qualifications for education	College diploma in IT field with specialization in IT/cyber security, network security or similar.

Required training	Cyber security operations training with industry-level certification in related field (e.g. security operations, network security, threat detection and mitigation, security appliance operations). Specialized training required for Operational Technology and related systems.
Required work experience	Initial experiential requirement is to have been successful working in an IT environment and technical team setting.
Tools & technology	▪ Incident management processes and procedures ▪ Defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms ▪ Security event and incident management systems and/or incident reporting systems and networks
Competencies	**Cyber security incident responder** The following knowledge, skills, and abilities (KSA) are applied at a basic level: ☐ Network security administration and management ☐ Network security architecture ☐ Hardware and firmware security ☐ Software defined security and application security ☐ Virtualization and VPN security ☐ Cloud-based security ☐ Wireless/mobile device security ☐ IT security zoning ☐ Encryption and cryptography including key management concepts and principles ☐ Vulnerability scanning and analysis ☐ Vulnerability management tools, processes and procedures ☐ Web application security ☐ Configuration and operational build books ☐ System acquisitions and projects ☐ Legal and ethical responsibilities associated with cyber security operations including conduct of investigations, privacy, and preservation of evidence ☐ Writing and briefing on technical matters (e.g. incident reports, technical reports, etc.) for managerial level understanding ☐ Business continuity and disaster response basics The following KSA are applied at an advanced level: ☐ Network security appliance concepts, operation and configuration (equipment specific based on role - network, server and desktop cyber defence systems and/or appliances) ☐ Types of intrusions and indicators of compromise (IoCs) ☐ Sources of threat information ☐ Common threat actor tactics, techniques, and procedures (TTPs) ☐ Incident management processes, responsibilities and authorities ☐ Intrusion detection and prevention methodologies, tools and systems ☐ Intrusion analysis and mitigation techniques ☐ Basic malware analysis ☐ Cyber security investigations and evidence preservation **For operational technology incident responder** In addition to the relevant KSAs above, the follow applied at the basic level: ☐ OT systems software and hardware, programmable logic controllers, and digital and analog relaying ☐ Threat and risk assessment to Internet connected OT (including implications and assessment of IoT devices) ☐ Legal and compliance requirements including organizational responsibilities for workplace and public safety related to OT/ production ☐ Telemetry systems, data communications, data acquisition and process control

	□ Operating systems, networking, and communications systems concepts □ Electrical distribution networks, power system equipment, transformer station operation and electrical theory □ Database management systems and applications □ Measures or indicators of OT system performance, availability, capacity, or configuration problems □ Analysis tools and network protocols □ Diagnostic tools and fault identification techniques
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or "cloud-based" services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cyber security incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of "bring your own device" (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.

D.4 Cyber security operations technician

NICE framework reference	Protect and defend, PR-INF-001, cyber security defence infrastructure support
Functional description	Tests, implements, deploys, maintains, and administers the security operations infrastructure hardware and software.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in security system failure or system compromise which may have a significant impact on organizational IT systems, capabilities or functions.
Development pathway	This is an often an entry-level job to the security domain after gained experience in technical, network administrative, or other similar functions. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.
Other titles	▪ Security infrastructure support specialist/technician ▪ Security systems analyst ▪ Security systems technician ▪ Security control analyst
Related National Occupational Classifications	21220 - Cyber security specialist 22220 – Computer network and web technicians 22221 – User support technicians
Tasks	▪ Actively monitor security system performance, troubleshoot and resolve hardware or software interoperability issues, and system outages and faults ▪ Install, configure, and maintain security system software, hardware, and peripheral equipment ▪ Develop, conduct, and maintain incident reports and vulnerability and impact assessments ▪ Develop and maintain tracking and solution database ▪ Analyze and recommend improvements and changes to support improved security operations ▪ Audit, log and report life-cycle management activities ▪ Administer security system accounts, privileges, and access to systems and equipment ▪ Conduct asset management or inventory control of system and equipment resources ▪ Develop, deliver, and oversee training material and educational efforts
Required qualifications for education	Post-secondary education (degree or diploma in related computer science or IT field
Required training	Training in cyber security systems, security systems operations and vendor-based tools (e.g. intrusion detection systems, firewalls, anti-virus, incident management, etc.)
Required work experience	2 – 3 years in network operations and security
Tools & technology	▪ Cyber security systems tools, logs, and procedures ▪ Organizational policies and directives ▪ Security event and incident management systems and/or incident reporting systems and networks
Competencies	Knowledge, skills, and abilities (KSA) applied at the basic level: □ Threats to information systems and their security □ Network security architecture concepts, protocols, components, and principles (e.g. application of defense-in-depth).

