STATE OF NORTH CAROLINA
invites applications for the position of:

Senior Risk Management Officer

JOB CLASS TITLE: Senior Risk Management Officer

POSITION NUMBER: 65026329

DEPARTMENT: Administrative Office of the Courts

DIVISION/SECTION: Technology Services Division

SALARY RANGE: $83,199.00 - $144,473.00 Annually

RECRUITMENT RANGE: $83,199.00 - $144,473.00

SALARY GRADE / SALARY GRADE EQUIVALENT: 29

COMPETENCY LEVEL: Not Applicable

APPOINTMENT TYPE: Permanent Full-Time

WORK LOCATION: Wake County

OPENING DATE: 03/21/19

CLOSING DATE: 04/21/19 5:00 PM Eastern Time

DESCRIPTION OF WORK:

RECRUITMENT RANGE: $83,199.00 - $144,473.00
SALARY GRADE: 29

Reporting to the Chief Technology Officer (CTO) and working collaboratively with the Chief Information Security Officer, the TSD executive management team, and AOC business managers, the Senior Risk Management Officer (SRMO) is responsible for managing the risk associated with the North Carolina Administrative Office of the Courts (NCAOC), Technology Services Division technology transition to cloud technologies as well as the continuous development of a cloud risk management framework, processes, and related documentation. This role is responsible to evaluate and oversee the information technology risk within the organization and its cloud business partners, maintain an active view of risk factors, and report on the actual, mitigated and residual risk within the NCAOC technology environment as it transitions to cloud solutions. This position requires a strategic thinker with strong collaboration skills, detailed working knowledge of IT, and experience with cloud security/vendor risk management best practices, as well as experience in transitioning large scale enterprise-wide technology environments to a cloud hosted architecture.

The Senior Risk Management Officer must be highly knowledgeable about the business environment given this position will support the North Carolina Judicial Branch / statewide unified court system and its various custom-built and off-the-shelf products that support 7,000 employees statewide, as well as other critical government entities outside of the Judicial Branch, such as law enforcement, Department of Transportation network interfaces to ensure that risks to both on-site legacy and cloud hosted information assets are pro-actively managed as well as managed cost effectively. All risk compliance closure activities are coordinated through this role, including the control and actual submissions for risk closure. This position will be directly responsible to oversee and report on the risk exposure of the NCAOC as it transitions to cloud applications and hosting infrastructure as well as manage the ongoing risk of the current technology environment throughout the transition to cloud services.

KNOWLEDGE, SKILLS AND ABILITIES / COMPETENCIES:

Knowledge of: experience within a SRMO role with at least 7 years in risk areas relevant for Information Technology Risk Management preferably within a government sector cloud management role; cloud vendor management SLA compliance, IRM, BCM, Change Control and IT processes; IT risk, security architecture, network security, cloud/mobile security, data security infrastructure; standards and frameworks (e.g.: ISO 27001, NIST-800, COBIT, FFIEC, ITIL); and technology best practices.

Skills in: providing expert-level technical leadership across a broad range of risk and compliance work efforts; serving as risk/compliance lead on functional teams or projects and serving as a best practice/quality resource to mitigate IT risk; leading highly complex risk and compliance reviews, evaluations, and root cause analyses; leading and mitigating risk with App/Infrastructure transitions to SaaS/IaaS services; very strong verbal and non-verbal communication skills; aptitude for IT Security and strong understanding of applied security concepts and best practices; acting with integrity; taking pride in work; seeking to excel; and adaptability

Ability to: develop risk management processes and workflows and then train and coach users of those workflows; identify and assess the severity and potential impact of risks and communicate risk assessment findings to risk owners in a way that consistently drives objective, fact-based decisions about risk that optimize the trade-off between risk mitigation and business performance; apply IT risk findings and frameworks to court systems in a practical and effective manner; communicate IT risk matters to all levels of employees within the judicial system; be successful in a highly dispersed and decentralized operating environment; work cooperatively across the organization; and make IT risk management related recommendations based on data, facts, and analysis.

MINIMUM EDUCATION AND EXPERIENCE REQUIREMENTS:

Bachelor's degree in computer science or a related information technology field and seven (7) years of related work experience in IT Risk and Compliance management; or an equivalent combination of education and experience. Certification preferred (e.g. CISSP, CRISC, CISA, CISM).

