
IT Security Compliance and Risk Specialist

Job Opening Id	: 44215	# Required	: 1
Business Unit	: Corporate Services	Division	: I.T. Solutions
Location:	: Regional Headquarters	Standard Hours	: 35.00 / week
Full/Part Time	: Full-Time	Regular/Temporary:	: Temporary
Salary Grade	: 6	Salary Range	: \$100,640.00 - \$118,400.00
Post Date	: 2026-01-14	Close Date	: 2026-01-27

Temporary Duration: Approximately 12 months

Job Summary

Salary under Review

Reporting to the IT Security Manager, the IT Security Compliance and Risk Specialist is responsible for analyzing, interpreting and developing solutions and strategies to manage the internal and external IT security audits and assessments. Acting as the liaison between potential auditors and technical teams, this role leads conversations with, and collaborates with key invested parties to identify risks and to ensure IT implemented solutions are compliant with corporate policies, regulations, and standards. The role is also responsible for monitoring remediation of audit findings up to completion, as well ensuring any mitigation strategies and security controls for all IT related findings are completed and documented.

Education

- Bachelor's degree in Information Technology, Computer Science, related discipline or equivalent combination of education and experience.

Knowledge

- A minimum of 5 years of experience managing IT audits, risk and compliance is required preferably within the public sector or medium to large-sized organization;
- A security certification through an accredited organization
- Addition Information security certifications (CRISC, CISM, CGEIT, CISSP, CCSP or GIAC) are considered an asset
- Experience working with auditors and the evidence collection process
- Knowledge of regulatory and industry standards such as ISO, NIST, COBIT, GDPR and other security frameworks

- Understanding of information systems and networks and all areas of Information Security including data protection, incident management, and vulnerability management
- Experience working with Security training tools, including creating and launching phishing campaigns, and remedial training
- Knowledge of development and management of business continuity and disaster recovery planning
- Previous experience with IT systems threat/risk assessments, IT audits and regulatory compliance such as SOX and GDPR would be an asset
- Experience with cloud security controls and administration such as AWS and Azure would be an asset

Responsibilities

Compliance and Risk Auditing. (40% of time).

- Assesses risks and internal control dependency on systems by identifying areas of non-compliance and evaluating risks related to key technology processes.
- Co-ordinates timely activities as it relates to internal, external and regulatory audit requests including SOX, SOC1, SOC2;
- Conducts and reviews business impact analysis, implements and coordinates disaster recovery planning and disaster recovery exercises where required;
- Conducts risk assessments and supports the invested parties in determining the appropriate treatment of identified risks; identify appropriate action plans for risk remediation;
- Inventory, assess significance, assign accountability, and develop appropriate monitoring for the control environment;
- Conducts IT compliance reviews including user access reviews, risk assessments, control objectives monitoring, and third party assessments;
- Liaises with Information Privacy Assessment Office and identify IT compliance requirements and assist with creation and maintenance and coordinate IT responses to regulatory audits;
- Works with and supports the development of the risk and compliance practice with IT management and the leadership team.
- Assists in the creation and maintenance of the information security risk register, audit requests, and third party consultant/vendor assessments.
- Assist in gathering information asset inventory, including identification and valuation, including any strategies and methodologies around loss scenarios
- Leads complex analysis, develops and generates KRIs/KPIs, validates compliance and develops actionable recommendations.

- Works with and supports the existing IT Security training platforms to identify high risk business users within the organization.

Information Security (30% of time)

- Conducts information systems controls assessments.
- Reviews and administers the Incident Response Process, and ensures updates to and ongoing assessments are coordinated as required.
- Reviews and actions the latest Indicators/Endpoints of Compromise as required, ensuring issues are addressed in a timely fashion to mitigate any potential attack(s).
- Performs the necessary technical support as required, in order to support the Corporate Security strategy and processes, such as remediation actions and/or tactics that may be deployed as a result of a security scan result.
- Documents, tracks and investigates information security events, requests, and incidents;
- Implements and reviews information security policies, guidelines, procedures, training materials, awareness campaigns, internal bulletins and portal contents.

Development, administration, and implementation of IT risk policies, procedures, guidelines and standards (20% of time)

- Supports the invested parties in understanding and applying IT risks, security best practices and processes framework;
- Performs consultation and development of the IT objectives and requirements of the risk program;
- Partners with IT managers and team members to ensure risk and compliance issues are identified, defined, communicated, and addressed.
- Provides effective mentoring and guidance to other IT personnel and may assist in developing policy, standards and procedures.
- Collaborates in change management communications and processes, with focus on facilitating risk and compliance training for all affected staff.

Disaster Recovery & Business Continuity & Incident Response (10% of time)

- Business Continuity and Disaster Recovery program administration including conducting impact assessments, disaster recovery plans development and coordinating disaster recovery exercises;
- Ensures Business Continuity, Disaster Recovery, and Incident Response plans are current, and supporting documentation is actioned by engaging with peers and other business supports where required;
- Assists in conducting tabletop and resiliency exercises with corporate teams.

Perform other related duties and responsibilities as assigned or required.

Special Requirements

- In accordance with the Corporate Criminal Record Check Policy, the position requires the incumbent to undergo a Criminal Records Check and submit a Canadian Police Clearance Certificate.
- Must maintain ability to travel in a timely manner to other offices, work locations or sites as authorized by the Corporation for business reasons.
- Regional staff strive to enable the strategic priorities of council and the organization through the completion of their work. Staff carry out their work by demonstrating the corporate values.

HOW TO APPLY

Uncover the wonder of the Niagara Region and join a team dedicated to meeting tomorrow's challenges TODAY!

We thank all candidates for their interest however, only those candidates selected for an interview will be contacted.

We confirm that we do not use AI in screening of applicants, and this position is an existing vacancy.

To view the full job description and requirements, visit our Careers page - [Job Opening #44215](#)

Let us know why you would be an excellent team member by submitting your online application **no later than January 27, 2026, before midnight** by visiting our 'Careers' page at www.niagararegion.ca.

We thank all candidates for their interest however, only those candidates selected for an interview will be contacted.

Application Link: <https://www.niagararegion.ca/government/hr/careers/default.aspx>

ABOUT US

Serving a diverse urban and rural population of more than 475,000, Niagara Region is focused on building a strong and prosperous Niagara. Working collaboratively with 12 local area municipalities and numerous community partners, the Region delivers a range of high-quality programs and services to support and advance the well-being of individuals, families and communities within its boundaries. Nestled between the great lakes of Erie and Ontario, the Niagara peninsula features some of Canada's most fertile agricultural land, the majesty of Niagara Falls and communities that are rich in both history and recreational and cultural opportunities. Niagara boasts dynamic modern cities, Canada's most developed wine industry, a temperate climate, extraordinary theatre, and some of Ontario's most breathtaking countryside. An international destination with

easy access to its binational U.S. neighbour New York State, Niagara attracts over 14 million visitors annually, as well as a steady stream of new residents and businesses.

At Niagara Region, we value diversity - in background and experience. We are proud to be an equal opportunity employer. We aspire to hire and grow a workforce reflective of the diverse community we serve. By doing so, we can deliver better programs and services across Niagara.

We welcome all applicants! For more information about diversity, equity, and inclusion at Niagara Region, Diversity, Equity and Inclusion - Niagara Region, Ontario or email related questions to diversity@niagararegion.ca. To send input on reducing barriers in the current hiring process, please email myhr@niagararegion.ca

For the Region's full employee equity statement, Working at Niagara Region - Niagara Region, Ontario.