Job Description

Job Title Application Security Specialist Level 3
Job ID 97945
Location Manhattan - Downtown

Return to Previous Page Switch to Internal View

Job Information

Job Title: Application Security Specialist Level 3

Salary Range: Min. $71,729 Mid. $95,639

POINTS: 393

Dept/Div: MTA Information Technology/Office of IT Security

Supervisor: Dir Off IT Security Identity

Location: 2 Broadway, New York, NY 10004

Hours of Work: 9:00 AM - 5:30 PM (7.5 hours/day) or as required

Summary

The position will be responsible for: risk assessment (identifying problems), vulnerability assessment (determining system and application weaknesses) and defense planning (implementing appropriate countermeasures). Responsibilities will include leading Application Security risk assessments and assisting the Identity and Access Management team in effectively maintaining an efficient Mainframe Security Operation at the MTA; analyzing technical and procedural controls for potential findings; assessing the likelihood, severity and potential business impact of findings; working with stakeholders to design, author and commit to risk mitigation actions; and tracking the status of these committed actions. Strong knowledge of Mainframe RACF activities related user requests / issues and violations to assess application and system vulnerabilities.

Additionally, this position must keep fully up to date on evolving Federal, FRA, and NYS Cyber Security, PCI industry standards, techniques and requirements for an ongoing risk/compliance assessment to secure MTA confidential, private intellectual assets from unauthorized access.

This position is required to be “on call” in the 24-hour, 365-day operating environment to ensure the availability and delivery of technology services in support of MTA corporate business goals and objectives.

Responsibilities

- Daily support for any Mainframe / RACF security and account administration issues
- Analyze all the Mainframe risk-related activities of MTA’s IT organization, planning, testing, reporting and recommending appropriate remediation measures.
- Assist in Application Security vulnerability analysis of existing and new Mainframe / RACF applications.
- Recommend corrective actions to fix the application security related problems such as user access / management in the Mainframe / RACF applications.
- Assist with the monitoring of risk mitigation and coordination of policy and controls with the compliance manager, director and the chief information security officer (CISO), to ensure that other managers and IT staff are taking effective remediation steps.
- Create, disseminate and (as required) update documentation of MTA’s matrix of identified IT risks and controls.
- Work directly with the Identity and Access Management Team and other internal departments and organizations to facilitate RACF Mainframe IT risk analysis and risk management processes, identify acceptable levels of residual risk, and establish roles and responsibilities related to information classification and protection within IDM SailPoint, Azure and Active Directory.
- Assist to design and conduct new risk assessments for the MTA and Agencies to ensure MTA IT assets are risk averse and mitigated when required.
- Assist with the technical risk assessments, PCI/DSS such as vulnerability scanning, application risk assessment, network design review, penetration testing while assisting with third-party assessment.
- Work in a team environment interacting with PCI QSA, business units and other security professionals to confirm findings, resolve misunderstandings resulting from the PCI risk assessment review analyze the QA test process and help develop procedural strategies for reviewing reports and services.
- Review risk assessments, analyze the effectiveness of MTA’s IT internal control activities within Mainframe / RACF and report on them — with actionable recommendations — to the Risk and Compliance officer, CISO and IT director and managers.

Qualifications

- Good leadership skills.
- Good troubleshooting and problem solving skills.
- Strong technical and analytical abilities.
- Strong oral and written communication skills
- Well-organized and highly motivated.
- Must be able to move and lift up to 25 lbs. of equipment such as monitors, keyboards, CPU's, laptops, firewalls, etc.
- Must possess a valid driver's license.

Education and Experience

- A Bachelor's degree in Computer Science, Business Administration, Engineering, Finance, and Information Services (or the equivalent of education and progressive responsible experience) plus a minimum of 3 - 4 year of Information Technology experience with minimum of 2 years of risk and compliance related experience.
- Knowledge and experience of a broad range of policy, standards and common risk management methodologies – for example, COSO, ISO 27001, PCI/DSS, COBIT, ITIL, ISO 2000, etc.
- Experience administering zSecure, zSecure Audit, zSecure Alert and working with z/OS Security and Administration of RACF.
- Experience with Identity and Access Management as well as Active Directory is preferred.
- CISSP certification preferred.

Other Information

As an employee of MTA Headquarters you may be required to complete an annual financial disclosure statement with the State of New York, if your position earns more than $101,379 (this figure is subject to change) per year or if the position is designated as a policy maker

How To Apply

Qualified applicants can submit an online application by clicking on the 'APPLY NOW' button from either the CAREERS page or from the JOB DESCRIPTION page.

If you have previously applied on line for other positions, enter your User Name and Password. If it is your first registration, click on the CLICK HERE TO REGISTER hyperlink and enter a User Name and Password; then click on the REGISTER button.

Equal Employment Opportunity

MTA is an Equal Opportunity Employer.

Return to Previous Page Switch to Internal View