	☐ Basic system, network, and OS hardening techniques. ☐ Transmission records and modes (e.g. Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)) ☐ Network traffic analysis (tools, methodologies, processes) ☐ Identity, credential and access management architectures and standards ☐ Cyber security incident management policy, procedures and practices ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution KSAs applied at an advanced level: ☐ Cyber security systems test procedures, principles, and methodologies ☐ Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications ☐ Install, configure, operate, maintain and monitor related applications ☐ Cyber security infrastructure troubleshooting, analysis and remediation ☐ Cyber security systems policies, account management and controls
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their responsibilities for cyber security systems management. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of “bring your own device” (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into identity and access management processes and the related technical and process changes. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.

D.5 Vulnerability assessment analyst

NICE framework reference	Protect and defend, PR-VAM-001, vulnerability assessment (VA) Analyst
Functional description	Scans applications and operating systems to identify flaws, and vulnerabilities; and conducts and presents vulnerability assessments on an organization's networks and systems.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in mis-identifying or not detecting vulnerabilities which could be comprised. This may have a significant impact on organizational IT systems, capabilities or functions.
Development pathway	This is often a Tier 2 position within a cyber security operations environment that is normally preceded by 2-3 years in a network or operational security role. This can lead to increased specialization as a vulnerability analyst, red/blue team leader, penetration tester or management roles.
Other titles	▪ Vulnerability tester ▪ Vulnerability assessor ▪ Vulnerability assessment manager
Related National Occupational Classifications	21220 – Cyber security specialist 21311 – Computer engineers (except software engineers and designers) 21231 – Software engineers and designers
Tasks	▪ Identify critical flaws in applications and systems that cyber actors could exploit ▪ Conduct vulnerability assessments of relevant technology (e.g. computing environment, network and supporting infrastructure, and applications) ▪ Prepare and present comprehensive vulnerability assessments ▪ Conduct network security audits and scanning ▪ Maintain deployable cyber defense audit toolkit (e.g. specialized cyber defense software and hardware) to support cyber defense operations ▪ Prepare audit reports that identify technical and procedural findings, and make recommendations on corrective strategies and solutions ▪ Conduct and/or support authorized penetration testing on organization networks and systems ▪ Define and review requirements for information security solutions ▪ Make recommendations on the selection of cost-effective security controls to mitigate risks ▪ Develop, deliver, and oversee training material and educational efforts
Required qualifications for education	Post-secondary education (degree or diploma) in related computer science or IT field.
Required training	Training in cyber security systems, vulnerability assessment and analysis. Vendor-based vulnerability system training.
Required work experience	2 – 3 years in a network or cyber security operations role.
Tools & technology	▪ Organizational security policies, procedures and practices ▪ VA tools ▪ Vulnerability management policies, processes and practices ▪ Common vulnerability databases
Competencies	KSAs applied at the basic level:

	☐ Advanced threat actor tools, techniques and protocols ☐ Penetration testing principles, tools, and techniques ☐ Risk management processes for assessing and mitigating risks ☐ System administration concepts ☐ Cryptography and cryptographic key management concepts ☐ Cryptology ☐ Identifying security issues based on the analysis of vulnerability and configuration data ☐ Vulnerability management policies, processes and practices KSAs applied at an advanced level: ☐ VA planning and scheduling including system risks and mitigations ☐ System and application security threats and vulnerabilities ☐ System administration, network, and operating system hardening techniques ☐ Packet analysis using appropriate tools ☐ Conducting vulnerability scans and recognizing vulnerabilities in security systems ☐ Conducting vulnerability/impact/risk assessments ☐ Reviewing system logs to identify evidence of past intrusions ☐ Using network analysis tools to identify vulnerabilities
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-base” services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cyber security incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of “bring your own device” (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy, understanding system vulnerabilities and how to mitigate quantum-related threats.

