This is a starting point for you, not the final copy. Please remember to revise it as needed for your particular organization's needs! If you have feedback, please contact editor@idpro.org.

Architecture – Identity Standards

Measurable Performance Indicators

- System scalability
- System resiliency
- Reduction in security breaches
- Reduction in fraud
- Minimize technical debt
- Authorship of Identity Standards in Recognized SDO

Key Skills to Do the Job

- Stakeholder management
- Ability to influence senior leadership
- Ability to influence at an industry level
- Collaboration, cross-functional, and cross-industry working
- Change Management in complex organizations
- Team leadership
- Strategic planning
- Budget management
- Design Patterns
- Ability to track the market and stay up-to-date on emerging threats and technologies
- Strong Written and verbal communication, especially presenting technical concepts to a non-technical audience.

Responsibilities

Design Target-State Architecture

- **Define Target-State**: collaborate with engineering, business units, and stakeholders to drive requirements and design the target-state IAM architecture.
- **Embed Industry Standards:** provide guidance as to where the organization can apply or extend industry standards in its target-state architecture.

- **Evaluate Trade-Offs and Manage Technical Debt**: assess business needs, target-state, time-to-market, dependencies, and minimize technical debt.
- **Develop Target-State Roadmap**: work with engineering and other partners to define and plan key IAM initiatives and implementations that move the business toward target-state.
- **Multi-Channel Patterns**: design multi-channel target-state patterns for user provisioning/deprovisioning, recovery, authentication, and authorization.
- **Continuous Improvement**: find opportunities to streamline IAM, drive automated solutions, increase efficiency of future change, and refine the target-state.

Target State Delivery

- **Scope Design**: collaborate with engineering to scope the engineering design for the target state IAM architecture.
- **Deployment Models**: understand and advise on common deployment models for IAM target-state.
- **Maintain and Optimize**: create and maintain architectural documents for the overall IAM solutions to ensure currency against business needs, capabilities, and the threat landscape.
- **Security-by-Design**: partner to ensure that the target-state architecture is delivered to best-in-class security standards aligned to company strategy.
- **Privacy-by-Design**: ensure that target-state delivery meets the privacy requirements of the business.

Application Management

- **Application Specifications**: develop specifications for applications, especially integration into wider IAM infrastructure.
- **Application Security**: collaborate with IT and Cybersecurity to ensure that applications are deployed using secure profiles and conduct regular application reviews to ensure ongoing performance and security.

Standards Development

- **Community Engagement:** engage in Standards Development communities to maintain industry knowledge and apply best-practice internally.
- **Thought Leadership:** contribute to prioritized standards development efforts in order to solve core company challenges in a standardized manner, achieve strategic objectives, and establish the organization as a thought leader on strategically relevant topics.

Risk Management

- **Mitigate Risk**: identify, assess, and mitigate risks and vulnerabilities.
- **Ensure Compliance**: Evaluation of current processes against policy as well as the defined industry standards and leading practices.
- **Incident Response**: investigate security incidents related to identify root causes and drive architectural remediation.

Financial Leadership

- **Business Case**: conduct cost/benefit analysis and engage stakeholders to justify IAM investments.
- **Prioritize Investments**: direct financial planning and execution, including capital investments, day-to-day operational spend, contractor management, and personnel.

People Leadership (Optional)

- **Team Management**: Manage a team of direct reports and contract service providers.
- **Capacity Building**: implement a staffing and continuous development strategy to ensure that the team remains well-equipped to manage in the modern threat landscape.

Knowledge and Qualifications

- Strong foundation in Identity and Access Management Technology or Cybersecurity
- Expertise in IAM protocols, such as SAML, SPML, XACML, SCIM, FIDO, OpenID Connect, and OAuth 2.0
- Expertise in key IAM and Cybersecurity concepts, like Directories, Single Sign-On, Multi-Factor Authentication, Delegated Administration, API Gateways, SOA Services, threat detection, etc.
- Experience working with IAM architecture within a diverse IT environment, including Cloud, On-Premises, IaaS, and SaaS platforms
- Deep understanding of common deployment models
- Familiarity with key regulatory requirements and industry standards, such as NIST 800-63, GDPR, CCPA, HIPAA, and SOX
- Professional certifications, like CIDPRO, CISSP, CISM, CIAM or those related to PAM tools.