Our company is looking to fill the role of lead security architect. Thank you in advance for taking a look at the list of responsibilities and qualifications. We look forward to reviewing your resume.

Responsibilities for lead security architect

- Responsible for coordination and documentation of testing phases
- Create all necessary documentations for SAP/GRC and Security projects
- Working knowledge of IT-related laws and compliance mandates
- Proficient in researching information security solutions and best practices
- Proficient in researching control solutions and best practices
- Working knowledge of project management principles, and ability to coordinate delivery of high quality solutions on time and within budget
- Ability to work closely and efficiently with internal and external auditors and legal department
- Excellent interpersonal skills with the ability to work on cross-functional project teams and foster team commitment to tasks collaborate with the Business
- Partner with the security group to plan and drive the implementation of the technology and its capabilities
- Recommends updates and changes to the Secure Software Development Policy, Design for Security requirements, and related organization-wide product security governance documents

Qualifications for lead security architect

- At least 5 years in working with information security governance, compliance, or auditing
- Master's degree, or demonstrated experience and delivery, in information

- 7-10+ years of progressive applied technology experience in enterprise architecture functions, ideally focused on information security or data management, modelling & quality
- Demonstrable ability to structure and execute programs with clearly defined long term goals, interim steps, required stakeholders and justifications
- Demonstrated ability to communicate complex transformation plans to varying organizational levels, including C-level staff, and delivery technologists
- Active professional security certifications (e.g., CISSP or other similar industry qualification), open source project, security research (e.g CAPEC, CVE, CEF, etc) or design framework/patterns contribution, or other continuous learning examples in the threat & security spheres