D.6 Penetration Tester

NICE framework reference	None.
Functional description	Conducts formal, controlled tests and physical security assessments on web-based applications, networks, and other systems as required to identify and exploit security vulnerabilities.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in mis-identifying or not detecting vulnerabilities which could be comprised. This may have a significant impact on organizational IT systems, capabilities or functions.
Development pathway	This is often a Tier 2/3 position within a cyber security operations environment that is normally preceded by significant experience (3-5 years) in a cyber security operations role including employment within Vulnerability Analysis, Malware Analysis or Technical Analysis of security systems. This is an advanced technical role, which can lead to increasing technical specialization, red team leadership or management roles.
Other titles	▪ Security testing and evaluation specialist ▪ Advanced vulnerability assessment analyst
Related National Occupational Classifications	21220 – Cyber security specialist 21311 – Computer engineers (except software engineers and designers) 21231 – Software engineers and designers
Tasks	▪ Complete penetration tests on web-based applications, network connections, and computer systems to identify cyber threats and technical vulnerabilities ▪ Conduct physical security assessments of an organization's network, devices, servers, and systems ▪ Develop penetration tests and the tools needed to execute them (e.g. standards, risks, mitigations) ▪ Investigate for unknown security vulnerabilities and weaknesses in web applications, networks, and relevant systems that cyber actors can easily exploit ▪ Develop and maintain documents on the results of executed pen testing activities ▪ Employ social engineering to uncover security gaps ▪ Define and review requirements for information security solutions ▪ Analyze, document, and discuss security findings with management and technical staff ▪ Provide recommendations and guidelines on how to improve upon an organization's security practices ▪ Develop, deliver, and oversee training material and educational efforts
Required qualifications for education	Post-secondary education (degree or diploma in related computer science or IT field).
Required training	Training in vulnerability analysis and penetration testing tools, techniques and procedures.
Required work experience	2-3 years' experience in an advanced cyber security operations role, preferably with VA experience.
Tools & technology	▪ Organizational security policies, procedures and practices ▪ Organizational systems map and network architecture ▪ VA tools ▪ Vulnerability management policies, processes and practices ▪ Common vulnerability databases ▪ Penetration testing tools and protocols

Competencies	Knowledge, skills, and abilities (KSA) applied at an advanced level: □ Network security architecture □ Advanced threat actor tools, techniques and protocols □ Penetration testing principles, tools, and techniques □ Risk management processes for assessing and mitigating risks □ System administration concepts □ Cryptography and cryptographic key management concepts □ Cryptology □ Identifying security issues based on the analysis of vulnerability and configuration data □ Vulnerability management policies, processes and practices □ Penetration test planning and scheduling including system risks and mitigations □ System and application security threats and vulnerabilities □ System administration, network, and operating system hardening techniques □ Packet analysis using appropriate tools □ Conducting vulnerability scans and recognizing vulnerabilities in security systems □ Conducting vulnerability/impact/risk assessments □ Reviewing system logs to identify evidence of past intrusions □ Using network analysis tools to identify vulnerabilities
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or “cloud-based” services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cyber security incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of “bring your own device” (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy, understanding system vulnerabilities and how to mitigate quantum-related threats.

