Security Metrics Evaluation Tool S(MET)

Evaluation guide

3 Categories 9 Criteria

The S(MET) training aid will assist the practitioner in developing and evaluating metrics using accepted psychometric principles in an easy to use format.

Category 1: Technical Criteria

Psychometric considerations of:
1. Reliability
2. Validity
3. Generalizerability

Category 2: Operational (Security) Criteria

Monetary costs of the metric:
1. Cost
2. Timeliness
3. Manipulation

Category 3: Strategic (Organizational) Criteria

Aspects important to senior leadership:
1. Return On Investment (ROI)
2. Organizational Relevance
3. Communication

Daniel McGarvey
daniel.a.mcgarveysr@gmail.com
540.398.7181

www.skillsdmo.com

DEFENSE AND INTELLIGENCE COUNCIL

Criteria 1 Reliability

Rate the degree to which the metric yields consistent scores that are unaffected by sources of measurement error

Rating: 1

Data for this metric is not collected very carefully;
repeated measurements by the same method reach different figurers;
different methods of measuring reach different counts when they should reach the same counts;
there is over or under counting;
the user has low confidence in the data

Rating: 3

Data for this metric is collected fairly carefully;
repeated measurements by the same method usually reach the same figures;
alternate counting methods usually reach the same figures;
there may be some over or under counting;
yet the totals are plausible

Rating: 5

Data for this metric is collected very carefully;
alternate counting methods reach the same figures;
repeated measurements by the same method reach the same figures;
there is no over or under counting;
overall there is a high likelihood that the metric is reliable

Criteria 2 Validity

Rate the degree to which evidence based on theory or quantitive research (conducted by the user or others) supports drawing conclusions from the metric

Rating: 1

The metric has only a weak relation to the problem it is trying to measure;
there is little or no evidence that the metric can be used to draw conclusions;
the user has not tested the metric to see whether decisions based on it are accurate

Rating: 3

The user has anecdotal evidence that the metric is a valid measure;
the metric appears, on its face, to be measuring what matters;
non-research literature (e.g., a trade publication) suggests that the metric is valid

Rating: 5

Research literature suggests the measure is valid;
the user has formally studied the connection between the metric and the security concern for which it is being collected, and has found the metric to be valid

Daniel McGarvey
daniel.a.mcgarveysr@gmail.com
540.398.7181

www.skillsdmo.com

DEFENSE AND INTELLIGENCE COUNCIL

Criteria 3
Generalizability

Rate the degree to which conclusions drawn from the metric are consistent and applicable across different settings, organizations, timeframe, or circumstances; extent to which metric results allow for external comparison across organizations

Rating: 1

The conclusions drawn from the metric are not consistent and not applicable across different settings, organizations, timeframes, and/or circumstances;
organizations are not willing to share the data derived from this metric;
comparisons to external organizations cannot be made based on this metric

Rating: 3

The conclusions drawn from the metric are sometimes consistent and sometimes applicable across different settings, organizations, timeframes, and/or circumstances;
organizations are sometimes willing to share the data derives from this metric;
comparisons to external organizations can sometimes be made based on this metric

Rating: 5

The conclusions drawn from the metric are consistent and applicable across different settings, organizations, timeframes. and/or circumstances;
organizations are willing to share the data derived from this metric;
comparisons to external organizations can almost always be made based on this metric

Criteria 4
Cost

Rate the degree to which monetary and non-monetary costs associated with metric development and administration; also, negative consequences associated with the metric

Rating: 1

The cost of developing or administrating the metric is high;
long or expensive training of administrators is required;
obtaining data places severe burdens on staff;
collecting the data is offensive to employees or customers (intrusiveness, complexity, etc.);
collecting the data puts priority or personal information at risk;
the metric create significant organizational strife or disruption;
calculating the metric is very difficult

Rating: 3

The cost of developing or administrating the metric is moderate;
only basic training of administrators is required;
obtaining data places only moderate burdens on staff;
collecting the data creates at most a minimal risk of offending employees or customers or disrupting operations;
calculating the metric requires a significant but acceptable level of effort;
overall there are few downsides to using the metric

Rating: 5

The cost of developing or administering the metric is minimal;
little or no training of administrators is required;
staff can obtain the data quickly and easily;
collecting the data does not offend employees or customers nor disrupts operations;
calculating the metric is quick and easy;
overall, there are no significant downsides to using the metric

