South Jersey Industries

*Position Title:* Governance Risk and Compliance Analyst III  
*Position Type:* Full-Time  
*Compensation:* Salaried  
*Start Date:* March 1, 2021  
*Location:* Folsom, NJ (about 30 minutes from Philadelphia)

*Job Description*

The role will be responsible for establishing appropriate Critical Access and SOD rule sets for different applications (Workday Financials and HCM, Oracle Customer Care & Billing (CC&B), Maximo and Hyperion), managing IT organizational policies and standards in support of legal and regulatory compliance needs, designing and testing general IT and organizational information security controls and interfacing with Internal Audit and business leaders to ensure that controls are designed and operating effectively. The GRC analyst will be responsible for helping to manage IT compliance for SJI utilizing Saviynt Security Manager (SSM). The individual will manage and support GRC activities within Saviynt; such as establishing user access requests and approval workflows, critical access and segregation of duties (SOD) assessments for multiple business processes, user access reviews, data governance, and IT and Cyber risk management functions.

**Essential Functions:**

- Work as a GRC lead to design, develop, build, and test the Saviynt IGA solution to support SJI business and audit requirements.
- Interact/coordinate with business stakeholders for various business processes supported by applications (Workday, Oracle CC&B, etc.), to define, build, test and support user access request and approval workflows, user access reviews and critical access and SOD assessments requirements.
- Ensure controls designed in Saviynt meet control objectives as defined by Management and tested by Internal and External Auditors.
- Continually monitor controls throughout the fiscal year to ensure controls are operating effectively and communicate status to appropriate business and audit stakeholders.
- Provide solution options, knowledge- and experience-based recommendations and projected impacts to address gaps between control objectives and designed control activities
- Resolve technical issues through debugging, research, and investigation
- Provide technical expertise and real-life experience in creating solutions, design, proof of concept and implementation.
- Plan and implement policies, procedures, standards, and controls to govern the protection of corporate information systems, networks, and data.
- Update SOD frameworks and matrix with strong partnership between the business and supporting functions.

**Qualifications/Skills:**

- Strong understanding of fundamental information security concepts and technology
- Experience with Workday and Oracle application security
- Java/J2EE and strong SQL knowledge is ideal, knowledge of Web Services (REST/SOAP)
- Strong technical presentation and communication skills, both verbal and written
- Ability to work independently, adapt quickly, and maintain a positive attitude
- Sound business and technical acumen
- Strong sense of task ownership and self-motivation
- Problem solver, ability to troubleshoot and break down complex issues into an actionable progression of tasks

**Education:**
- 5+ years overall relevant experience, including identity governance, audit, cyber risk, consulting, or related services
- Significant experience with legal and regulatory compliance standards such as SOX, GDPR, HIPAA, NERC-CIP, etc.
- Familiarity with control frameworks, such as ISO or NIST Cybersecurity Frameworks
- Experience with IT governance, risk, and compliance management in a large environment
- Utility industry experience is ideal
- Experience with documenting and testing controls with experience in following test procedures that include Test of Design and Test of Operating Effectiveness.

**Certification(s):** Certified Information Security Auditor (CISA), Certified Risk and Information Systems Controls (CRISC), Certified Information Systems Security Professional (CISSP)

**Travel:** Less than 10%

---

**Contact Information**

- **Contact Name:** Bianca Gonzalez and James Clark
- **Email Address:** bgonzalez@sjindustries.com and jclark@sjindustries.com
- **Telephone:**
- **Fax:**
- **Website:**
- **Company Information:**
- **Special Instructions:**