Athabasca University

Professional Job Position Description

Section I: Position information

Effective date 2024-12-01 ☐ Update only ☒ Classification review	
Position title	Manager, IT Governance, Risk & Compliance (GRC)
Position number	998584
Classification level	TBD
Position affiliation	☐ AUFA ☒ Excluded
Location	Virtual
Department	Information Technology
Reports to	Chief Information Security Officer

Position summary

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

The Manager, IT Governance, Risk & Compliance (GRC) is responsible for overseeing key components of the AU's security program, ensuring the protection of its digital assets and infrastructure and ensuring the avoidance or reduction of impact on the university's core operations from cybersecurity threats. This role involves, managing the implementation and maintenance of security policies, and leading a dedicated team focused on IT governance, risk, compliance, security awareness, and training.

The Manager, IT Governance, Risk & Compliance collaborates with various departments and external partners to establish effective security risk management measures, coordinates internal and external audits, and oversees the university-wide information security awareness and training program. This position requires strong leadership skills to mentor and manage the security program team, facilitate knowledge sharing, and ensure continuous improvement in security practices.

Duties and responsibilities

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

Strategic Alignment

- Work with the CISO and leadership team to develop and maintain the university's security program, plans and processes ensuring alignment with the university's strategic direction. Provide quarterly reports on the progress and effectiveness of security initiatives.
- Monitor the progress of the information security plan, ensuring that performance is aligned with the objectives. Make suggestions for changes as needed to maintain alignment.

Leadership and Team Management

- Lead, mentor, and manage the security program team, including providing caring and challenging feedback, to foster an environment of trust and continuous improvement.

- Conduct weekly team meetings to review ongoing projects and address challenges, provide one-on-one mentoring sessions to support team members' professional growth, and implement a feedback system for continuous performance improvement. Track team progress and report monthly on key performance indicators (KPIs).
- Facilitate regular training sessions and mentorship opportunities to facilitate knowledge sharing and technical and personal development within the team.
- Lead the recruitment process for new staff members or contract outside services to supplement the team's capabilities when needed.

IT Governance, Risk, Compliance and Security Awareness/Training

- Lead the Security GRC Team in establishing operational goals and priorities.
- Oversee the review, implementation and ongoing maintenance of security policies, standards and procedures.
- Work with the CISO's leadership team to define and develop the security program portfolio of services, then oversee its socialization and communication.
- Build, prioritize and maintain business relationships with staff to help ensure security services and processes are well-communicated and integrated within the organization.
- Coordinate and lead meetings with the Security Committee to help ensure good governance of the security program
- Working with the CISO, lead the maturation of the security risk management strategy, process and program. Including maintenance of the cybersecurity risk register and other related artifacts.
- Support the departments and faculties in the identification and assessment of cybersecurity-related risks, working hand in hand to identify mitigation requirements, and ensuring transparency and clarity in the risk management decision-making process.
- Working closely with the Security Operations Manager and CISO to provide a realistic overview of risks and threats to AU. Lead the documentation of security controls and their effectiveness.
- Work with various stakeholders to identify information asset owners to classify data and systems as part of a control framework implementation.
- Coordinate internal and external IT and Security audits, working closely with internal and external audit functions.
- Ensure that controls implemented, adequately address security and compliance requirements.
- Oversee the implementation of a university-wide information security awareness and training program.

Collaboration

- Work closely with all departments (IT, University Relations, Enterprise Risk Management, HR, Privacy, Finance, Internal Audit etc.) and faculties, to ensure a cohesive approach to security. Measure the effectiveness of collaborative efforts through inter-departmental feedback and project outcomes.
- Manage the process of gathering, analyzing, and assessing the current and future threat landscape.

Reporting and Metrics

- Work closely with the Security Operations Manager and CISO to develop and report on cybersecurity metrics to Senior Leadership and the Board.
- Generate regular reports on security program activities, goals, and performance metrics for senior management and stakeholders. Detailing security program status and providing recommendations for improvements.

Future Readiness

- Stay informed on emerging business functions and technologies that impact information security and incorporate them into the program as needed.
- Propose changes to existing policies, standards and procedures to ensure operating efficiency and regulatory compliance.
- Work with the CISO to develop budget projections based on short and long-term goals and objectives.

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

- Excellent communication and interpersonal skills are required -including the ability to effectively communicate security and/or risk-related concepts to technical and non-technical audiences.
- The incumbent will communicate with a broad set of stakeholders at all levels within the university community as well as external bodies.
- Works closely with the Chief Information Security Officer, IT Directors, VPITCIO, IT Managers, and other senior university decision-makers to oversee and integrate the security program.
- Possess strong decision-making capabilities, with a proven ability to weigh the relative costs and benefits of potential actions and identify the most appropriate one.
- They collaborate with various departments to ensure a cohesive approach to security and maintain clear communication on the threat landscape, providing cybersecurity advisory services to help improve decision-making.

