Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

WORKFORCE DEVELOPMENT AND CURRICULUM GUIDE

A ROLE-BASED GUIDE FOR HIRING MANAGERS, EDUCATION, AND TRAINING PROVIDERS

Version 2

Canada

FOREWORD

The *Workforce Development and Curriculum Guide: A Role-Based Guide for Hiring Managers, Education, and Training Providers* is an UNCLASSIFIED publication. This guide provides a role-based perspective on careers in the cyber security field as well as post-secondary cyber security curriculum in two domains: technical and non-technical. As a curriculum guide, the intent is not to prescribe, but to provide a catalogue of curriculum elements that establish a national benchmark against which post-secondary academic institutions can assess their programs and courses.

This guide was developed by leveraging multiple sources and with the support of representatives of the Communications Security Establishment, Canada School of Public Services, Department of National Defence, Public Safety, Royal Canadian Mounted Police, and Treasury Board Secretariat.

This guide recognizes that there are several academic institutions that have already introduced programs or courses that support cyber security educational or training outcomes, some of which surpass the curricular guidance provided. Notwithstanding, the skills shortage is anticipated for the coming years and small, medium, and large enterprises within the public and private sector will continue to face cyber challenges. This guide is distinct in that it focuses on curricular elements that prepare graduates for specific technical and non-technical roles within a common organizational security context.

REVISION HISTORY

Revision	Amendments	Date
1	Public Review Draft.	31 January 2019
2	Reorganization of information, validation of roles and addition of new roles, addition of list of currently offered programs, and new diagrams.	17 June 2020

Table of Contents

1 INTRODUCTION

There continues to be a growing demand for qualified cyber security professionals and practitioners. One forecast estimates that there will be a shortage of 3.5 million cyber security professionals globally by 2021 [1]. The dynamic nature of the cyber security field has subsequently transformed, and is no longer simply dependent on technical/computer-based disciplines, but requires encompassing non-technical fields of study, including business, law, policy, and ethics, to tackle the growing changes in the field.

To develop the required talent, several academic institutions have introduced programs or courses of study within existing programs to support cyber security educational or training outcomes. Whether developing full new programs, defining new concentrations within existing programs, or augmenting existing course content, academic institutions may need curricular guidance based on a comprehensive understanding of the cyber security field, the demands of the discipline, and the relationship between academic curriculums and cyber security workforce frameworks [2].

Due to the highly dynamic nature of cyber security, this guide will be reviewed on a regular basis to reflect post-secondary education and training requirements for cyber security workforce roles and specializations. Suggested changes can be submitted by email to contact@cyber.gc.ca.

1.1 THE CANADIAN CENTRE FOR CYBER SECURITY

The Canadian Centre for Cyber Security (Cyber Centre) was officially launched in October 2018. The Cyber Centre's Academic Outreach and Engagement team works with universities, colleges, educational associations, education ministerial boards and private sector educators to build cyber security talent and capacity in Canada. The team also works with educators to enhance the community's understanding of cyber security. Its mission is to ensure Canada is a global leader in cyber security by elevating cyber education.

1.2 PURPOSE

The purpose of this curriculum guide is twofold:

- To provide a role-based perspective on careers in cyber security
  - to help career counsellors prepare students for technical and non-technical cyber security workforce roles;
  - to help students understand the different types of professions available in the cyber security field;
  - to help employers recruit qualified professionals; and
- To develop comprehensive curricular guidance in cyber security education that will support future program development and associated efforts at the post-secondary level.

1.3 AUDIENCE

The primary audience for this guide is academic institutions that are interested in developing cyber security programs, defining new cyber security concentrations within existing programs, or augmenting existing programs to incorporate cyber security content.

Secondary audiences include:

- Prospective students and professionals who are interested in the cyber security field and who wish to gain an understanding of the work tasks and proficiency requirements, including knowledge and skills, expected in technical and non-technical organizational roles;
- Cyber security industry members who can assist with cyber security program development in academic institutions, and later recruit and hire students from these programs;
- Professional and training organizations that have a role in supporting Canadian workforce development;
- Policy makers who are looking for guidance on the competencies and human capabilities to support security requirements; and
- Members of the K-12 educational community who are preparing students to enter post-secondary education in cyber security.

1.4 HOW TO USE THIS GUIDE

This guide frames the curriculum (what is taught) as well as methods (how it is taught), and is presented in four sections to provide a broad perspective on cyber security related roles within an organization:

1. Govern and Support;
2. Protect and Defend;
3. Operate and Maintain; and
4. Design and Develop.

Each section provides role-based curriculum suggestions progressing from foundational requirements to specialized roles. Each curriculum topic area is divided into components that support further identification of knowledge and skills requirements. Each topic area can be integrated into current academic curriculums based on learner needs, or used as stand-alone curriculum elements in support of new or existing programs, or individual courses.

Academic institutions can use this guide to further develop cyber security programs or augment existing programs to incorporate cyber security content. Definitively, industry members can use this guide to assist academic institutions in developing cyber security programs, and later recruit and hire graduates of these programs. Students and career counsellors can also use this guide to gain an understanding of the work tasks as well as the education, experience, and proficiency requirements expected in technical and non-technical cyber security roles.

It is not proposed that these cyber security related roles equate to jobs or areas of personal responsibility. The sections are intended to provide curricular guidance to academic institutions, career counsellors, and students, among others, to prepare students and professionals for technical and non-technical workforce roles based on a comprehensive understanding of the cyber security landscape.

Upon review, new versions of this guide will expand on and include new or alternative cyber security roles that impact industries including, among others, energy, health, law, and manufacturing, as they come available.

Further interpretations or questions on how to use this guide can be submitted by email to contact@cyber.gc.ca.

1.5 SOURCES

This guide builds upon prior work in cyber security education, training and workforce development. In addition to the sources listed at the end of this guide under References, major sources used in the development of this guide include:

- US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CWF);
- Requirements of the US National Security Agency and the US Department of Homeland Security National Centers of Academic Excellence in Cyber Defence and Cyber Operations;
- Global Information Technology (IT) Skills Framework for the Information Age (SFIA);
- NATO Cybersecurity: A Generic Reference Curriculum;
- The Public Services and Procurement Canada Task-Based Informatics Professional Service – Requirements for Services; and
- The Canadian Centre for Cyber Security's IT Security Learning Pathways.

1.6 CONTRIBUTING TO THE GUIDE

The Cyber Centre regularly receives inquiries about cyber security education and training opportunities. Several academic institutions have introduced programs or courses of study within existing programs that can serve as examples or exemplars for the larger community. If any institution or organization believes it has a program or a course that should be considered an example or exemplar, please submit it by email to contact@cyber.gc.ca.

2 THE CYBER SECURITY DISCIPLINE

The Government of Canada defines cyber security as “the protection of digital information and the infrastructure on which it resides [3]”. Cyber security is predominately a computer-based discipline involving technology, people, information, and processes to enable assured operations that protect the confidentiality, integrity and availability of information from deliberate or accidental cyber security threats [2].

Five primary computer-based disciplines are recognized as the foundation of cyber security:

- Computer Engineering
- Computer Science
- Information Systems
- Information Technology
- Software Engineering

As a discipline, cyber security has become essential with the evolution of information and communication technology (ICT). Technological advancements have altered the way people communicate and exchange information electronically, raising challenges to the security of that information. The growing threat of cyber attacks has made governments and industries more aware of the need to protect and defend critical systems. Despite its small market size, Canada was the third most exposed country to possible cyber-attacks in 2018 [4]. As a result of society’s increasing dependence on computer networks and systems, it is no surprise that cyber security is growing as a recognizable discipline with a breadth and depth of content that encompasses multiple fields in the computing ecosystem.

Although only a subset of businesses participates directly in the ICT industry by producing or selling ICT solutions that protect against cyber threats, or by building or operating IT infrastructure, in effect every business uses ICT to deliver its own goods and services to the marketplace and contributes its own experience and innovation to the ICT industry. Canada’s industries involve multiple types of relationships that often overlap but are supported by technological solutions that communicate with each other as a network. Cyber security, as a result, becomes more pertinent in protecting the corresponding computer systems in Canada’s industries. Such industries include Canada’s top ten critical infrastructures:

- Health – a prime target for cyber-attacks as the industry holds a large amount of sensitive information (e.g., electronic records and patient information) and encompasses medical implant devices such as pacemakers that are exploitable;
- Food – an industry vulnerable to growing threats of cyber-attacks to food production and safety, environmental damage, and financial loss;
- Finance – an ideal target for cyber-attacks as the industry maintains valuable information (e.g., client identities, bank account information, financial assets, and intellectual property);
- Water – an industry vulnerable to growing threats of cyber-attacks to efficient renewable water supply. wastewater collection, and treatment facilities;
- Information and Communication Technology – a prime target for cyber-attacks as the industry maintains an excessive amount of sensitive information (e.g., online retail transactions, email messages, web-browsing activity, social media platforms, and user private information);
- Safety – an industry vulnerable to growing threats of cyber-attacks to emergency response teams, law enforcement, call-center communications-management software, closed-circuit TV camera systems, interactive voice response systems, and emergency alert;

- Energy and utilities – an ideal target for cyber-attacks on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) programs to access large amounts of data, and to cause physical damage to network infrastructure;
- Manufacturing – an industry increasingly vulnerable to supply chain attacks that can have an impact on the production and distribution of goods and services. Manufacturing disruptions and can lead to defective products, production downtime, physical damage and threaten lives;
- Government – a prime target for cyber-attacks on government entities at the federal, provincial/territorial, and municipal levels, and more recently on democratic institutions, to access excessive amounts of private and sensitive information (e.g., personal information, income tax returns, and government records); and
- Transportation – an industry increasingly vulnerable to cyber-attacks to freight and passenger rail, civil and freight aviation systems, and ground transportation. As well, the transportation industry hold sensitive and valuable information such as birth dates, and passport numbers.

Highlighting the growing cyber security field is, therefore, important to meet the demand for professionals across a range of work roles to assure the security of Canadian computing networks and systems [5].

2.1 CYBER SECURITY: AN INTERDISCIPLINARY FIELD

While cyber security is predominately a computer-based discipline, with the majority of education and training programs technically oriented, the field has evolved to become interdisciplinary and includes aspects of business, law, policy, human factors, ethics, and risk management [2]. Cyber security not only includes technical issues but also non-technical, and more importantly, business concerns faced by governments and industries. Organizations increasingly need professionals who posses the skills to manage information security policies, procedures, and practices as well as managerial and communications skills [5]. Figure 1 illustrates the nexus between the technical and business dimensions of cyber security, which together, are critical for developing an organizational culture that will rapidly identify and counter deliberate or accidental cyber security threats.

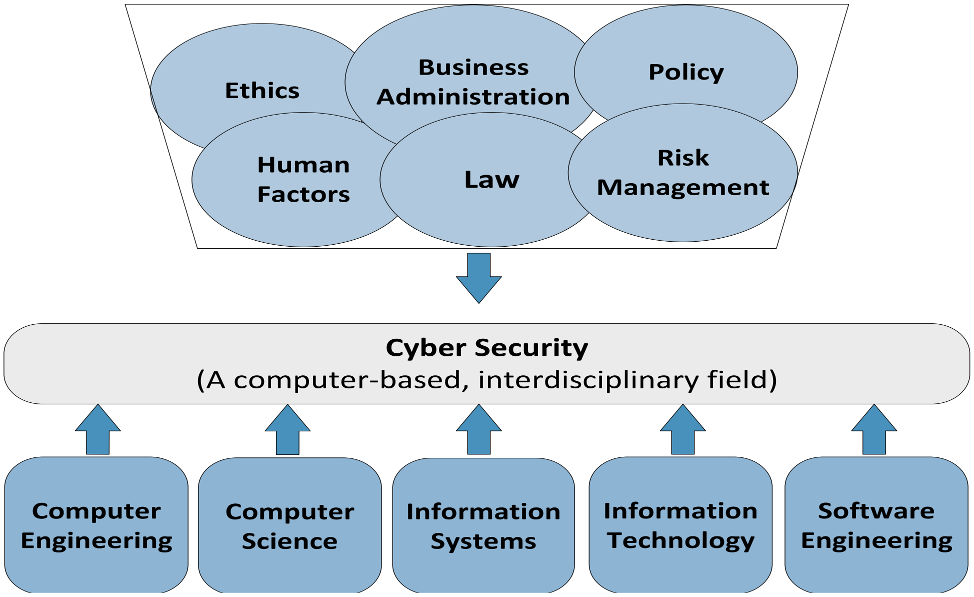


Figure 1: Structure of Cyber Security Discipline

Cyber security as an identifiable discipline is still developing. Driven by workforce demands, several academic institutions have introduced educational programs or courses of study within existing programs. As such, academic programs in cyber security need to have a curriculum that includes the following characteristics:

- Aspects of both computer-based and business-oriented fundamentals;
- Concepts that are broadly applicable across a wide range of cyber security related fields;
- A body of knowledge containing essential cyber security knowledge and proficiencies including the Nine Essential Skills required regardless of program focus;
- A direct relationship to the range of disciplines meeting workforce demands; and
- An emphasis on the ethical conduct and professional responsibilities associated with the cyber security field. [5]

This guide aims to help academic institutions develop cyber security programs and courses that meet each of these criteria.

