



INFORMATION RISK MANAGEMENT ARCHITECTURE

Statement of Work:

SECURINESS, Fred Cohen & Associates (SFCA) will work with [CLIENT] to develop a 3-5 year future information risk management (IRM) architecture. This will consist of the following tasks:

Task 1: As-Is IRM Situation

SFCA will perform a series of telephonic and/or on-site interviews, meetings, and collect information provided by CLIENT to gather information on the current IRM program, business modeling for IRM, the definitions of duties to protect, and IRM practices in order to create an "As-Is IRM Situation" report. This includes:

- Within 10 business days of the completion of these interviews and meetings, SFCA will provide a draft copy "As-Is IRM" report on the current status and architecture of the IRM program. This report will be about 15 pages in length and consist of:

An executive summary

A review of the as-is state of IRM at the enterprise covering:

- Business drivers for IRM
- IRM business modeling
- Duty to protect
- Risk management processes

- This report will be returned to CLIENT for review and modification within 10 business days of the delivery of the report
- CLIENT will return changes and additional information as appropriate to support those changes.
- SFCA will deliver a final report within 10 business days of the return of comments on the draft report, reflecting changes per CLIENT's identified corrections.

Task 2:

SFCA will perform a gap analysis identifying the gaps between current IRM practices at CLIENT and current sound practices for IRM. This includes:

- SFCA will either examine the business modeling approach or other methods used to map the business into IRM and identify gaps between current business modeling techniques and results and current sound practices in this area.
- SFCA will perform a Duty to Protect analysis based on documents and information provided during Task 1 and compare results of this analysis to currently defined duties to protect associated with the IRM efforts now underway.
- SFCA will review the risk management methodologies and techniques in use and identify gaps between the current approaches and sound practices.



- ☛ SFCA will provide a draft “IRM Gap Analysis” report to CLIENT within 15 business days of acceptance of the Task 1 report by CLIENT. This report will extend the previous report to total about 45 pages in length and consist of:

An executive summary

A review of the as-is state of IRM at the enterprise:

- Business drivers for IRM
- IRM business modeling
- Duty to protect
- IRM processes

Identified desired final state of IRM at the enterprise:

- Desired IRM business modeling
- Expected future duty to protect
- Desired future IRM processes

Gap analysis

- ☛ CLIENT will return changes and additional information as appropriate to support those changes.
- ☛ SFCA will deliver a final report within 10 business days of the return of comments on the draft report, reflecting changes per CLIENT's identified corrections.

Task 3:

SFCA personnel will hold a 2-day on-site IRM workshop in which SFCA will provide detailed information on IRM approaches, review options for enterprise IRM in light of the gap analysis results, and produce a preliminary set of IRM management and technical positions in the form of an IRM architecture which can be viewed as an objective for the 3-5 year future of IRM at CLIENT. Following the workshop:

- ☛ SFCA will provide a draft “IRM Future Architecture and RoadMap” report to CLIENT within 15 business days of completion of the IRM workshop. This report will total about 45 pages in length and consist of:

An executive summary

The future IRM architecture for the enterprise:

- IRM business modeling and supporting processes
- Duty to protect and supporting processes
- IRM processes and structure

A roadmap to achieving the desired architecture in 3-5 years

Summary and conclusions

- ☛ CLIENT will return changes and additional information as appropriate to support those changes.
- ☛ SFCA will deliver a final report within 10 business days of the return of comments on the draft report, reflecting changes per CLIENT's identified corrections.



Additional information:

SFCA will facilitate this effort by using our “Enterprise Information Protection Architecture” as a guiding framework. Through extensive experience in working with other large enterprises, SFCA has developed this highly structured framework for enterprise information protection architecture planning. This framework includes the following components that will be used for this effort:

Enterprise business modeling for information protection includes:

People and things that is key to the business

Sales, marketing, and brand-related issues

Process, Work Flow, and Results

Resources, Transforms, and Value

Supply, Inventory, and Transport

AR/AP, Collections, Write-offs

Infrastructure, Services, and users

Cost, Shrinkage, and Collapse

Modeling approaches and integration

Modeling tools and techniques

Handling changes over time

Duties to Protect (DTP) for information protection includes:

Laws, regulations, and jurisdictional issues

Ownership and owner controls and requirements

Board processes and mandates

Auditors and other external reviewers

Executive decision-making and orders

Information Risk Management (IRM) for the enterprise includes:

Risk identification and evaluation

Threats, vulnerabilities, and consequences analysis framework

Risk treatment alternatives and mixes

Interdependencies, risk aggregation, and SPOF analysis

Risk and surety level matching

What to protect and how well



Data collection, interviews, analysis, and the workshop will be facilitated using custom built tools designed to allow groups to process the complex information associated with these issues and produce reasonable and readily justified decisions based on sound practices. As results are developed, they will be justified and clarified to the participants to help them gain understanding of the underlying issues while making clearer decisions about the key architectural issues.

Additional terms and conditions:

- ✿ **Single Point of Contact:** CLIENT will provide SFCA 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 SFCA and holds SFCA 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:** SFCA 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, SFCA MAKES NO WARRANTY, EITHER EXPRESSED OR IMPLIED, AS TO THE RESULTS OF THESE EFFORTS.
- ✿ **Confidentiality:** All CLIENT information is held in strictest confidence by SFCA
- ✿ **Ownership of results:** With the exception of the report and draft reports provided to CLIENT by SFCA, all materials used in the performance of this effort are the intellectual property of SFCA and will remain so.
- ✿ **No risk management decisions:** SFCA will not make any risk management decisions on behalf of CLIENT in the course of this effort. Any decision support provided by SFCA in this matter is strictly by example and nothing indicated by SFCA shall be in any way interpreted as a risk management decision made on behalf of CLIENT.

All work orally as in writing will be conducted in English.

Small to medium business with one location - Price estimate for this type of task begins at DKK 520.000,-.

Large but not highly diverse business - Price estimate for this type of task begins at DKK 760.000,-.

Enterprise and Government - Price estimate for this type of task begins at DKK 1.080.000,-.