Job Title	Senior Specialist Risk Quantification
Division	Office of the Chief Information Security Officer
Reports To	Manager Strategy & Architecture
Salary Range	$110,947.20 to $130,353.60
Work Location	55 John Street, Toronto
Job Type	Permanent Full Time
Shift Information	Monday to Friday, 35 hours work week

JOB SUMMARY:

To support the execution of the Chief Information Security Officer's (CISO) mandate, cyber vision and strategy, providing technical and business advice, support and services to all City divisions, agencies and corporations.

To define, develop and support the measurement and quantification of cyber risks and enhance decision making by accurately translating results into meaningful solutions.

To provide subject matter expertise, strategic advice, senior level guidance and operational support for the quantification of cyber risks to all level of stakeholders.

MAJOR RESPONSIBILITIES:

- Leads the development, deployment and management of the City's cyber risk management and quantification program.
- Provides expert support in risk measurement and quantitative analysis related to cyber assessments.
- Implements processes, procedures and tools for the measurement and communication of risks within the business units.
- Develops key risk indicators (KRIs), risk event reporting, setting quantitative and qualitative risk threshold limits and conducting scenario analysis, trends spotting and KRI benchmarking.
- Assess future risk, opportunities, and effectiveness by utilizing advanced analytics
- Quantify risk and aggregate exposures by utilizing industry best practices
- Responsible for the development of complex systems and programs that measure aggregate risk exposures.
- Influence business analysis and communicate analytical results, findings, and solutions to governance committees and business process owners
- Builds collaborative and productive working relationships across the organization to establish, maintain, and continuously improve cyber risk management capabilities, and promote risk awareness, and intelligent risk taking.

QUALIFICATIONS/CERTIFICATIONS:

- Post-secondary degree in Business, Technology, Statistics or Mathematics or in a quantitive field or a related discipline.

- Over 6 years experience in risk quantification and data management.
- Extensive experience with Risk Management.
- Extensive experience in enterprise level Governance, Risk and Compliance (GRC) management.
- Experience with risk analysis, data analytics, or visualizations.
- Knowledge of elements of risk, including vulnerability, threat, likelihood, impact, mitigation, and remediation
- Preferred Certifications (any in the list): CISSP, CRISC, CISM or CISA.

SKILLS:

- Ability to work in transformative programs.
- Ability to lead efficient communication between all project stakeholders, including internal teams and clients
- Ability to achieve business objectives through influencing and effectively working with key stakeholders.
- Excellent written & verbal communication skills (comfortable & confident communicating at all levels including business partners, leadership and vendors.
- Excellent problem-solving skills with capability to identify solutions to unusual and complex problems.
- Keen attention to detail and strong organizational skills.
- Highly organized, proactive, self-motivated team player who takes initiative and is able to work independently.
- Ability to work in a fast-paced environment managing multiple priorities with proven time management skills.
- Strong analytical skills and ability to prioritise and multitask.
- Ability to prioritize and effectively manage competing priorities and projects.
- Ability to manage multiple initiatives while adhering to strict deadlines.
- Able to work extremely well under pressure while maintaining a high level of professionalism
- Self-motivated person with desire to go above and beyond tasks
- 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.