2.2 EMERGING TECHNOLOGIES

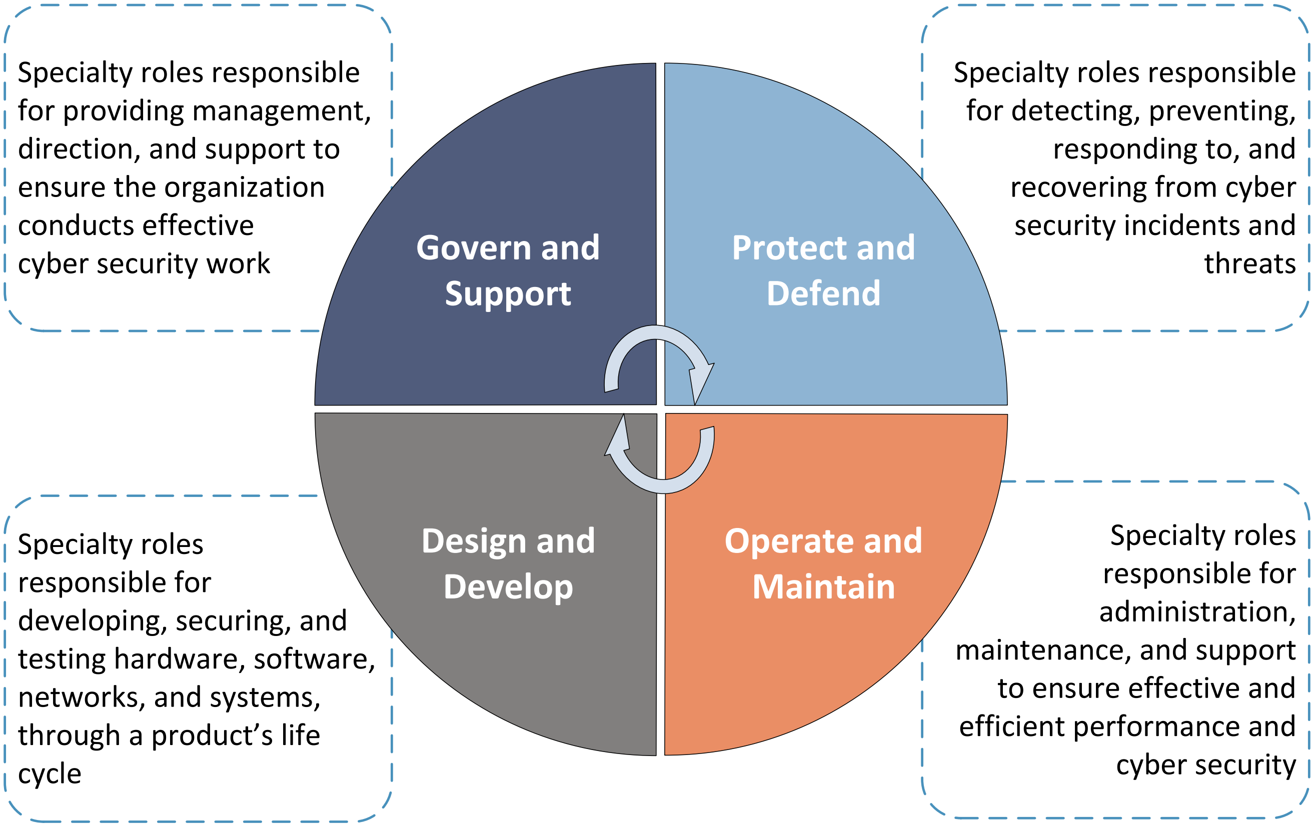
The cyber security field continues to evolve as industries generate more data and information than before. The applications of emerging technologies in industries, including artificial intelligence (AI), blockchain technology, cloud-computing, the Internet of things (IoT), and quantum computing, have enabled more devices and systems to be connected in a network, allowing for greater control and performance of processes. However, these technologies also increase the risk of being targeted by a cyber-attack. The 2017 Wannacry ransomware attack is a prominent example in which companies and individuals in more than 150 countries were affected by a vulnerability discovered in Microsoft Windows systems [6].

Innovative opportunities to defend and protect emerging technologies from cyber threats continue to develop and grow, and therefore, new types of knowledge and skills in areas such as data science and analytics are generating new cyber security roles on the job market.

This guide aims to expand on and include new cyber security roles as future technology trends pave the way forward.

3 ROLE-BASED FRAMEWORK

This curriculum guide has been structured to provide a role-based perspective based on cyber security curriculum learning requirements and outcomes that contribute to specific technical and non-technical organizational roles. Illustrated below in Figure 2, the role-based model categorizes cyber security workforce roles into four main functions based on desired knowledge and skills without neglecting adjacent and contributing work.



Specialty roles responsible for providing management, direction, and support to ensure the organization conducts effective cyber security work

Specialty roles responsible for detecting, preventing, responding to, and recovering from cyber security incidents and threats

Specialty roles responsible for developing, securing, and testing hardware, software, networks, and systems, through a product's life cycle

Specialty roles responsible for administration, maintenance, and support to ensure effective and efficient performance and cyber security

Figure 2: Cyber Security Roles and Specializations

As cyber security is an interdisciplinary course of study, both computer-based and business-oriented disciplines are part of this guide's focus in an attempt to provide a more comprehensive understanding of the cyber security workforce field. The majority of the non-technical cyber security related workforce roles are grouped under the Govern and Support function as the positions primarily involve decision making and governance. The technical workforce roles and specializations are grouped under the other three functions as they are more computer-based professions. These functions are guided by an appropriate level of leadership and extend into specializations that often require additional task-based training and expertise within the work area to become proficient. Some of these technical and non-technical roles, however, can overlap with roles within the other functions, particularly where key functional proficiencies are required. Individuals from other domains who have the experience may fill these workforce roles.

Those familiar with the NICE Cybersecurity Workforce Framework will note that there are many commonalities in specialized tasks, knowledge, and skills. This guide is focused only on cyber security elements, without reference to other common technical and non-technical curriculum. Additionally, this guide provides common proficiencies that should be included in the development of cyber security practitioners intended to support organizational security requirements.

3.1 CYBER SECURITY WORKFORCE ROLES

3.1.1 GOVERN AND SUPPORT

The cyber security workforce roles within the Govern and Support function (Table 1) are responsible for providing management, direction, and support to ensure an organization conducts effective cyber security work. The roles range from entry-level, to intermediate, to advanced, often requiring a significant amount of education, training, and work experience. Each of the workforce roles is explained in further detail in the tables under the **Govern and Support** section.

Govern	Cyber Legal Advisor Policy Analyst Privacy Officer Risk Analyst Strategic Planner
Support	Business Analyst Communications Disaster Recovery Planner Procurement Analyst
Manage	Chief Information Security Officer Cyber Security Manager Information Systems Security Manager Project Manager Supply Chain Manager

Table 1: Govern and Support Roles

3.1.2 PROTECT AND DEFEND

The cyber security workforce roles within the Protect and Defend function (Table 2) are responsible for detecting, preventing, responding to, and recovering from cyber incidents and threats. The roles range from entry-level, to intermediate, to advanced, often requiring a significant amount of education, training and work experience. Each of the workforce roles is explained in further detail in the tables under the **Protect and Defend** section.

Cyber Defence	Cyber Security Analyst Industrial Control Systems Security Analyst Information Security Analyst
Vulnerability Assessment	Vulnerability Assessment Analyst Penetration Tester
Incident Response	Cyber Security Incident Responder/Handler
Digital Forensics	Digital Forensics Analyst

Table 2: Protect and Defend Roles

3.1.3 OPERATE AND MAINTAIN

The cyber security workforce roles within the Operate and Maintain function (Table 3) are responsible for the administration, maintenance, and support to ensure effective and efficient performance and cyber security. The roles range from entry-level, to intermediate, to advanced, often requiring a significant amount of education, training and work experience. Each of the workforce roles is explained in further detail in the tables under the **Operate and Maintain** section.

Systems and Networks	Network Security Operator/Specialist System Administrator
Data	Cryptographer/Cryptanalyst
Technical Support	Technical Support Specialist

Table 3: Operate and Maintain Roles

3.1.4 DESIGN AND DEVELOP

The cyber security workforce roles within the Design and Develop function (Table 4) are responsible for developing, securing, testing, and integrating hardware, software, and systems throughout a product's life cycle. The roles range from entry-level, to intermediate, to advanced, often requiring a significant amount of education, training and work experience. Each of the workforce roles is explained in further detail in the tables under the **Design and Develop** section.

Architecture and Engineering	Critical Infrastructure Engineer Requirements Analyst Security Architect Security Engineer
Research and Development, Testing and Evaluation	Cyber Security Researcher Security Tester and Evaluator Supply Chain Integrity Analyst
Systems and Software Development	Application Developer Information Systems Security Developer Secure Software Developer

Table 4: Design and Develop Roles

3.2 CORE CURRICULUM TOPICS

The curriculum for technical workforce roles assumes that individuals have technical education, training and/or experience within a cyber or IT related field, and that fundamental knowledge requirements of IT systems/software and networks have been met.

For those participants with limited or no technical background, they should be provided opportunities to attain a basic knowledge of the following:

- Data analysis;
- Scripting or introductory programming;
- Cyber defence;
- Cyber threats;
- Fundamental security design principles;
- Cryptography;
- IT system components;
- Networking concepts;
- System administration;
- Security approaches and models;
- Security management frameworks;
- Vulnerability management;
- Communications protocols, Internet security protocols, directory standards;
- Cloud computing and virtualization technologies;
- Network architecture and enterprise architecture models; and
- System and/or software development lifecycle, software development processes.

In general, a basic knowledge of the following is required for all technical and non-technical practitioners. The depth of understanding will vary for roles, depending on the business or organization:

- Cyber threat context (including class of attack (active, passive, insider); type of cyber threat; type of cyber actors and their tactics, techniques, and procedures (TTPs);
- Legal, policy, ethics and compliance related to cyber security and privacy;
- Cyber security risk management processes;
- Cyber security incident management – incident response and mitigation;
- Cyber security processes, technology, trends, and emerging issues;
- Sources of cyber security expertise and resources;
- Business continuity and disaster recovery; and
- Research, analysis and reporting.

3.3 ROLE-BASED CURRICULUM COMPONENT STRUCTURE

Each of the role-based cyber security curriculum components provides:

- Role-based title;
- Basic job description;
- Cyber security related tasks;
- Commonly requested education, training and work experience;
- Primary training requirements – learning outcomes; and
- Key proficiencies.

Requirements for specific roles are identified in the tables that follow in the next section.

4 GOVERN AND SUPPORT

4.1 CYBER LEGAL ADVISOR

Basic Job Description

- Provides legal advice and recommendations on relevant topics related to cyber security.

Cyber Security Related Tasks

- Advocate organization's official position in legal and legislative proceedings;
- Interpret and apply laws, regulations, policies, standards, or procedures to specific issues;
- Evaluate the effectiveness of laws, regulations, policies, standards, or procedures;
- Resolve conflicts in laws, regulations, policies, standards, or procedures;
- Maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, standards, procedures, or other issuances;
- Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policies;
- Conduct research and analysis on various legal matters of the organization using multiple sources;
- Provide legal analysis and decisions to compliance personnel, management, and privacy officers, among others regarding compliance with cyber security laws, regulations, and policies;
- Provide advice and guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients;
- Monitor and assess the potential impact of emerging technologies on laws, regulations, policies, standards, or procedures;
- Evaluate the impact of changes to laws, regulations, policies, standards, or procedures;
- Implement new or revised laws, regulations, policies, standards, or procedures; and
- Prepare legal reports, briefing notes, and other relevant documents.

Commonly Requested Education, Training and Work Experience

- Post-secondary University Degree in Law and acquired provincial licensure to practice. A Master's Degree is preferred;
- Certifications an asset: Computing Technology Industry Association (CompTIA); Certified Information Systems Security Professional (CISSP); and
- Previous training and experience in law and cyber security is preferred -- 2-5 years of experience for entry-level; 5-10 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Domestic and international laws, regulations, and ethics as they relate to cyber security and privacy;
- Information security policies, procedures, and regulations;
- 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;
- Specific impacts of cyber security gaps and breaches;

- Information gathering principles, policies, and procedures including legal authorities and restrictions;
- Investigative tools, reporting, and laws and regulations;
- Business or military operation plans, orders, policies, and rules of engagement; and
- Privacy disclosure statements based on laws and regulations.

