Our company is growing rapidly and is searching for experienced candidates for the position of risk mgr. If you are looking for an exciting place to work, please take a look at the list of qualifications below.

Responsibilities for risk mgr

- Utilize the IT Risk Model portion of the Service Maturity Model (SMM) framework to identify, assess and evaluate risk for all IT Services
- Provide an independent point of view on risk exposure and risk taking, including support, advice, counsel and challenge to business partners and senior business leaders, on overall risk management related to the achievement of the IIES mission, goals and strategy
- Leverage ERM standards, processes, tools and approaches to guide the business in the identification, measurement, monitoring and management of risk, including emerging risks
- Help establish Risk Appetite and provide guidance on risk treatment and oversight of mitigation
- Conduct detailed risk analysis on proposed and existing Institutional investment and income products and services being offered by IFS, as required
- Review overall asset allocation policy and approaches, as appropriate
- Help oversee, from the IFS perspective, the risks and investment approaches related to the General Account – both assets and liabilities – which is a key component of many of the insurance products provided by IFS
- Assume a leading role on specified risk and business committees, including representing risk on all IFS Product and Service governance processes related to IIES products and services
- Provide guidance and assistance to ensure that local IIES policies and procedures are in line with corporate guidelines

Continuity and provide effective challenge to the work done to be compliant with them

Qualifications for risk mgr

- Compiled/interpreted programs and the types of security issues possible in each
- Debuggers and disassemblers
- Source code reviews (at least c/c++ and java) for security vulnerabilities
- Reverse engineering binaries (at least x86) for security vulnerabilities
- Bachelor Degree minimum, with 7 years of Cyber Security Risk Analysis experience
- Experience with programming languages, such as VBA and/or SAS