Professional Position Description

Section I Position Information	Update Only ☐ Classification Review ☒
Position Title	**Identity and Access Management Analyst, Digital Security**
Position #	
Department	Information Technology
Classification Level	Excluded C
Reports to	Director, Digital Security Office
Effective Date	
Position Summary Briefly describe the main purpose(s) of the position	The Identity and Access Management Analyst (IAMA) is responsible for supporting the Digital Security Program. The IAMA will work with the Chief Information Security Officer (CISO), the Director, Digital Security Office (DDSecO), members of the Digital Security Office (DSecO) team, AU faculties, and other business units, in the planning, building, delivery and support of the AU IAM program. Assisting with the CISO and DDSecO, the IAMA will provide direction and guidance on the development, specifications, and communications of IAM applications, as well as provide in-depth technical consultation to AU faculties, business units and IT management. The IAMA will also assist in developing plans and direction for the alignment of digital business objectives to digital security control requirements. The IAMA is responsible for researching, scoping and designing of IAM cybersecurity solutions that comply with AU digital security policies and standards. IAMA will work with other digital security and IT operations team members to deliver digital security strategy, tactical, and operational activities to mature the digital security program. Individual will assist with the deployment of cloud-centric IAM technologies that enable realization of AU business IAM objectives in all AU environments (AWS and Azure cloud, on-premises, 3rd party etc.).
Duties and Responsibilities Organize by key responsibility area and include % of time spent where possible	• Map business requirements to IAM solutions. Envisions business outcomes and enables alignment with them. • Enables the use of technology-based tools or methodologies to review, design, and/or implement products and services to provide a strong AU IAM program that balances access with compliance and confidentiality. • Understand emerging IAM technologies and trends – then using this understanding to envisage capabilities need based on the AU business context. • Identifies and evaluates complex business and technology risks. Then designs IAM controls that mitigate these risks, recommending related opportunities for digital security control improvements.

	• Identifies the broader impact of current decisions related to user access, data access, and digital business security. • Aligns IAM processes across AU, and develops and documents standards for use. • Along with IT and business unit leaders, co-leads IAM solution selection processes. IAMA also evaluates existing and emerging technologies and tools in the selection of IAM service offerings. • Understands business and IT management processes; and demonstrates advanced understanding of business processes, internal control risk management, IT controls and related standards. • Fosters an understanding of the need for, and application of, IAM systems, and facilitates decision making with essential stakeholders. • Builds and nurtures positive working relationships. • Identifies opportunities to improve IAM engagements. • Effective implementation, transfer, and operationalization of IAM controls that enable enhanced digital security.
Occupational Health and Safety	Responsible for awareness of one's OHS Responsibilities as an AU employee and for participating in the AU OHS Program as required. See: https://ohs-pubstore.labour.alberta.ca/li008
Classification Factors	
Communication	• Excellent written and verbal communication skills. • Strong interpersonal and collaborative skills. • Tracks and reports on project and controls implementation drift. Always seeking to find and communicate improvement opportunities. • Along with the DDSecO, works closely with other IT teams to develop and implement updated IAM controls as applicable. • The IAMA is responsible for communicating IAM design, revisions, and implementation status to DDSecO. • Ability to effectively communicate security and / or risk-related concepts to technical and nontechnical audiences. • Fosters an understanding of the need for, and application of, IAM systems, that enables decision making with essential stakeholders. • Strong skills as a negotiator; to enable commitment to, and sign-off on, requirements to incorporate IAM controls to specific environments. • Can translate cybersecurity-related matters into business terms that are clear and understandable to AU executives. • All members of the DSecO handle extremely sensitive information regarding security breaches and incidents that must be kept confidential and can include investigation of staff or student accounts or online behaviour. Absolute confidentiality is required.
Supervision	• Has no direct reports/supervision