Key Proficiencies

- Research and Analytical, Attention to Detail, Problem-solving, Interpersonal, Negotiation, Communication Skills

4.2 POLICY ANALYST

Basic Job Description

- Develops and maintains cyber security policies to support and align with organizational cyber security initiatives and regulatory compliance.

Cyber Security Related Tasks

- Develop and implement cyber security policies and guidelines;
- Research and analyze organizational cyber security policies, guidelines, and requirements;
- Assess policy needs and collaborate with management and staff to develop policies to govern cyber security activities;
- Review existing and proposed policies and guidelines with management;
- Prepare and publish cyber security policies;
- Interpret and apply applicable laws and regulatory documents into cyber security policy;
- Monitor the application of cyber security policies and guidelines;
- Establish and maintain communication channels with management and staff on existing and proposed policies and communicate any policy changes;
- Provide guidance to management and staff; and
- Ensure cyber security policies and guidelines are reflected in the organization’s mission and goals.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in an applicable field related to cyber security (e.g.; Business Administration, Economics, Law, Political Science, Social Sciences or equivalent); and
- Previous training and experience in policy analysis/policy development – 1-3 years of experience for entry-level; five years of experience for advanced-level.
- Individuals employed in this role can have diverse levels of cyber security expertise and may not have any background in the work domain. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Business analysis techniques;
- Current and emerging technology and cyber security technologies;
- Technological trends and security risks and their potential impact on cyber security policies;
- Applicable laws, regulations and guidelines as they relate to cyber security;
- Leveraging best practices and lessons learned of external organizations and academic institutions with a cyber focus;
- Identify gaps in cyber security policies; and
- Develop, draft, and communicate cyber security policies in support of organizational activities.

Key Proficiencies

- Research, Analytical, Problem-solving, Interpersonal, Communication skills

4.3 PRIVACY OFFICER

Basic Job Description

- Develops, implements, and administers all aspects of the organization privacy compliance program, responsible for safeguarding private and confidential information.

Cyber Security Related 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;
- Report security breaches to management and appropriate authorities; and
- Develop, deliver, and oversee privacy training material and awareness activities.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in an applicable field related to cyber security (e.g.; Business Administration, Law, Political Science, Social Sciences or equivalent);
- Certifications as asset: International Association of Privacy Professionals (IAPP); and
- Previous training and experience in policy analysis – 2-3 years of experience for entry-level. Requested experience will depend on the organizational need.

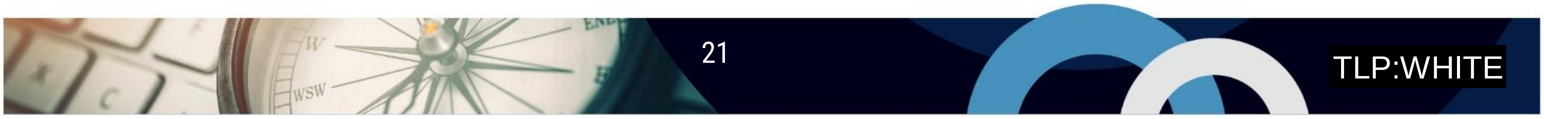
Primary Training Requirements – Learning Outcomes

- Domestic and international laws, regulations, policies, and procedures;
- Information security policies, procedures, and regulations;
- 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;
- Specific impacts of cyber security gaps and breaches;

- Monitor advancements in privacy laws and policies;
- Privacy impact assessments; and
- Privacy disclosure statements based on laws and regulations.

Key Proficiencies

- Analytical, Attention to Detail, Organizational, Time Management, Interpersonal, Communication skills



4.4 RISK ANALYST

Basic Job Description

- Assesses and manages information security and cyber security risks and ensures risks and controls are assessed accurately, objectively and independently;
- Conducts research, analyzes information, prepares reports and plans to resolve organizational problems related to cyber security to acceptable levels.

Cyber Security Related Tasks

- Investigate and report on risks and exceptions on a regular basis to management, and formulate action plans to remediate them;
- Conduct research and develop models to analyze, explain and forecast patterns and trends, and devise methods for collection and analysis of data;
- Determine cyber security risk profiles for various cyber security projects and strategies;
- Assess the risk for implementing cyber security tools and technology within the organization;
- Develop and maintain risk and impact assessments for various projects and strategies;
- Maintain and report the organizational risk register with management on a periodic basis;
- Define, develop and manage policies, procedures and guidelines on cyber security requirements;
- Ensure compliance with cyber security policies, laws, regulations, and practices;
- Develop or contribute to reviews of implemented projects and strategies to identify potential risks; and
- Integrate cyber security with other organizational risk management activities.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Information Security, Information Management, IT Risk Management, or equivalent);
- Certifications an asset: Certified in Risk and Information Systems Control (CRISC); and
- Previous training and experience in risk management or cyber security is preferred – 2-5 years of experience for entry-level; 5-10 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Information and data analysis techniques;
- Risk management processes, responsibilities and authorities;
- Risk identification, risk documentation, risk analysis, risk reduction and risk reporting;
- Business continuity and disaster response planning;
- Cost/benefit analysis;
- A working knowledge of cyber security principles and elements;
- Technical knowledge to understand data security and integrity and security requirements; and
- Applicable laws, regulations and guidelines as they relate to cyber security.

Key Proficiencies

- Analytical, Problem-solving, Organizational, Time Management, Interpersonal, Communication skills

4.5 STRATEGIC PLANNER

Basic Job Description

- Develops and maintains cyber security plans and strategies to support and align with organizational cyber security initiatives and regulatory compliance.

Cyber Security Related Tasks

- Design and implement cyber security strategies and programs that outline and align with organization goals and activities;
- Research and analyze organizational cyber security practices and procedures that define specific business direction and constraints;
- Assess organizational needs and collaborate with management and staff to develop strategic plans to promote cyber security;
- Review, conduct, or contribute to audits of organizational cyber security programs and projects;
- Draft and publish cyber security plans and practices;
- Interpret and apply applicable laws and regulatory documents into cyber security strategies and objectives;
- Monitor the application of cyber security plans; and
- Establish and maintain communication channels with management, staff, and users on existing and proposed strategic plans and communicate any changes.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in an applicable field related to cyber security (e.g.; Business Administration, Economics, Political Science, Social Sciences or equivalent); and
- Previous training and experience in security or strategic planning and development – 1-3 years of experience for entry-level; five years of experience for advanced-level.
- Individuals employed in this role can have diverse levels of cyber security expertise and may not have any background in the work domain. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Business analysis techniques;
- Current and emerging technology and cyber security technologies;
- Technological trends and security risks and their potential impact on cyber security practices;
- Applicable laws, regulations and guidelines as they relate to cyber security;
- Leveraging best practices and lessons learned of external organizations with a cyber focus;
- Identify gaps in cyber security practices and programs;
- Using risk or threat assessments in preparing strategic plans; and
- Develop, draft, and communicate cyber security practices in support of organizational goals and activities.

Key Proficiencies

- Research, Analytical, Problem-solving, Attention to Detail, Organizational, Time Management, Interpersonal, Communication skills

4.6 BUSINESS ANALYST

Basic Job Description

- Performs an extensive range of complex technical and/or professional work, such as assesses and improves an organization's processes and systems, and analyzes its business model.

Cyber Security Related Tasks

- Report on key metrics related to information quality and security, cyber security issues, etc.;
- Define, develop and manage policies, controls, standards, and processes for creation of regular operational security metrics for continuous improvement;
- Ensure compliance with cyber security policies, laws, regulations, and practices;
- Develop or contribute to business cases, including assessing costs and risks for implementing effective cyber security solutions;
- Collaborate with stakeholders to deliver strategic initiatives throughout the system life cycle;
- Advise and report on security requirements and risk management process activities, including performing impact assessments as part of disaster recovery and contingency plans;
- Ensure proper risk management is performed at the program and project levels.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Business Administration, Commerce, Economics, Technology Management, IT Risk Management, or equivalent); and
- Previous training and experience in cyber security is preferred.
- Individuals employed in this role can have diverse levels of cyber security expertise and may not have any background in the work domain. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Business analysis techniques;
- Information and data analysis techniques;
- 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;
- Risk management processes, responsibilities and authorities;
- Cost/benefit analysis, revenue and cost forecasting, etc.;
- System life cycle management principles, including software security and usability; and
- Develop risk or impact assessments, business cases, and risk management documents.

Key Proficiencies

- Research, Analytical, Attention to Detail, Organizational, Time Management, Interpersonal, Communication skills

4.7 COMMUNICATIONS

Basic Job Description

- Develops and implements communication strategies and resources in support of an organization's cyber security goals and objectives.

Cyber Security Related Tasks

- Develop and implement cyber security communication products; including translating organization policies into clear outgoing cyber security messages;
- Review incoming communications for the organization as it relates to cyber security;
- Provide guidance on cost/benefit analysis process by establishing and administering policies, processes, and procedures;
- Communicate the value of cyber security through all levels of the organization;
- Provide cyber security and risk management guidance for development of business continuity operations, strategic plans, and procedures;
- Ensure that cyber security action plans are reviewed, validated, and implemented as required;
- Develop or contribute to business cases, including conducting cost/benefit analysis and risk analysis for implementing effective cyber security communication products;
- Recognize a possible cyber security incident and take appropriate measures to report the incident;
- Provide guidance on issuing key messages during routine and crisis cyber security events; and
- Conduct and coordinate media events to bring awareness to effective cyber security solutions.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a related field (e.g., Business Administration, Commerce, Communications, Public Relations, IT Risk Management, or equivalent); and
- Previous training and experience in Communications or cyber security is preferred – 1-4 years of experience for entry-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Business analysis techniques;
- Maintain 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 cyber security solutions;
- Risk management processes, responsibilities and authorities;
- Communications security terminology, guidelines, and procedures;
- Cost/benefit analysis, risk analysis, etc.;
- Resource management principles and techniques; and
- Develop business cases and risk management documents.

Key Proficiencies

- Research, Analytical, Attention to Detail, Organizational, Time Management, Interpersonal, Communication skills

4.8 DISASTER RECOVERY PLANNER

Basic Job Description

- Develops, tests, implements, and manages emergency responses, recovery and resumption processes, procedures and/or plans, as needed, to recover and protect an organization's IT infrastructure, (e.g., networks, systems, controls) in the event of a disaster.

Cyber Security Related Tasks

- Establish, maintain and test disaster recovery and contingency plans for potential disaster and operation interruption scenarios;
- Develop disaster recovery and contingency budgets;
- Interpret national and provincial laws and regulations, and ensure compliance of contingency and disaster recovery plans;
- Develop and maintain risk and impact assessments of disasters on organization functions and information systems;
- Develop and administer disaster recovery and contingency plan training; and
- Coordinate crisis communications.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Business Administration, Commerce, Economics, IT Risk Management or equivalent);
- Certifications an asset: EC-Council certifications; and
- Individuals typically employed in this role have extensive experience in either security or IT incident response coordination or management. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Risk management processes, responsibilities and authorities;
- Risk identification, risk documentation, risk analysis, risk reduction and risk reporting;
- Business continuity and disaster response planning;
- Cost/benefit analysis, revenue and cost forecasting, etc.;
- Maintain a working knowledge of cyber security principles and elements; and
- Applicable laws, regulations and guidelines as they relate to cyber security.

Key Proficiencies

- Business Acumen, Problem-solving, Organizational, Time Management, Attention to Detail, Interpersonal, Communication skills

4.9 PROCUREMENT ANALYST

Basic Job Description

- Researches, analyzes, and acquires inventory and services for the organization.

Cyber Security Related Tasks

- Research and analyze technical and cyber security solutions available on the market that best meet the organization’s needs;
- Assess and document any cyber security risks throughout the procurement life cycle;
- Ensure compliance with purchasing guidelines and with cyber security policies, regulations, and procedures of the organization;
- Ensure compliance with security requirements of organization networks and systems;
- Coordinate with cyber security experts to regularly monitor systems and to update organization policies and procedures;
- Develop and maintain risk assessments and related reports on vendors and procured products and services, based on reliability and credibility;
- Coordinate with the finance department, the organization and the vendor to negotiate terms or agreement and conditions; and
- Research and analyze market trends based on sales and performance data, forecast future opportunities, and make procurement recommendations to management.

Commonly Requested Education and Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Business Administration, Economics or equivalent); and
- Previous training and experience in cyber security is preferred.
- Individuals employed in this role can have diverse levels of cyber security expertise. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Business analysis techniques;
- Cost/benefit analysis and forecasting, etc.;
- Maintain a working knowledge of cyber security principles and elements;
- Technical knowledge to understand data security requirements, and the functional and technical design of networks and system, and cyber security solutions;
- Applicable laws, regulations and guidelines as they relate to cyber security;
- System life cycle management principles, including software security and usability; and
- Develop risk assessments.

Key Proficiencies

- Analytical, Attention to Detail, Organizational, Time Management, Interpersonal, Communication skills

4.10 CHIEF INFORMATION SECURITY OFFICER

Basic Job Description

- Establishes, maintains and oversees organization-wide cyber security operations and programs, procedures and policies, systems and assets, and budget and resources, ensuring the protection of information assets.

