**The competency requirements of cybersecurity professionals in Canadian financial sector organizations.**

By Marc-André Léger, MScA (MIS), MBA, C.ADM, PhD Candidate  
Université du Québec en Outaouais  
**Contact:** [marcandre@leger.ca](mailto:marcandre@leger.ca)  
**Keywords:** information security, cybersecurity, competency, KSA

**Summary:** This article presents the competencies and competency elements that are required of cybersecurity professionals that were identified during a study on cybersecurity competencies in Canadian financial institutions, between 2019 and 2021. The main goal of this article is to help financial institutions and educational institutions design and implement competency-based continuous education programs. Financial institutions can use this article and the data that supports the recommendations to help them to increase the expertise of cybersecurity workers. Colleges and Universities may find this article interesting to assist them in the design of new programs or the improvement of existing programs.

# Introduction

Canadian financial organizations face multiple cybersecurity challenges in today’s world. Since 2019, with the COVID crisis, an increase the reliance on connected technologies combined with an uprise in cybercrime, has put pressure on cybersecurity teams. While this can be tackled in many ways, we chose to investigate the question of cybersecurity competencies of actors, central to our interests as cybersecurity workforce developers, researchers, and post-secondary educators. It is well documented that the human factor is an important source of vulnerability, leading to increased likelihood of risk. The individuals in cybersecurity work roles, because of their central role in the operation, monitoring and support of cybersecurity activities, which support information technology, supporting the business activities of the firm, are one of many sources of these human factor vulnerabilities. Thus, an underlying hypothesis to our empiric enquiry is that more competent actors will lead to reduced unacceptable risk.

In this article, we present some of the results of a study that was performed in a large Canadian financial institution, between 2019 and 2021.

# Methodology of the research study

The study adopted the action design research (ADR) approach to implement the design science research (DSR) methodology taking advantage of activities from ADR (Mullarkey & Hevner, 2019). ADR was chosen because it has been successfully deployed in an organizational setting to generate knowledge through an iterative process of construction and evaluation of artifacts (Keijzer-Broers & de Reuver, 2016; McCurdy et al., 2016; Sein et al., 2011). Through multiple iterations of a Building, Intervention and Evaluation, the BIE cycle, the research question, and the sub-questions, were investigated. Theses were eventually documented in a PhD dissertation, submitted to the jury. This article presents some of the results from the study, which are in the process of being implemented in the participating Canadian financial institution.

# Research questions investigated in the study

The main goal of the study was to determine whether a cybersecurity competency ontology could provide an effective tool for financial institutions to manage cybersecurity talents. The research question was further structured into three parts:

1. Cybersecurity competency ontology engineering,
2. Mapping the ontology to the cybersecurity subject domain,
3. Validation and testing using semantic queries and rule-based inferences based on cybersecurity scenarios.

For the first part, approaches for ontology development were investigated, such as those proposed by several researchers (Keet, 2020), (Sure-Vetter et al., 2009) or reviewed by others (Stadlhofer et al., 2013). However, it was decided to proceed with ADR to develop and document a competency ontology engineering methodology to facilitate future reuse and provide useful evidence of the rigor of the process. As a result of this, a cybersecurity competency ontology engineering methodology was developed and documented.

To address the second part, mapping the subject domain into the ontology, the cybersecurity competency model (CCM) (Administration) proposed by the United States Department of Labor, Employment and Training Administration (US DOLETA) and the National Institute of Science and Technology (NIST) was used as the primary source. This model is best known as the National Cybersecurity Workforce Framework (NCWF) (NIST) from the National Initiative for Cybersecurity Education (NICE) (Newhouse et al., 2017; NIST, 2021; Petrella, 2017). The NCWF had already been selected by the participating organization prior to the commencement of this study. This was complemented by the data collected in the study. Following this, a cybersecurity competency ontology was developed. This ontology can serve multiple purposes, such as helping organizations and educations institution defining curriculums, as are presented in this article.

Finally, for the third part, several tools were considered to perform the test. Stardog was selected and used with SPARQL queries to match work roles to MITRE Att&ck risk scenarios based on the ontology. The results of 50 queries were analyzed to identify true positives, true negatives, false positives, and false negatives. This allowed the calculation of the precision, recall, F1-scores and MCC. The Matthews Correlation Coefficient (MCC) provides information regarding the correlation between the observed and predicted classifications (Tharwat, 2020). It is considered a good indicator of the quality and accuracy of classification (Chicco et al., 2021). A summary of these results is presented in this table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Precision** | **Recall** | **F1-score** | **MCC** |
| **Sample mean** | 0.77 | 0.63 | 0.67 | 0.06 |
| **Sample SD** | 0.02 | 0.16 | 0.13 | 0.03 |
| **Sample variance** | 0.000 | 0.027 | 0.018 | 0.001 |

Table 1: Summary of results for 50 scenarios

We concluded that the test was successful and the predictive value of the cybersecurity competency ontology using Stardog and job postings, as presented above, is statistically significant. This would support the third sub-question, indicating that the ontology can accurately represent the cybersecurity domain and be used as a talent management decision tool.

# Competency

At the center of the study is the concept of competency, which can be defined as a characteristic of a successful performer in a work role (Boyatzis, 2008; Prescott, 2012; Subramaniam et al., 2019), demonstrated through behavior and actions (Man et al., 2002a). Competencies are learnable, which allows intervention to affect them, such as education (Draksler & Širec, 2018a; Man et al., 2002a; McClelland, 1973; Mitchelmore & Rowley, 2010). They can be defined in relation to know-how, know-what, and know-how-to-be but also in some models in relation to knowledge, skills, and abilities.

Know-how is knowledge. Know-how can be acquired through education as a blend of tacit and explicit knowledge (Draganidis & Mentzas, 2006). It does not imply the capability to successfully fulfill a work role, but it is a step in the direction of competency. It requires problem-solving abilities adhering to best practices and recognized standards in a field, as well as technical and business acumen. At high levels of competency, actors are able to combine know-how to propose innovative solutions to real-world problems (Bacigalupo et al., 2016; Man et al., 2002a).

Know-what refers to the ability of competent individuals to skillfully demonstrate practical knowledge of the work, tasks, methods, business, and ecosystem of an organization applying know-how. It is linked to skills and abilities in some competency models, such as the NCWF. When individuals have know-what, they also have in-depth mastery of how their domain of competency operates as a coherent system. Likewise, know-how and know-what, effective performance and career efficiency can also be linked to the emotional, social, and cognitive intelligence of individuals, i.e., know-how-to-be (Bacigalupo et al., 2016; Boyatzis, 2008, 2008; Man et al., 2002b).

