Athabasca University

Professional Job Position Description

Section I: Position information

Effective date 2025-11-27 ☒ Update only ☐ Classification review	
Position title	Cybersecurity Risk Analyst
Position number	998745-00
Classification level	Excluded C
Position affiliation	☐ AUFA ☒ Excluded
Location	Virtual (Remote)
Department	Digital Security, Information Technology
Reports to	Manager IT GRC, Digital Security

Position summary

Briefly describe the main purpose(s) of the position.

The Cybersecurity Risk Analyst (CRA) is responsible for supporting the Digital Security Programs and will work with the Chief Information Security Officer, Manager IT GRC, Digital Security, and other members of the Digital Security team in identifying, evaluating, presenting, and reporting on cybersecurity risks.

This role partners with IT, compliance, and risk management teams to ensure that cybersecurity threats are effectively managed within AU's risk appetite and regulatory requirements. The Analyst is also responsible for maintaining the organization's cybersecurity risk register, supporting policy development, and administering appropriate security tools. The CRA must understand the AU Policy Framework and create risk indicators that show variances to policy framework adoption or adherence

Duties and responsibilities

Organize by key responsibility area and include % of time spent where possible.

1. **Vulnerability Management & Risk Remediation**
   - Manage and administer the Vulnerability Management Program by administering the necessary tools.
   - Analyze outputs from vulnerability scans and penetration tests; collaborate with IT teams and Risk Owners to assess risks and prioritize remediation.
   - Conduct follow-ups to ensure timely mitigation of identified cyber risks and maintain accurate records in the risk register.
2. **Risk Assessment, Governance & Third-Party Risk**
   - Perform digital risk assessments, including reviews of new applications, systems, and changes.
   - Partner with AU business units to identify and evaluate cybersecurity risks in business processes and technology deployments.
   - Assess the security posture of third-party vendors and service providers, identifying

potential risks and recommending appropriate controls.
- Ensure identified risks remain within AU's risk appetite and do not exceed defined tolerance levels.

3. Policy, Standards & Best Practices
- Stay current with evolving cybersecurity standards, regulations, and industry best practices.
- Contribute to the development and maintenance of AU's digital security policies, procedures, and awareness initiatives.
- Support enforcement and alignment of security practices across business units and technology teams.

4. Documentation & Risk Reporting
- Maintain and update the Digital Security Risk Register.
- Generate regular risk reports highlighting trends, key exposures, mitigation progress, and opportunities for improvement.

5. Asset Discovery & Information Sharing
- Manage asset discovery activities using implemented tools to maintain visibility across AU's IT environment.
- Share relevant asset inventory insights with IT counterparts to help identify compliance gaps and reduce cyber risks.

6. Cross-Functional Collaboration and Backup Duties
- Serve as backup to the Security Awareness Analyst, supporting Audit coordination when needed.

Occupational health and safety

Employees:
Responsible to participate in the AU sponsibilities as an AU employee and supervisor, for participating in the AU OHS Program as required, and for ensuring the participation of employees in the AU OHS Program as required.

See: https://ohs-pubstore.labour.alberta.ca/li008

Classification factors

Communication

- Clearly communicates cyber risk and vulnerability-related concepts to both technical and non-technical stakeholders.
- Influences teams and leadership to adopt risk-informed decisions that align with organizational security policies and best practices.
- Collaborates with IT and security teams to develop, implement, and maintain risk-based controls, including CIS benchmarks and vulnerability mitigation strategies.
- Demonstrates strong negotiation skills to align stakeholders on security requirements, remediation timelines, and risk acceptance decisions.

- Members of the Digital Security Team are responsible for handling highly sensitive and confidential issues. This includes responding to and investigating potential security breaches, misuse of digital resources, and inappropriate online behaviour involving staff or students. This role demands the highest level of discretion, integrity, and confidentiality.

Supervision

No direct supervisory responsibilities but will advise security remediations to be implemented by members who are in several areas of the IT division.

Impact of service or product

- Upholds a high level of personal integrity and professionalism when handling confidential risk, vulnerability, and incident data.
- Leads and supports the vulnerability management lifecycle by identifying, assessing, prioritizing, and tracking remediation of security weaknesses across the organization.
- Strengthens the university's risk management framework by proactively identifying and mitigating cybersecurity risks, ensuring informed decision-making, regulatory compliance, and long-term protection of institutional assets and data.

Independence of action

- Develops and maintains risk assessment plans, manages changes in risk posture, and implements risk communication strategies, ensuring all documentation is clear, actionable, and aligned with organizational goals.
- Participates in security incident response activities, particularly those involving vulnerability exploitation or control failures, contributing to root cause analysis and risk remediation efforts.
- Collaborates with the Chief Information Security Officer, Security Operations, Technical Project Managers, and other stakeholders to implement and maintain CIS Controls and risk mitigation strategies.

Complexity

- Must be able to assess and respond to complex and time-sensitive risk scenarios, demonstrating sound judgment in prioritizing vulnerabilities and recommending risk treatment options.
- Balances technical, operational, and stakeholder concerns when planning and implementing risk mitigations, ensuring alignment with business objectives and compliance requirements.
- Capable of prioritizing and managing multiple assessments, vulnerabilities, and control initiatives in high-pressure or time-sensitive situations.

Planning

- Develops and maintains detailed risk assessment and vulnerability management plans, incorporating diverse input from systems, teams, and technologies to ensure accuracy and feasibility.
- Promotes efficient use of existing controls and technologies, supports best practices in risk mitigation, and ensures teams receive operational training to address evolving vulnerabilities and threats.

Signatures for section I

Incumbent signature		Date 2025-11-27
Supervisor signature		Date 2025-11-27

Section II: Qualifications

Qualifications

Includes education, experience, skills, abilities, and any other special qualifications required. The qualifications relate to the position not the incumbent.

- 5+ years of progressive experience in IT risk, cybersecurity risk management, IT audit, or information security, with emphasis on cybersecurity technology and implementation projects.
- Degree or diploma in computer science, information systems, engineering, or a related field (Canadian-recognized). Equivalent experience may be considered in lieu of formal education.
- Preferred certifications: AWS Security Specialty, CRISC, CISM, CISSP.
- Strong understanding of cybersecurity risk assessment methodologies and mitigation strategies.
- Excellent communication skills to articulate risk and technology issues to both technical and non-technical stakeholders.
- Skilled in managing contracts, negotiating timelines, resources, and resolving project-related challenges.
- Experience working with Managed Security Services Providers (MSSPs) is an asset.
- Adept at leading multiple projects simultaneously in high-pressure environments.
- Proven track record of strong interpersonal, leadership, and organizational skills.
- Demonstrated ability to work independently, think critically, and solve complex problems.
- Familiar with systems development life cycle (SDLC) and hands-on experience in analysis, design, testing, and implementation.
- Deep knowledge of industry standards and frameworks (ISO 27001, NIST, CoBIT, ITIL).
- Passionate about delivering excellent customer service and continuous professional development.

Signatures for sections I and II

Department Head signature		Date Select a date.

Executive Officer signature		
Human Resources review		Date Select a date.