SSE CMM Metrics Overview

The attached metrics were developed by the ISSEA Metrics Working Group (MWG) to facilitate measuring ISO/IEC 21827, *System Security Engineering Capability Maturity Model* (SSE CMM) implementation, effectiveness, and impact. The MWG would like to thank the primary contributors to the effort:

- Michael Grimaila
- Joyce Richardson
- Michele Moss
- Nadya Bartol
- Betsy Stoddard

To develop the metrics, MWG adopted the metrics development approach described by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, *Security Metrics Guide for Information Technology Systems*. To more effectively utilize this method the approach was tailored to focus on development of metrics directly related to the ISO/IEC 21827. ISSEA MWG used ISO/IEC 21827 Process Areas (PA) and Best Practices (BP) as goals and objectives for metrics development. While useful in relation to these PAs and BPs, the proposed metrics can be decoupled from them and used in conjunction with a different set of goals and objectives and with a variety of security controls as goals and objectives. Organizations and individuals can use this list as a resource for their information security measurement efforts, including those beyond the scope of SSE CMM. The list provides the following detail for each metric:

Goal	Desired results of implementing one or several objectives that are measured by the metric.
Type	Metric type, similar to NIST SP 800-55. The types in the spreadsheet map to the metrics types as follows: Implementation/Acitivity — Implementation; Results/Output — Effectiveness/Efficiency; Impact/Outcome —Impact.
Objective	Actions that are required to accomplish the performance goal.
Description	Statement of the quantitative measurement(s) provided by the metric.
Purpose	Overall functionality obtained by collecting the metric, whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, or regulatory or legal reasons for collecting a specific metric.
Data Sources	Location of the data to be used in calculating the metric.
Implementation Evidence	Proof of the security controls' existence that validates implementation. Implementation evidence is used to calculate the metric, provides indirect indicators that validate that the activity is performed, and identifies causation factors that may point to the causes of unsatisfactory results for a specific metric.
Formula	Calculation to be performed that results in a numeric expression of a metric.
Frequency	Time periods for data collection.
Indicators	Information about the meaning of the metric and its performance trend; possible causes of trends; possible solutions to correct the observed shortcomings; performance target, if it has been set for the metric; and indication of what trends would be considered positive in relation to the performance target.

Please send questions, comments, and suggestions about the metrics list to ***slindquist@ewa.com.***