Know-how-to-be is a characteristic of competent individuals who demonstrate high emotional and human relations abilities, mental and physical capacities, basic sense attitudes, strong value systems, and behaviors compatible with the organization’s culture and the dominant socio-cultural values of various internal and external stakeholders, including the ability to interact with colleagues (Bacigalupo et al., 2016; Boyatzis, 2008, 2008; Draksler & Širec, 2018b; Man et al., 2002b; McClelland, 1973; Mitchelmore & Rowley, 2010).

# Cybersecurity competency mapping

The consensus that emerged from the study is that there are two main categories of cybersecurity positions with some common cybersecurity competency requirements and some that are distinct. Using the categories and work roles from the NCWF was not practical as it is perceived as too complex. A simpler categorization, at a high level, was perceived by the participants in management roles as more practical and representing the reality observed in the field. This can be like a matrix organizational structure, where an actor in a work role can be in a high-level category along the lines presented, as well as being in a NCWF work role. For example, a business analyst who is in a governance team can also be defined as a System Security Analyst, NCWF work role OM-ANA-001.

The first category, **cybersecurity business**, is composed of actors who are experts of the business aspects or cybersecurity. These actors have more of a strategic outlook, understanding how cybersecurity provides value to the organization, clients, and other stakeholders. The second category, **cybersecurity technical**, includes actors involved with various technical aspects of cybersecurity, often including the management and use of hardware, software, and tools. However, considering this, the participants in the study informed us that business experts need some technical knowledge and know-how, while the technical experts need to understand the business before gaining effective competence in their job. There is seen as a continuum of cybersecurity competency from business roles to technical roles, with many work roles in between. This continuum led us to identify nine specialties within the two categories that were identified in the model. Moreover, within each specialty, there are varied levels of competency requirements identified, depending on the role. For instance, there could be a justified need for a range from junior, or a specialist entering a work role, all the way to a more senior, experienced, and highly competent worker.

This article presents some the NCWF competency elements that have been identified, using the KSA ID numbers from the NCWF, along with the competency elements proposed in the study. The NCWF numbers can be very useful as many studies and training, certification and other vendors use them to present the learning outcomes of their offering. This can be seen as a Rosetta Stone to connect this study and article with third parties. The details of the codes can be seen on the NCWF or on the project’s GitHub here: <https://github.com/ITriskMgr/CyberSecOnto/blob/main/KSA-001/CompetencyData_v3-0c.xlsx>

# Measuring competency levels

An important aspect of the use of competency in an organizational setting is how it can be measured and appraised. Having a metric to quantify competency is an essential aspect of evaluating the cybersecurity competency levels of the actors in cybersecurity work roles. This will be used for many purposes, such as measuring the effectiveness of continuous education programs or demonstrating compliance of competency requirements to regulators. What is proposed as an outcome of the study is to use the evaluation of levels of competency for the cybersecurity competency elements in relation to the six levels of Bloom’s revised taxonomy (Krathwohl, 2002). A seventh level is implied, zero (0), to indicate the absence of any knowledge or competency for a particular competency element. The six levels are:

1. **Remember:** At this first level, actors exhibit a memory of previously learned materials. At this level, there is no competency.
2. **Understand:** This is the minimum level at which an embryonic competency can be considered. At this level, actors demonstrate an understanding of facts and ideas. They begin to develop know-how but not necessarily know-what.
3. **Apply:** When actors can successfully use their know-how to solve problems and apply the same – know-what – competencies and abilities are demonstrated to find and apply solutions to problems in the real world. They demonstrate the ability to function with other stakeholders within organizational constraints, demonstrating know-how-to-be.
4. **Analyze:** At this more advanced level, competent actors can also identify motives or causes, make inferences, and find evidence to support generalizations.
5. **Evaluate:** At a high level of competency, actors can further present and defend opinions and make judgments about information, validity of ideas, or quality of work based on a predetermined criterion.
6. **Create:** At the highest level of competency in this model, highly competent actors can compile information, combine elements in new ways, or propose alternative solutions to existing or new problems they confront.

# Findings

In the next sections of this article, we present some of our findings from the study about the competencies required of cybersecurity workers in a Canadian financial institution. It starts with the identification of the core competencies for all categories. It then presents the competencies by work role categories and include the various specialties for each of the two categories. It should be noted that this could be further detailed by looking at the requirements by specific work roles, such as the 52 roles describes by the NCWF or by actual work roles in a particular organization. This article, as the study, focused on the two higher-level categories and nine specialties and did not seek to describe the specific competencies of a specific actor in a work role, which could be inferred from the information presented here, complemented by the duties and situation of the actor.

# Core knowledge for all cybersecurity workers

Throughout the study, the knowledge combination that form the competency elements of all cybersecurity work roles in the organization were defined. Already, this information was used by the organization to rethink cybersecurity talent management and training. At the same time, the level of competency required of each competency element of a work role were determined, in reference to the seven levels (0 to 6). For example, it was determined that the minimum competency level required of all core competency elements is level 2, “Understand”. This has led to define level 2 as the required base knowledge requirement for the competency elements common to all cybersecurity work roles. This was set as a baseline requirement. It was used to define a minimal training program for all cybersecurity workers in the organization, as presented in the next section. This baseline know-how competencies includes:

* Problem-solving
* Networking concepts and protocols
* Laws, regulations, policies, and ethics regarding cybersecurity and privacy
* Principles of cybersecurity and confidentiality
* Cyber ​​threats and vulnerabilities management
* Cybersecurity standards, management framework, and methodologies
* Risk management
* Change management

In addition to the baseline know-how, it was identified that all actors in cybersecurity work roles must have minimal competencies in know-how-to-be. These include communication and interpersonal competencies, often referred to as soft skills, at a minimal level of 3, “Apply”. These competencies were often described as problematic for many cybersecurity workers. For example, it was observed and also mentioned in discussions that it is not unusual for some workers with high levels of competency in their particular area, to be less efficient in their work role due to the difficulty interacting with stakeholders, thus being perceived as less competent.