Daniel McGarvey
daniel.a.mcgarveysr@gmail.com
540.398.7181

www.skillsdmo.com

DEFENSE AND INTELLIGENCE COUNCIL

Criteria 5

Timeliness

Rate the extent to which metric data can be gathered in a timely fashion so the results can have an impact

The data for this metric is out-of-date by the time it can be gathered and interpreted;
the data collection process is very time consuming;
the data is unlikely to have and impact (as it does not reflect current conditions)

Rating: 1

Rating: 3

The data for this metric is fairly up-to-date by the time it can be gathered and interpreted;
the data collection process is somewhat time consuming;
the data is somewhat likely to have an impact (as it somewhat reflects current conditions)

The data for this metric is very up-to-date when gathered and interpreted;
the data collection process is not time consuming;
the data is very likely to have an impact (as it reflects current conditions)

Rating: 5

Criteria 6

Manipulation

Rate the extent to which metric data cannot be coached, guessed, or faked by staff; extent to which metric has built-in data quality checks or oversight

The metric data is quite susceptible to manipulation;
the persons providing the data likely have an incentive to manipulate it;
there are no built-in data quality checks or oversight

Rating: 1

Rating: 3

The data underlying this metric is mostly reliable, but the providers of the data could alter the data if they wanted;
there is little incentive to manipulate the data;
there are minimally acceptable built-in data quality checks or oversight

The data underlying this metric cannot be tampered with;
the data is generated by people with no motive for manipulating it;
there are built-in data quality checks or oversight

Rating: 5

Daniel McGarvey
daniel.a.mcgarveysr@gmail.com
540.398.7181
www.skillsdmo.com

DEFENSE AND INTELLIGENCE COUNCIL

Criteria 7

Return On Investment

Rate the extent to which metric can be used to demonstrate cost savings or loss prevention in relation to relevant security spending. This involves expressing the following in terms of dollars of dollars or some other unit relevant to decision makers; the cost of the intervention, the effects of the intervention, and any unintended consequences directly related to the intervention

Rating: 1

The casual relation between the measure and the benefits gained is not clear;
the cost of the measure is hard to isolate;
the benefits of the measure are hard to calculate;
the action being measured has negative consequences that are significant but not measurable

Rating: 3

The metric theoretically captures the benefits of an action in relation to the costs of the measure;
however, it is sometimes difficult to measure the benefits, or it may sometimes be difficult to isolate the cost of the actions

Rating: 5

The metric very clearly shows the relation between a security action, policy or system and the benefits or the returns it provides;
both the benefits and the costs are readily measurable, not vague or theoretical;
the relation between the measure and the benefit gained is clear and direct.

Criteria 8

Organizational Relevance

Rate the extent to which metric is linked to organizational risk management or a strategic mission, objective, goal, asset, threat, or vulnerability relevant to the organization-- in other words, linked to the factors that matter most to senior management

Rating: 1

The metric is not linked to a specific mission, objective, goal, asset, risk, threat, or vulnerability;
if linked, the linkage is weak and of minimal relevance to the organization;
the data derived from this metric is of little importance to senior management

Rating: 3

The metric is somewhat linked to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability;
the linkage is moderate and of some relevance to the organization;
the data derived from this metric is of some importance to senior management

Rating: 5

The metric is explicitly linked to a specific organizational strategic mission, objective goal, asset, risk, threat, or vulnerability;
the linkage is strong and of high relevance to the organization;
the data derived from this metric is of great importance to senior management

Daniel McGarvey
daniel.a.mcgarveysr@gmail.com
540.398.7181
www.skillsdmo.com

DEFENSE AND INTELLIGENCE COUNCIL

Criteria 9
Communication

Rate the extent to which metric, metric results, and metric value can be communicated easily, succinctly, and quickly to key stakeholders, especially senior management

The metric and purpose of the metric are difficult to explain to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers);
it is difficult to explain the value the metric will add to the organization;
the results of the metric and implications of the results are difficult to explain

Rating: 1

Rating: 3

The metric and purpose of the metric are somewhat easy to explain to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers);
it is somewhat easy to explain the value the metric will add to the organization;
the results of the metric and implications of the results are somewhat easy to explain

The metric and purpose of the metric are easy to explain to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers);
it is easy to explain the value the metric will add to the organization;
the results of the metric and implications of the results are easy to explain

Rating: 5

Total Possible Rating: 45

Sum Metric Rating:

Notes:

Daniel McGarvey
daniel.a.mcgarveysr@gmail.com
540.398.7181
www.skillsdmo.com

DEFENSE AND INTELLIGENCE COUNCIL