

SECTION B: WORK ASSIGNMENT DESCRIPTION

Job Title	Senior Specialist Risk Management
Division	Office of the Chief Information Security Officer
Reports To	Manager Governance, Risk & Compliance
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:

Risk Assurance is the internal process or methodology the Office of the CISO (OC) employs to create 'checks' within the City of Toronto's governance and risk frameworks. The main focus of the risk assurance practice is to ensure cyber risks are effectively managed.

In this role, the Senior Specialist Risk Management will ensure that all risks identified, during risk assessment processes, are assigned to risk owners, Risk Treatment Plans (RTP) are developed and signed by key stakeholders. In addition, RTPs are monitored, control owners identified, and controls effectiveness are addressed. Further, the Senior Specialist Risk Management will work with key cybersecurity partners such as the City's Internal Audit Division, Technology Services Division, and Auditor General's Office to ensure cybersecurity related audit findings are effectively closed.

MAJOR RESPONSIBILITIES:

- Supports the implementation and post production activities of the Integrated Risk Management Team
- Supports the implementation of Governance, Risk, and Compliance (GRC) tools
- Supports the implementation of cyber audit management tools
- Supports the implementation of the City's Cyber Risk Management Framework
- Leads or supports Third Party Risk Management activities
- Develops artifacts to support the implementation of a risk assurance program
- Oversees the execution of cybersecurity controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and City of Toronto standards and policies.
- Executes an impartial assessment process to validate the existence and functionality of appropriate cybersecurity controls, prior to a system, application or service being used in a production environment or post implementation.
- 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:

- Mandatory

- Post-secondary degree in Business or Technology or a related discipline.
- Over 6 years experience in Risk Management, primarily focused on Risk Assurance/IT audit practices
- Extensive experience with Risk and Issue Management lifecycle including Identifying, Analyzing, Evaluating, Treating, Monitoring, and Reviewing risks.
- Extensive experience conducting IT audits and with various audit management tools
- Extensive experience in enterprise level Governance, Risk and Compliance (GRC) management.
- Experience with various GRC tools and processes, and in particular, implementation of GRC tools
- Extensive experience conducting Third Party Risk Assessments
- Preferred Certifications (at least two in the list): CISSP, CISA, CISM, CRISC
- Experience with Cyber Risk Management Framework (CRMF) especially ISO 27001, and NIST SP 800-37 R2 Risk Management Framework (RMF)
- Knowledge of elements of risk, including vulnerability, threat, likelihood, impact, mitigation, and remediation

SKILLS:

- Mandatory
 - Excellent written & verbal communication skills (comfortable & confident communicating at all levels including business partners, leadership and vendors.
 - Keen attention to detail and strong organizational skills.
 - 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 problem-solving skills with capability to identify solutions to unusual and complex problems.
- Ability to work in transformative programs.
- 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.