Lead IT Auditor - Office of the Inspector General (ID: 22906)

Description –
Under the Office of the Inspector General's (OIG's) team approach to auditing, the information technology (IT) auditor participates on and leads IT audits, attestations, inspections, and evaluations (hereafter referred to as reviews) of the mainframe and distributed computer processing environments of the Board of Governors of the Federal Reserve System (Board) and the Bureau of Consumer Financial Protection (Bureau). These reviews are designed to evaluate the effectiveness of information security controls; assess and promote economy, efficiency, and effectiveness; and help prevent and detect fraud, waste, and abuse in the Board and Bureau programs and activities.

Also leads follow-up reviews of previous OIG reviews to determine whether recommended actions were implemented and participates in the Systems Development Life Cycle of major systems under development to identify internal controls, efficiency, effectiveness, and project management issues. May participate on non-IT reviews of Board and Bureau programs and operations and OIG investigations. Audit and attestation work is conducted in accordance with generally accepted government auditing standards (GAGAS); inspection and evaluation work is conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) Quality Standards for Inspection and Evaluation. May also assist in the development of the OIG's annual and strategic plans.

Qualifications –
Bachelor's degree from an accredited college or university in IT, accounting, finance, economics, business, or related field, or equivalent experience, plus at least five years of progressive specialized experience in the reviewing of IT programs/systems, obtained in an OIG or similar position. At the FR-27 grade, at least seven years of progressive specialized experience that demonstrates managerial or leadership skills. Additional professional experience in a financial, managerial, or consulting position is preferred. Knowledge of principles, theories, practices, and techniques of information systems management, computer science, management, and auditing/inspecting/evaluating to independently plan and conduct reviews of the Board's or the Bureau's operational programs and activities. Knowledge of information technology and its application to Board and Bureau programs and operations and reviewing such programs and operations. Knowledge and skill to evaluate compliance with applicable laws and regulations, the adequacy of internal controls, and the operational efficiency and effectiveness of systems and activities. Strong knowledge/understanding of automated data processing procedures and controls. Ability to assist in non-IT reviews. High degree of proficiency in oral and written communication skills. Excellent interpersonal skills and ability to work well in a team environment. At the FR-27 grade, ability to integrate complex analysis of policies, programs, and operations. Ability to develop new approaches for the study and evaluation of programs.
Ability to obtain a Secret, or at the FR-27 grade Top Secret, clearance, and is subject to the Board's drug testing program. Prefer certification in one or more of the following: Certified Public Accountant, Certified Internal Auditor, Certified Fraud Examiner, Certified Information Systems Auditor, and/or Certified Information System Security Professional.
What We Do
FISMA
IT Audit FAQs

REMARKS

- Prior experience conducting IT and cybersecurity-related audits within a federal IT environment is strongly preferred.
- Prior experience conducting FISMA and security control reviews is strongly preferred.

- Knowledge of federal IT initiatives, including zero trust architecture, cloud computing, supply chain risk management, and SDLC is preferred.
- Knowledge of data analytics and other tools to test IT controls is a plus.
- Past performance evaluations may be requested
- Full vaccination for COVID-19 is required as a condition of employment, unless a legally required exception applies.
- When the OIG resumes an in-office presence, its interim telework policy will require employees to be physically present in the office a minimum of 4 days per month. Employees may be expected to be physically present in the office more than 4 days per month, as required by business needs. The OIG will revisit its interim policy after a year to determine whether any changes will be made.