Cyber Security Related Tasks

- Direct and approve the design of cyber security risk management programs and systems;
- Lead and align cyber security priorities with strategic plans;
- Identify, acquire and oversee management of financial, technical and personnel resources required to support cyber security objectives;
- Advise senior management on cyber security programs, policies, processes, standards, and procedures;
- Oversee implementation strategies and requirements to ensure procedures and guidelines comply with cyber security policies;
- Ensure disaster recovery plans, business continuity operations, and procedures are implemented and tested;
- Review and approve cyber security policies, controls and incident response planning;
- Initiate, facilitate and promote awareness of cyber security issues within the organization and ensure cyber security priorities are reflected in the organization's vision and goals;
- Review investigations after cyber incidents, including impact analysis and recommendations for avoiding similar vulnerabilities;
- Oversee protective or corrective measures when a cyber incident or vulnerability is discovered;
- Maintain a current understanding of the cyber threat landscape for the organization context;
- Ensure compliance with cyber security policies, laws, regulations, and procedures;
- Schedule periodic security audits and reviews;
- Oversee identity and access management;
- Prepare financial forecasts for cyber security operations and proper maintenance coverage for information and security assets; and
- Provide leadership, training opportunities and guidance to personnel.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Business Administration, Computer Science, IT Management, Information Security, or equivalent). A Master's in Business Administration or a Master's in Cyber Security is an asset;
- Certifications an asset: Global Information Assurance Certification (GIAC); Computing Technology Industry Association (CompTIA); Certified Information Systems Security Professional (CISSP); and
- Previous training and experience in IT security infrastructure, requirements analysis or program management is preferred – 10+ years of relevant IT experience with at least 5+ years of that experience in management. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer architecture, data structures, and algorithms;
- Cryptography and cryptographic key management concepts;
- Maintain a working knowledge of cyber security and privacy principles and elements;
- Network access, identity, and access management;

- System life cycle management principles, including software security and usability;
- Business analysis techniques;
- Information and data analysis techniques;
- Risk management processes, responsibilities and authorities;
- Cost/benefit analysis, revenue and cost forecasting, risk analysis, etc.;
- Resource management principles and techniques; and
- Applicable laws, regulations, policies and ethics as they relate to cyber security; and
- Technological trends and security risks and their potential impact on cyber security policies.

Key Proficiencies

- Research, Analytical, Problem-solving, Organization, Time Management, Interpersonal, Communication skills

4.11 CYBER SECURITY MANAGER

Basic Job Description

- Manages detection, prevention, response, and recovery of cyber incidents and threats; ensures computer networks and systems are well protected against cyber-attacks, intrusions, and various types of data breaches.

Cyber Security Related Tasks

- Monitor and assess all aspects of cyber security activities and infrastructure and address any issues;
- Provide expert strategy, threat, and technical advice, guidance, and support on irregular/malicious activities and potential threats to network resources;
- Define, develop, implement, maintain, and review cyber security policies and procedures;
- Ensure compliance with cyber security policies, regulations, and procedures of the organization,
- Implement security measures, controls, and protocols to protect digital files and information systems against cyber incidents or threats;
- Maintain awareness of key trends and reporting, and understand how they impact responses to cyber incidents, or threats;
- Lead the underlying operations and procedures that support the organization's activities;
- Establish and maintain communication channels with stakeholders on cyber security;
- Develop, deliver, and oversee training material and educational efforts; and
- Identify and address cyber security workforce planning and management issues.

Commonly Requested Education, Training, and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Engineering, Computer science, Information Technology or equivalent). A Master's degree is an asset;
- Certifications an asset: Global Information Assurance Certification (GIAC); Certified Information Systems Security Professional (CISSP); Certified Information Security Manager (CISM); and
- Previous training and experience in network security is preferred – 5-10 years of experience. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer architecture, data structures, and algorithms;
- C, C++, Java, Python, and similar computer programming languages;
- Cryptography and cryptographic key management concepts;
- A working knowledge of cyber security and privacy principles and methods (e.g., firewalls, encryption, virtual private network devices);
- Authentication, authorization, and access control methods, mechanisms;
- Controls related to the use, processing, storage and transmission of data;
- Network access, identity, and access management;
- Network protocols and packet analysis tools;
- Operating systems and system administrations hardening techniques;
- Intrusion detection system (IDS)/Intrusion prevention system (IPS), penetration and vulnerability testing;
- System testing and evaluation methodologies and processes;
- Data loss prevention (DLP), anti-virus and anti-malicious software;

- Incident response and handling methodologies;
- Current and emerging technology and cyber security technologies;
- Risk management policies, requirements, and practices;
- Resource management principles and techniques;
- Develop threat assessments, audit reports, risk management documents; and
- Applicable laws, regulations, policies and ethics as they relate to cyber security.

Key Proficiencies

- Analytical, Problem-solving, Organizational, Time Management, Interpersonal, Communication skills

4.12 INFORMATION SYSTEMS SECURITY MANAGER

Basic Job Description

- Manages information system security throughout the systems life cycle, and reports on information system performance in providing confidentiality, integrity, and availability.

Cyber Security Related Tasks

- Monitor and assess all aspects of information systems security development and address any issues;
- Assess technological trends and risks, and determine potential impact to system development;
- Develop mechanisms to monitor and measure risk, compliance, and information assurance efforts;
- Develop, conduct, and maintain security reviews and vulnerability and impact assessments, and direct responses to network or system intrusions;
- Provide guidance for development of disaster recovery plans, business continuity operations, and procedures;
- Review costs, design concepts, and any changes;
- Review, implement, update, and document cyber security policies, standards, and procedures for organization;
- Ensure compliance with cyber security policies, regulations, and procedures of the organization;
- Resolve conflicts in laws, regulations, policies, or procedures;
- Ensure compliance with security requirements of organization networks and systems;
- Coordinate with information systems security experts to regularly monitor systems and controls, and to update organization policies and procedures;
- Lead the underlying operations and procedures that support the organization's activities;
- Establish and maintain communication channels with stakeholders on information systems security;
- Develop, deliver, and oversee training material and educational efforts; and
- Identify and address cyber security workforce planning and management issues.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Science, Mathematics, Network Technology, Computer Engineering or equivalent);
- Certifications an asset: Certified Secure Software Lifecycle Professional (CSSLP); and
- Previous training and experience in system development and security or system management is preferred. Requested experience will depend on the organizational need.

Primary Training Requirements– Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software;
- Principles in information security, engineering, networking, mathematics;
- Cryptography and cryptographic key management concepts;
- Concepts in operating systems, microprocessors, network access, identify, and access management, penetration testing;
- Data security conceptions and functions;
- Data security analysis methodologies, testing and protocols;
- System design tools, methods, and techniques;

- Secure coding and configuration techniques;
- System life cycle management principles, including software security and usability;
- System testing and evaluation methodologies and processes;
- Conducting vulnerability scans and recognizing vulnerabilities in security systems;
- Networking protocols and design processes;
- System, application and data security threats, risks and vulnerabilities;
- Designing countermeasures to identified security risks;
- Risk management policies, requirements, and practices;
- Business continuity and disaster response planning;
- Cost/benefit analysis;
- A working knowledge of cyber security principles and elements;
- Industry standards and organizationally accepted analysis principles and methods; and
- Develop and conduct risk or impact assessments, business cases, and risk management documents.

Key Proficiencies

- Research, Analytical, Problem-solving, Organization, Time Management, Interpersonal, Communication skills

4.13 PROJECT MANAGER

Basic Job Description

- Manages information technology projects throughout their life cycle.

Cyber Security Related Tasks

- Monitor and assess all aspects of cyber security projects and address any issues;
- Assess technological trends and risks, and determine potential impact to projects;
- Develop mechanisms to monitor and measure risk, compliance, and assurance efforts;
- Provide cyber security and risk management guidance for development of business continuity operations, strategic plans, and procedures;
- Review project costs, design concepts, and any changes;
- Review, implement, update, and document cyber security policies, standards, and procedures;
- Resolve conflicts in laws, regulations, policies, or procedures;
- Review or conduct audits of security projects or reports, identifying any significant issues, initiating corrective action and ensuring that outstanding issues are followed up;
- Lead the underlying operations and procedures that support the organization's activities;
- Establish and maintain communication channels with stakeholders on cyber security operational procedures that support the organization's activities;
- Prepare and publish risk management documents;
- Develop, deliver, and oversee training material and educational efforts; and
- Identify and address cyber security workforce planning and management issues.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Science, Computer Engineer, Information Technology, Management Information Systems, System Engineer, or equivalent);
- Certifications an asset: Project Management Professional (PMP); and
- Previous training and experience in IT security infrastructure or project management is preferred. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Business analysis techniques;
- Maintain a working knowledge of cyber security principles and elements;
- Technical knowledge of computer and network systems, embedded security, and platforms;
- Current and emerging technology and cyber security technologies;
- Risk management policies, requirements, and practices;
- Resource management principles and techniques;
- System life cycle management principles, including software security and usability; and
- Develop risk assessments, audit reports, risk management documents.

Key Proficiencies

- Research, Analytical, Problem-solving, Organizational, Time Management, Interpersonal, Communications skills

4.14 SUPPLY CHAIN MANAGER

Basic Job Description

- Manages 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.

Cyber Security Related Tasks

- Create processes and methods to gather supply chain information;
- Define, develop, review, and maintain policies, standards, and processes for identifying, assessing, and mitigating supply chain risks;
- Develop and maintain risk and threat assessments and related reports on vendors and procured products or services, based on risk or threat level;
- Assess and document cyber security risks and vulnerabilities throughout the procurement life cycle;
- Develop, maintain, and refine risk mitigation approaches and procedures;
- Analyze cyber security solutions available on the market that best meet organizational needs;
- Ensure compliance with cyber security policies, regulations, and procedures of the organization;
- Ensure compliance with security requirements of organization networks and systems; and
- Coordinate with cyber security experts to regularly monitor systems and controls, and to update organization policies and procedures;
- Lead the underlying operations and procedures that support the organization’s activities;
- Establish and maintain communication channels with stakeholders on supply chain;
- Develop, deliver, and oversee training material and educational efforts; and
- Identify and address cyber security workforce planning and management issue.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Business Administration, Computer Science, Computer Engineering or equivalent); and
- Previous training and experience in cyber security preferred. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Information and data analysis techniques;
- A working knowledge of cyber security and privacy principles and methods (e.g., firewalls, encryption, virtual private network devices);
- Technical knowledge to understand data security and integrity, security requirements, and the functional and technical design of networks and system, and cyber security solutions;
- Risk management processes, responsibilities and authorities;
- System life cycle management principles, including software security and usability;
- Current national supply chain processes;
- Configuration management related to cyber security;
- Applicable laws, regulations and guidelines as they relate to cyber security; and
- Develop risk and threat assessments.

Key Proficiencies

- Analytical, Problem-solving, Attention to Detail, Organizational, Time Management, Interpersonal, Communication skills

5 PROTECT AND DEFEND

5.1 CYBER SECURITY ANALYST

Basic Job Description

- Coordinates and remediates cyber incidents and threats to and within an organization by using data collected from various cyber defence tools to monitor, identify, analyze, report, and prevent threats and events.

Cyber Security Related Tasks

- Differentiate and analyze network traffic to identify irregular/malicious activity and potential threats to network resources;
- Analyze irregular/malicious activity and potential threats using information gathered from various sources within the organization to gain situational awareness and determine the root cause and the effectiveness of an attack;
- Provide timely detection, identification, and alerting of irregular/malicious activities and potential threats/attacks and distinguish these incidents and events from benign activities;
- Document and escalate incidents or threats that may cause ongoing and immediate impact to the organization;
- Notify management, cyber incident responders/handlers, and colleagues of suspected incidents and threats and potential impact for further action based on the organization's cyber incident response plan;
- Use cyber defence tools for continual monitoring and analysis of network traffic/systems to identify irregular/malicious activity and potential threats;
- Recommend and install appropriate tools and countermeasures based on threats and vulnerabilities;
- Define, develop, implement, and maintain cyber security policies and procedures;
- Plan, implement and upgrade security measures, controls, and protocols to protect information systems against cyber incidents or threats;
- Conduct vulnerability testing, risk analyses, and security assessments;
- Isolate and remove malicious software;
- Anticipate security alerts, incidents and threats and reduce their likelihood;
- Assist and coordinate with colleagues to validate security alerts, incidents and threats; and
- Conduct research, analysis and prepare cyber defence trend reports and internal and external audit reports.

