Athabasca University

Professional Job Position Description

Section I: Position information

Effective date 2025-12-01 ☐ Update only ☒ Classification review	
Position title	Security Awareness Analyst
Position number	998747
Classification level	Excluded C
Position affiliation	☐ AUFA ☒ Excluded
Location	Virtual
Department	Digital Security, Information Technology
Reports to	Manager – IT GRC, Digital Security

Position summary

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

The Security Awareness Analyst is responsible for developing, executing, and sustaining AU's Cybersecurity Awareness and Training Program. This position plays a critical role in managing human-centric cybersecurity risks by driving behavioral change, strengthening security culture, and promoting awareness of evolving digital threats.

Working collaboratively with IT, Internal Audit, and business stakeholders, the analyst delivers targeted awareness initiatives that inform, engage, and empower staff, students, and third parties. The role also administers the security awareness platform, monitors effectiveness metrics, and ensures alignment with AU's cybersecurity policies, standards, and regulatory requirements.

In addition to awareness efforts, the analyst supports the coordination of internal and external audit activities supporting evidence gathering and compliance follow-ups.

As part of the broader digital security function, this role may also serve as a backup to other GRC functions as needed.

Duties and responsibilities

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

1. **Cybersecurity Awareness Program Development and Execution (40%)**

- Plan, manage, and evolve AU's cybersecurity awareness and training program.
- Structure the program for long-term effectiveness with clear objectives for behavioral change and risk reduction.
- Provide regular reports on awareness progress to IT GRC Manager, Digital Security.

- Establish and manage a Digital Security Champions/Ambassadors Network to extend security culture influence.
- Establish and maintain new hire phishing campaign and training program
- Plan and execute Cybersecurity Awareness Month.

2. **Content Development, Campaigns, and Role-Based Training (20%)**

• Design and deliver engaging, relevant, and innovative cybersecurity awareness campaigns using videos, infographics, LMS modules, simulations, and interactive content.

• Administer the security awareness platform, monitor user participation, and ensure training completion.

• Collaborate with University Relations and internal stakeholders to ensure wide reach and message consistency.

3. **Audit Engagement & Issue Remediation (15%)**

• Assist the coordination effort with Internal Audit and stakeholders to track and resolve cybersecurity-related audit observations in a timely manner.

• Provide support in monitoring the progress of remediation plans, provide status updates, and escalate delays where necessary.

• Offer risk-informed guidance to close audit issues and enhance overall control effectiveness.

4. **Digital Security Team Onboarding Coordination (5%)**

- Coordinate onboarding of new Digital Security team members.
- Maintain onboarding checklists and coordinate with HR and IT for provisioning.
- Serve as the main point of contact for onboarding-related questions and support.

5. **Security Governance & Committee Administration (10%)**

- Schedule and manage Security Steering Committee meetings.
- Prepare and circulate agendas, minutes, and follow-up actions.
- Track governance decisions and maintain historical records of meeting outcomes.

6. **Administrative & Operational Support (10%)**

- Maintain internal templates, trackers, and documentation repositories.
- Provide hands-on support to team members across GRC and broader Digital Security initiatives as needed.
- Administer and maintain Digital Security and Security Awareness SharePoint sites, ensuring content is current and well-organized.
- Oversee the folder structure, permissions, and data organization of GRC SharePoint libraries.
- Supports the Digital Security Team in the Request for Proposal (RFP) processes related to creating, issuing, reviewing, and rewarding RFPs for external services in coordination with the Cloud Business Office Licensing Specialist and the AU Office of Procurement.
- Accountable for ensuring own and all DSecO staff enter their internal labour on operating and capital initiatives via use of ServiceNow time reporting.

- Closely collaborates with the Cloud Business Office Management Officer and the Cloud Business Office Licensing Specialist regarding requisition, purchase order and invoicing processes for all DSecO external contracts.
- Closely collaborates with the Cloud Business Office Management Officer on administrative activities related to all financial and HR processing for the DSecO of the IT division

7. Cross-Functional Collaboration and Backup Duties

• Serve as backup to other GRC functions when needed.

Occupational health and safety

Employees:
Responsible to participate in the AU OHS program as required.

