* Develop, publish and monitor Information Security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements
* Knowledge of national and international regulatory compliances and frameworks such as COBIT,NIST,PCI, ISO, etc
* Strong understanding of cyber security controls and frameworks (COBIT, COSO, ISACA, ISO2700x, NIST, SANS, etc.)
* Knowledge of regulative controls related to security (SOX & PCI)
* Develop and manage the Information Security Risk Acceptance program
* Assist with the reports to senior management, Audit Committee and Board of Directors
* Providing support for Internal IT audits
* Monitor and advise on information security issues related to internal systems and workflow to ensure that security controls for the company are appropriate and operating as intended
* Advanced knowledge of various security technologies, frameworks and products
* Develop Information Security Policies, Standards and Guidelines
* Establishes goals and objectives for team performance and manages attainment of those goals
* Work closely with IT department on corporate technology development to fully secure information, computer, network, and processing systems
* Proficient in both Manual and Automated Testing.
* Developed
* Creation of QA Strategy, QA Planning, Monitoring and mentoring the team, Preparation of High Level Test Scenarios, Test Cases and Test Scripts
* Expert in writing test cases using the test scenarios and preparing test data.
* Worked extensively for preparing traceability matrix, to ensure that all the requirements are mapped with test cases, and updated it regularly.
* Performed Sanity testing, Functional and System testing.
* Experience in preparing test strategy for development project.
* Expertise in GUI Testing, functionality testing, Integration Testing, Black box techniques, Regression Testing, Security testing, User Acceptance testing (UAT), Smoke testing and System testing.
* Experience in performing Backend Testing (Oracle and SQL Server databases and XMLs).
* Extensively involved in Defect Reporting and Defect Tracking process using Team Track, Test Director, Quality Center (QC) and MS-Excel.
* Well versed in documenting test results and creating test reports.
* Experience in creating user acceptance test cases and supporting User Acceptance Testing (UAT).
* Work across multiple cross-functional teams to execute full system, interface, and end-to-end testing.
* Coordinated testing efforts and effectively managed Off-Shore teams.
* Worked closely with the Development Team to ensure that test requirements are clearly defined, functionality related issues are addressed  and end users are satisfied
* Involved in peer review and re-work.
* Clear understanding of Quality assurance role in all phases of Software Development Life Cycle (SDLC).
* Performed Sanity testing, Functional and System testing.
* Tracked down the blocking issues and reported them through
* Extensive experience in analyzing business requirements, ensuring that the requirements are correct and complete and using the same in preparing use cases.
* Expertise in preparing test scenarios from use case documents.
* Good team leader skills and ability to train, develop and coach staff
* Strong analytical skills to evaluate risks and control processes
* Excellent communication skills both verbal and written and ability to deal with people at all levels in a global matrix organization
* Flexible, pro-active and innovative
* A certificate from an Information Security Professional Consortium such as ISC², ISACA is an advantage

**Dallas, TX**

**MOORE GROUP**

* Reporting security performance against established security metrics
* Knowledge of national and international regulatory compliances and frameworks such as NIST,PCI, ISO, etc
* Develop Information Security Policies, Standards and Guidelines
* Collaborate with Business Information Security Managers to deliver end to end deep-dive risk assessments for business initiatives. The assessment should focus on critical layers of the product/solution and define the associated risks, business and technical impacts, remediation and residual risk
* Provide technical direction to analysts, associates and contractors
* Assist in the investigations of high level, complex violations of Information Security Policies
* Identify project risks and work effectively to mitigate them

**Detroit, MI**

**AUFDERHAR AND SONS**

present

* Contribute to the definition, development, and oversight of a global network and endpoint security threat management strategy and framework
* Provide education and assistance to application developers for applying security software development life cycle
* Working knowledge of industry security frameworks such as ISO 27001, HIPAA, NIST Cyber Security Framework
* Performing regular review of activities performed by the Access Control Group administrators
* Strong track record in a consulting, relationship management, key account management, sales or marketing role
* Security tool development: researching, planning, and implementing new tool features to make security tools more effective and add value; and
* Proactively identify technical and architectural risks, commenting and/or providing alternatives for improvement