Sr. Information Security Analyst, Governance, Risk, and Compliance

📍 Shoreland

Posted 14 Days Ago
Full time
JR10394

Department
BSD DIV - Center for Translational Data Science: Security

About the Department
The Center for Translational Data Science at the University of Chicago is a research center pioneering the discipline of translational data science to advance biology, medicine, and environmental research. We architect ecosystems of large-scale commons of research data, computing resources, applications, tools, and services for the broader research community to use data at scale to pursue scientific inquiry and accelerate discovery. These growing data commons offer petabytes of rich research data to scientists across the world.

Job Summary
The job uses best practices and knowledge of to develop and implement information security and identity management solutions. Guides teams to deploy new technologies and manage existing security infrastructure as well as respond to cyber security incidents. Anticipates risks to the organization and leads security penetration testing and security awareness outreach.

This at-will position is wholly or partially funded by contractual grant funding which is renewed under provisions set by the grantor of the contract. Employment will be contingent upon the contin-

About Us
The University of Chicago is an urban research university that has driven new ways of thinking since 1890. Our commitment to free and open inquiry draws inspired scholars to our global campuses, where ideas are born that challenge and change the world.

We empower individuals to challenge conventional thinking in pursuit of original ideas. Students in the College develop critical, analytic, and writing skills in our rigorous, interdisciplinary core curriculum. Through graduate programs, students test their ideas with UChicago scholars, and become the next generation of leaders in
ued receipt of these grant funds and satisfactory job performance.

Responsibilities

- Development of diverse and impactful risk metrics.
- Monitor and manage compliance of implemented enterprise information security controls.
- Lead and conduct risk analysis, assessments, and security audits using internal solutions and third-party vendor partners.
- Identify, implement, monitor, and lead enforcement of information security compliance, regulatory, and control frameworks.
- Provide Information Security consulting and security awareness education.
- Improve, monitor, and coordinate Third Party Vendor Risk Management activities.
- Conduct research on information security best practices, solutions, strategies.
- Develop, maintain, and lead enforcement of strong information security policy, procedures, standards, and position papers.
- Develop, maintain, and lead enforcement of strong security governance of all Information Security strategy and operational process.
- Plan and review annually the risks influencing the effectiveness of information security, privacy, and Information security risk management.
- Represent Information Security and foster positive collaboration amongst CTDS peers, University departments, agency sponsors, and organizational partners.
- Uses a deep understanding of IT expertise to develop and implement security and compliance policies, guidelines, and safe practices for university-wide computing and networking systems.
- Leads teams to conduct in-depth information technology risk assessments; makes recommendations and designs improvements to IT security procedures.
- Guides communications with users to understand their security needs and supports the implementation of procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security.
- Performs other related work as needed.

Minimum Qualifications

Education:
**Education:**
Minimum requirements include a college or university degree in related field.
---

**Work Experience:**
Minimum requirements include knowledge and skills developed through 5-7 years of work experience in a related job discipline.
---

**Certifications:**
---

**Preferred Qualifications**

**Experience:**
- 5-7 years business/technical/information security/risk compliance experience.
- Experience in information security risk analysis, auditing, compliance, policies, and overall governance and communication.
- Demonstrated success implementing and Information Security control frameworks and standards such as ITIL, CIS Top 20, Soc2, GDPR, NIST CSF / 800-53, FISMA, and FedRAMP.
- Strong knowledge of audit and risk management methodologies, such as COBIT, NIST 800-37/800-30, FAIR.
- Experience with GRC, IAM, and risk management tools and solutions.
- Experience with information security tools and solutions.

**Certifications:**
- CISA, CRISC, GIAC, CISM, or CISSP certifications.

**Preferred Competencies**
- Knowledge of hybrid IT systems, networking, and cloud environments (AWS, Google, etc.).
- Ability to respond to changing priorities and operate effectively in a dynamic demand-based environment, requiring extreme flexibility and responsiveness.
- Ability to weigh Center, partner, and agency needs against security and risk tolerance.
- Ability to conceptualize a course of action and to organize for the successful completion of that action are critical, often under tight deadlines.
- Ability to present information in a consistent and concise manner.
cise manner.

- Strong written and verbal communication skills and ability to foster collaborative working relationships.

**Working Conditions**

- Office environment.

**Application Documents**

- Resume (required)
- Cover Letter (preferred)

When applying, the document(s) **MUST** be uploaded via the My Experience page, in the section titled Resume/CV of the application.

**Job Family**

Information Technology

**Role Impact**

Individual Contributor

**FLSA Status**

Exempt

**Pay Frequency**

Monthly

**Scheduled Weekly Hours**

40

**Benefits Eligible**

Yes

**Drug Test Required**

No

**Health Screen Required**

No
Motor Vehicle Record Inquiry Required

No

Posting Statement

The University of Chicago is an Affirmative Action/Equal Opportunity/Disabled/Veterans Employer and does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender identity, national or ethnic origin, age, status as an individual with a disability, protected veteran status, genetic information, or other protected classes under the law. For additional information please see the University’s Notice of Nondiscrimination.

Staff Job seekers in need of a reasonable accommodation to complete the application process should call 773-702-5800 or submit a request via Applicant Inquiry Form.

We seek a diverse pool of applicants who wish to join an academic community that places the highest value on rigorous inquiry and encourages a diversity of perspectives, experiences, groups of individuals, and ideas to inform and stimulate intellectual challenge, engagement, and exchange.

All offers of employment are contingent upon a background check that includes a review of conviction history. A conviction does not automatically preclude University employment. Rather, the University considers conviction information on a case-by-case basis and assesses the nature of the offense, the circumstances surrounding it, the proximity in time of the conviction, and its relevance to the position.

The University of Chicago’s Annual Security & Fire Safety Report (Report) provides information about University offices and programs that provide safety support, crime and fire statistics, emergency response and communications plans, and other policies and information. The Report can be accessed online at: http://securityreport.uchicago.edu. Paper copies of the Report are available, upon request, from the University of Chicago Police Department, 850 E. 61st Street, Chicago, IL 60637.

Apply