D.7 Digital Forensics Analyst

NICE framework reference	Investigate, cyber defence forensic analyst, INV-FOR-002
Functional description	**The following role-based description is for security operations only and does not include criminal or audit forensics functions which are provided for within the related law enforcement or audit related occupations**. Conducts digital forensics to analyze evidence from computers, networks, and other data storage devices. This includes investigating and preserving electronic evidence; planning and developing tools; prioritizing activities; and supporting recovery operations and post-incident analysis.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in a failure to determine the source and mitigate a compromise, but additionally may result in impacts to organizational information systems to include criminal charges or civil litigation.
Development pathway	This is often a Tier 2/3 position within a cyber security operations environment that is normally preceded by a minimum of 2-3 years in a network or operational security role including as a malware analyst. This can lead to increased specialization within digital forensics or security assessment activities as well as red/blue team leader, penetration tester or management roles.
Other titles	▪ Digital forensics investigator (normally reserved for cybercrime environment) ▪ Digital forensics examiner (normally reserved for cyber audit environments)
Related National Occupational Classifications	21220 – Cyber security specialist 21311 – Computer engineers (except software engineers and designers) 21231 – Software engineers and designers
Tasks	▪ Perform real-time cyber defence incident investigations (e.g. forensic collections, intrusion correlation and tracking, and threat analysis) ▪ Investigate security incidents as per terms of reference ▪ Plan forensics analysis activities for cyber incidents ▪ Collect and analyze intrusion artifacts (e.g. source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents ▪ Identify and accurately report on digital forensic analysis artifacts ▪ Capture and analyze network traffic associated with malicious activities using network monitoring tools ▪ Contribute to post-analysis on security incidents and make recommendations based on forensics activities ▪ Develop and maintain investigative and technical reports ▪ Provide technical assistance on digital evidence matters to appropriate personnel ▪ Compile evidence for legal cases, and provide expert testimony at court proceedings ▪ Manage digital evidence in accordance with appropriate chain of custody requirements ▪ Identify and manage secure analysis infrastructure/laboratory ▪ Operate digital forensics systems (as required based on function and systems available) ▪ Prepare and review forensics policies, standards, procedures and guidelines ▪ Develop, deliver, and oversee training material and educational efforts
Required qualifications for education	Post-secondary education (degree or diploma in related computer science or IT field).

Required training	Training in digital forensics tools, techniques and procedures. Also, depending on the organizational technical context and systems/devices used, specialized digital forensics training may be required (e.g. mobile device, digital media, etc.)
Required work experience	2-3 years' experience in an advanced cyber security operations role, preferably with malware analysis experience in "dead box" and active environments.
Tools & technology	▪ Organizational security policies, procedures and practices ▪ Organizational systems map and network architecture ▪ Digital forensics tools, techniques and procedures ▪ Malware analysis tools ▪ Security Event and Incident Management System ▪ Common vulnerability databases ▪ Security investigation terms of references, responsibilities and limits of authority
Competencies	Knowledge, skills, and abilities (KSA) applied at an advanced level: ☐ Threat actor tools, techniques and procedures ☐ Incident response and handling methodologies ☐ Security Event and Incident Management System ☐ Digital forensics methodologies, processes and practices ☐ Anti-forensics tactics, techniques, and procedure ☐ Processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data ☐ Seizing and preserving digital evidence ☐ Applicable laws, regulations, policies and ethics as they relate to investigations and governance ☐ Legal rules of evidence and court procedures, presentation of digital evidence, testimony as an expert witness ☐ System or device specific forensics (e.g. memory, active director, mobile device, network, computer (dead box), etc.) ☐ Malware analysis tools and techniques ☐ Reverse engineering ☐ Deployable digital forensics capabilities ☐ Types of digital forensics including tools, techniques and procedures (organization and information system dependent) which may include the following forensics for: ○ computer ○ network and active directory ○ mobile devices ○ digital media (image, video, audio) ○ memory
Future trends affecting key competencies	▪ The increased reliance on virtualized and/or "cloud-based" services will require knowledge of responsibilities of the services provider including their responsibilities for cyber security systems management. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of "bring your own device" (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into identity and access management processes and the related technical and process changes. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment.

	▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.

Annex E Cyber adjacent roles

In conjunction with the core roles that define the cyber security occupation discussed in this publication, there are a number of adjacent roles that have cyber security responsibilities which typically form only part of their overall responsibilities within an organization. While often only employed in cyber security in a part-time capacity, the scope and extent to which they perform these roles will vary based on organizational size, type and degree of IT/Internet enabled infrastructure. For example, for larger IT enabled organizations, all of the following roles may apply. For smaller organizations that are not overly reliant on IT or Internet connectivity for the conduct of their business, it's likely that a majority of the technical expertise and services will be outsourced. Accordingly, the remaining non-technical cyber security responsibilities will be distributed within the organization.