Supervisors:
Responsible for awareness of one's OHS Responsibilities 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

- Effectively communicates cybersecurity awareness, policy, and risk-related concepts to both technical and non-technical audiences in a clear, engaging manner.
- Influences organizational behavior by promoting a security-conscious culture through targeted training, messaging, and stakeholder collaboration.
- Works collaboratively with IT, Internal Audit, Digital Security, and business units to align training, policy, and communication strategies with cybersecurity goals.
- Demonstrates strong negotiation and facilitation skills to coordinate policy development, awareness content, and audit issue resolution across diverse stakeholder groups.
- 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 provides guidance and subject matter expertise on cybersecurity awareness, policy, and audit remediation activities across multiple departments.

Athabasca University

Impact of service or product

- Demonstrates a high level of integrity and professionalism in handling sensitive audit data, awareness metrics, and compliance-related communications, fostering trust in the Security Team across the university community.
- Strengthens the university's cyber defense posture by reducing human-related risks through targeted awareness campaigns, driving adoption of security policies, and promoting a culture of proactive cybersecurity across all departments and stakeholder groups.
- Collaborates with cross-functional teams to ensure security awareness initiatives align with organizational goals, creating measurable improvements in user behavior, policy adherence, and overall resilience against cybersecurity threats.

Independence of action

- Develops and maintains security awareness and risk communication strategies that align with organizational goals and compliance requirements, exercising independent judgment to design initiatives while escalating complex or high-impact decisions to leadership as appropriate.
- Supports incident response efforts by analyzing human factors, identifying trends, and recommending targeted training or policy updates, with work reviewed for accuracy, effectiveness, and alignment with organizational policies and regulatory standards.
- Coordinates closely with the CISO, Security Operations, and Audit teams to ensure awareness programs align with CIS Controls and broader risk mitigation initiatives, balancing independent solution development with collaborative input from cross-functional stakeholders to address multi-faceted cybersecurity challenges.
- Exercises a high degree of autonomy in identifying emerging cybersecurity awareness needs, designing and implementing proactive initiatives, and adjusting strategies based on evolving threats and organizational priorities, while ensuring alignment with university policies and risk management objectives.

Complexity

- Assesses complex behavior patterns, audit findings, and policy compliance issues, applying advanced analytical skills and critical thinking to identify gaps and guide improvements in awareness programs and policy development, often navigating ambiguous or novel situations.
- Balances technical accuracy with user-friendly communication, translating complex cybersecurity concepts into effective training and risk messaging that engages diverse audiences across the university.
- Manages multiple awareness, audit, and policy review initiatives under tight deadlines and shifting priorities, collaborating with cross-functional teams—including IT, Security Operations, and Audit—to deliver integrated, multi-faceted solutions that support organizational risk management and compliance objectives.

- Leverages independent judgment to develop solutions and recommendations while escalating high-impact or high-risk decisions to leadership as needed, ensuring initiatives are both innovative and aligned with institutional policies and goals.

Planning

- Maintains awareness plans and audit support documentation reflecting current risks, policies, and training needs.
- Coordinates policy review cycles and integrates changes into awareness content and communication plans.
- Promotes use of tools and best practices to enhance awareness delivery and track effectiveness.

Signatures for section I

Incumbent signature		Date Select a date.
Supervisor signature		Date Select a date.

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 in security awareness, compliance training, or cybersecurity/GRC roles.
- Degree or diploma in InfoSec, Communications, Education, or related field; equivalent experience considered.
- Preferred certifications: CISSP, CISM, CRISC, or security awareness-specific (e.g., SANS, Proofpoint, H Layer).
- Strong knowledge of risk management, security policies, and frameworks (NIST, ISO 27001/27002).
- Experience supporting audits and aligning awareness programs with compliance and policy requirements.
- Skilled in creating and delivering engaging content for technical and non-technical audiences.
- Proficient with LMS platforms and eLearning tools.

- Excellent communicator with strong project coordination and stakeholder engagement abilities.
- Self-driven, organized, and able to manage multiple priorities in a fast-paced environment.

Signatures for sections I and II

Department Head signature		Date Select a date.
Executive Officer signature		Date Select a date.
Human Resources review		Date Select a date.