Commonly Requested Education and Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Computer Science, Information Technology, Computer Engineering or equivalent);
- Certifications an asset: Global Information Assurance Certification (GIAC); Certified Information Systems Security Professional (CISSP); Computing Technology Industry Association (CompTIA) Security+; and
- Previous training and experience in network security is preferred – 1-3 years of experience for entry-level; 5 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

Knowledge of and skills in

- Technical knowledge of networks, computer architecture, data structures, and algorithms;
- C, C++, Java, Python, and similar computer programming languages;
- Cryptography and cryptographic key management concepts;
- A working knowledge of cyber security and privacy principles and methods (e.g., firewalls, encryption, virtual private network devices);
- Authentication, authorization, and access control methods, mechanisms;
- Controls related to the use, processing, storage and transmission of data;
- Network access, identity, and access management;
- Network protocols and packet analysis tools;
- Operating systems and system administrations hardening techniques;
- Intrusion detection system (IDS)/Intrusion prevention system (IPS), penetration and vulnerability testing;
- System testing and evaluation methodologies and processes;
- Data loss prevention (DLP), anti-virus and anti-malicious software;
- Incident response and handling methodologies;
- Current and emerging technology and cyber security technologies; and
- Applicable laws, regulations, policies and ethics as they relate to cyber security.

Key Proficiencies

- Analytical, Attention to Detail, Interpersonal, Communication skills

5.2 INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY ANALYST

Basic Job Description

- Performs engineering and technical tasks in support of industrial control system (ICS) to ensure they are functioning properly and secure.

Cyber Security Related Tasks

- Actively monitor ICS system performance and health, and troubleshoot and resolve hardware or software interoperability issues, and system outages and faults, and cyber threats;
- Design, install, operate and maintain equipment, servers, networks and other components to ICS system;
- Conduct maintenance and upgrades;
- Conduct vulnerability testing, risk analyses, and security assessments;
- Conduct analysis and review, and report on system vulnerability;
- Research and evaluate new technologies and processes that enhance security capabilities;
- Research and develop a system security context and define system security requirements based on industry standards and cyber security policies and practices;
- Ensure acquired or developed systems are consistent with cyber security policies and practices;
- Conduct security reviews and identify gaps or cyber threats in ICS system;
- Prepare technical reports that document the system development process;
- Document and address an organization's information security and systems security engineering requirements throughout the system life cycle;
- Define, develop, implement, and maintain infrastructure policies, standards, and procedures;
- Develop and maintain project reports, assessments, and other relevant documents; and
- Develop, deliver, and oversee training material and educational efforts.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Engineering, Computer Science, Information Systems, Control Systems Engineering, Mathematics, or equivalent);
- Previous training and experience in a process control or ICS is preferred – 2-3 years of experience for entry-level; 5-10 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- ICS systems software and hardware, programmable logic controllers, and digital and analog relaying;
- Telemetry systems, data communications, data acquisition and process control;
- Operating systems, networking, and communications systems concepts;
- Computer and networking troubleshooting and maintenance procedures;
- Network administration principles and practices;
- System life cycle management principles, including software security and usability;
- 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; and

- Develop assessments, reports and relevant documents.

Key Proficiencies

- Research, Analytical, Problem-solving, Organizational, Interpersonal, Communication skills

5.3 INFORMATION SECURITY ANALYST

Basic Job Description

- Coordinates the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Cyber Security Related Tasks

- Monitor and analyze systems to identify security breaches;
- Provide timely detection, identification, and alerting of security breaches;
- Document and escalate breaches that may cause ongoing and immediate impact to the organization;
- Notify management and colleagues of suspected security breaches and potential impact for further action based on the organization's cyber incident response plan and cyber security policies;
- Recommend and install and maintain software to protect information;
- Define, develop, implement, and maintain cyber security policies and procedures;
- Plan, implement and upgrade security measures, controls, and protocols to protect digital files and information systems against cyber incidents or threats;
- Conduct vulnerability testing, risk analyses, and security assessments; and
- Conduct research, analysis and prepare cyber defence trend reports and internal and external audit reports.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Computer Science, Information Technology, Computer Engineering or equivalent);
- Certifications an asset: Global Information Assurance Certification (GIAC); Certified Information Systems Security Professional (CISSP); Computing Technology Industry Association (CompTIA) Security+; and
- Previous training and experience in information security is preferred – 1-3 years of experience for entry-level; 5 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer architecture, data structures, and algorithms;
- C, C++, Java, and similar computer programming languages;
- Cryptography and cryptographic key management concepts;
- A working knowledge of cyber security and privacy principles and methods (e.g., firewalls, demilitarized zones, encryption, virtual private network devices);
- Authentication, authorization, and access control methods, mechanisms;
- Controls related to the use, processing, storage and transmission of data;
- Information assurance;
- Network access, identity, and access management;
- Transmission Control Protocol and Internet Protocol;
- Intrusion detection system (IDS)/Intrusion prevention system (IPS), penetration and vulnerability testing;
- System testing and evaluation methodologies and processes;
- Data loss prevention (DLP), anti-virus and anti-malicious software;
- Incident response and handling methodologies;
- Current and emerging technology and cyber security technologies; and

- Applicable laws, regulations, policies and ethics as they relate to cyber security.

Key Proficiencies

- Analytical, Problem-solving, Attention to Detail, Organization, Time Management, Interpersonal, Communication skills

5.4 VULNERABILITY ASSESSMENT ANALYST

Basic Job Description

- Scans applications and operating systems to identify flaws, and vulnerabilities; and conducts and presents vulnerability assessments on an organization's networks and systems.

Cyber Security Related Tasks

- Identify 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 defence audit toolkit (e.g., specialized cyber defence software and hardware) to support cyber defence 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; and
- Make recommendations on the selection of cost-effective security controls to mitigate risks.

Commonly Requested Education, Training, and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Information Technology, Computer Science or equivalent);
- Certifications an asset: Certified Information Systems Security Professional (CISSP); and
- Previous training and experience in identity and access management is preferred – 2-3 years of related work experience for entry-level; 5-7 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- System and application security threats and vulnerabilities (e.g., buffer overflow, cross-site scripting, structured query language (SQL), malicious code);
- Penetration testing principles, tools, and techniques;
- System administration, network, and operating system hardening techniques;
- Packet analysis using appropriate tools;
- Risk management processes for assessing and mitigating risks;
- System administration concepts;
- Cryptography and cryptographic key management concepts;
- 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;
- Using social engineering techniques; and
- Identifying security issues based on the analysis of vulnerability and configuration data.

Key Proficiencies

- Research, Analytical, Attention to Detail, Interpersonal, Communication skills

5.5 PENETRATION TESTER

Basic Job 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.

Cyber Security Related 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, systems, and facilities;
- Develop penetration tests and the tools needed to execute them;
- Investigate for unknown security vulnerabilities and weaknesses in web applications, networks, and relevant systems that cyber actors can exploit;
- Develop and maintain documents on the results of executed pentesting 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; and
- Provide recommendations and guidelines on how to improve upon an organization's security practices.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Information Technology, Computer Science, Computer Engineering, Computer Forensic or equivalent);
- Certifications an asset: Global Information Assurance Certification (GIAC); Computing Technology Industry Association (CompTIA) Security+; Offensive Security Certified Professional (OSCP); and
- Previous training and experience in cyber security role supporting cyber defence, incident or vulnerability management is preferred – 1-3 years of security-related experience for entry-level; 7-10 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Cryptography and cryptographic key management concepts;
- Virtual Private Network devices and encryption solutions;
- Penetration testing principles, tools, and techniques;
- Vulnerability assessment and penetration testing methodologies and applications;
- System and application security threats and vulnerabilities (e.g., buffer overflow, cross-site scripting, structured query language (SQL), malicious code);
- Network security architecture concepts and principles;
- Conduct security audits;
- Develop secure code;
- Using reverse engineering techniques.

Key Proficiencies

- Research, Analytical, Interpersonal, Communication skills

5.6 CYBER SECURITY INCIDENT RESPONDER/HANDLER

Basic Job 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.

Cyber Security Related Tasks

- Perform real-time cyber defence incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation);
- Conduct 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 to detect threats;
- 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;
- 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; and
- Create a program development plan that includes security gap assessments, policies, procedures, playbooks, and training manuals.

Commonly Requested Education, Training, and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Computer Science, Computer Engineering, Computer Forensics or equivalent);
- Certifications an asset: Global Information Assurance Certification (GIAC); Certified Information Systems Security Professional (CISSP); and
- Previous training and experience in network security is preferred – 2-3 years of security/incident response experience for entry-level; five years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- System and application-based security threats and vulnerabilities;
- Cyber threat actor tactics, techniques, and procedures (TTPs);
- Malware analysis methodologies, tools and techniques;
- Cyber security investigations and evidence preservation;
- Vulnerability assessment basics;
- Incident management processes, responsibilities and authorities;
- Incident handling and response methodologies;
- Incident handling in the cloud and virtualized environments;

- Incident handling in wireless and mobile device environments; and
- Business continuity and disaster response basics.

Key Proficiencies

- Analytical, Problem-solving, Organizational, Time Management, Interpersonal, Communication skills

5.7 DIGITAL FORENSICS ANALYST

Basic Job Description

- 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.

Cyber Security Related Tasks

- Perform real-time cyber defence incident investigations (e.g., forensic collections, intrusion correlation and tracking, and threat analysis);
- Investigate security incidents;
- 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 defence 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); and
- Prepare and review forensics policies, standards, procedures and guidelines.

Commonly Requested Education, Training, and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Science, Computer Forensic, Computer Engineering or equivalent);
- Certifications an asset: Certified Information Systems Security Professional (CISSP); Global Information Assurance Certification (GIAC); and
- Previous training and experience in IT security analyst or incident response activities is preferred – 1-3 years of forensics experience for entry-level; five years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Incident response and handling methodologies;
- 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, mobile device, network, computer (dead box), etc.);
- Malware analysis tools and techniques; and
- Reverse engineering.

Key Proficiencies

- Research, Analytical, Attention to detail, Interpersonal, Communication skills

6 OPERATE AND MAINTAIN

6.1 NETWORK SECURITY OPERATOR/SPECIALIST

Basic Job Description

- Develops, creates, integrates, tests, and maintains computer and information system security throughout the systems life cycle, and reports on information system performance;
- Actively monitoring networks to detect, prevent, and recover from security threats.

Cyber Security Related Tasks

- Define and review an organization's networks and computer 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;
- Plan, research, implement, and maintain secure networks and computer systems using scientific analysis and mathematical models;
- Research current and emerging technologies to understand capabilities of required networks or systems;
- 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;
- Define, develop, implement, and maintain cyber security policies and procedures;
- Develop and conduct network testing and validation procedures, programming, and secure coding, and report on functionality and resiliency;
- Conduct vulnerability testing and security reviews on networks to identify gaps, and examine controls and measures required to protect against irregular/malicious activity and potential threats to networks;
- Actively monitor and analyze network traffic/systems to identify irregular/malicious activity and potential threats;
- Provide timely detection, identification, and alerting of irregular/malicious activities and potential threats/attacks and distinguish these incidents and events from benign activities;
- Document and escalate incidents or threats that may cause ongoing and immediate impact to the organization;
- Notify management, cyber incident responders/handlers, and colleagues of suspected incidents and threats and potential impact for further action based on the organization's cyber incident response plan; and
- Recommend and install and upgrade security measures, controls, and protocols to protect digital files and networks or systems against cyber threats and vulnerabilities.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Computer Science, Information Technology, Computer Engineering or equivalent);
- Certifications an asset: Certified Information Systems Security Professional (CISSP); and
- Previous training and experience in network security is preferred – 1-3 years of experience for entry-level; 5 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, power supply technology, system protocols, cyber security-enabled software;
- Principles in information security, engineering, networking, mathematics;
- Cryptography and cryptographic key management concepts;
- Concepts in operating systems, microprocessors, network access, identity and access management, penetration testing;
- Network protocols and packet analysis tools;
- Operating systems and system administrations hardening techniques;
- System design tools, methods, and techniques;
- Secure coding and configuration techniques;
- Computer architecture, data structures, and algorithms;
- Linear/matrix algebra and/or discrete mathematics;
- C, C++, Java, Python, and similar computer programming languages;
- System life cycle management principles, including software security and usability;
- System testing and evaluation methodologies and processes;
- Intrusion detection system (IDS)/Intrusion prevention system (IPS), penetration and vulnerability testing;
- System, application and data security threats, risks and vulnerabilities;
- Incident response and handling methodologies;
- Designing countermeasures to identified security risks;
- Risk management policies, requirements, and practices;
- Business continuity and disaster response planning;
- A working knowledge of cyber security and privacy principles and methods (e.g., firewalls, demilitarized zones, encryption, virtual private network devices);
- Industry standards and organizationally accepted analysis principles and methods;
- Develop and conduct risk assessments and relevant documents; and
- Current and emerging technology and cyber security technologies.

Key Proficiencies

- Research, Analytical, Attention to Detail, Interpersonal, Communication skills

6.2 SYSTEM ADMINISTRATOR

Basic Job Description

- Sets up and maintains networks or specific components of a computer system (e.g.: installing, configuring, and updating hardware, software and networks; monitoring system performance and troubleshooting issues; implementing operational and technical security controls; and adhering to organizational cyber security policies and procedures).