This table briefly outline common cyber security adjacent roles, the related NICE framework ID if applicable, the associated National Occupation Classification (NOC) and the main cyber security responsibilities. Assuming that the majority of individuals in such roles already have the required competencies for their primary roles and functions, only cyber security functions are provided with key competencies. Specifically, for the existing workforce community and, in particular, educators, these should guide discussion around adapting training and education programs to more closely reflect the cyber security realities of the Canadian labour market.

Note that the protect & defend category is not included in the figure as that activity area/work category is exclusively employed in cyber security.

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
Oversee & govern	CEO/senior leadership/owner	OV-EXL-001	00011 00012	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.	Strategic cyber planning Business & threat context Risk management Cyber legal and policy context Cyber compliance requirements Cyber security controls (management, operational, technical) Cyber security program management
	Chief Information Officer/Chief Technical Officer	None	00011 00012 20010 20012	Leads and executes decision-making authorities related to organizational IT, infrastructure and technical services. This often includes cyber security services.	Strategic cyber planning Business & threat context Risk management

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
					Cyber legal and policy context Cyber compliance requirements Cyber security controls (management, operational, technical) Cyber security program management Cyber security assessment and measurement
	Cyber legal advisor	OV-LGA-001	41101 42200	Provides legal advice and recommendations on relevant topics related to cyber law.	Cyber legal and policy context Cyber compliance requirements Threat context
	Privacy officer/privacy compliance manager	OV-LGA-002	20012	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.	Cyber legal and policy context Cyber compliance requirements Threat context Privacy relevant security controls
	Communications security (comsec) manager	OV-MGT-002	10030 20012	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).	Security program management BCP/DRP Supply chain risk management COMSEC policies, guidelines and management requirements COMSEC accounting Encryption/PKI infrastructure and applications COMSEC incident management
	Cyber Workforce Developer and Manager	OV-SPP-001	41321	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to	Cyber security career paths Cyber security labour market information and sources Cyber security occupational standards

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
				cyberspace policy, doctrine, materiel, force structure, and education and training requirements.	Cyber security certifications and accreditations Assessing cyber security competencies
	Cyber instructional curriculum developer	OV-TEA-001	41200 41210 43109	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.	Relevant cyber domain knowledge (topic-based) Assessing cyber security competencies
	Cyber instructor	OV-TEA-002	41200 41210 43109	Develops and conducts training or education of personnel within cyber domain.	Relevant cyber domain knowledge (topic-based) Assessing cyber security competencies
	Cyber Policy and Strategy Planner	OV-SPP-002	40011 41400	Develops and maintains cyber security plans, strategy, and policy to support and align with organizational cyber security initiatives and regulatory compliance.	Cyber security program management BCP/DRP Cyber legal and policy context Business & threat context Cyber policy planning & development Cyber security controls (management, operational, technical)
	Program manager	OV-PMA-001	00011 00012 20010	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.	Cyber security risk management Business and threat context Cyber security program management BCP/DRP Supply chain risk management Cyber maturity models Cyber security standards Cyber security assessment and measurement
	IT project manager	OV-PMA-002	20010 20012	Directly manages IT projects.	Threat and risk assessment Cyber security risk management

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
					Business and threat context Technical context Cyber systems integration Cyber security project management Cyber procurement requirements Supply chain risk management Cyber security standards Cyber security assessment and measurement Cyber security controls (management, operational, technical)
	Product support manager	OV-PMA-003	20010 20012	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.	Threat and risk assessment Cyber security risk management Business and threat context Technical context Cyber systems integration Cyber security project management Supply chain risk management Cyber security standards Cyber security controls (management, operational, technical) Cyber security product testing and evaluation processes Cyber security product lifecycle management
	IT investment/portfolio manager	OV-PMA-004	20010 20012	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.	Cyber security risk management Business and threat context Cyber security program management Supply chain risk management

