SECTION B: WORK ASSIGMENT DESCRIPTION

Job Title	Manager Digital Trust - Digital Identities & Cyber Assessments
Division	Office of the Chief Information Security Officer
Reports To	Director Digital Trust
Max Salary Range	$128,728.60 to $151,278.40
Work Location	55 John Street, Toronto
Job Type	Permanent Full Time
Shift Information	Monday to Friday, 35 hours work week

JOB SUMMARY:
To provide senior level strategic and tactical guidance to the Director Digital Trust, as well as the Chief Information Security Office (CISO) in the execution of its mandate to establish and maintain a City-wide cyber program to ensure the City is adequately protected.

To provide leadership, guidance and manage the design, integration and implementation of cyber solutions that support the organization and the CISO's strategic objectives.

To lead the development and management of information, data, privacy and cyber security risk for the City.

To lead the digital product build, execution and operations of digital properties pertaining to customer authentication and identity, access management and related products.

To implement and oversee the Governance, Risk & Compliance Programs and socialize Risk Management principles across the organization to promote awareness and effective management of cyber risks.

To administer the unit's financial and administrative responsibilities including the operating budget process, monitoring spending and revenues and directing the unit's cyber information technology program services, communications, human resources planning and decisions, quality assurance and staff training.

To collaborate with other segments of the organization to manage City-wide cyber initiatives.

MAJOR RESPONSIBILITIES:

- Manages and mainten the Identity and Access Management (IAM) and the Privileged Access Management (PAM) program.
- Identifies, evaluates and manages initiatives required to integrate into the Digital Identity Management product platforms.
- Leads the performance improvement of digital products to enhance the user experience, reduce pain points, and reduce calls to our help desks.

- Develops and contribute to IAM and PAM standards and approaches to enable seamless and secure integrated solutions.
- Ensures the IAM and PAM programs are effectively governed in order to maximize security and mitigate risk.
- Drives and support continuous improvement of the capabilities related to the IAM and PAM programs.
- Defines and reports metrics to measure IAM and PAM compliance to the senior management.
- Design, implement and lead enterprise-wide risk management strategy relating to cyber for the organization.
- Define and quantify the organization's risk appetite' for cyber related risks and ensure risk approach adheres accordingly.
- Align to organizational governance mandates and advocate for governance within Divisions, Agencies & Corporations.
- Accountable for implementing, facilitating, and improving governance mechanisms.
- Manage the successful delivery of risk management initiatives ensuring technical excellence and a practical/business focused approach.

QUALIFICATIONS/CERTIFICATIONS:

- Post-secondary degree in Business or Technology or a related discipline.
- Over 7 years of senior level experience in Information Security
- Strong relevant digital identity experience in a fast paced environment.
- Product Management and end-to-end product lifecycle experience in digital identity related field.
- Keen understanding of the digital ecosystems and customer needs.
- Extensive knowledge of security industry standards and best practices such as ISO 27001 and NIST standards.
- Strong understanding of security risks, threats, and vulnerabilities and the judgment to assess and articulate risk effectively.
- Extensive senior level experience in Information Security or Governance, Risk & Compliance (GRC).
- Extensive experience preparing comprehensive reports and presentations for all levels of an organization.
- Experience in establishing strategy and implementation of GRC Programs.
- Experience leading transformative multi-year programs.
- Strong understanding of security risks, threats, and vulnerabilities and the judgment to assess and articulate risk effectively
- Strong knowledge of security methodoogies, industry standards and best practices such as ISO 27001 and NIST standards.
- Knowledge of architectural design and implementation methodologies including software, network and infrastructure.
- Knowledge of network and information security methods, standards, architectures, policies and procedures.
- Preferred Certifications (any in the list): CISSP, CCSP, CISA, CISM

SKILLS:

- Ability to work in transformative programs

- Excellent leadership and organizational skills and the ability to work effectively with all level of stakeholders.
- Motivated self-starter demonstrating integrity, initiative and innovation qualities.
- Strong analytical ability where problems are typically unusual and difficult.
- Strong analytical skills and ability to prioritise and multitask.
- Excellent problem-solving skills with capability to identify solutions to unusual and complex problems.
- Ability to make quick decision.
- Strong business acumen with budgeting experience.
- Excellent understanding of audit and compliance standards.
- Experience with the audit process and performing risk-based audits.
- Ability to work with the broader IT organization and business management to align priorities and plans with key business objectives.
- Demonstrated capacity to lead under pressure, make decisions in ambiguous situations and drive cross functional collaboration in a short period of time.
- Demonstrated influence and persuasion skills, able to present to senior levels.
- Strong understanding of the business impact of security tools, technologies and policies.
- Ability to handle ambiguity and make decisions and recommendations with limited data
- Ability to prioritize and effectively manage competing priorities and projects.
- Ability to manage multiple initiatives while adhering to strict deadlines.
- Excellent communication and active listening skills with an aptitude for extracting and synthesizing complex information.
- Exceptional written and oral communication skills.
- Transferable skills, like communication and decision-making, are equally important.
- Being able to think on your feet and show good judgment are especially valuable in this field. “Security pros should always be ready to react to cyber-related incidents quickly.

ADDITIONAL COMMENTS/INFORMATION:

A normal work week is 35 hours, however, unforeseen situation may require extended hours of work with little or no prior notice. In case of a cyber incident or breach, rotation shift, continuous extended hours may be required with little or no prior notice.

*Subject to a police check, background check, psychological assessment and/or any other checks on a regular basis as the Office of the CISO handles highly sensitive and confidential information.

EQUITY, DIVERSITY AND INCLUSION

The City is an equal opportunity employer, dedicated to creating a workplace culture of inclusiveness that reflects the diverse residents that we serve. Learn more about the City’s commitment to employment equity.

ACCOMODATION

The City of Toronto is committed to creating an accessible and inclusive organization. We are committed to providing barrier-free and accessible employment practices in compliance with the Accessibility for Ontarians with Disabilities Act (AODA). Should you require Code-protected accommodation through any stage of the recruitment process, please make them known when contacted and we will work with you to meet your needs. Disability-related accommodation during

the application process is available upon request. Learn more about the City’s Hiring Policies and Accommodation Process.