Supervision

This role will have responsibility for recruitment, supervision, evaluation and performance management of employees, consultants, and contractors.

The role reports to the CISO and will operate with high autonomy. Receiving strategic objectives and performance expectations from the CISO.

Impact of service or product

- The Security Program Manager ensures the university's digital assets and infrastructure are protected, minimizing disruptions to academic and administrative operations. They lead the development and implementation of security policies and risk management strategies, ensuring regulatory compliance and effective threat mitigation.

- Capability Development: Mentors and develops less experienced team members, building a stronger, more knowledgeable, and capable cybersecurity team.

Independence of action

- This position reports directly to the CISO and works independently. The solutions implemented by this position will normally be considered correct but may be reviewed for departmental consistency.
- This role participates and may take actions related to confidential investigations of employees. This role provides input into investigation procedures, review and assessment of investigations, and recommendations for discipline. The highest degree of confidentiality and no conflict of interest is required for the role.

Escalation Criteria:

- Strategic decisions that involve significant changes to the university's overall cybersecurity strategy or major alterations to existing IT infrastructure must be escalated to the CISO.
- Any decision that requires substantial financial investment or has a considerable impact on the university's budget must be reviewed and approved by the CISO.
- Decisions that may impact multiple departments or require cross-departmental coordination should be escalated to ensure alignment and collaboration.

Complexity

Nature of Work: manages complex security initiatives involving multiple stakeholders, and cross functional processes. Responsible for developing and implementing policies, ensuring regulatory compliance and oversight of the security awareness and training program. Manages people's performance, which requires the acumen to be able to tackle performance-related issues while navigating relationships and the impact on team dynamics.

Problem Solving: Requires broad experience and skill to address diverse cybersecurity risks and themes. Must balance short-term operational and tactical execution with long-term strategic thinking.

Multiple Stakeholders: involved in the execution of the security program. Stakeholder concerns and many control implementation touchpoints also lead to complexity indices.

Planning

- Develops operational and tactical plans that require consideration of people, processes and technology, to support the organizational and department strategy.

- Plans are approved in collaboration with the CISO
- The plans must be sufficiently detailed to support accurate budgeting and scheduling.
- Ensures team resourcing and capabilities are adequate for execution of the security program.

Signatures for section I

Incumbent signature		
Supervisor signature		

Section II: Qualifications

Qualifications

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

Education

Candidates will be evaluated based on their ability to demonstrate the competencies described above. The typical work experience and educational background for this role include:

A degree or diploma in Computer Science, Information Security, Business Administration. An equivalent combination of education and experience may be considered.

Certifications

Relevant Certifications include:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Cloud Security Professional (CCSP)
- Certified in Risk and Information Systems Controls (CRISC)
- Certified in Governance, Risk and Compliance (CGRC)

Experience

- 5 years of experience in cybersecurity roles, with a focus on security program management, resourcing, privacy, IT governance, risk, compliance and security awareness and training or an equivalent combination of education and experience.
- Prior experience leading IT and Cybersecurity Governance, Risk and Compliance initiatives and teams.
- Experience developing, implementing or overseeing a security awareness and training program.
- Experience implementing regulatory compliance and cybersecurity frameworks and associated controls (e.g., NIST CSF/800:53, CIS CSC, PCI DSS, etc.).

- Understanding of current cloud best practices, design principles, market trends, and emerging technologies
- Strong understanding of cybersecurity risk management and risk mitigation strategies.
- Strong understanding of information security fundamentals and general security technologies.
- Understanding of technology security and its relation to service delivery, project management, and the software development life cycle.
- Understanding of data privacy regulations and frameworks (FOIP, GDPR, etc.)

Skills

- Stakeholder and customer-focused to ensure the security program and initiatives are centred around the organization
- Ability to develop security roadmaps and assess the financial impact of security solutions.
- Demonstrated problem-solving abilities to identify root causes of issues and develop creative solutions.
- Strong negotiation skills for resources, changes, issues, budgets, and timelines.
- Ability to lead and inspire a team, fostering a collaborative and high-performance environment.
- Strong analytical skills to assess complex security issues and make informed decisions.
- Flexibility to adapt to rapidly changing environments and evolving threats.
- Strong interpersonal skills to build relationships with stakeholders and work effectively in cross-functional and remote teams.
- Ability to manage and resolve conflicts constructively and diplomatically.
- Excellent time management skills to prioritize tasks and meet deadlines in a fast-paced environment.
- Strong verbal and written communication skills with a keen eye for detail to ensure accuracy and thoroughness in all security documentation and reporting.

Signatures for sections I and II

Department Head signature		
Executive Officer signature		
Human Resources review		