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
					Cyber maturity models Cyber security standards Cyber security assessment and measurement Cyber security product lifecycle management
	IT program auditor	OV-PMA-005	20010 20012	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.	Cyber security audit policies, practices and procedures Threat and risk assessment Cyber security risk management Business and threat context Technical context Legal and policy context Compliance requirements Cyber procurement requirements Supply chain risk management Cyber security standards Cyber security assessment and measurement Cyber security controls (management, operational, technical) Vulnerability assessment Cyber security testing and evaluation processes
	Business analyst	None	11201 21221 41401	Analyzes and identifies needs, recommends solutions that deliver business value to stakeholders.	Cyber security governance, roles and responsibilities Cyber security risk management Business and threat context Technical context Legal and policy context

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
					Compliance requirements Cyber procurement requirements Supply chain risk management Cyber security standards Cyber security assessment and measurement Cyber security controls (management, operational, technical) Vulnerability assessment Cyber security testing and evaluation processes
	Financial analyst	None	11101	Collects and analyzes financial information and risks. Provides related financial estimates, forecasts and trends. Provides advice to support financial and investment activities.	Cyber security risk management Business and threat context Legal, policy and financial context Cyber security program requirements Cyber security procurement and acquisition Cyber security assessment and measurement
	Risk analyst	None	41401	Collects and analyzes organizational risks. Provides related risk assessments and advice on mitigations.	Cyber security risk management Threat and risk assessment methodologies Business and threat context Legal, policy and financial context Cyber security program requirements
	Communications Specialist	None	10022 11202	Plan, organize, and develop advertising, marketing and public relations.	Cyber threat context Legal and policy context Compliance requirements BCP/DRP

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
					Communications during a cyber incident (crisis communications)
	Webmaster/Online Communications Manager	None	21233 21234	Researches, designs, develops and produces Internet and Intranet sites and web-based media.	Cyber security threats Web application vulnerabilities Software testing and evaluation Cyber security incident response requirements
	Learning and Development Specialist	None	41200 41210 43109	Develops, plans, coordinates, and evaluates organizational and individual learning and development programs and activities	Organizational cyber security requirements Cyber security roles and responsibilities Cyber security career pathways Assessing cyber security competencies
	Business Continuity/ Resiliency Planner	None	11101 21220	Identify, coordinate and oversee development of a business continuity plan to support organizational resilience to fraud, financial crime, cyber-attack, terrorism, and infrastructure failure.	Threat and risk assessment Cyber security risk management Business and threat context Technical context Organizational cyber security requirements Cyber security roles and responsibilities Cyber security plans, processes and procedures Cyber security incident management Cyber security controls (management, operational, technical)
	Procurement Specialist	None	12102	Identify and acquire general and specialized equipment, materials, land or access rights and business services for use or for further processing by their organization.	Threat and risk assessment Cyber security risk management Business and threat context Technical context

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
					Cyber security project management Supply chain risk management Cyber security standards Cyber security controls (management, operational, technical) Cyber security product testing and evaluation processes Cyber security product lifecycle management
Design & develop (securely provision in the NICE)	Authorizer (often CIO or system owner)	SP-RSK-001	00011 00012 20010	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 (CNSSI 4009).	Strategic cyber planning Business & threat context Risk management Cyber legal and policy context Cyber compliance requirements Cyber security controls (management, operational, technical) Cyber security program management Cyber security assessment and measurement
	Enterprise Architect	SP-ARC-001	20010 21311	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops IT rules and requirements that describe baseline and target architectures.	Organizational cyber goals Cyber security architecture and design Cyber security engineering Threat and risk assessment Cyber legal and policy context Cyber compliance requirements Cyber security controls (management, operational, technical) Cyber systems integration Encryption/PKI

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
	Software developer	SP-DEV-001	21232 22302 22312	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.	System and software vulnerabilities Software security testing and evaluation Software security tools, techniques and procedures Vulnerability assessment and penetration testing practices and tools Identity, credentials and authentication
	Systems requirements planner	SP-SRP-001	21311 21220 21222	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions	Organizational cyber goals Cyber security architecture and design Cyber security engineering Threat and risk assessment Cyber legal and policy context Cyber compliance requirements Cyber security controls (management, operational, technical) Cyber systems integration Encryption/PKI Cyber security standards Cyber security assessment and measurement Cyber security product lifecycle management Identity, credentials and authentication
	System testing and evaluation specialist	SP-TST-001	21220 21222 21230 21231 22222	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.	System and software vulnerabilities System and software security testing and evaluation Software security tools, techniques and procedures Vulnerability assessment and penetration testing practices and tools