Cyber Security Related Tasks

- Install, configure, and update hardware, software, and networks;
- Conduct functional and connectivity testing to ensure continuing operability and efficiency;
- Manage network servers and technology tools, including performance, capacity, availability, serviceability, and recoverability, and access to systems and workstations;
- Monitor performance and maintain systems/server configuration according to security requirements;
- Troubleshoot hardware or software interoperability issues and outages;
- Diagnose and repair faulty systems and servers;
- Maintain system security through access controls, backups, and other controls, in accordance to organizational policies and procedures;
- Implement cyber security policies, network security, application security, access controls and organizational data safeguards; and
- Develop documentation on system administration standard operating procedures.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Computer Science, Information Technology or equivalent);
- Certifications an asset: Certified Information Systems Security Professional (CISSP); Computing Technology Industry Association (CompTIA) Security+; and
- Previous training and experience in network security is preferred – 1-3 years of experience for entry-level; five years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Technical knowledge, security principles, and methods (e.g., firewalls, encryption), and the functional and technical design of networks and system, and cyber security solutions;
- System life cycle management principles, including software security and usability;
- Measures or indicators of system performance, availability, capacity, or configuration problems;
- Analysis tools and network protocols;
- System administration, network, and operating system hardening techniques;
- Server and client operating systems;
- Systems administration concepts;
- Configuring and optimizing software, systems or servers;
- System security and data backup/recovery; and
- Diagnostic tools and fault identification techniques.

Key Proficiencies

- Problem-solving, Attention to Detail, Organizational, Time Management, Interpersonal, Communication skills

6.3 CRYPTOGRAPHER/CRYPTANALYST

Basic Job Description

- Develops algorithms, ciphers, and security systems to encrypt information.
- Analyzes coding systems and decodes messages.
- Code makers and code breaker protecting the privacy of organizations and individuals by supervising the online security of data systems.

Cyber Security Related Tasks

- Protect important information from interception, access and modification;
- Evaluate, analyze and target weaknesses in security systems and algorithms;
- Develop robust security systems to prevent vulnerabilities;
- Develop statistical and mathematical models to analyze data and troubleshoot security problems;
- Test computational models for reliability and accuracy;
- Identify, research and test new cryptology theories and applications;
- Decode cryptic messages and coding systems for organization;
- Develop and update methods for efficient handling of cryptic processes;
- Prepare technical reports that document security processes or vulnerabilities; and
- Provide guidance to management and personnel on cryptical or mathematical methods and applications.

Commonly Requested Education, Training and Work Experience

- Post-secondary University degree in Computer Engineering, Computer Science, or Mathematics. A Master's of Science or Doctorate is strongly preferred;
- Previous training and experience in cyber security or IT security infrastructure is preferred – 3 years of experience for entry-level; 5-10 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Computer architecture, data structures, and algorithms;
- Linear/matrix algebra and/or discrete mathematics;
- Probability theory, information theory, complexity theory and number theory;
- C, C++, Java, Python, and similar computer programming languages;
- 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.); and
- Applicable laws, legal codes, regulations, policies and ethics as they relate to cyber security.

Key Proficiencies

- Analytical, Problem-solving, Time Management, Interpersonal, Communications skills

6.4 TECHNICAL SUPPORT SPECIALIST

Basic Job Description

- Provides technical support to an organization based on established or approved process components, systems, and protocols.

Cyber Security Related Tasks

- Actively monitor computer system performance and health, and troubleshoot and resolve hardware or software interoperability issues, and system outages and faults;
- Install, configure, and maintain operating system software, hardware, and peripheral equipment based on organizational policies, standards, and procedures;
- 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 computing environments;
- Administer user accounts, network privileges, and access to systems and equipment;
- Conduct asset management or inventory control of system and equipment resources; and
- Develop, deliver, and oversee training material and educational efforts.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Computer Science, Information Systems or equivalent); and
- Previous training and experience in technical support is preferred – 1-3 years of related work experience for entry-level; 5-7 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software, cloud technology;
- System administration, operating system, microprocessor, and identity and access management concepts;
- System life cycle management principles, including software security and usability;
- Measures or indicators of system performance, usability, and availability;
- A working knowledge of cyber security principles and elements;
- Operations and processes for incident, security problems, and event management;
- Industry standards and organizationally accepted analysis principles and methods; and
- Develop, update, and maintain standard operating procedures, and incident, security problem or event reports.

Key Proficiencies

- Analytical, Problem-solving, Interpersonal, Communication skills

7 DESIGN AND DEVELOP

7.1 CRITICAL INFRASTRUCTURE ENGINEER

Basic Job Description

- Designs, builds, deploys, and maintains the information technology (IT) infrastructure; ensures all IT systems support the organization operate efficiently.

Cyber Security Related Tasks

- Define and review an organization's information systems, configurations, and controls, 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 design robust solutions for systems and networks;
- Ensure acquired or developed systems are consistent with cyber security policies and practices;
- Conduct routine preventative maintenance of network infrastructure including implementing software, updates, and examine and address potential gaps in infrastructure, and cyber threats;
- Conduct vulnerability testing, risk and security assessments;
- Document network malfunctions and corresponding actions taken to ensure a detailed record of activity;
- Analyze and recommend improvements and changes to computing environments;
- Maintain security of system and inter-application information transfers;
- Enhance, plan capacity, and design related to infrastructure engineering projects;
- Prepare technical reports that document the system development process;
- Document and address an organization's information systems engineering requirements throughout the system life cycle;
- Advise on security requirements and risk management process activities and other related documents;
- Conduct security reviews and advise on business continuity plans, and contingency and disaster recovery plans;
- Develop project reports, assessments, and other relevant documents;
- Respond to security-related incidents and provide a thorough post-event analysis; and
- Define, develop, implement, and maintain infrastructure policies, standards, and procedures; and
- Develop, deliver, and oversee training material and educational efforts.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Engineering, Computer Science, or equivalent);
- Previous training and experience in cyber security or IT security infrastructure is preferred – 3 years of experience for entry-level; 5-10 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software;
- Security engineering models;
- Cryptography and cryptographic key management concepts;
- Virtual Private Network devices and encryption;
- Engineering concepts and practices as applied to computer 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;
- Networking protocols and design processes;
- Industry standards and organizationally accepted analysis principles and methods;
- Configuring and using software-based computer protection tools; and
- Designing hardware and software solutions.

Key Proficiencies

- Research, Analytical, Attention to Detail, Problem-solving, Organizational, interpersonal, Communication skills

7.2 REQUIREMENTS ANALYST

Basic Job Description

- Evaluates functional and security requirements of controls and systems, and translates requirements into cyber security solutions.

Cyber Security Related Tasks

- Define project scope and objectives based on organization’s goals and activities;
- Conduct research and analysis to develop, document, and refine functional and security requirements of controls and systems;
- Ensure functional and security requirements are consistent with organization’s cyber security policies and practices and applicable industry guidelines;
- Consult with management and colleagues to evaluate functional and security requirements;
- Translate functional and security requirements into cyber security solutions;
- Develop and document functional and security requirements, capabilities, and constraints for design and develop procedures and processes;
- Coordinate with Security Architects, Security Engineers, and Developers, as needed, to provide oversight in the development of cyber security solutions;
- Oversee and make recommendations regarding implementation of security controls and systems based on functional and security requirements;
- Identify and document risks related to cyber security solutions and organization activities;
- Develop or contribute to risk assessments of controls and systems and related cyber security solutions;
- Conduct analysis to determine opportunities for new and improve organization cyber security solutions; and
- Develop and document system security concept of operations.

Commonly Requests Education, Training and Work Experience

- Post-secondary education diploma in a cyber or IT related field (e.g., Computer Engineering, Computer Science or equivalent);
- Certifications an asset: Global Information Assurance Certification (GIAC); Computing Technology Industry Association (CompTIA); Certified Information Systems Security Professional (CISSP); and
- Individuals typically employed in this role have extensive experience in cyber security activities. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, power supply technology, system protocols, cyber security-enabled software;
- Cryptography and cryptographic key management concepts;
- Virtual Private Network devices and encryption;
- Engineering concepts and practices as applied to computer architecture;
- Security architecture concepts and enterprise architecture reference models;
- Network access, identity, and access management;
- Secure configuration management techniques;
- Security assessment and authorization processes;
- Capabilities and requirements analysis;

- 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;
- Functionality, quality, and security requirements and how these apply to specific items and tools;
- Networking protocols and design processes;
- Industry standards and organizationally accepted analysis principles and methods; and
- Controls related to the use, processing, storage and transmission of data.

Key Proficiencies

- Research, Analytical, Problem-solving, Interpersonal, Communication skills

7.3 SECURITY ARCHITECT

Basic Job 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.

Cyber Security Related Tasks

- 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;
- Respond immediately to security incidents and provide a thorough post-event analysis; and
- Update and upgrade security systems as needed.

Commonly Requested Education, Training and Work Experience

- Post-secondary University Degree in Computer Engineering or related discipline. Cyber or IT security specialization preferred;
- Certifications an asset: Global Information Assurance Certification (GIAC); Computing Technology Industry Association (CompTIA); Certified Information Systems Security Professional (CISSP); CISSP- Information Systems Security Architecture Professional (ISSAP); and
- 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. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software;
- Cryptography and cryptographic key management concepts;
- Virtual Private Network devices and encryption;
- Engineering concepts and practices as applied to computer 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;
- Networking protocols and design processes;
- Industry standards and organizationally accepted analysis principles and methods;
- Security compliance frameworks;
- Configuring and using software-based computer protection tools; and
- Designing hardware and software solutions.

Key Proficiencies

- Research, Analytical, Problem-solving, Interpersonal, Communication skills

7.4 SECURITY ENGINEER

Basic Job Description

- Develops and maintains robust security solutions for an organization’s networks and systems, ensuring security requirements are adequately addressed in all aspects of system design based on industry standards and practices, and organization policies and procedures, and advises on security-related issues and vulnerabilities through all phases of the system life cycle.

Cyber Security Related Tasks

- Define and review an organization’s technology and information systems, configurations, and controls, 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 design robust security solutions for systems and networks;
- Conduct vulnerability testing, risk and security assessments;
- Investigate intrusion incidents, conduct forensic investigations and mount incident responses;
- Collaborate with colleagues on authentication, authorization and encryption solutions;
- Research and evaluate new technologies and processes that enhance security capabilities;
- Research and develop a system security context and define system security requirements based on industry standards and cyber security policies and practices;
- Ensure acquired or developed systems are consistent with cyber security policies and practices;
- Conduct security reviews and identify gaps in security architectures and designs (e.g., firewall, virtual private networks, routers, servers, etc.);
- Prepare technical reports that document the system development process;
- Document and address an organization’s information security and systems security engineering requirements throughout the system life cycle;
- Advise on security requirements and risk management process activities and other related documents;
- Conduct security reviews and advise on business continuity plans, and contingency and disaster recovery plans;
- Respond to security-related incidents and provide a thorough post-event analysis; and
- Update and upgrade security systems as needed.

Commonly Requested Education, Training and Work Experience

- Post-secondary University degree in Computer Engineering, Computer Science or related discipline. Cyber or IT security specialization preferred;
- In Canada, the term ‘engineer’ means a licensed professional engineer as defined in the provincial jurisdiction. Accordingly, all security engineers must be licensed to practice engineering within their jurisdiction;
- Certifications an asset: Global Information Assurance Certification (GIAC); Certified Information Systems Security Professional (CISSP); CISSP- Information Systems Security Engineering Professional (ISSEP); and
- Previous training and experience in IT security infrastructure, requirements analysis or program management is preferred – 5-10 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software;
- Security engineering models;
- Cryptography and cryptographic key management concepts;
- Virtual Private Network devices and encryption;
- Engineering concepts and practices as applied to computer 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;
- Networking protocols and design processes;
- Industry standards and organizationally accepted analysis principles and methods;
- Security compliance frameworks;
- Configuring and using software-based computer protection tools; and
- Designing hardware and software solutions.

Key Proficiencies

- Research, Analytical, Problem-solving, Interpersonal, Communication skills

7.5 CYBER SECURITY RESEARCHER

Basic Job Description

- Researches and evaluates current and emerging technology to develop capabilities, ensuring cyber security is fully integrated; and
- Engages and maintains a professional research network aligned to organizational requirements.

