Information Security Lead Auditor

The **Multi-State Lottery Association** (**MUSL**) is a non-profit, government-benefit association responsible for the operation of **Powerball®** and other multi-jurisdictional lottery games in the United States. As an **Information Security Lead Auditor** at MUSL, you will be an integral part of the team that ensures the integrity of lottery games throughout the United States.

The Information Security Lead Auditor will be responsible for the preparation of reports, including or similar to Service Organization Control (SOC) 1, SOC 2, ISO27001. Audits will apply most areas of the governing standard as necessary while documenting, validating, testing, and assessing various control systems.

This position requires excellent interpersonal skills, the ability to multi-task, and a solid understanding of security and information technology principles. The analyst is responsible for furnishing assessment reports, conducting meetings with internal and external staff, communicating trends and analysis to staff and management, and helping ensure the organization understands and appropriately manages risk. This headquarters for this position is located at the MUSL office in Johnston, Iowa but may be performed remotely. Remote candidates must be located within a reasonable distance from a major airport.

Primary Job Tasks and Responsibilities

- **This position is external/member lottery focused (travel to jurisdictional lotteries throughout the U.S. up to 5 days at a time, 15-20 trips per year)**
- Represent the Association in a positive, professional, and courteous manner.
- Assist in all aspects of audits, including risk assessments, audit planning, audit testing, control evaluation, draft report review, and follow-up verification of issue closure.
- Audit and design test procedures for IT controls across a range of areas/technologies (e.g., IT General Controls, application controls, system implementations, cybersecurity, privacy, database management systems, operating systems, ERPs).
- Document audit workpapers, results, and reports with minimal intervention from management.
- Complete assignments in an efficient manner while ensuring high quality is maintained.
- Perform audit work in accordance with firm methodologies and professional standards.
- Manage multiple projects and competing priorities in a rapidly growing, fast-paced, remote team environment.
- Demonstrate and maintain technical competency in audit, compliance, and security areas.
- Continue to learn from daily job experience and the study of internal audit standards, procedures, tools, and techniques.
- Research and recommend process, security, technology, operations, and compliance enhancements.

Experience and Education

- Bachelor’s or Master’s degree in Technology, Computer Science, Engineering, or similar.
- ISO 27001 Lead Auditor certification is required.
- Minimum of 5 years of prior experience performing external audits is highly desired.
- 5 years of experience performing SOC 1 / SOC 2, PCI DSS, HITRUST, or ISO 27001 assessments is preferred.
- Certifications such as CISSP/CISM/CISA or the ability and willingness to acquire.
- Understanding and experience planning and coordinating the stages to perform an internal audit or third-party attestation engagement.
- Software development or scripting coursework or experience.
- One or more years of work experience (including internship/coop) as a network/system engineer, security analyst, penetration tester, forensics specialist, software developer, or similar.
- Strong communication and organizational skills, including writing and public speaking.
- Strong, demonstrable knowledge in the domains of access control; application security; business continuity and disaster recovery planning; information security and risk management; operations security; physical security; security architecture and design; and telecommunications and network security.
- General knowledge of the following is preferred: Windows, Linux, mobile OSes, firewalls, DNS, IDS/IPS, anti-virus, Internet Protocol (IP), VLAN, VPN, SIEM, APTs, LDAP/Active Directory, penetration testing, IT auditing, system administration, software development, encryption, ISO27001, NIST 800-53.
- Passion for information security and a strong desire to learn.

Key Competencies

- critical thinking and problem solving
- decision-making
- communication
- influencing and leading
- delegation
- teamwork
- conflict management
- adaptability
- stress tolerance
- organization and planning
- information gathering and monitoring
- initiative
- time management
- attention to detail, accuracy

When applying, please include a brief cover letter describing why you are a good fit for the role.

Job Type: Full-time