

Statement of Work:

Fred Cohen & Associates (FCA) will work with [CLIENT] to develop and get operational a risk management program. This will consist of the following items:

Phase 1:

1. FCA personnel will hold a 2-day on-site risk management workshop in which FCA will provide detailed information on risk management approaches, go through options for a risk management architecture for the enterprise and get enterprise decisions regarding these options, gather information on the current risk management program, and come to agreement on key business systems to be used to wring out the program as it rolls out.

2. FCA will create a *“Risk Management Workshop Report”* that will summarize the results of the workshop and the decisions made about risk management approaches. This report will consist of:

- An executive summary
- A review of all of the decisions made and their basis
- A review of the current state of risk management at the enterprise
- A plan for phase 2 including the key business systems to be examined

Optional Phase 2:

1. FCA will create a set of preliminary risk management documents, procedures, database elements, and checklists, and return them to CLIENT. These will be designed to meet the specific requirements identified in phase 1 and will be used to test the risk management approaches and train the risk assessment and decision teams in what their tasks.

- The documents, procedures, and checklists will be delivered in PDF format licensed for unlimited internal use by the CLIENT
- The database elements will be delivered as sets of CSV formatted spreadsheets that can be imported into database or spreadsheet programs as needed.

2. CLIENT will work with FCA to perform initial risk assessments for the key enterprise systems identified in Phase 1 and to make decisions about risk treatment for those systems. The documents, procedures, and checklists will be tested in this process and CLIENT will integrate the initial database into whatever execution environment it desires for internal use.

3. Over the period of five assessments and decision processes, these deliverables will be evaluated and adapted and final deliverables will be provided at the end of that process.

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 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.