Cyber Security Related Tasks

- Research current and emerging technologies to understand capabilities of required networks or systems;
- Design and develop new tools or technologies as they relate to cyber security;
- Collaborate with colleagues to identify and develop appropriate technology solutions;
- Follow software and systems engineering life cycle standards and processes;
- Troubleshoot prototype design and process issues throughout product development phases;
- Evaluate network or system vulnerabilities to enhance capabilities being developed;
- Document and present research findings to appropriate stakeholders;
- Participate in research and development forums and related events; and
- Develop, deliver, and oversee training material and educational efforts.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Science, Computer Engineering or equivalent);
- Certifications an asset: Global Information Assurance Certification (GIAC); Certified Information Systems Security Professional (CISSP); and
- Previous training and experience in security operation roles or security testing and evaluation activities. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software;
- Cryptography and cryptographic key management concepts;
- Current and emerging technology and cyber security technologies;
- System life cycle management principles, including software security and usability;
- Critical infrastructure systems;
- Network security architecture concepts including topology, protocols, components, and principles;
- Operating system structures and internals;
- Network analysis tools;
- Applying engineering concepts and processes;
- Creating and using mathematical models; and
- Designing technology processes and solutions.

Key Proficiencies

- Research, Analytical, Problem-solving, Interpersonal, Communication skills

7.6 SECURITY TESTER & EVALUATOR

Basic Job 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.

Cyber Security Related 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 findings;
- Develop test plans to address specifications, policies, and requirements;
- Validate specifications, policies and requirements for testability;
- Create verifiable evidence of security measures;
- Prepare assessments that document the test results and any security vulnerabilities present;
- Deploy, validate, and verify network infrastructure device operation system software; and
- Develop, deliver, and oversee training material and educational efforts.

Commonly Requested Education, Training and Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Engineering, Computer Science or equivalent);
- Certifications an asset: Certified Information Systems Security Professional (CISSP); and
- Training and experience in an IT security role associated with system and/or software security measurement such as vulnerability assessment, software security. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software;
- Conducting independent validation and verification security testing;
- Systems testing and evaluation methods and techniques;
- Security assessment and authorization processes;
- Security architecture concepts and enterprise information security architecture models;
- Identifying test and evaluation policies and requirements;
- Collect, analyze, verify and validate test data and translate data and test results into conclusions;
- Designing and document test and evaluation strategies; and
- Writing technical and test and evaluation reports.

Key Proficiencies

- Analytical, Problem-solving, Attention to Detail, Interpersonal, Communication skills

7.7 SUPPLY CHAIN INTEGRITY ANALYST

Basic Job Description

- 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.

Cyber Security Related Tasks

- 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 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; and
- Develop and maintain risk assessments and related reports on vendors and products and services, based on reliability and credibility.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g.; Business Administration, Computer engineering, Computer Science, Information Technology or equivalent); and
- Previous training and experience in cyber security preferred.
- Individuals employed in this role can have diverse levels of cyber security expertise. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Information and data analysis techniques;
- A working knowledge of cyber security and privacy principles and methods; (e.g., firewalls, encryption, virtual private network devices);
- Technical knowledge to understand data security and integrity, security requirements, and the functional and technical design of networks and system, and cyber security solutions;
- Risk management processes, responsibilities and authorities;
- System life cycle management principles, including software security and usability;
- Configuration management related to cyber security;
- Applicable laws, regulations and guidelines as they relate to cyber security; and
- Develop risk and threat assessments.

Key Proficiencies

- Analytical, Problem-solving, Attention to Detail, Organizational, Time Management, Interpersonal, Communication skills

7.8 APPLICATION DEVELOPER

Basic Job Description

- Designs, develops, tests, and improves software and applications aimed at helping an organization complete tasks or programs.

Cyber Security Related Tasks

- Research, analyze and implement secure application development techniques;
- Develop, implement, and modify applications using scientific analysis and mathematical models;
- Analyze code requirements to determine time and cost constraints, and risks to organization;
- Develop and conduct application testing and validation procedures, programming, and secure coding, and report on functionality and resiliency;
- Conduct vulnerability scans and reviews on applications, and examine controls and measures required to protect applications;
- Conduct testing of applications to ensure desired information is produced and security levels and procedures are correct;
- Prepare documentation on applications and subsequent revisions;
- Update and upgrade applications as needed to correct errors, and to improve performance and interfaces;
- Prepare reports on applications patches or releases that would leave systems vulnerable;
- Develop countermeasures against potential exploitations of vulnerabilities in applications;
- Perform risk analysis whenever an application undergoes a change; and
- Provide advice and guidance, and coordinate efforts on application security procedures to protect sensitive data from threats and vulnerabilities.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Engineering, Computer Science, or equivalent). A Master’s degree is preferred;
- Previous training and experience in developing and designing applications is preferred – 2-3 years of experience for entry-level; 5-10 years of experience for advanced-level. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software;
- Application security system concepts and functions;
- Software and system design tools, methods, and techniques;
- Software analysis methodologies, testing and protocols;
- Secure coding and configuration techniques;
- Cryptography and cryptographic key management concepts;
- Computer architecture, data structures, and algorithms;
- Linear/matrix algebra and/or discrete mathematics;
- Probability theory and information theory;
- C, C++, Java, Python, and similar computer programming languages;
- Principles in computer programming, software design and debugging, and testing;

- System life cycle management principles, including software security and usability;
- Creating or tailoring programs and code for application specific concerns;
- System testing and evaluation methodologies and processes;
- Conducting vulnerability scans and recognizing vulnerabilities in security systems;
- System, application and data security threats, risks and vulnerabilities;
- Designing countermeasures to identified security risks;
- Industry standards and organizationally accepted analysis principles and methods; and
- Develop and conduct risk or impact assessments, business cases, and risk management documents.

Key Proficiencies

- Research, Analytical, Problem-solving, Interpersonal, Communication skills

7.9 INFORMATION SYSTEMS SECURITY DEVELOPER

Basic Job 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.

Cyber Security Related Tasks

- 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;
- Plan, research, and implement secure information systems using scientific analysis and mathematical models;
- Research current and emerging technologies to understand capabilities of required networks or systems;
- 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, programming, and secure coding, and report on functionality and resiliency;
- Conduct 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 tests of information systems to ensure security levels and procedures are correct and develop a security risk management plan;
- Develop 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 an organization's information security, cyber security architecture, and systems security engineering requirements 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; and
- Provide advice and guidance, and coordinate efforts on risk management and disaster recovery procedures to protect sensitive data from threats and vulnerabilities.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Science, Mathematics, Network Technology, Computer Engineering or equivalent);
- Certifications an asset: Certified Secure Software Lifecycle Professional (CSSLP); and
- Previous training and experience in system development and support is preferred – five years of experience. Requested experience will depend on the organizational need.

Primary Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, system protocols, cyber security-enabled software;
- Principles in information security, engineering, networking, mathematics;
- Cryptography and cryptographic key management concepts;
- Concepts in operating systems, microprocessors, network access, identity and access management, penetration testing;
- Data security conceptions and functions, analysis methodologies, testing, and protocols;
- System design tools, methods, and techniques;
- Secure coding and configuration techniques;
- Computer architecture, data structures, and algorithms;
- Probability theory and information theory;
- C, C++, Java, Python, and similar computer programming languages;
- System life cycle management principles, including software security and usability;
- System testing and evaluation methodologies and processes;
- Conducting vulnerability scans and recognizing vulnerabilities in security systems;
- Networking protocols and design processes;
- System, application and data security threats, risks and vulnerabilities;
- Designing countermeasures to identified security risks;
- Risk management policies, requirements, and practices;
- Business continuity and disaster response planning;
- Cost/benefit analysis;
- A working knowledge of cyber security principles and elements;
- Industry standards and organizationally accepted analysis principles and methods; and
- Develop and conduct risk or impact assessments, business cases, and risk management documents.

Key Proficiencies

- Research, Analytical, Problem-solving, Interpersonal, Communication skills

7.10 SECURE SOFTWARE DEVELOPER

Basic Job Description

- Develops, creates, integrates, and maintains security software, applications or specialized programs, and reports on software/data security achievements and recommends corrective action to address deficiencies.

Cyber Security Related Tasks

- Research, analyze and implement secure application development techniques;
- Develop, implement, and modify software systems or applications using scientific analysis and mathematical models;
- Analyze software requirements to determine time and cost constraints, and risks to organization;
- Develop and conduct software system or application testing and validation procedures, programming, and secure coding, and report on functionality and resiliency;
- Conduct vulnerability scans and reviews on software systems or applications, and examine controls and measures required to protect software systems or applications;
- Conduct tests of software systems or applications to ensure desired information is produced and security levels and procedures are correct;
- Prepare reports on system or application developments and subsequent revisions;
- Update and upgrade software systems or applications as needed to correct errors, and to improve performance and interfaces;
- Prepare reports on software systems or 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; and
- Provide advice and guidance, and coordinate efforts on application security procedures to protect sensitive data from threats and vulnerabilities.

Commonly Requested Education, Training and Work Experience

- Post-secondary education in a cyber or IT related field (e.g., Computer Science, Mathematics, Network Technology, Computer Engineering or equivalent);
- Certifications an asset: Certified Secure Software Lifecycle Professional (CSSLP); and
- Previous training and experience in software development or coding is preferred – five years of experience. Requested experience will depend on the organizational need.

Primary Technical Training Requirements – Learning Outcomes

- Technical knowledge of networks, computer components, power supply technology, system protocols, cyber security-enabled software;
- Principles in computer programming, software design and debugging, and penetration testing;
- Application security system concepts and functions;
- Data security conceptions and functions;
- Software and system design tools, methods, and techniques;
- Software/data security analysis methodologies, testing and protocols;
- Secure coding and configuration techniques;
- Computer architecture, data structures, and algorithms;

- Linear/matrix algebra and/or discrete mathematics;
- Probability theory and information theory;
- C, C++, Java, Python, and similar computer programming languages;
- Creating or tailoring programs and code for application specific concerns;
- Conducting vulnerability scans and recognizing vulnerabilities in security systems;
- System, application and data security threats, risks and vulnerabilities; and
- Designing countermeasures to identified security risks.

Key Proficiencies

- Research, Analytical, Problem-solving, Interpersonal, Communication skills

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Abbreviation	Definition
CCCS	Canadian Centre for Cyber Security
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CISM	Certified Information Security Manager
CompTIA	Computing Technology Industry Association
CSE	Communications Security Establishment
CSO	Chief or Corporate Security Officer
CSSLP	Certified Secure Software Lifecycle Professional
CWF	Cybersecurity Workforce Framework
GIAC	Global Information Assurance Certification
IAPP	International Association of Privacy Professionals
ICT	Information and Communication Technology
IS	Information System
IT	Information Technology
ITS	Information Technology Security
NICE	(U.S.) National Initiative on Cybersecurity Education (NICE)
OSCP	Offensive Security Certified Professional
SFIA	(Global IT) Skills Framework for the Information Age
TRA	Threat and Risk Assessment
TTPs	Tactics, Techniques, and Procedures

9 REFERENCES

[1] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Josang, T. Pereira and E. Stavro, "Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline," in *In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE Companion '18)*, Larnaca, 2018.

[2] Association for Computing Machinery (ACM); , IEEE Computer Society (IEEE-CS); , Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC); , International Federation for Information Processing Technical, "Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," 2017.

[3] Public Safety Canada, "National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age," Ottawa, 2018.

[4] Rapid7 Labs, "National Exposure Index," 7 June 2018. [Online]. Available: https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf. [Accessed July 2019].

[5] ITAC Talent, "Canadianization of the NICE Cybersecurity Workforce Framework: A Proposed Model," Mississauga, 2019.

[6] D. O'Brien, "Internet Security Threat Report: Ransomware 2017," Symantec, 2017.

[7] J. Porup, "What is cyber security? How to build a cyber security strategy," CSO Online, 27 December 2017. [Online]. Available: https://www.csoonline.com/article/3242690-what-is-cyber-security-how-to-build-a-cyber-security-strategy.html. [Accessed July 2019].

[8] US Department of Homeland Security, "Cybersecurity Careers of the Future," 2018.

10 APPENDIX A: METHODOLOGY AND ANALYSIS

The Communications Security Establishment (CSE) conducted an environmental scan of academic curriculums between 2016 and 2017 to identify current cyber security related educational and training programs and courses offered in post-secondary institutions across Canada. This scan was subsequently updated in 2018. Post-secondary educational programs and courses were located through keyword searches primarily using the universitystudy.ca search engine, as well as other websites such as canadian-universities.net, studyincanada.com, ontariocolleges.ca, and Google searches. For each environmental scan, several different keyword searches were conducted using the terms 'security,' 'cyber,' 'computer security,' 'information system,' and 'network.'

The environmental scan addressed two typologies: cyber security specific programs, which were largely technical in nature, and business-related programs, which were largely non-technical in nature. The scan included college diplomas, and university undergraduate and post-graduate degree programs. Those programs identified as cyber security specific included computer-based or IT-related disciplines such as computer science, computer or communications engineering, software development, IT systems administration, where there were significant cyber security components, and IT or cyber security specialized courses. Those programs identified as business-related were surveyed to determine the degree to which cyber security concepts and principles were integrated. This stream included programs such as business administration, communications, finance, management, and project management.

In addition to the environmental scan and the subsequent analysis of those results, there has been a significant amount of anecdotal information collected from subject matter experts, business councils, professional associations, community groups, and others that have reinforced the results.

