Functional Practice Statements - Administration

Level 1: Initial

1.1 There is no, or limited, security metrics performed throughout the organization.

1.2There are no, or limited, formal high-level risk assessment processes in place.

1.3 Risk assessments are done on an as-needed basis, but not yet systematically integrated into strategic planning.

Level 2: Managed

2.1Some lines of business have processes and standards for performing risk assessments.

2.2 Risk assessment criteria are defined and documented for specific items (such as credit risk) and the process is repeatable.

2.3 There is limited context to validate that the risks identified are significant to the organization as a whole.

2.4 Some general security metrics are performed

Example Work Products:

- Percentage of enterprise computers having the most recent security patches installed
- Percentage of enterprise computers having up-to-date anti-malware software installed and running
- Percentage of new hires who have had successful background checks

Level 3: Defined

3.1 Enterprise-wide adoption of risk assessments for specific items.

Example Work Products:

• The privacy risk of a third-party vendor relationship uses a common scoring methodology. Risk assessment criteria are defined and documented for specific items and the process is repeatable.

3.2 Data security policies account for the distribution of data across the different service models.

Level 4: Measured

4.1 Enterprise-wide adoption of high-level risk assessments for all components of the organization such as new projects, products, technologies, vendor relationships and/or applications and systems exist.

1.2 Risk assessment criteria are defined and documented for all items and processes are repeatable. Data on risk assessments is aggregated.

1.3 Data security benefits are linked to to organizational initiatives.

The organizations includes objective metrics for data security activities in their balanced scorecard measurements and project evaluations.

Level 5: Optimized

5.1A consistent controls framework exists and is customized to the specific profile of the firm.

5.2 Output of the controls assessment process is integrated into incident, reporting, and customer notification processes. A formal, ongoing high-level risk assessment process exists.