Alberta

Job Description

Public (when completed)

Common Government

New

Ministry

Technology and Innovation

Describe: Basic Job Details

Position

Position ID

Position Name (30 characters)

Identity and Access Analyst

Requested Class

Systems Analyst Level 3

Job Focus

Operations/Program

Supervisory Level

Agency (ministry) code

Cost Centre

Program Code: (enter if required)

Employee

Employee Name (or Vacant)

Organizational Structure

Division, Branch/Unit

☑ Current organizational chart attached?

Supervisor's Position ID

Supervisor's Position Name (30 characters)

Supervisor's Current Class

Design: Identify Job Duties and Value

Job Purpose and Organizational Context

Why the job exists:

Reporting to the Manager, Product Operations, the Identity and Access Analyst provides operational and technical support to program and delivery teams onboarding to the Government of Alberta's enterprise identity and access management (IAM) platform. The role helps teams understand onboarding requirements, prepare integration inputs, and move through onboarding activities in a secure, consistent, and efficient way.

This position supports identity assurance and onboarding processes by coordinating information, reviewing documentation for readiness and completeness, and helping teams identify when specialized review by Cybersecurity, Privacy, or identity assurance partners is required. The role works across technical and non-technical groups to improve clarity, reduce delays, and support consistent adoption of enterprise IAM requirements. The position also uses approved AI and automation tools appropriately to improve drafting, analysis, and documentation quality while maintaining human judgment, accountability, and protection of sensitive information.

Responsibilities

Job outcomes (4-6 core results), and for each outcome, 4-6 corresponding activities:

1. Support Onboarding to Enterprise IAM Services

- Provide program and technical teams with onboarding guidance, including architecture expectations,

design requirements, security considerations, data attribute standards, and relevant integration dependencies.
- Guide teams through onboarding steps, required inputs, timelines, and handoffs.
- Maintain onboarding materials such as checklists, templates, FAQs, and knowledge resources.
- Help teams understand enterprise IAM requirements and prepare for implementation planning.
- Use approved AI tools, where appropriate, to support drafting, organizing, and improving onboarding materials, with all outputs reviewed for accuracy and suitability before use.

2. Support identity risk assessment and readiness activities
- Help program teams complete identity risk assessment inputs using established frameworks, templates, and guidance.
- Review submitted materials for completeness, clarity, and readiness before they move forward for specialized review.
- Identify missing information, inconsistencies, or unresolved issues and work with teams to correct them.
- Escalate complex interpretation issues or higher-risk matters to the appropriate standards, cybersecurity, privacy, or identity assurance partners.
- Use judgment when applying approved AI tools to support analysis or document review, ensuring outputs are checked for privacy, security, and policy alignment.

3. Review onboarding and supporting documentation
- Review onboarding and supporting documents to confirm they are complete and aligned with enterprise IAM onboarding expectations.
- Identify documentation gaps or issues that could delay onboarding, expert review, or implementation.
- Help ensure materials are organized and ready for specialized review without performing specialist approvals outside the role's mandate.
- Promote consistency in the documentation used to support onboarding decisions and implementation planning.

4. Enable coordination across stakeholders
- Translate technical IAM onboarding requirements into clear, practical guidance for business and delivery teams.
- Coordinate with program areas, technical teams, Cybersecurity, Privacy, and identity assurance partners to support smooth handoffs and issue resolution.
- Clarify roles, responsibilities, dependencies, and next steps throughout onboarding and implementation activities.
Support onboarding-related readiness activities, including planning, issue tracking, and coordination with affected teams.

5. Contribute to continuous improvement
- Identify recurring onboarding issues, process gaps, and documentation weaknesses, and recommend practical improvements.
- Contribute to updates to templates, guidance materials, checklists, and support processes.
- Share lessons learned and emerging needs with the manager and relevant partners.
- Identify appropriate opportunities to use approved AI and process automation tools to improve research, drafting, documentation, or workflow efficiency within the role's scope.

Problem Solving

Typical problems solved:

- Helping teams interpret and apply IAM onboarding requirements in different delivery contexts.
- Identifying gaps or inconsistencies in onboarding materials and risk assessment inputs.
- Resolving coordination issues that slow onboarding progress or create rework.
- Determining when an issue can be addressed through existing guidance and when it should be escalated.
- Explaining technical requirements clearly to non-technical stakeholders without losing important detail.

Types of guidance available for problem solving:

- Enterprise IAM onboarding processes, technical standards, architecture requirements, identity assurance frameworks, and branch procedures.
- Relevant standards and frameworks, including NIST 800-63, Pan-Canadian Trust Framework guidance, Government of Alberta digital standards, and applicable privacy and security requirements.
- Direction from the Manager, Product Operations, with consultation available from architects, cybersecurity, privacy, and identity assurance specialists.
- Approved AI tools may support drafting, analysis, and information organization, but do not replace professional judgment, specialist review, or final decisions.