In the study, we identified the common competency elements for all cybersecurity work roles. These are the core competencies being recommended for all cybersecurity workers:

* Knowledge of networking concepts, protocols, and security methodologies (K0001)
* Knowledge of risk management processes (K0002)
* Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy (K0003)
* Knowledge of cybersecurity and privacy principles and organizational requirements (K0004, K0044, A0123 and S0367)
* Knowledge of cyber defense and information security policies, procedures, and regulations (K0157)
* Knowledge of an organization's information classification program and procedures for information compromise (K0287)
* Knowledge of information technology (IT) supply chain security and supply chain risk management practices, policies, requirements, and procedures (K0126, K0169)
* Knowledge of cyber threats and vulnerabilities (K0005)
* Knowledge of specific operational impacts of cybersecurity lapses (K0006)
* Interpret and adhere to global standards and standardization (WPC0022A)
* Knowledge of applicable laws, statutes, guidelines, procedures, standards, and compliance requirements in support of organizational cyber activities (K0168, A0033, K0267)
* Knowledge of new and emerging information technology (IT) and cybersecurity technologies ( K0059)

At an entry level, a cybersecurity worker would need a very basic competency level of “Understand”, level 2, which helps to explain the use of the term knowledge. This is not indicative of any competency, as a level of “Apply”, level (3) or better is necessary for any competency to be considered. Thus, a new worker in an entry level position, such as a recent university graduate in cybersecurity hired in a Canadian financial institution, would quickly require exposure to real world situations, coaching and training to gain competency. This would be done as they are being on-boarded into the organization and receive initial training coming into the work role. The next sections present the competency requirements by work role category and specialty, starting with the business category and specialties.

**Cybersecurity business work roles**

The cybersecurity business category (CAT002) is made up of actors who are experts in all business aspects of cybersecurity related to the organization's mission and business objectives. They combine an understanding of technologies with a strong strategic understanding of cybersecurity and understand how cybersecurity brings value to the organization and all its stakeholders. For example, a strategic advisor to a manager in a business unit who can advise him or her on information security planning in a project is in this category. To ensure that the minimum level of competence is reached, the organization realized that the CISSP training would be the most opportune and cost-effective path, as this was offered by local universities. While developing the ontology, it was shown that there was a good fit between the required competencies and the CISSP training. Thus, it was made mandatory for all actors in the cybersecurity business work role category. Business Cybersecurity 1 and 2 training paths were also created on Udemy to complete the training of all workers.

The main tasks of the cybersecurity business work role category:

* Support and advise information security stakeholders and the organization in terms of logical and physical security to adequately protect information and ensure its confidentiality.
* Help protect the information of customers, employees, and suppliers by developing, maintaining, and monitoring security processes and frameworks. Ensure that it is linked to business processes and technologies to make them more secure.
* Ensure that security requirements are properly considered in all aspects of information management, including management frameworks, architectures, solutions, and systems necessary to achieve the mission of the organization and the delivery of products and services to customers.

The main responsibilities of the cybersecurity business work role category:

* Determine information protection needs and translate them into requirements while respecting the culture, values, risk appetite, constraints, and business strategy of the organization.
* Identify, analyze, quantify, prioritize, verify (audit), and document cybersecurity risks.
* Recommend and follow risk treatment plans for unacceptable risks.
* Evaluate and design appropriate security management mechanisms.
* Monitor the evolution of security threats, vulnerabilities, and risks, and make recommendations.
* Define, operationalize, monitor, verify, measure, and improve security management processes.
* Define, implement, and monitor strategic, tactical, and operational level security frameworks as per the best practices and information security standards.
* Provide advice, opinions, and recommendations on security requirements to be included in projects or to be integrated into IT operations.
* Produce and monitor key performance indicators to measure the achievement of security objectives and ensure accountability to targeted stakeholders.
* Identify, produce, disseminate, measure, and monitor continuing education and security awareness programs for customers, employees, and managers.

Some of the most common tasks of cybersecurity Business workers include:

* Provide business context to cybersecurity.
* Contribute to governance, risk management, compliance, and cybersecurity activities.
* Provide input on cybersecurity requirements.
* Translate and user requirements into actionable cybersecurity information and technical requirements
* Analyze needs and make recommendations as required by the organization
* Translate and explain the cybersecurity requirements to the stakeholders
* Contribute to cybersecurity system architecture design, analysis, and implementation.
* Perform project management and change management activities.

Many different job titles and business cybersecurity positions can be identified in this category, such as:

* Cybersecurity analyst
* Cybersecurity compliance advisor
* Cybersecurity auditor
* Business Information Security Officer (BISO)
* Chief Information Security Officer (CISO)

The common core competency elements for all cybersecurity business specialties (4) and work roles (26) are already present in the core competency elements for all cybersecurity workers identifies previously. The cybersecurity analyst (SP006) and the cybersecurity advisor (SP007) form the largest cohorts of the business work role. It appears appropriate to put them in a continuum with respect to the tasks and responsibilities mentioned above. In cybersecurity business work roles, the minimum competency level required is “Apply”, level 3. For example, in a cybersecurity governance team continuum, an actor in a cybersecurity analyst role should be at the “Analyze” competency level (4) and in the cybersecurity advisor role be at the “Evaluate” level (5) or at the “Create” level (6), in a senior advisor work role.

Another work role in the business category is the specialist in cybersecurity awareness and training (SP008). Although this specialty is often more in support of cybersecurity awareness activities of the organization, it is nonetheless very critical, as customers, employees, and other stakeholders, often form the weakest link of cybersecurity in financial organizations. Finally, the manager work role (SP005) is identified as the fourth cybersecurity business specialty. For each of these specialties, the organization identified the detailed competency elements requirements, an overview of which is presented in the next sections.

**Cybersecurity manager specialty**

The manager work role comprises the most senior level position in the cybersecurity teams of the organization. The typical actor in this work role is a graduate from a university undergraduate or, in most cases observed in the participating organization, a graduate program in business technology management, engineering, governance or management, such as an MBA with many years (8+) of experience in the organization or in the financial industry. In addition to the core competency elements already identified for all cybersecurity roles, the cybersecurity manager must have high-level competencies in know-how-to-be as well as in areas related to the specific team or role of the actor.

