Job Title	Manager Offensive Security
Division	Office of the Chief Information Security Officer
Reports To	Director Threat Management
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 Threat Management 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, deployment, and management of a vulnerability management program and penetration testing program to mitigate existing and future security gaps within the organization.

To lead the remediation of vulnerabilities and the creation of solutions that couples business continuity with information and cyber security regulatory requirements.

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:
- Leads the strategy, roadmap, development and ongoing management of the vulnerability management program and penetration testing program.
- Engages with internal teams and MSSP to architect quality solutions that are performant and resilient.
- Prioritizes vulnerabilities discovered along with remediation timeline(s).
- Monitors and reports on compliance with the related policies and standards.
- Proposes changes to existing policies and procedures to ensure operating efficiency and regulatory compliance.
- Prepares and deliver metrics, reports for senior management to show efficiency and compliance of security functions.

- Provide support to security operation investigations, and indirect operational availability to support peers when necessary.
- Contributes to the overall successful development and execution of the cyber program to adequately protect the City.
- Interprets units' goals, develops and establishes broad scale, longer-term objectives, goals, or projects (e.g., affecting a business, division, several divisions or the organization).
- Provides senior level advice, expertise, and consultation to all levels of internal and external stakeholders on cyber matters including assessing risks, monitoring risks, identifying potential gaps, and providing cyber solutions to mitigate risks and protect the City.
- Drives forward the cyber mandate with internal, external, regulatory stakeholders to execute a cyber strategy.
- Develops, recommends and evaluates the units' strategic planning activities as well as divisional integrated planning initiatives.
- Develops business strategies, operational plans and provides for contingencies.
- Applies established strategies to effectively manage changes into the recognized ways of operating and implements when appropriate.
- Manages, defines, communicates and leads cyber initiatives within the unit. Oversees the delivery of all initiatives within the respective portfolio.
- Develops and implements detailed plans and recommends policies regarding program specific requirements.
- Manages the development and implementation of programs, policies, guidelines, standards, processes and procedures, ensuring they address emerging needs and have an impact on the City's ability to detect, protect and respond to cyber threats.
- Manages, motivates and trains the units staff, ensuring effective teamwork, high standards of work quality and organizational performance, continuous learning and encourages innovation in others.
- Supervises the day to day operation of all assigned staff including the scheduling, assigning and reviewing of work. Authorizes and controls vacation and overtime requests. Monitors and evaluates staff performance, approves salary increments and recommends disciplinary action when necessary.
- Leads talent management and identification to develop the team for future growth within the Office of the CISO and the City.
- Develops, recommends and administers the annual budget for the unit, ensures that the units expenditures are controlled and maintained within approved budget limitations.
- Identifies, monitors and evaluates key performance indicators. Works to improve operational management systems, processes and best practices to ensure continuous improvement within the unit.
- Engages with technology teams across the organization to build alignment on key projects and initiatives and develop execution roadmaps.
- Promotes the use of innovation to produce financially viable, sustainable and equitable results.
- Sets standards, evaluates the outcome and adjusts the individual/team/organizational approach accordingly.
- Allocates resources to meet the operational and business goals of the organization.
- Mitigates risks by ensuring that due diligence is completed for each project/initiative. Monitors program results, performance measures and adjusts accordingly.
- Manages performance metrics to show efficiency and compliance of cyber functions.

- Manages the development, implementation, integration, and deployment of related technology solutions to protect the City's assets, translating business needs into technical requirements.
- Prepares briefing notes and reports to Council on related risk management, and cyber issues. Attends Committee meetings to answer questions or provide clarification as required by Members of Council.
- Plans, manages and implements projects and service requests including the determination of project scope, action plans, identifying critical success factors.
- Enforces and monitors leading edge information cyber standards across the organization.
- Researches cyber industry best practices and emerging technology and its' applicability to new initiatives.
- Maintains an active external network of contacts to seek, share and explore information and technology risk management, information and cyber security trends. Keeps up to date on industry trends and continually evolving methods cybercriminals use to gain systems access, and how their actions can lead to a data breach.
- Maintains active involvement in related professional associations, and related professional development organizations and conferences.
- Establishes relationships with strategic partners, business leaders and relevant stakeholders from the organization including agencies, boards, commissions, and corporations, to gain support in order to achieve business goals and enable continuous improvement within the program.
- Manages and develops processes to identify, and monitor information cyber related business risks. Ensures senior management is briefed and aware of potential risks. Proactively informs senior management of the strategies developed and employed to mitigate these risks.
- Works closely with stakeholders such as the Corporate Access & Privacy Office to ensure that risk management and cyber best practices are embedded in the solution development design process.
- Coordinates evaluations of information security procedures, and reports on these evaluations to senior management, and makes recommendations for improvement as required.
- Plans, manages and executes technology audits in accordance with industry methodology and standards.
- Performs risk assessments and ensures that audit scope covers all significant risks. Ensures that audit programs and audit testing is comprehensive at addressing the significant risks.

QUALIFICATIONS/CERTIFICATIONS:

- Post-secondary degree in Business or Technology or a related discipline.
- Over 7 years of senior level experience in Information Security.
- In-depth knowledge of enterprise-level information security, vulnerability management and penetration testing.
- Strong understanding of multiple information security platforms and able to solve complex issues.
- 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.
- Preferred Certifications (any in the list): CISSP, CRISC, CSIM, CISA

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.
- Must be able to travel to all City of Toronto's office locations and outside city/country for conferences if required.

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.