Statement of Work:

Fred Cohen & Associates (FCA) will create a set of control standards derived from a previously written ISO17799:2005 based Policy for [CLIENT]. This will consist of the following items:

1. FCA personnel will take each element of the policy previously developed for CLIENT and create from it a control standard based on the CISO ToolKit series of books. There will typically be several control standards for each policy element, however, this effort will only provide the control standards associated with the information protection aspects of the effort. CLIENT will be responsible for writing applicable control standards for the remainder of the enterprise associated with the aforementioned policies. This will produce as a series of deliverables including one or more control standard for each ISO17799:2005 policy, at the rate of about one control standard per two weeks for a period of about 6 months. If minor revisions are desired, they will be provided over a period of 7 days from the delivery of each control standard at no added cost. Policy elements covered will include:
    - Risk assessment and treatment
        - Assessing security risks
        - Treating security risks
    - Security policy
        - Information security policy document
        - Review and evaluation
    - Organizational security
        - Internal organization
        - External parties
        - Asset management
        - Responsibility for assets
        - Information classification
    - Human resources security
        - Prior to employment
        - During employment
        - Termination and change of employment
    - Physical and environmental security
        - Secure areas
        - Equipment security
    - Communications and operations management
        - Operational procedures and responsibilities
        - Third party service delivery management
        - System planning and acceptance
        - Protection against malicious and mobile code
        - Backup
        - Network security management
        - Media handling

        - Exchange of information
        - Electronic commerce services
        - Monitoring
    - Access Control
        - Business requirements for access control
        - User access management
        - User responsibilities
        - Network access control
        - Operating system access control
        - Application and information access control
        - Mobile computing and teleworking
    - Systems development and maintenance
        - Security requirements of information systems
        - Correct processing in applications
        - Cryptographic controls
        - Security of system files
        - Security in development and support processes
        - Technical vulnerability management
    - Information security incident management
        - Reporting information security events and weaknesses
        - Management of security incidents and improvements
    - Business continuity management
        - Information security aspects of BCM
    - Compliance
        - Compliance with legal requirements
        - Compliance with policies, standards, and technical compliance
        - Information security audit controls

Additional terms and conditions:

- **Single Point of Contact:** CLIENT will provide FCA with a single point of contact (SPOC) to coordinate all efforts associated with this task and that SPOC will be authorized and able to provide all necessary information.
- **Liability limitations:** CLIENT indemnifies FCA and holds FCA harmless for all costs and consequences, whether direct or indirect, arising out of this effort, in all jurisdictions, in all forms, and in all cases.
- **Best efforts:** FCA will undertake best efforts to perform its tasks using the most suitable available technologies in a manner consistent with current usage, methodologies, techniques, and knowledge, however, because of the ever changing nature of the security, technology, business, regulatory, and physical environment, FCA MAKES NO WARRANTY, EITHER EXPRESSED OR IMPLIED, AS TO THE RESULTS OF THESE EFFORTS.
- **Confidentiality:** All CLIENT information is held in strictest confidence by FCA
- **Ownership of results:** With the exception of the actual control standards provided to CLIENT by FCA, all materials used in the performance of an this effort are the intellectual property of FCA and will remain so.