10.1 MAIN FINDINGS

To summarize, the scan and subsequent analysis revealed the following:

- The number and quality of university and college programs and courses is expanding annually;
- University and college programs predominately focus on generating graduates for the workforce;
- The majority of university and college programs and courses and programs are found within technical departments (e.g. computer science, IT, etc.). They predominantly focus on security operations roles related to detecting, responding to, and mitigating cyber threats;
- Among computer or communications engineering programs, there appears to be very limited content related to cyber security or security writ large as a curriculum requirement;
- Some university and college programs or courses labelled as 'cyber security' only deal with certain aspects of cyber security or are a re-design of existing IT courses to include some cyber security elements. While contributing to role-based requirements, these courses or programs could perhaps be better labelled to indicate the curricular focus (e.g. Cyber Security Operations or Cyber Security Incident Handling).
- Some university and college programs or courses labelled as 'cyber security' reflect the interdisciplinary nature of the field. While attending to the broader educational needs of the generalists, or those who may be employed in the proximity of cyber security, university and college programs or courses often do not provide sufficient depth to support specific cyber security responsibilities within an organization;
- Some university and college programs and courses labelled as 'cyber security' have not attracted enough enrollment to sustain them year to year. Some that are planned and advertised could not even muster enough interest to run;

- Few university and college business-related programs have integrated relevant cyber security content that is applicable to organizations; and
- Relevant, yet underrepresented topics include the Canadian legal and policy context including personal information protection and privacy; ethical considerations including workplace and investigatory practices in organizational contexts; integrated risk management; business communications; and emerging issues.

11 APPENDIX B: POST-SECONDARY CYBER SECURITY RELATED PROGRAMS

The Cyber Centre regularly receives inquiries about cyber security education and training opportunities. Several academic institutions have introduced programs or courses of study within existing programs that serve as examples or exemplars for the larger community. If any institution or organization believes it has a program or a course that should be considered an example or exemplar, please submit it by email to contact@cyber.gc.ca.

Institute	Province	Program Title	Certification
Alison College	Alberta	Information Technology and Cyber Security	Diploma
Algonquin College	Ontario	Computer Systems Technology - Security (Additional Year to the Computer Systems Technician Program)	Diploma
Athabasca University	Alberta	Post-Baccalaureate Certificate in Information Security (PBC-IS)	Certificate
Bow Valley College	Alberta	Cybersecurity	Certificate
British Columbia Institute of Technology	British Columbia	Forensic Investigation - Digital Forensics and Cybersecurity Option	Certificate
		Network Administration and Security Professional (NASP)	
		Industrial Network Cybersecurity	Diploma
		Computer Systems - Network Security Administration Option	Bachelors
		Computer Systems - Network Security Applications Development Option	
		Forensic Investigation - Digital Forensics and Cybersecurity Option	
		Bachelor of Technology in Computer Systems, Network Security Applications Development	
Carleton University	Ontario	Graduate Diploma in Infrastructure Protection and International Security	Diploma
		Master of Infrastructure Protection and International Security	Masters
		Computer and Internet Security	Bachelors
CDI College	Alberta	Cyber Security Specialist	Certificate

Institute	Province	Program Title	Certification
	Manitoba	Network and Internet Security Specialist	Certificate
	Québec	Gestionnaire en réseautique: Spécialiste sécurité	Attestation de Collégiale (AEC)
Cégep de l'Outaouais	Québec	Techniques de l'informatique - Programmation et Sécurité	Diplôme de Collégiale (DEC) technique
		Techniques de l'informatique - Réseaux et Cybersécurité	
Cégep de Saint-Hyacinthe	Québec	Techniques de l'informatique - Réseaux et Cybersécurité	Diplôme de Collégiale (DEC) technique
Cégep de Sherbrooke	Québec	Cybersécurité et sécurité intégrée	Attestation de Collégiale (AEC)
Cégep Garneau	Québec	Cyberenquête	Attestation de Collégiale (AEC)
Cégep Limoilou	Québec	Techniques de l'informatique - Gestion des réseaux	Diplôme de Collégiale (DEC) technique
Cégep Saint-Jean-sur-Richelieu	Québec	Administration des réseaux et sécurité informatique	Attestation de Collégiale (AEC)
Centennial College	Ontario	Cybersecurity	Graduate Certificate
College of the North Atlantic	Newfoundland	Cyber Security Infrastructure	Advanced Diploma
Collège Ahunstic	Québec	Réseautique et sécurité informatique	Attestation de Collégiale (AEC)
		Techniques de l'informatique - profil réseaux et sécurité	Diplôme de Collégiale (DEC) technique
Collège communautaire du Nouveau-Brunswick	New Brunswick	Réseautique et Sécurité Informatique	Diploma
		Cybersécurité	
Collège de Bois-de-Boulogne	Québec	Sécurité informatique et réseautique	Attestation de Collégiale (AEC)

Institute	Province	Program Title	Certification
		Techniques de l'informatique - Profil Infrastructures et Sécurité	Diplôme de Collégiale (DEC) technique
Collège de Maisonneuve	Québec	Gestion de réseaux et sécurité des systèmes	Attestation de Collégiale (AEC)
		Techniques de l'informatique - Infrastructure et Sécurité des réseaux	Diplôme de Collégiale (DEC) technique
Collège La Cité	Ontario	Technologie de l'information - sécurité informatique	Diploma
Collège LaSalle	Québec	Techniques de l'informatique - Gestion de réseaux et sécurité	Diplôme de Collégiale (DEC) technique
Collège Lionel-Groulx	Québec	Administration des réseaux et sécurité informatique	Attestation de Collégiale (AEC)
Collège Montmorency	Québec	Techniques de l’informatique - Spécialisation: Réseaux et sécurité informatiques	Diplôme de Collégiale (DEC) technique
Collège Rosemont	Québec	Microprogramme de perfectionnement en sécurité des réseaux	Attestation de Collégiale (AEC)
		Techniques de l'informatique - Profil réseautique: sécurité et virtualisation	Diplôme de Collégiale (DEC) technique
Concordia University	Québec	Information Systems Security (MASc)	Masters
		Information Systems Security (MEng)	
Concordia University of Edmonton	Alberta	Graduate Diploma in Information Assurance	Diploma
		Graduate Diploma in Information Security	
		Master of Information Systems Assurance Management	Masters
		Master of Information Systems Security Management	
Conestoga College	Ontario	Network Security Investigations	Certificate

Institute	Province	Program Title	Certification
		Cyber Security	Graduate Certificate
		Computer Application Security	
		Information Technology Network Security	
Durham College	Ontario	Information Systems Security – Computers and Networking	Graduate Certificate
Eastern College	New Brunswick	Advanced Systems Management and Cyber Security	Diploma
Fanshawe College	Ontario	Cyber Security	Diploma
		Information Security Management	Graduate Certificate
		Network and Security Architecture	
Fleming College	Ontario	Computer Security and Investigations	Diploma
George Brown College	Ontario	Network Security Fundamentals Certificate	Certificate
		Information Security Management Certificate	
		Network and System Security Analysis	Graduate Certificate
Georgian College	Ontario	Information Systems Security	Graduate Certificate
HEC Montréal	Québec	Certificat en analyse de la sécurité de l'information et des systèmes	Certificate
Heritage College	Québec	Microsoft Network and Security Administrator	Attestation de Collégiale (AEC)
Humber College	Ontario	Cyber Crime Specialist	Certificate
Institut supérieur d'informatique	Québec	Computer Networks and Security	Attestation de Collégiale (AEC)
		Réseaux Informatiques et Sécurité	

Institute	Province	Program Title	Certification
Lambton College	Ontario	Cyber Security and Computer Forensics	Graduate Certificate
		Cyber Security	
		Cyber Infrastructure Specialist	
Loyalist College	Ontario	Cyber Security	Certificate
Manitoba Institute of Trades and Technology	Manitoba	Network Security Diploma	Diploma
		Cyber Defence and Cloud Administration Diploma	
Mohawk College	Ontario	Computer Systems Technology - Network Engineering and Security Analyst	Diploma
		Cyber Security Analytics	Graduate Certificate
Mount Royal University	Alberta	Cyber Security Fundamentals	Certificate
		Advanced Cyber Security	Certificate
New Brunswick Community College	New Brunswick	Information Technology: Cybersecurity	Post-graduate diploma
New York Institute of Technology	British Columbia	Master of Information, Network, and Computer Security	Masters
Northeastern University	Ontario	Master of Science in Cybersecurity	Masters
Northern Alberta Institute of Technology	Alberta	Core Security+ Certificate	Certificate
		Enterprise Security Certificate	
		System Security Certificate	
Nova Scotia Community College	Nova Scotia	Cyber Security	Diploma
		IT Systems Management and Security	

Institute	Province	Program Title	Certification
Okanagan College	British Columbia	Blockchain Certificate	Certificate
Oulton College	New Brunswick	System Management and Cyber Security	Diploma
Polytechnique Montréal	Québec	Certificat en Cyberenquête	Certificate
		Certificat en cyberfraude	
		Certificat en Cybersécurité des réseaux informatiques	
		Undergraduate microprogram in Networking and Security	Microprogramme
		Microprogramme de 1er cycle en Cyberinvestigation	
		Microprogramme de 1er cycle en Réseautique et sécurité	
QCT College	Alberta	Cyber Security Specialist	Diploma
Queen's University	Ontario	NSERC CREATE Cybersecurity	
Red River College	Manitoba	Information Security	Post-graduate Diploma
Robertson College	Alberta	Network Security Technician	Diploma
Ryerson University	Ontario	Computer Security and Digital Forensics	Certificate
		MBA in Management of Technology and Innovation, Data Security and Privacy Specialization	Masters
Saskatchewan Polytechnic	Saskatchewan	Cyber Security	Post-graduate Certificate
Sault College	Ontario	Network Architecture and Security Analytics	Graduate Certificate
		Cyber Security Canadian Context	Certificate

Institute	Province	Program Title	Certification
Seneca College	Ontario	Honours Bachelor of Technology - Informatics and Security	Bachelors
		Cyber Security and Threat Management	Certificate
		Cyber Security	Graduate Certificate
Sheridan College	Ontario	Honours Bachelor of Applied Information Sciences (Information Systems Security)	Bachelors
		Cybersecurity - Legal and Ethical Policies and Procedures	Recognition of achievement
		Cybersecurity Foundations	
Southern Alberta Institute of Technology	Alberta	Cyber Security for Control Systems	Certificate
		Information Security Analyst	
		Information Systems Security	
		IT Security Certificate of Achievement	
The King's University	Alberta	Computer Science – Cyber Security Stream	Bachelors
Université de Moncton	New Brunswick	Certificat en gestion de la sécurité de l'information des entreprises	Certificate
Université de Sherbrooke	Québec	Gouvernance, audit et sécurité des technologies de l'information	Diplôme d'Études Supérieures Spécialisées (DESS)
		Gouvernance, audit et sécurité des technologies de l'information	Microprogramme
		Gouvernance, audit et sécurité des technologies de l'information (GASTI)	Masters
University of Alberta	Alberta	Information Access and Protection of Privacy	Certificate
University of Calgary	Alberta	Bachelor of Computer Science (Security Concentration Option)	Bachelors
		Graduate Certificate in Network Security	Graduate Certificate
		Graduate Certificate in Software Security	

Institute	Province	Program Title	Certification
University of Guelph	Ontario	Certificate in Information Management, Privacy, and Access	Certificate
		Cybersecurity Threat Intelligence Program	Masters
University of New Brunswick	New Brunswick	Computer Science (Cybersecurity specialization)	Bachelors
		Cyber Security	Masters
University of Ontario Institute of Technology	Ontario	Information Technology (Honours) – Bridge	Bachelors
		Information Technology (Honours) Networking and Information Technology Security	
		Information Technology (Honours) Networking and Information Technology Security – Advanced Entry	
		Information Technology Security	Masters
University of Toronto	Ontario	Computer Science (H.B.Sc.) Specialist Program in Information Security	Bachelors
	Ontario	Certificate in Cyber Security Management	Certificate
		M. Eng. in Communications with focus on Identity, Privacy and Security (IPS)	Masters
		Master of Information, with a Specialization in Identity, Privacy and Security	
University of Victoria	British Columbia	Master of Engineering in Telecommunications and Information Security (MTIS)	Masters
University of Waterloo	Ontario	Graduate Diploma (GDip) in Computer Networking and Security	Diploma
University of Winnipeg	Manitoba	Information Assurance and Security Certificate	Certificate
		Network Security Diploma	Diploma
Willis College	Ontario	Cyber Security Analyst Diploma Program	Diploma
York University	Ontario	Certificate in Advanced Cyber Security	Certificate

Institute	Province	Program Title	Certification
		Certificate in Cyber Security	
		Certificate in Cyber Security Fundamentals	
		Computer Security (BSc, BA)	Bachelors
		LLM in Privacy and Cybersecurity Law	Masters