Downloaded from <https://www.velvetjobs.com/job-descriptions/cyber-info-assurance-analyst>

# Example of Cyber Info Assurance Analyst Job Description

Our innovative and growing company is searching for experienced candidates for the position of cyber info assurance analyst. Please review the list of responsibilities and qualifications. While this is our ideal list, we will consider candidates that do not necessarily have all of the qualifications, but have sufficient experience and talent.

## Responsibilities for cyber info assurance analyst

* Supporting the assessment team on proper methods to determine risk levels for security controls
* Characterizing aggregate levels of risk to include recommendations to fix, mitigate, or accept risk and documenting results
* Providing support on security guidance control requirements, assessment, and risk analysis techniques, and assist in the development of the agency and system’s continuous monitoring program
* Establish strict program control processes to ensure mitigation of risks and support obtaining certification and accreditation of systems
* Supporting process, analysis, coordination, security certification test, security documentation, investigations, software research, hardware introduction and release, emerging technology research inspections and periodic audits
* Control, prepare, and brief vulnerability scan reporting and compliance reports to Government and Tier 2 CSSP
* Understand Host Based Security System and the requirements that drive compliance with DISA direction
* Perform assessments utilizing Defense Information Systems Agency (DISA) approved tools• Fulfill Network Security Monitoring/Intrusion Detection functions
* Compile information by coordinating with service providers
* Keep mission partners abreast of security note requirements by researching publications and relaying guidance

## Qualifications for cyber info assurance analyst

* 9 years in IA related work
* 5+years in Computer/IT related work
* Proven ability to manage and maintain System Security Plans (SSPs) from inception through decommissioning following the NSA Risk Management Framework process within Xacta for national level mission systems
* Coordinate with program management and other stakeholders to track and maintain risks associated with multiple mission Information Systems to ensure compliance with all IA requirements and national level directives
* Knowledge in Multi-level Security/Cross Domain systems and operations with special requirements such as Program Protection, Anti-Tamper, Red/Black Separation and OPSEC are assets
* Experience with analysis, disposition, and evaluation of both hardware and software in support of Intelligence Community (IC), Department of Defense, in addition to Federal Sector Government Agencies