Management preferences:

- Self-motivated and able to effectively manage multiple concurrent priority deliverables requiring tight deadlines.
- An enthusiasm for risk management and a desire for continued learning are essential.
- Demonstrated project management experience managing key deliverables.
- Experience with managing an enterprise change management process / implementation of ITIL processes Change and Configuration Management.
- Past onsite app/infrastructure transition to cloud IaaS/SaaS risk management experience.
- Experience with implementation of an enterprise Risk Management framework (e.g. Actual implementation of a governance and risk compliance tool set).
- Business continuity and disaster recovery experience within AZURE/AWS technology and architecture.
- Thorough understanding of Microsoft O365 technology and licensing to allow for guidance and recommendations related to email/cloud storage within transition to cloud technologies.
- Service Level Agreement and vendor management experience with cloud hosting solutions (e.g. IaaS, SaaS, PaaS, MDM, DaaS).
- Information Security experience within a government sector, with an emphasis on Microsoft Identity and Access technologies and architecture.
- Demonstrated understanding and application of information security principles, accreditations, and best practices (e.g. ISO-2701).
- Demonstrated experience integrating a Risk Framework for compliance within a security program policies/standards/procedures and auditing requirements.
- Hold one or more respected industry qualifications (e.g. CISSP / RMP / CRMP / CRMA / RIMS / ITIL).
- Sound written and verbal communications skills (formal training desirable).

Attach cover letter, résumé, and writing sample.

Out of state applicants are encouraged to apply; however, NCAOC does not reimburse travel or relocation expenses.

SUPPLEMENTAL AND CONTACT INFORMATION:

The Technology Services Division of the NC Administrative Office of the Courts is an award winning team! Check out our recent accolades:

Center for Digital Government - Digital Government Achievement Awards
2012 State Level - Government to Government
2008 State Level - Government to Citizen
2003 State Level - Best of the Web (BOW)

Government Computer News Award
2014 IT Excellence - Public Sector Projects

National Association of State Chief Information Officers
2012 State Level - Government to Business

2007 State Level - Government to Government

Meet the TSD Team of the NC Administrative Office of the Courts.

Our facility is close to I-40 and convenient to all the **Research Triangle** area has to offer.

Campus Amenities
17.5 Acre Campus
180,000 SF Building
Ample Free Parking
Full Service Cafeteria
Patio Dining

Health & Wellness Benefits
Modern Fitness Center
Yoga & Pilates Classes
Walking Trail
CPR Training
Annual Flu Shot Clinic for Employees and Families
Wellness Fair
Agency Softball Team
Lunch & Learn Programs

Employment Benefits
Generous Insurance Options
Retirement Package (purchase option for other government plans)
Flexible Benefits Package
401(k)
Vacation & Sick Leave
Longevity Program
Service Awards

Come join a great team! Learn more about the NC Administrative Office of the Courts here: http://www.nccourts.org/Careers

INSTRUCTIONS:

Applicants must complete an application through NeoGov, the North Carolina state government job application program. Go to http://www.oshr.nc.gov/jobs/ to apply for this position. Mailed or faxed applications will not be accepted.

Before applying, please read the Online Employment Application Guide for instructions on creating your profile and applying for specific postings.

It is important your application includes all of your relevant education and work experience and that you answer all questions associated with the application to receive proper credit. Résumés are not accepted in lieu of fully completed applications.

NOTE Many job postings require certain documents be attached to an application. Verify your application is complete and uploaded documents are attached to your application *before* submitting it. Applications may not be altered after they have been submitted.

Carefully review the FAQs if you experience difficulty with the application process or attaching documents. For technical issues with applications or attachments, call the NeoGov Help Line at 855-524-5627.

All NC Judicial Branch agencies are Equal Opportunity Employers.

The North Carolina Judicial Branch participates in E-Verify, an internet-based system that compares information from an employee's Form I-9, Employment Eligibility Verification, to data from the US Department of Homeland Security and Social Security Administration records to confirm employment eligibility. To learn more, click on these links:

E-Verify Participation
E-Verify Participation (Spanish)

Right to Work
Right to Work (Spanish)

Travis Davis
NC Administrative Office of the Courts
Human Resources Division
https://www.nccourts.gov/about/about-judicial-branch/careers