Crown Investments Corporation of Saskatchewan (CIC) is the holding company for Saskatchewan's commercial Crown corporations.

The Finance & Administration division provides financial reporting, analysis and recommendations to CIC and the CIC Board on a wide range of business issues. The division also supports CIC's corporate technology environment through oversight of technology integration and risk, information security, third-party service providers, business continuity and disaster recovery, internal control effectiveness, and the responsible governance of artificial intelligence (AI) and other emerging technologies.

Manager, Technology Risk & Security

Reporting to the Corporate Controller, the Manager, Technology Risk & Security will lead CIC's technology-risk, cybersecurity, information-security and AI governance. The Manager will advise on technology to be integrated into CIC's systems and work with internal leaders and external service providers to support responsible technology adoption, information protection and organizational resilience.

Key responsibilities include:

- Establishes, maintains and continuously improves CIC's technology, cybersecurity, information-security and AI governance frameworks in alignment with organizational objectives, risk appetite, legislation, policy and recognized industry standards.
- Integrates technology, cyber, AI and third-party risks into CIC's enterprise risk management framework, including risk identification, assessment, treatment, monitoring and reporting.
- Oversees CIC's external technology and cybersecurity service providers, evaluates service performance and control effectiveness, coordinates remediation, and ensures clear accountability for priorities, deliverables and escalation.
- Leads information-security governance, including access and control monitoring, vulnerability and incident reporting, policy development, security awareness, vendor assurance and follow-up on audits, assessments and testing.
- Maintains cyber-incident readiness and supports CIC's business continuity and disaster recovery programs through plans, exercises, lessons learned and corrective actions.
- Leads the responsible adoption and oversight of AI and other emerging technologies, including governance principles, risk and privacy assessments, acceptable-use requirements, control design, training, monitoring and advice to management.
- Conducts research into technology and information-security tools, methods, threats, risks, regulatory developments and industry practices, and translates technical findings into practical business advice.
- Develops strategies, business cases, cost-benefit analyses, feasibility studies and project plans for approved technology initiatives, including objectives, risks, resources, milestones and deliverables.
- Prepares and presents clear technology-risk, cybersecurity, AI and resilience information and recommendations to senior leadership, governance committees, the CIC Board and external stakeholders, and represents CIC in meetings with Crown corporations, ministries and industry partners.

The following competencies are essential for this position:

- Strong knowledge of technology-risk management, cybersecurity governance, information security, IT controls and recognized frameworks such as NIST.
- Knowledge of AI governance, responsible AI practices and the privacy, security, legal, ethical and operational risks associated with emerging technologies.

- Ability to oversee third-party service providers, assess technical performance and controls, manage contracts and service expectations, and drive timely remediation.
- Ability to translate complex technical issues into clear business risks, options, recommendations, reports and presentations for non-technical audiences, executives and the CIC Board.
- Strong research, analytical, problem-solving and decision-support skills, including the ability to assess emerging threats and opportunities.
- Demonstrated project-management and business-analysis skills, including scope, timelines, resources, risks, requirements, costs and deliverables.
- Strong collaboration, influencing, relationship-management and organizational skills, with the ability to work across business units and with external experts.
- Ability to work independently, exercise sound judgment, manage competing priorities and respond effectively during technology disruptions or cyber incidents.

The ideal candidate will have a post-secondary degree in computer science, engineering or a related discipline, along with progressively responsible experience in technology risk, cybersecurity, information security, artificial intelligence, IT audit or assurance. Experience working with third-party technology providers and applying security and control frameworks is required. Knowledge of AI governance and responsible technology adoption is essential. Relevant professional certifications are considered an asset. An equivalent combination of education and experience may be considered.

The successful candidate will be subject to an Employment Screening Check as a condition of employment.

Position Details:
Number of Positions Available: one (1)
Position Type: Permanent Full-Time
Salary will be commensurate with the candidate's knowledge, competence, and experience.

Position Location:
Regina, Saskatchewan

Hours of Work:
Monday to Friday - 38.75 hour work week

Closing Date:
Friday November 6, 2026

How to Apply: Resumes should be forwarded in confidence to careers@cicorp.sk.ca.

CIC would like to thank all applicants for their interest and wish to inform that only those selected for further consideration will be contacted.

CIC is committed to providing an accessible recruitment process. Candidates who require an accommodation at any stage of the recruitment process are encouraged to email careers@cicorp.sk.ca