The cybersecurity manager specialty (SP005) includes several NCWF work roles:

* Executive Cyber Leadership (OV-EXL-001)
* Information Systems Security Manager (OV-MGT-001)
* Communications Security (COMSEC) Manager (OV-MGT-002)
* Cyber Workforce Developer and Manager (OV-SPP-001)

The competency elements of the cybersecurity manager specialty are:

* Knowledge of the organization's core business/mission processes (K0146)
* Knowledge of the organization’s enterprise information technology (IT) goals and objectives (K0101)
* Knowledge of Risk Management Framework (RMF) requirements (K0048)
* Knowledge of system and application security threats and vulnerabilities and risks (K0070, K0624)
* Knowledge of resource management principles and techniques (K0072)
* Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data (K0038)
* Knowledge of controls related to the use, processing, storage, and transmission of data (K0622)

**Cybersecurity analyst specialty**

The cybersecurity analyst work role (SP006) is sometimes a junior role, but more often at an intermediate level in the organization. The typical actor in this work role is a graduate from a university undergraduate program in business technology management, computer science, management or a related field who would join a cybersecurity team as an analyst. Likewise, the holder of a vocational college degree in IT who has a few years (5+) of experience in the organization could occupy an analyst position. In some cases, it was observed that individuals from other fields, such as criminology, law enforcement or psychology, as well as military veterans, can perform well in this specialty with some additional on-the-job cybersecurity training provided once hired, when the work role is appropriate. In addition to the core competency elements already identified, the cybersecurity analyst must have competencies at “Analyze” (level 4) in the areas that are relevant to their specific role in the organization, which could include:

* Information systems and operating systems
* Principles of data classification
* Information security technologies
* Network service management
* Management of critical infrastructures
* Operational technologies
* Identity and access management
* Personal information protection solutions
* Cryptography

The following NIST NCWF work roles fall into this specialty:

* Systems Security Analyst (OM-ANA-001)4
* Cyber Intel Planner (CO-OPL-001)
* Cyber Ops Planner (CO-OPL-002)
* Authorizing Official/Designating Representative (SP-RSK-001)
* Security Control Assessor (SP-RSK-002)
* Research and Development Specialist (SP-TRD-001)
* Systems Requirements Planner (SP-SRP-001)
* Data Analyst ( OM-DTA-002)
* Knowledge Manager (OM-KMG-001)
* IT Program Auditor (OV-PMA-005)
* All Source-Collection Manager (CO-CLO-001)
* All Source-Collection Requirements Manager (CO-CLO-002)

The competency elements of the cybersecurity analyst specialty are:

* Knowledge of operating systems (K0060)
* Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations (K0170)
* Knowledge of service management and related standards (K0200)
* Knowledge of cryptography, and cryptographic key management (K0018, K0019)

As well, other competency elements will be required depending on the work role of a specific cybersecurity analyst.

**Cybersecurity advisor**

The cybersecurity advisor (SP007) is a senior role. Business information security officers (BISO) are an example of a very senior advisor role. This is not a role for a new cybersecurity worker; however, a recent graduate of a university master’s program in business technology management, computer science, engineering, cybersecurity, governance, or management with a previous experience in the financial sector could join the security teams as an advisor. Likewise, the holder of a baccalaureate or a college degree who has several years (8+) of experience in the financial sector could occupy a position of advisor. In addition to the elements already identified, the cybersecurity advisor specialist must have competencies at “Evaluate” (level 5) or “Create” (level 6) in several of the following areas, depending on their responsibilities:

* Strategic business process
* Identification and management of IT needs
* Human–machine Interface
* IT architecture
* Networking and connected services
* Virtualization, containers, and DevSecOps
* Cloud computing
* Emerging threats and vulnerabilities
* Emerging cybersecurity technologies

In addition to all the work roles from the cybersecurity analyst specialty, the following NWCF work roles fall into this category:

* Enterprise Architect ( SP-ARC-001)
* Security Architect (SP-ARC-002)
* Cyber Legal Advisor (OV-LGA-001)
* Privacy Officer/Privacy Compliance Manager (OV-LGA-002)
* Cyber Policy and Strategy Planner (OV-SPP-002)
* Program Manager (OV-PMA-001)
* IT Project Manager (OV-PMA-002)
* Product Support Manager (OV-PMA-003)
* IT Investment/Portfolio Manager (OV-PMA-004)

The competency elements of the cybersecurity advisor specialty are:

* Ability to apply critical reading/thinking skills (A0070)
* Knowledge of the organization's core business/mission processes (K0146)
* Knowledge of how information needs, and collection requirements are translated, tracked, and prioritized across the extended enterprise (K0120)
* Knowledge of human-computer interaction principles (K0036)
* Knowledge of physical computer components and architectures, including the functions of various components and peripherals (K0109)
* Knowledge of fundamental cyber concepts, principles, limitations, and effects (K0435)
* Knowledge of computer networking and data communications (K0395, K0417)
* Knowledge of evolving/emerging communications technologies (K0431)
* Knowledge of Internet applications, wireless, digital and telephony networks (K0444, K0445, K0446, K0560)
* Knowledge of the common networking and routing, services, and how they interact to provide network communications (K0565)
* Knowledge of the basics of network security and threats (K0480, K0561, K0612)
* Knowledge of virtualization products (K0610)
* Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration (K0194)

**Cybersecurity awareness and training specialist**

The awareness and training specialty (SP008) is also a role at different levels, from junior to senior. A recent graduate from a university certificate program in pedagogy or andragogy could fill this position. The holder of an undergraduate or graduate degree in psychology, sociology, criminology, or public security, ideally with an internship, a capstone project, or a dissertation on an aspect of cybersecurity would be an ideal candidate. Likewise, a cybersecurity analyst or advisor who has several years (5+) of experience as a post-secondary lecturer could fill this position. In this specialty, we also find specialists in pedagogy and andragogy, learning content creation and management, and education. The NWF work roles Cyber Instructional Curriculum Developer (OV-TEA-001) and Cyber Instructor (OV-TEA-002) fall into this category.

**Cybersecurity Technical work roles**

The cybersecurity technical category (CAT001) includes information technology specialists, programmers, technicians, and engineers who are involved in the various technical aspects of cybersecurity. They select, configure, operate, and manage the hardware, software, and tools that protect the organization from unacceptable risks and contribute to risk mitigation. The technical category workers combine strong technical expertise with an understanding of business context. Some of the actors in this work role category have IT support roles, which include a cybersecurity component. For example, a network administrator who configures Microsoft Active Directory services on servers, penetration testers, or vulnerability assessment analyst are in a cybersecurity technical work role. To ensure that the minimum level of competency is reached, the organization use the CEH certification training as an opportune and cost-effective learning path. There was a good fit between the required competency elements and the CEH training. Thus, it was made mandatory training for all actors in the cybersecurity technical work role category. This was offered to all technical workers in partnership with a local university. Technical cybersecurity 1 and 2 learning paths were also created on Udemy to complete the training.

The main tasks of the cybersecurity technical category:

* Select, install, configure, and use tools, techniques, and methods for the secure management of data, information systems, networks, and buildings.
* Identify, analyze, report, and resolve threats, vulnerabilities, events, and incidents that occurred or could occur within the network to adequately protect data, information systems, networks, and buildings.

