Information Security Risk Assessment Guidelines

Introduction and Overview

Information security risk assessment is an on-going process of discovering, correcting and preventing security problems.

The risk assessment will help determine the acceptable level of risk and the resulting security requirements for data.

The risk assessment report:

- Summarizes the data, and its overall level of security;
- Recommends safeguards, and describes the expected level of risk that would remain if these safeguards were put in place;
- Presents these findings to management.

The Risk Assessment Report

A Risk Assessment (RA) Report applies to a selected information system. An information system is a group of computing and network components that share a business function, under common ownership and management. The Report will include:

- A documented system inventory, listing all system components and establishing the system boundary for the purposes of the Report;
- Documentation of the system's policies and procedures, and details of its operation;
- List of safeguards for controlling relevant threats and vulnerabilities;

The Report will reflect the security policies and objectives of Spectrum Analysis' information technology management.

A Risk Assessment Report is not intended to create or include the following, however it should be used as input for:

- A system security plan to cover any highly confidential client data;
- System security policies, or assignment of staff responsibility for system security;
- Detailed dataflows;
- In-depth analysis or resolution of specific security incidents or violations;

Appendix 1 provides a template for the documentation of the Risk Assessment report.

Appendix 1: Information Security Risk Assessment Template

1.1 System Identification	
Customer Name	
Data description	
Spectrum Manager in charge	

1.2 System Purpose and Description	
Function and purpose of the data	
System components used within Spectrum	
Technical and business users (list)	

1.3 Information Security Levels and Overall System Security Level	
Information Category	
Information Security Level	
Information Category	
Information Security Level	
Information Category	
Information Security Level	
Overall System Security Level	

Signatures

Submitted by: _____ Date: _____
              Chief Data Scientist

Reviewed by:_____ Date: _____
              [Title]