Direct or indirect impacts of decisions:

- Improves the quality and consistency of onboarding to enterprise IAM services.
- Reduces delays, rework, and avoidable gaps in onboarding documentation and readiness.
- Supports secure and effective adoption of enterprise IAM requirements.
- Improves coordination between business, technical, and specialist partners.

Key Relationships

Major stakeholders and purpose of interactions:

Internal:

- Application development teams
- Digital services teams
- Cybersecurity and SARTR Special Investigation teams
- Privacy teams
- Communications teams
- Partner ministries, relying parties, and proxy identity providers

External:

- Public sector security and risk communities
- Law enforcement and fraud prevention groups (as required)

Required Education, Experience and Technical Competencies

Education Level	Focus/Major	2nd Major/Minor if applicable	Designation
Bachelor's Degree (4 year)	Science		

If other, specify:

Job-specific experience, technical competencies, certification and/or training:

Job-specific Experience and Competencies:

- Experience supporting identity and access management onboarding, implementation, integration, or operational delivery
- Knowledge of IAM concepts, onboarding practices, and enterprise integration requirements
- Working knowledge of standards or frameworks such as NIST 800-63 and the Pan-Canadian Trust Framework
- Experience with enterprise IAM platforms such as ForgeRock, Okta, Microsoft Entra ID / Azure AD, Ping Identity, or similar tools
- Ability to review documentation for completeness, quality, and readiness for further review
- Ability to translate technical requirements into practical guidance for non-technical audiences
- Ability to recognize when issues require escalation to Cybersecurity, Privacy, or other specialized partners
- AI fluency: daily, effective use of approved generative AI and agentic tools for drafting, analysis, structured retrieval, and documentation support, with strong judgment in validating outputs for accuracy, risk, and sensitivity
- Process automation literacy: working knowledge of workflow automation, digital forms, and AI-supported process improvement relevant to operational delivery
- Understanding of responsible AI use in a government context, including human accountability, privacy, security, and protection of sensitive information

Preferred Certifications:
- Certified Identity and Access Manager or similar identity-related certification.
- Relevant IAM, cloud identity, or security administration certification.
- Privacy, risk, or security certification as an asset.

Behavioral Competencies

Pick 4-5 representative behavioral competencies and their level.

Competency	Level A B C D E	Level Definition	Examples of how this level best represents the job
Systems Thinking	○ ○ ◉ ○ ○	Takes a long-term view towards organization's objectives and how to achieve them: • Takes holistic long-term view of challenges and opportunities • Anticipates outcomes and potential impacts, seeks stakeholder perspectives • Works towards actions and plans aligned with APS values • Works with others to identify areas for collaboration	Incorporates enterprise-wide impacts into risk analysis and identity strategy planning. Requires a sharp focus on digital trust, authentication risk management, fraud prevention, and compliance — key components of modern IAM programs.
Agility	○ ○ ◉ ○ ○	Identifies and manages required change and the associated risks: • Identifies alternative approaches and supports others to do the same • Proactively explains impact of changes • Anticipates and mitigates emotions of others • Anticipates obstacles and stays focused on goals • Makes decisions and takes action in uncertain situations and creates a backup plan	Adapts quickly to evolving identity threats, standards updates, and legislative changes. The role must operate tactically in managing risk at the identity layer of digital services.
Build Collaborative Environments	○ ○ ◉ ○ ○	Collaborates across functional areas and proactively addresses conflict: • Encourages broad thinking on projects, and works to eliminate barriers to progress • Facilitates communication and collaboration	Facilitates risk discussions across technical and non-technical stakeholder groups.

		• Anticipates and reduces conflict at the outset • Credits others and gets talent recognized • Promotes collaboration and commitment	
Develop Networks	○ ○ ◉ ○ ○	Leverages relationships to build input and perspective: • Looks broadly to engage stakeholders • Open to perspectives towards long-term goals • Actively seeks input into change initiatives • Maintains stakeholder relationships	Establishes and maintains strong working relationships with internal and external risk and fraud prevention communities.
Creative Problem Solving	○ ○ ◉ ○ ○	Engages the community and resources at hand to address issues: • Engages perspective to seek root causes • Finds ways to improve complex systems • Employs resources from other areas to solve problems • Engages others and encourages debate and idea generation to solve problems while addressing risks	Proactively identifies and mitigates emerging identity fraud trends and risks.

Benchmarks

List 1-2 potential comparable Government of Alberta: Benchmark

513SA02 Senior Systems Analyst/Database Administrator
513SA10 Senior Business Intelligence Analyst