The main responsibilities of the cybersecurity technical category:

* Exploit security tools and monitor cybersecurity.
* Determine the safe operation of information systems.
* Apply best practices in cybersecurity to organizational requirements.
* Evaluate controls in accordance with best practices.
* Evaluate the adequacy of cybersecurity measures in requirements.
* Recognize and classify vulnerabilities and associated attacks.
* Provide recommendations for threats and vulnerabilities.
* Receive and analyze data to identify abnormal activities, potential threats, suspected malicious activity, methods of exploitation, and impacts.
* Identify, document, and manage cybersecurity incidents.
* Perform threats and vulnerabilities strategic watch, research, and analysis.

Many different job titles and technical cybersecurity positions can be identified in this category, such as:

* Penetration tester
* Threat and vulnerability analyst
* Incident response team member or coordinator
* Security architect

In addition to the common core competencies for all work roles mentioned previously, the common competency elements for all cybersecurity technical specialties work roles are:

* Knowledge of cybersecurity and privacy principles and organizational requirements (K0044)
* Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards (K0260, K0261)
* Knowledge of cyber-attack stages, targets, attack methods and techniques, infections, and methods of infection (K0362, K0177, S0229, S0228, K0392)
* Knowledge of computer components, operating systems, and architectures, including the functions of various components and peripherals (K0060, K0109)
* Knowledge of concepts, terminology, and operations of a wide range of communications media (K0108)
* Knowledge of computer networking, physical and logical network devices and infrastructure, digital communications, telephony networks fundamentals and data communications terminology and protocols (K0395, K0417, K0471, K0516)
* Knowledge of network protocols such as TCP/IP, DHCP, DNS, and directory services (K0332)
* Knowledge of network security architecture concepts including topology, protocols, components, principles, and security models (K0179, K0203)

For all the core competencies of cybersecurity technical work, the minimum level of competency required is “Apply”, level 3. Ideally, all actors in this work role should be able to “Analyze”, level 4, and in the senior work roles “Evaluate”, level 5, or in many cases the competency to successfully “Create”, level 6. There are five specialties in the technical cybersecurity category, such as IT exploitation, defensive security, offensive security, security architect, and physical security.

**Offensive cybersecurity specialist**

The offensive cybersecurity specialist (SP001) plays the role of an attacker who seeks to test the limits of protections and processes to identify and mitigate unacceptable risks and avoid unwanted incidents. This role is highly know-how-oriented and focuses on the ability to ethically test the limits of an organization’s cybersecurity. Work roles are at several levels, from junior to senior. There are no specific academic degree requirements for this work role. A wide range of individuals, from high school to post-secondary graduates, with demonstrated talent could find their place in offensive security teams. For example, a finalist in a national cybersecurity capture-the-flag competition with a high school diploma or a vocational college certification would be an ideal candidate for this role. In addition to the elements already identified, the offensive cybersecurity specialist must have a minimum of level 4 competency in the following areas:

* Penetration and intrusion techniques
* Planning and execution of attacks

The following NIST NCWF work roles fall into this specialty:

* Mission Assessment Specialist (AN-ASA-002)
* Target Developer (AN-TGT-001)
* Target Network Analyst (AN-TGT-002)
* Multi-Disciplined Language Analyst (AN-LNG-001)

Other competency elements of the offensive cybersecurity specialty are:

* Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability (K0440)
* Knowledge of evolving/emerging communications technologies (K0431)
* Knowledge of penetration testing principles, tools, and techniques (K0342)
* Knowledge of website types, administration, functions, and content management system (K0349)
* Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists (A0080)
* Ability to evaluate, analyze, and synthesize large quantities of data and metadata, identify intelligence gaps, and produce usable results (A0084, K0449, A0066, A0091, A0101, A0102, A0106, A0109, S0187, S0194, S0218)

**Defensive cybersecurity specialist**

The defensive cybersecurity specialist (SP002) intervenes to proactively protect information systems and data, for example, by identifying and mitigating vulnerabilities or by using the results of the work performed by the offensive cybersecurity specialists. This role is at all competency levels. A recent graduate of a post-secondary program in business technology management, computer science, or engineering could enter a defensive security team in a junior role. Likewise, the holder of a technical vocational college degree with a few years (5+) of work experience could fill this role. As well, computer science and engineering graduates can be good candidates. In addition to the elements already identified, the defensive cybersecurity specialist must have a minimum of level 3 competency in several of the following areas:

* Application security
* Operationalization of security patches
* TCP-IP and derived protocols (DNS, DHCP, LDAP)
* Microsoft server networks and services (AD, GPO, etc.)
* Network security architecture
* OWASP top 10, Common vulnerabilities and exposures and MITRE ATT&CK

The following NIST NCWF work roles fall into this specialty:

* Software Developer (SP-DEV-001)
* Secure Software Assessor (SP-DEV-002)
* System Testing and Evaluation Specialist (SP-TST-001)
* Cyber Defense Analyst (PR-CDA-001)
* Cyber Defense Infrastructure Support Specialist (PR-INF-001)
* Cyber Defense Incident Responder (PR-CIR-001)
* Vulnerability Assessment Analyst (PR-VAM-001)
* Threat/Warning Analyst (AN-TWA-001)
* All Source-Collection Manager (CO-CLO-001)
* Cyber Crime Investigator (IN-INV-001)
* Law Enforcement /Counterintelligence Forensics Analyst (IN-FOR-001)
* Cyber Defense Forensics Analyst (IN-FOR-002)

The additional Competency elements of the defensive cybersecurity specialty are:

* Knowledge of programming languages (K0068, K0139)
* Knowledge of organization's evaluation and validation requirements (K0028)
* Knowledge of incident response and handling methodologies (K0042)
* Knowledge of legal governance related to admissibility of Evidence (K0123, K0155, K0156)
* Knowledge of collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody (K0118, K0125, S0047, S0068)
* Knowledge of data backup and recovery (K0021)
* Knowledge of organization's enterprise information security architecture, security architecture concepts and enterprise architecture reference models (K0027, K0199)
* Knowledge of how traffic flows across the network and network traffic analysis methods (K0058, K0061)
* Knowledge of packet-level analysis using appropriate tools (K0301, K0565)
* Knowledge of host/network access control mechanisms (K0033)
* Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions (K0046)
* Knowledge of different classes of and cyber attackers (K0161, K0162)
* Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities (K0106)
* Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations (K0170)
* Knowledge of types and collection of persistent data (K0128)
* Knowledge of system administration, network, and operating system hardening techniques (K0167)
* Knowledge of system and application security threats and vulnerabilities (K0070, K0624)
* Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations. (K0107)
* Knowledge of penetration testing principles, tools, and techniques (K0342, S0001)

**Cybersecurity architect**

A cybersecurity architect (SP004) is a senior role. In this role, actors collaborate with development teams in the design and implementation of solutions that respect the organization's risk appetite. The holder of a bachelor’s degree or a vocational college degree in IT with several years (8+) of experience in system architecture, ideally in the financial sector, and an expertise in cybersecurity could occupy a position of Cybersecurity Architect. The Enterprise Architect (SP-ARC-001) and Security Architect (SP-ARC-002) NCWF work roles are in this specialty.

