Cybersecurity Governance, Risk and Compliance Analyst
Austin Community College

Job Title	Cybersecurity Governance, Risk and Compliance Analyst
Department	IT
Institution	Austin Community College Austin, Texas
Date Posted	Dec. 6, 2024
Application Deadline	Open until filled
Position Start Date	Available immediately
Job Categories	Professional Staff
Academic Field(s)	Administration - Other
Apply Online Here	https://apptrkr.com/5849345
Apply By Email	
Job Description	

Cybersecurity Governance, Risk and Compliance Analyst

Austin Community College

Job Posting Closing Times: Job postings are removed from advertising at **12:00 A.M.** on the closing date e.g., at midnight on the day before the closing date.

If you are a current Austin Community College employee, please click this link to apply through your Workday account.

Austin Community College is a public two-year institution that serves a multicultural population of approximately 41,000 credit students each Fall and Spring semester. We embrace our identity as a community college, as reflected in our mission statement. We promote student success and community development by providing affordable access, through traditional and distance learning modes, to higher education and workforce training, including appropriate applied baccalaureate degrees, in our service area.

As a community college committed to our mission, we seek to recruit and retain a workforce that:

- Values intellectual curiosity and innovative teaching
- Is attracted by the college's mission to promote equitable access to educational opportunities
- Cares about student success and collaborates on strategies to facilitate success for populations including; first generation college students, low-income students, and students from underserved communities.
- Focused on student academic achievement and postgraduate outcomes
- Welcomes difference and models respectful interaction with others
- Engages with the community both within and outside of ACC

Job Posting Title:
Cybersecurity Governance, Risk and Compliance Analyst

Job Description Summary:
Under the supervision of the Cybersecurity Governance, Risk, and Compliance Manager, the GRC Analyst assumes a pivotal position within the GRC team, ensuring our organization adheres to regulatory frameworks, effectively manages risks, and upholds exemplary governance standards. The GRC Analyst serves as a vital resource for staff and leadership, offering expertise in information security policy development, implementation, interpretation, and compliance. Additionally, they play a crucial role in fostering a security-first culture throughout the organization by spearheading comprehensive training and awareness programs.

Job Description:

Description of Duties and Tasks

Essential duties and responsibilities include the following. Other duties may be assigned.

Cybersecurity Governance, Risk and Compliance Analyst
Austin Community College

The GRC Analyst will be responsible for the following functions:.

- Assists with the development of System Security Plans, Continuous Monitoring, Plan of Action and Milestones, Security Controls Assessment, Risk Exposure analysis, all in accordance with TCF/NIST requirements
- Researches, recommends, and contributes to information security policies, standards, and procedure development. Assists with the lifecycle management of information security policies and supporting documents.
- Manages an exception review and approval process, and assures exceptions are documented and periodically reviewed
- Updates security controls and provides support to all stakeholders on information security controls covering internal assessments, regulations, and protecting FERPA and Personally Identifying Information (PII).
- Assists and performs IT security control effectiveness reviews. Manage remediation efforts for the identified gaps including assessment of new or enhanced implemented controls.
- Collaborates with internal teams to conduct regular assessments of information security policies, procedures, and controls to ensure compliance with relevant regulations and standards
- Prepare detailed reports on assessment findings, monitor status updates, and ensure that corrective actions are implemented effectively and sustainability.
- Creates information security and cyber awareness communications and training content for all employees.
- Supports the development and upkeep of a measured and managed Security and Privacy training program tailored to roles, with oversight of phishing campaigns.
- Keeps abreast of security industry trends, emerging threats, pertinent regulatory compliance requirements, and best practices in security.
- Participates in cross-functional projects related to risk management, data protection, and security governance.
- Conducts third-party supplier risk assessments to oversee supply chain risk across the supplier's lifecycle. Evaluates and communicates business risks and benefits, and enforces supplier compliance mandates.

Cybersecurity Governance, Risk and Compliance Analyst
Austin Community College

Knowledge

Must possess required knowledge and be able to explain and demonstrate, with or without reasonable accommodations, that the essential functions of the job can be performed.

- Working knowledge of various Security Frameworks , primarily NIST.
- Knowledge of information security management, governance, and compliance principles, practices, laws, rules and regulations.
- Knowledge of information technology systems and processes, network infrastructure and data architecture
- Knowledge of best practices in security training and awareness.

Skills and Experience

Must possess required skills and be able to explain and demonstrate, with or without reasonable accommodations, that the essential functions of the job can be performed.

- Skills and or/experience in developing/delivering security awareness training either directly or through managed third party providers/tools.
- Skills in business process mapping and documentation as well as policy and procedure development.
- Recent experience in Information Security with up-to-date knowledge of the current threat landscape.
- Analytical, conceptual thinking and strategic planning skills.
- Proactive self-starter with the talent to think through technical solutions to potentially open-ended problems.
- Maintaining an established work schedule.
- Effectively using interpersonal and communications skills.
- Effectively using organizational and planning skills with attention to detail and follow-through.
- Maintaining confidentiality of work-related information and materials.
- Establishing and maintaining effective working relationships, including the ability to coordinate the work of others.
- Strong oral and written communication skills and the ability to work well with people from many

different disciplines with varying degrees of technical expertise.
- Ability to prioritize assignments while working on multiple projects.

Required Work Experience

- One year of experience working in the technology industry.

Preferred Work Experience

- Work experience specifically in cybersecurity governance, risk and compliance or related roles.
- Work experience in a Texas government or government-adjacent organization
- Work experience in an institution that is FERPA regulated.
- Working knowledge of the concepts of data privacy regulations, including FERPA requirements or similar regulated data classifications.

Required Education

- Bachelor's degree in computer science, Information Technology, or related field
- 4 Years of relevant work experience may be substituted for the degree requirement

Licenses/Certifications; Other

- Valid Texas Driver's License and reliable transportation for travel in the Austin area as required.

Other Preferred Qualifications

- ITIL Foundation-level certification or above preferred but not required.
- Relevant certifications such as CISSP, CISA, CRISC are preferred but not required.

Physical Requirements

- Work is performed in a standard office or similar environment.
- Subject to standing, walking, sitting, bending, reaching, pushing, and pulling.
- Occasional lifting of objects up to 10 pounds.

Safety

- Work safely and follow safety rules. Report unsafe working conditions and behavior. Take reasonable and prudent actions to prevent others from engaging in unsafe practices.

Salary Range

$75,560 - $94,449

Number of Openings:
2

Job Posting Close Date:
December 19, 2024

Clery Act

As required by the US Department of Education, employees are required to report violations under Title IX and, under the Jeanne Clery Disclosure of Campus Security Policy and Crime Statistics Act (Clery Act), select individuals are required to report crimes. If this position is identified as a Campus Security Authority (Clery Act), you will be notified, trained, and provided resources for reporting.

Disclaimer

The above description is an overview of the job. It is not intended to be an all-inclusive list of duties and responsibilities of the job, nor is it an all-inclusive list of the skills and abilities required to do the job. Duties and responsibilities may change with business needs. ACC reserves the right to add, change, amend, or delete portions of this job description at any time, with or without notice. Employees may be required to perform other duties as requested, directed, or assigned. In addition, reasonable

accommodations may be made by ACC at its discretion to enable individuals with disabilities to perform essential functions of the job.

To apply, please visit: https://austincc.wd1.myworkdayjobs.com/en-US/External/job/Highland-Campus/Cybersecurity-Governance--Risk-and-Compliance-Analyst_R-6396-1

Contact Information

Please reference Academickeys in your cover letter when applying for or inquiring about this job announcement.

Contact

IT
Austin Community College

,