Statement of Work:

Fred Cohen & Associates (FCA) will perform an ISO 27001 Scope and Boundary Identification, and Gap Analysis Study for [CLIENT]. This effort will consist of the following items:

Phase 1:

FCA personnel will visit CLIENT at an agreed location on dates to be determined by mutual agreement. During that visit, facilitated discussions designed to collect information about the structure and makeup of information protection at CLIENT will be undertaken and documentation will be gathered and generated to produce an overview of CLIENT scope, boundary, and status with regard to meeting the requirements of ISO 27001. This will include but not be limited to issues related to ISO27001 components:

- Process approach
- The ISMS follows the ISO standards
- Establishment of the ISMS
- Management Commitment
- Internal ISMS audit
- Management Review of the ISMS
- Continual Improvement
- Control Objectives and Controls
- ISMS-B (informative) OECD Principals

Phase 2:
FCA will create a "*ISO 27001 Scope, Boundaries, and Gap Analysis Report"* that will summarize the results of the discussions. This report will consist of:

- An executive summary
- A review of the discussions and meetings.
- Scope and Boundaries definitions for ISO-27001 at CLIENT.
- A review of the current state ISO-27001 compliance at CLIENT
- A gap analysis identifying gaps between current compliance levels and desired compliance levels to become certified.
- A review of how PG&E ISS-SRM would likely perform in an audit.

FCA will provide a draft report to CLIENT for review within 15 days of completion of the site visit. FCA will invoice CLIENT for this study at that time, and CLIENT will pay all fees due in a timely fashion based on that invoice date.

Phase 3:
CLIENT will respond within 15 days of receipt of the draft report with any suggested changes and additional information. After no more than 4 such exchanges of draft reports, FCA will provide a final report to CLIENT if and when requested.

Investment:

The total investment for this work will be a firm fixed price of $45,000 to be payed net 30 days of invoice, inclusive of all expenses and fees.

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 will be held in strictest confidence by FCA and all FCA techniques, processes, and activities will be held in strictest confidence by CLIENT.
- **Ownership of results:** With the exception of the report and draft reports provided to CLIENT by FCA, all materials used in the performance of this effort are the intellectual property of FCA and will remain so.
- **No risk management decisions:** FCA will not make any risk management decisions on behalf of CLIENT in the course of this effort. Any decision support provided by FCA in this matter is strictly by example and nothing indicated by FCA shall be in any way interpreted as a risk management decision made on behalf of CLIENT.