The additional Competency elements of the cybersecurity Architect specialty are:

* Knowledge of mathematics (K0052)
* Knowledge of Information Theory (K0325)
* Knowledge of analysis principles and methods (K0043, S0050 S0122)
* Knowledge of system and software engineering (K0082, K0102, S0005, S0024)
* Knowledge of systems testing and evaluation methods (K0091)
* Knowledge of organizational process improvement and maturity models (K0198)
* Knowledge of service management and related standards (K0200)
* Ability to optimize systems to meet performance requirements (A0038)
* Knowledge of confidentiality, integrity, and availability (K0211, S0374)
* Knowledge of cybersecurity-enabled software products (K0212, S0027)
* Ability to conduct vulnerability scans (A0015)
* Knowledge of the Risk Management Assessment (K0214)
* Knowledge of key concepts in security management (K0074).
* Knowledge of Security Assessment and Authorization process (K0037)
* Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations (K0170)
* Knowledge of system fault tolerance methodologies (K0323)
* Knowledge of various types of computer architectures (K0227)
* Knowledge of the enterprise information technology architecture (K0291)
* Knowledge of integrating goals and objectives in architecture (K0293, A0027)
* Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations (A0170)
* Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an architecture (A0008)
* Knowledge of program protection planning (K0264)
* Knowledge of installation, integration, and optimization (K0035)
* Knowledge of configuration management techniques (K0275)
* Knowledge of database systems (K0024)
* Knowledge of organization's enterprise information security architecture (K0027)
* Knowledge of N-tiered typologies (K0286)
* Knowledge of parallel and distributed computing concepts (K0063)
* Knowledge of multi-level security systems and cross domain solutions (K0240)
* Knowledge of electrical engineering as applied to computer architecture (K0030)
* Knowledge of telecommunications concepts (K0093)
* Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services (K0332)
* Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs (K0333)
* Knowledge of network access, identity, and access management (K0056)
* Knowledge of network management (K0180, A0172)
* Knowledge of how traffic flows across the network (K0061)
* Knowledge of demilitarized zones (K0326)

**Cybersecurity exploitation specialist**

The cybersecurity exploitation specialty (SP003) includes several management and IT support roles where one of the components of the work role of the actor is related to cybersecurity. Sometimes part of an IT department, outside the main cybersecurity department, this work role is often a gateway for a worker to eventually join the cybersecurity department. This plays a critical role in controlling and managing risk in the organization. A recent graduate of a high school vocational program, post-secondary technical program, or undergraduate program in business technology management, computer science, or IT support could be hired in an IT Exploitation work role. Subsequently, after a few years in the organization this actor could take on a defensive or offensive security position or an analyst role in a cybersecurity department.

The following NIST NCWF work roles fall into this specialty:

* Information Systems Security Developer (SP-SYS-001)
* Systems Developer (SP-SYS-002)
* Database Administrator (OM-DTA-001)
* Technical Support Specialist (OM-STS-001)
* Network Operations Specialist (OM-NET-001)
* System Administrator (OM-ADM-001)
* Exploitation Analyst (AN-EXP-001)
* All-Source Analyst (AN-ASA-001)
* Partner Integration Planner (CO-OPL-003)
* Cyber Operator (CO-OPS-001)

The additional competency elements of the exploitation specialty are:

* Ability to communicate complex information (A0013)
* Ability to collaborate effectively with others (A0074, A0089)
* Ability to source data (A0066)
* Knowledge of organization objectives (K0560)
* Knowledge of human-computer interaction principles (K0036)
* Knowledge of information technology (IT) security (K0049)
* Knowledge of local area and wide area networking (K0050)
* Knowledge of telecommunications concepts (K0093)
* Knowledge of indicators of system performance and availability (K0053)
* Knowledge of network access, identity, and access management (K0056)
* Knowledge of network access, identity, and access management (K0061)
* Knowledge of policy-based and risk adaptive access controls (K0065)
* Knowledge of service management concepts (K0200)
* Knowledge of security models (K0203)

# Continuing education in cybersecurity

A practical outcome of this research project for the participating organization was the creation of a cybersecurity continuing education strategy. The strategy focuses on three areas: formal training, active learning, and opportunism, in addition to a goal of increasing the competency level of actors in their current work roles. The study seeks to mitigate potential vulnerabilities caused by the lack of certain competency elements at the required level. It also seeks to increase organizational cybersecurity resilience. The training activities, per specialty and work role, are based on the information that was collected in the research project and integrated into the ontology. The continuing education strategy encompasses four levels:

1. A common core for all cybersecurity work roles. An internal recognition was created, named the Security Certificate, and was used to recognize the achievement of this common core. The main goal of this training was to ensure a minimum competency level of 2 for all cybersecurity work roles for the essential competency elements, as mentioned in Section 9.3.1.
2. A required learning path was then created for each of the two work role categories. Using a mapping of existing cybersecurity certifications to the NCWF, the CISSP training was selected for all the actors in the cybersecurity business category and the CEH training was selected for all in the cybersecurity technical category. In addition, targeted learning paths in Udemy and Pluralsight were created for all actors who were interested in using these online learning services.
3. A selection of targeted courses was made available, adapted by specialties, for all actors. For example, for the defensive cybersecurity specialty, the organization is in the process of implementing the Immersive Labs Cyber-range training system hands-on training system. Lists of suggested exercises have been identified by work role, as the vendor of this tool has mapped all the exercises to the NCWF.
4. Individual courses have been offered to actors as per an individualized training plan created for each actor, at their request or at the request of their manager. In addition to considering the current and future needs of the organization, the individualized plan considers the current and future interests of the employee.

# How the competency information in curriculum development

As an example, we present two examples of the use of the results from the study for competency-based post-secondary curriculum design. The first example is for an undergraduate program for cybersecurity analysts and the second is for a graduate program for an offensive cybersecurity worker. To achieve the result presented, it is necessary to use the competency elements presented in this article for the selected work in combination with the detailed competency elements information in the cybersecurity competency ontology, provided on the GitHub mentioned. An analysis can be done using various technologies, such as using inference with Stardog, as was done in the study, or manually using Excel.