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
					Cyber security standards Cyber security assessment and measurement
	Systems developer	SP-SYS-002	21311 21231 21230	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.	Cyber security architecture and design Cyber security engineering Threat and risk assessment Cyber legal and policy context Cyber compliance requirements Cyber security controls (management, operational, technical) Cyber systems integration Encryption/PKI Cyber security standards Cyber security assessment and measurement Cyber security product lifecycle management Identity, credentials and authentication
	Web developer	None	21234	Researches, designs, develops and produces Internet and Intranet sites and web-based media.	Cyber security threats Web application vulnerabilities Software testing and evaluation Cyber security incident response requirements
Operate & maintain	Database administrator	OM-DTA-001	21223	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.	System and data security Data systems threats and vulnerabilities Disaster Recovery Planning Data back-up and recovery Identity, credentials and authentication

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
	Data analyst	OM-DTA-002	21223	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.	System and data security Data systems threats and vulnerabilities Disaster Recovery Planning Data back-up and recovery Identity, credentials and authentication
	Information manager (NICE knowledge manager)	OM-KMG-001	20012	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	Cyber security risk management Business and threat context Information/data categorization System and data security Data systems threats and vulnerabilities Disaster Recovery Planning Data back-up and recovery Identity, credentials and authentication
	Technical support specialist	OM-STS-001	22220 22221	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).	Business and threat context System and data security Data back-up and recovery Cyber threats and vulnerabilities Incident response Cyber systems policies, practices and operations.
	Network operations specialist	OM-NET-001	22220, 22221	Plans, implements, and operates network services/systems, to include hardware and virtual environments.	Business and threat context System and data security Data back-up and recovery

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
					Cyber threats and vulnerabilities Incident response Cyber systems policies, practices and operations.
	System administrator	OM-ADM-001	22220	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).	Business and threat context System and data security Data back-up and recovery Cyber threats and vulnerabilities Incident response Cyber systems policies, practices and operations. Identity, credentials and authentication
	Data systems analyst	None	21223	Identifies, develops and analyzes data system needs for the organization. Supports, and designs and implements data systems.	Cyber security risk management Business and threat context System and data security Data systems threats and vulnerabilities Disaster Recovery Planning Data back-up and recovery Identity, credentials and authentication Cyber security tools, techniques and procedures used to protect data and data systems Encryption and PKI
	Systems manager (includes system, software and data	None	20012	Plans, organizes, directs, controls and evaluates the activities of organizations that analyze, design, develop, implement, operate and administer computer and	Threat and risk assessment Cyber security risk management Business and threat context

Activity area/work category	Common title or work role	NICE ID	NOC	Major cyber security responsibility (NICE and other sources)	Key cyber security competencies
	systems manager roles)			telecommunications software, networks and information systems	Technical context Cyber systems integration Cyber security project management Cyber procurement requirements Supply chain risk management Cyber security standards Cyber security assessment and measurement Cyber security controls (management, operational, technical)

Annex F Cyber talent alliance

Launched in 2019, the Cyber Talent Alliance (CTA) is a partnership of government, academia, and industry leaders working together to build on existing programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cyber security professionals in Canada's private and public sectors. Members collaborate to design strategies, develop and promote initiatives, and pursue actions to help advance cyber security education, training, and workforce development.

CTA members include:

- Bank of Canada
- Canadian Nuclear Laboratories
- Canadian Chamber of Commerce
- Canadian Centre for Cyber Security
- Cyber NB
- Cyber Québec
- Digital Nova Scotia
- Employment and Social Development Canada
- Government of Saskatchewan
- IBM Canada Ltd.
- Innovation, Science and Economic Development Canada
- Public Safety Canada
- Quantum Safe Canada
- Rogers Cybersecure Catalyst
- SERENE RISC
- TECHNATION
- Toronto Finance International
- University of Waterloo, Institute for Quantum Computing