Manitoba Hydro
energy for life

EMPLOYMENT OPPORTUNITY

Closing Date: 2026/08/25

Security Risk Management Lead

Winnipeg, MB

Manitoba Hydro is consistently recognized as one of Manitoba's Top Employers! We are a leader among energy companies in North America, recognized for providing highly reliable service and exceptional customer satisfaction. Join our team of Manitoba's best as we continue to build a company that champions safety, supports innovation, and delivers on our commitment to customer service - while actively fostering a diverse, equitable, and inclusive workplace reflective of the communities we serve.

Great Benefits

- Competitive salary and comprehensive benefits package.
- Defined-benefit pension plan for long-term financial security.
- Nine-day work cycle, typically resulting in every other Monday off to support a balanced approach to work, family life and community.

Position Overview:

Under the general direction of the Security Portfolio Governance Risk & Compliance Lead, you will supervise and lead the Security Risk Management team responsible for delivering enterprise security risk management services, including security risk assessments, third-party security risk reviews, risk acceptance and exception management, risk registers, remediation tracking, audit support, investigation support, and post-loss assessment activities. This position provides day-to-day leadership, oversight, quality review, and risk reporting to ensure security risks are consistently identified, documented, communicated, tracked, and escalated in support of informed business decisions and effective security risk governance across Manitoba Hydro.

Responsibilities:

- Provide leadership, guidance, and direction to the Security Risk Management section.
- Provide Cyber Security consulting services to the Enterprise, including EMS/SCADA systems support and Telecommunications, to ensure consistency of Cyber Security practices across all systems and networks.
- Responsible for translating business unit goals into specific strategic actions and measures within the section and taking remedial action necessary to ensure goals are achieved.
- Plan for the short-term and assist with the long-term utilization of available resources (human, financial, and technology) to meet corporate plans and priorities in a systematic and economical manner as it pertains to Enterprise cyber security.
- Support the security risk acceptance process, including intake, analysis, documentation, escalation, approval tracking, expiry monitoring, and reporting of accepted risks and exceptions.
- Develop and maintain security risk reporting for leadership and stakeholders, including risk trends, open issues, remediation status, exceptions, third-party risks, and other key indicators.
- Coordinate risk registers and related risk management records, including evidence management, remediation tracking, exception management, status updates, and follow-up with accountable owners.
- Conduct Cyber Security risk assessments and reviews of technology, systems, applications, networks, processes, and controls.
- Maintain contact with industry cyber security standards setting groups, and an awareness of legislation and regulations pertaining to Cyber.
- Stay abreast of and inform Enterprise stakeholders and technical support staff of applicable global and Canadian cyber security developments and trends.
- Ensure adequate performance measures are in place; develop and implement plans to meet performance objectives, reporting results, and follow up on exceptions.
- Interview, evaluate, and recommend staff replacements, promotions, suspensions, and dismissals. Prepare performance reviews, job development planning, job descriptions, and review responsibilities to ensure positions are properly classified.

Qualifications:

- Four-year degree in a relevant discipline such as cybersecurity, information systems, computer science, engineering,

business, risk management, or a related field from a university of recognized standing, plus six years of progressively responsible related experience in security risk management, cybersecurity governance, third-party risk management, audit support, or related functions, including three years of supervisory or team leadership experience;
OR

- Two-year diploma in a relevant discipline such as cybersecurity, information systems, computer science, engineering, business, risk management, or a related field from a institution of recognized standing, plus eight years of progressively responsible related experience in security risk management, cybersecurity governance, third-party risk management, audit support, or related functions, including three years of supervisory or team leadership experience.
- Membership as a Professional Engineer with EGM would be considered an asset where engineering experience is directly relevant to the position.
- Certified or be willing to obtain certification as a Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), or equivalent.
- Ability to plan, manage, evaluate, and supervise programs and personnel.
- Ability to effectively lead teams in multiple projects.
- Demonstrated ability to identify, assess, document, communicate, and monitor cybersecurity and security-related risks, including the development of appropriate risk mitigation, acceptance, escalation, and reporting strategies.
- Effective communication skills, with a demonstrated ability to articulate complex technical concepts to non-technical audiences, fostering understanding and collaboration between technical and business stakeholders.
- Knowledge of cybersecurity principles and practices, including risk management, security controls, security investigations, incident response processes, and post-loss assessment activities.
- Experience with cybersecurity frameworks, standards, and regulatory requirements such as the NIST Cybersecurity Framework, CIS Critical Security Controls, and NERC CIP where applicable.
- Experience supporting risk acceptance, exception management, risk registers, remediation tracking, evidence management, and follow-up with accountable owners.
- Experience supporting third-party security risk management activities, including vendor risk reviews, security requirements in contracts, penetration testing coordination, issue tracking, and escalation of material vendor risks.
- Experience coordinating internal and external audit support activities, including control testing, evidence collection, audit response, management action plans, and remediation tracking.
- Ability to develop and maintain meaningful security risk reporting for leadership and stakeholders, including trends, open issues, remediation status, exceptions, third-party risks, and key performance indicators.
- Knowledge of methodologies and best practices in conducting risk assessments, implementing risk mitigation strategies, and monitoring risk management effectiveness.
- Ability to effectively work with other cybersecurity teams, such as Threat and Vulnerability, to help prioritize systems that need remediation or containment.
- Possess a valid Province of Manitoba Driver's Licence.
- Must obtain and maintain a current Personnel Risk Assessment and a "Clear" security rating in accordance with Manitoba Hydro policy P513.
- Must complete Manitoba Hydro Standards of Conduct training.
- NERC Critical Infrastructure Protection (CIP) Training is required and must be completed prior to transfer date and renewed annually.

Salary Range

Starting salary will be commensurate with qualifications and experience. The range for the classification is $52.88-$72.45 Hourly, $101,332.40-$138,828.30 Annually.

Apply Now!

Ready to join a team that energizes Manitoba and puts safety, innovation, and inclusion at the heart of everything we do? Visit www.hydro.mb.ca/careers to learn more about this position and to apply online.

Application deadline: AUGUST 25, 2026.

We appreciate your interest in Manitoba Hydro and thank all applicants. Only those selected for the next stage of the selection process will be contacted.

If you require accommodations during the recruitment process or need this posting in an accessible format, please let us know - we're committed to a barrier-free experience for all candidates.

#IND1