**Example 1: Cybersecurity analyst work role (SP006) undergraduate program**

This first example presents how the information about the cybersecurity analyst work role (SP006) a three year, 90 credit, university undergraduate program in business technology management. As the goal is to develop level 4 or better competency, the proposed program would integrate either Work-Integrated learning or internships. What is described in this example is a program based on three semesters per calendar year, with two semesters of courses in the core competencies and a paid summer internship.

**Semester 1**

* Information systems
  + Information security technologies
  + Operating systems
* Business analysis
  + communication and interpersonal competencies
  + Problem-solving
* Cybersecurity 101
  + Principles of data classification
  + Principles of cybersecurity and confidentiality
* Networking 101
  + networking concepts, protocols
  + Network service management
* Applied networking

**Semester 2**

* Cybersecurity 201
  + Data classification program
  + Data loss prevention
* Cybersecurity policy design and implementation
  + Guidelines and procedures
  + Compliance requirements
* Networking 201
  + Management of critical infrastructures
  + Operational technologies
* Server management concepts
  + Directory services
  + Server hardening
* Introduction to penetration testing
  + Tools and utilities (in lab setting)
  + Cyber kill chain

**Semester 3**

* Legal aspects of cybersecurity
  + Laws, regulations, policies, and ethics
  + Canadian federal and provincial privacy regulations
* Best practices, standards and frameworks
  + The standardization processes
  + ISO
  + COBIT
  + NIST standards and frameworks
  + Service management
  + Other related standards
* Governance 101
  + Governance principles
* Cybersecurity 301
  + Threats and vulnerabilities (K0005)
  + Threats and vulnerabilities management
* Risk management 101
  + risk management practices, policies, requirements, and procedures
  + security methodologies
* Change management
  + Process and strategies

**Semester 4**

* Risk management 201
  + Risk management methodologies
  + Cases
* Internal controls
  + Controls selection and implementation
* Compliance and certification
* Business continuity planning
  + Business impact analysis
  + Plan design and approval
  + Testing the plan

**Semester 5**

* Privacy principles
  + Identity and access management
  + Personal information protection solutions
* Risk management 301
  + Application of risk management in a real context
* Cybersecurity Audits
  + Internal audits
  + External audits
* Incident management
* Cryptography

**Semester 6**

* Cybersecurity professional certifications
  + CISSP, CCSP or CISA (depending on preferred path)
* Emerging cybersecurity technologies
* Capstone project

**Example 2: Offensive cybersecurity work role (SP006) undergraduate program**

This first example presents how the information about the offensive cybersecurity specialist (SP001) a 1.5 year, 60 credit, university graduate program in business technology management. As the goal is to develop level 4 or better competency, the proposed program would integrate either Work-Integrated learning that includes a thesis or capstone project.

Admission into the program could require one of the following profiles:

* A highly motivated post-secondary graduate, with 3+ years’ experience
* A finalist in a national cybersecurity capture-the-flag competition
* An ungraduate in computer science or engineering with a 3.0 GPA or better

**Semester 1**

* Applied data analytics with Python
* Introduction to advanced offensive cybersecurity
* Law and ethics applied to offensive cybersecurity
* Host-based security
* Penetration testing 101 (principles, tools, and techniques)

**Semester 2**

* Communication and interpersonal competencies
* Server-based security
* Network security
* Penetration testing 201 (Planning and execution of attacks, with labs)
* Capture-The-Flag

**Semester 3**

* Internet and cloud security
* Penetration testing 301 (Using the results)
* Cyber-range battlefield
* Emerging communications technologies
* Capstone project or thesis

# Limitations of this study

There are limitations to the effectiveness of qualitative methodologies in general and cybersecurity matters in particular (Richter & Koch, 2004). Cybersecurity is a sensitive topic for any organization and introduces limits to what it can allow to be published and made public. At the same time, the organization and researchers recognize that as this is an important subject that has national and strategic interests, there are good reasons for the research to be conducted and published. This study was able to ensure the scientific merit of the endeavor. Mechanisms to control biases and adherence to a scientific research methodology, ADR, were part of the effort to maximize validity. Notwithstanding, to obtain permission from the participating organization, some information was only shared with the research team and was not published in the results, the dissertation, or subsequent articles in scientific journals at the request of the organization. This has introduced limits to this study that will be documented but not necessarily published. Without this, however, the research could not take place.

Moreover, this study had certain limitations inherent to formal validation and testing processes (Whittemore et al., 2001). The researchers were confronted with a difficult challenge in part because of the difficult balance to maintain between rigor, subjectivity, and creativity. The ongoing peer review process involving the research team, including the academic dissertation supervisors, the subject matter experts within the organization, and the informants, contributes to ensuring the integrity, authenticity, and credibility of the results, thereby allowing descriptive and interpretative quality. At the same time, the choice of ADR allowed us to maximize the congruence and thoroughness of the results. These all contribute to the internal validity of the study, faithfully presenting and interpreting the reality of the financial institution where this study was conducted and enabling the researchers to develop an understanding of the situation that led to successfully developing and testing the proposed solution. As to the notion of external validity, because of the implication of industry players, there are some aspects of the solution that could be generalized, and this applied to other similar financial organizations in Canada. However, this would require further studies and additional empirical research.

# Ethical considerations

The study did not include experimentation on human beings, which does not indicate the absence of ethical concerns. The qualitative approach in research being adopted in organizations requires the establishment of trust between the research team and the participants in the study. This trust cannot exist without respect for the individuals involved. The researchers needed to remain attentive and sensitive to the values and culture of the participants and the organization. Trust made it possible to acquire access to the data of the organization and the internal perspective of participants that formed the raw knowledge that was required to successfully execute the study.

This study was submitted to and approved by the UQO Research Ethics Committee at the start of the project. In addition, informed consent was obtained in writing from the participants when they were enrolled in the study before the data collection process could start. Participation in this study was voluntary and that the participants had the option to withdraw at any time. A few participants participated only in some phases of the study. In particular, a few participants in the initial interviews moved on to another organization during the study. However, their contribution had ended at that time, and they had no objection to the use of the information they provided be included in the study. Furthermore, as per the confidentiality agreement to perform the study, no information that can make it easy to identify the organization and the participants is included in this article.

# Future work

This study resulted in a completed cybersecurity competency ontology that describes the work roles of cybersecurity workers in a Canadian financial institution. This allows the institution to improve information security by reducing the vulnerabilities that can result from competency gaps and other benefits mentioned. Once the study was completed, the organization has developed competency metrics, a measurement tool and management dashboard. These metrics can contribute to limit the subjectivity and biases in allocating human and economic resources to mitigate the risks created by cybersecurity competency gaps and vulnerabilities. This can also help to create individual learning paths for cybersecurity workers.