Impact of Service or Product	• High level of personal integrity, with the ability to handle confidential and otherwise sensitive matters professionally and with the appropriate level of judgment and maturity. • Under- or over-reporting of cybersecurity risks to AU stakeholders presents risks to the university. Underreporting on magnitudes could cause AU to operate outside of risk tolerances, exposing the university to enterprise risks. Overreporting on magnitudes could cause AU to overcompensate, unnecessarily utilizing critical resources and time, or lose competitive advantages by forgoing relevant opportunities.
Independence of Action	• Formulates project plans, manages change, develops and implements communication strategy, and prepares related documentation throughout. • Work with the CISO, DDSecO, and other stakeholders to implement necessary IAM controls.
Complexity	• As digital projects complexity increasingly arise from rapidly changing third party managed, multiple stakeholder owned, and increasingly complex, technology environments, there is a need to ensure the AU community understands where interactions with digital technologies could introduce IAM, and other negative digital security, risks. The IAMA must be able to adapt to changing operating models, and revise IAM controls as required. • The IAMA must consider stakeholder concerns and implementation touchpoints prior to activating controls in Production.
Planning	• The IAMA develops plans that include a wide variety of inputs and technologies. These plans must be sufficiently detailed to allow accurate budgets and schedules to be created. Plans must include contingencies to account for potential changes in the operational environment. A high level of organizational and planning skills is required.

Signatures for Section I

Incumbent's Signature _____ Date _____

Supervisor's Signature _____ Date _____

Section II

Qualifications

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

Education / Experience

- Minimum 5 years progressive experience managing technology related projects, with an emphasis on cybersecurity and information security technology implementation projects.
- Identity management familiarity in one or more of the following cloud platforms; AWS, Azure or Google Cloud.
- AWS Certified Security Specialty Certification required (where candidate is not yet certified, ability to acquire certification in 2 years is mandatory).
- Diploma or degree in computer science, management, or engineering, recognized in Canada. In lieu of a degree or diploma, additional experience over and above the minimum requirement may be considered.
- CRISC, CISM, and/or CISSP certification preferred.
- Experience with regulatory compliance and information security management frameworks (such as International Organization for Standardization [IS0] 27000, COBIT, National Institute of Standards and Technology [NIST] 800).
- Good understanding of web security standards, architecture, web security best practices and application security best practices.
- Identity management familiarity in at least one or more of the following areas:
  - single sign-on (SSO);
  - data management;
  - identity federation;
  - enterprise directory architecture; and
  - design - including directory schema, directory services, namespace and replication topology experience, resource provisioning and process integration.
- Expert understanding of IAM concepts, including federation, authentication, authorization, access controls, access control attacks, identity and access provisioning life cycle.
- Identity and access governance; including role-based access control, access request and certification, user life cycle management processes, and organizational change management.
- Experience with administrating authentication technologies, such as Microsoft Active Directory/Windows authentication, OpenLDAP, Shibboleth, SimpleSAMLphp, Kerberos, OpenID Connect, OAuth, and federated identity management.
- Familiarity with, and experience, managing Linux servers, including Apache and configuration management with Salt, Ansible, Chef or Puppet.
- Familiarity with Ruby, Python, PHP, PowerShell, SQL and/or shell scripting.
- Understanding of cybersecurity risk management and risk mitigation strategies.
- Ability to communicate project and technology risks effectively.
- Strong negotiation skills to negotiate resources, changes, issues, budgets, and timelines.
- Passionate about customer service excellence.
- Multi-tasking ability - must be comfortable with simultaneously managing multiple projects.
- Excellent interpersonal, communication, leadership, motivational, organizational, and planning skills.
- Resourceful, creative and self-motivated.
- Strong problem-solving skills, including the ability to take a practical approach to dealing with shifting priorities, demands and timelines.
- Highly self-motivated, self-directed, and attentive to detail.
- Ability to effectively prioritize and execute tasks in a high-pressure environment.
- Extensive experience working in a team-oriented, collaborative environment.