Another area for investigation is the integration of machine learning or other components to help match potential candidates for work roles using big data sources, such as LinkedIn, Indeed or other sources. Using the ontology as the basis of the solution could help organizations narrow down the lists of potential candidates to identify individuals who could be potential recruits, including non-traditional candidates, such as minorities or other underrepresented groups. Furthermore, there is a potential to identify competent individuals who can emerge from other sources than the usual academic and degree-granting profiles and have acquired competencies that could be recognized and proven. The ontology can also provide a tool for organizations to assist with legal and regulatory compliance issues.

# Conclusion

In this research, as presented in this research proposal, the action design research methodology, ADR, was used to develop and test an ontology of cybersecurity professional skills for the financial services industry in Canada. With the help of a panel of experts, the study successfully combined renowned frameworks, such as the NIST NICE, bodies of knowledge (Newhouse et al., 2017; NIST, 2021; Petrella, 2017), and current best practices with the actual in vivo experiences of the cybersecurity practitioners of a world-class Canadian financial institution working with a team of academic researchers.

This allowed the researchers to design, develop, populate, and test a cybersecurity competency ontology representing the actual need for competencies of financial organizations that are required to fulfill its mission successfully. How successfully this ontology can assist them is one of the elements that were tested in the field. Nonetheless, the cyclical iterative nature of ADR should allow us to emerge from the study with a useful tool that can be further improved when it is implemented. The reflective nature of ADR and the implication of members of the organization provided additional benefits by helping create a culture of security and life-long learners.

As IT is such an important component of creating a competitive advantage for financial institutions, cybersecurity has become a crucial topic. In addition, various challenges faced in today’s world, such as pandemics, increase cybercrime cases, the reduction of the number of available, competent talents, and the number of many other issues increase the importance of cybersecurity and the need for this study. This is a critical issue for which organizations need solutions.

# Bibliography

Bacigalupo, M., Kampylis, P., McCallum, E., & Punie, Y. (2016). *Promoting the entrepreneurship competence of young adults in Europe : Towards a self-assessment tool*. 611‑621. https://doi.org/10.21125/iceri.2016.1150

Boyatzis, R. E. (2008). Competencies in the 21st century. *Journal of Management Development*, *27*(1), 5‑12. https://doi.org/10.1108/02621710810840730

Chicco, D., Tötsch, N., & Jurman, G. (2021). The Matthews correlation coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData Mining*, *14*(1), 13. https://doi.org/10.1186/s13040-021-00244-z

Draganidis, F., & Mentzas, G. (2006). Competency based management : A review of systems and approaches. *Information management & computer security*.

Draksler, T. Z., & Širec, K. (2018a). Conceptual Research Model for Studying Students’ Entrepreneurial Competencies. *Konceptualni raziskovalni model za raziskovanje podjetniških kompetenc študentov.*, *64*(4), 23‑33. https://doi.org/10.2478/ngoe-2018-0020

Draksler, T. Z., & Širec, K. (2018b). Conceptual Research Model for Studying Students’ Entrepreneurial Competencies. *Konceptualni raziskovalni model za raziskovanje podjetniških kompetenc študentov.*, *64*(4), 23‑33. https://doi.org/10.2478/ngoe-2018-0020

Keet, C. M. (2020). *An Introduction to Ontology Engineering*.

Keijzer-Broers, W., & de Reuver, M. (2016). Action Design Research for Social Innovation : Lessons from Designing a Health and Wellbeing Platform. *Proceedings of International Conference on Information Systems (ICIS)*, 1‑20.

Man, T. W. Y., Lau, T., & Chan, K. F. (2002a). The competitiveness of small and medium enterprises A conceptualization with focus on entrepreneurial competencies$. *Journal of Business Venturing*, 20.

Man, T. W. Y., Lau, T., & Chan, K. F. (2002b). The competitiveness of small and medium enterprises A conceptualization with focus on entrepreneurial competencies$. *Journal of Business Venturing*, 20.

McClelland, D. C. (1973). Testing for competence rather than for" intelligence.". *American psychologist*, *28*(1), 1.

McCurdy, N., Dykes, J., & Meyer, M. (2016). Action Design Research and Visualization Design. *Proceedings of the Beyond Time and Errors on Novel Evaluation Methods for Visualization - BELIV ’16*, 10‑18. https://doi.org/10.1145/2993901.2993916

Mitchelmore, S., & Rowley, J. (2010). Entrepreneurial competencies : A literature review and development agenda. *International Journal of Entrepreneurial Behavior & Research*, *16*(2), 92‑111. https://doi.org/10.1108/13552551011026995

Mullarkey, M. T., & Hevner, A. R. (2019). An elaborated action design research process model. *European Journal of Information Systems*, *28*(1), 6‑20. https://doi.org/10.1080/0960085X.2018.1451811

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (NIST SP 800-181). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181

NIST. (2021). *NICE Cybersecurity Workforce Framework*. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

Petrella, E. (2017, janvier 10). *NICE Cybersecurity Workforce Framework*. NIST. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Prescott, R. K. (2012). *The Encyclopedia of Human Resource Management, Volume 1 : Short Entries* (Vol. 1). John Wiley & Sons.

Richter, A., & Koch, C. (2004). Integration, differentiation and ambiguity in safety cultures. *Safety science*, *42*(8), 703‑722.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS quarterly*, 37‑56.

Stadlhofer, B., Salhofer, P., & Durlacher, A. (2013). *An Overview of Ontology Engineering Methodologies in the Context of Public Administration*. 36‑42. https://www.thinkmind.org/index.php?view=article&articleid=semapro\_2013\_2\_30\_50039

Subramaniam, T., Nizam, I., & Kamil Eissa, A. M. (2019). The Impact of Core Competencies of IT Professionals on Business Success in Malaysia. *International Journal of Management, Accounting & Economics*, *6*(7), 496‑520.

Sure-Vetter, Y., Staab, S., & Studer, R. (2009). Ontology Engineering Methodology. In *Handbook on Ontologies* (p. 135‑152). https://doi.org/10.1007/978-3-540-92673-3\_6

Tharwat, A. (2020). Classification assessment methods. *Applied Computing and Informatics*, *17*(1), 168‑192. https://doi.org/10.1016/j.aci.2018.08.003

Whittemore, R., Chase, S. K., & Mandle, C. L. (2001). Validity in Qualitative Research. *QUALITATIVE HEALTH RESEARCH*.