The Anatomy and Lifecycle of a Metric

Recent best practice frameworks, including ISO 27000 and CobiT, are now prescribing or mandating metrics as a required component of certification. Applying regular, repeatable metrics to IT governance, risk and compliance (GRC) initiatives can benefit an organization in a number of ways, including:

- Measuring the effectiveness of controls
- Identifying and targeting areas for improvement
- Communicating the effectiveness of risk management programs
- Driving proper actions in focused areas and extending accountability
- Providing hard evidence of compliance
- Providing actionable views across the enterprise, lines of business or specific areas of IT infrastructure

Despite the benefits, few IT organizations have implemented centralized metrics initiatives. What makes it so hard? Typically, vital IT and security information is dispersed across the enterprise in disparate data silos. It is not uncommon for individual business units to develop their own solutions for the same requirement or for IT organizations to deploy multiple technologies to address a common issue. Centralizing these individual initiatives can be challenging if you don’t have an integrated, automated technology solution.

A second challenge is that the right set metrics is never the same for any two organizations. The metrics you track must be relevant to your organization and communicated effectively within the context of your business so you can align your IT initiatives with your business priorities. As a result, security metrics are shrouded in mystery and are considered “too hard” to do.

To help demystify metrics, this paper defines what makes a metric good, identifies the typical inputs and outputs, and describes the three phases of the metric lifecycle: create, calculate, communication.

WHAT IS A METRIC?

Measurements are generated by counting and provide specific views of discrete factors. Metrics, on the other hand, are generated through analysis. They are derived from measurements, to which contextual information has been added for comparison to a pre-determined baseline, or trends in measurements taken over time. Truly useful metrics indicate the degree to which goals are being met and they drive actions to improve organizational processes.
When applied to IT and security performance, a metric is the expression of the state and/or quality of a critical aspect of your IT and security infrastructure. It is the basis for directing investments to areas of high risk, as well as a forum for communication to stakeholders both inside and outside the organization.

WHAT MAKES A GOOD METRIC?
Good metrics incorporate all of the following components:

• Identification: A unique identifier that includes the author, version, and a digital signature that assures the integrity of the metric definition.

• Data Requirements: Explicit definition of the data required to drive the metric. Each data set is bound to an authoritative external data provider.

• Business logic: Complete specification of all processing required to compute the metric based upon input data sets.

• Persistence specifications: Complete specification of all steps involved in saving metric results to a metric results database.

• Schedule specifications: Instructions that ensure that the metric is run regularly according to a well-known schedule.

• Default visualization: Complete specification of one visual presentation of metric results. A metric designer is given a list of visualization options from which one may be selected.

• Business context: Additional metric attributes that map metric results to relevant entities in the business.
Upon execution, a metric consumes data from authoritative sources, such as: Asset Management, Human Relations (HR), Customer Relationship Management (CRM), Regulatory, Vulnerability and Threat Systems; Network and System Management facilities, Response Centers, and Policy Information. This raw data is transformed via special components called data actions into fully populated data sets which are consumed by deployed metrics.

A metric produces results that are stored in the form of tables in a metric results database. The metric results database, accessible via standard SQL, JDBC and other standard interfaces, can be used by other commercial products or homegrown systems to support the following functions:

- **Risk Management**: Metrics that compute threat probability, vulnerability, countermeasure coverage and asset value yield results that can be used to model risk.
- **Budget Management**: Metrics that measure level of effort or impact can be transformed into dollar values for the purpose of establishing budgets as well as computing return on investment.
- **Audit & Compliance Assessment** (Internal or External): Metrics that measure policy compliance for individual as well as groups of controls yield results that can enhance reports generated by compliance tools.
- **Security Operations**: Metrics that accumulate data over time can be used to identify trends that suggest specific actions to be taken by data center operations staff.

**THE PHASES OF THE LIFECYCLE**

The business logic associated with a metric follows a simple processing pattern:

- **Create**: Obtain primary input data from one or more authoritative sources, including commercial products or homegrown customer applications.
- **Calculate**: Apply a series of analytic operations (called actions) on the primary data to derive a result and store the result in the metric result database in the form of one or more rows in a table.
- **Communicate**: Communicate the metric results in a variety of formats including scorecard visualization, email notification, or email alert based upon detection of some policy violation.

**CREATE PHASE**

During this phase, security analysts must create, test, and deliver customized security performance metrics and scorecards. This includes identifying the authoritative sources and related data actions. Authoritative sources may include
existing infrastructure tools and enterprise applications, such as directory systems, vulnerability managers, asset managers, etc. Data sets encapsulate the business logic and communication drivers that are explicitly designed to obtain appropriate data from the specified authoritative source.

The output of this phase is atomic, executable metrics and scorecards.

CALCULATE PHASE
The calculate phase has three objectives.

- Transform raw data from one or more sources into metric results.
- Enrich the results by “mapping them to the business.”
- Store the results in a simple relational table to make them available for communication, the next phase in the lifecycle of a metric.

The transformation of raw data into metric results is typically a quantitative calculation. Examples include data cleansing to eliminate clearly inaccurate or missing data, calculating statistics such as mean, standard deviation or Z-score, applying models for forecasting, correlation or anomaly detection, aggregating details into higher level summaries, and applying policies to assign status values (red, yellow, green) or key performance indicators or grades (A, B, C, etc.).

The data enrichment step most often involves the fusion of data across two or more sources. An example of this is using data from a Human Resource database to enrich account login data from an Identity Management System. This type of enrichment operation is necessary to determine how many terminated employees still have active login accounts. In this specific example, neither raw source has all the information necessary to support the metric – namely terminated employee login account statistics.

The above described data enrichment example illustrates the process of “mapping a metric to the business.” The enrichment step allows for the identification of how well a business requirement is met. In the above example, the business requirement is to enhance security by removing login accounts for terminated employees. Without the “enriched HR data,” the metric becomes much less useful.

The process of mapping a metric to the business requires that the metric be associated with entities that are business centric, not technology centric. Each time a metric is executed, the last step is to store its results in the form of record instances within a specific database table within the metric results database.
Each stored record instance holds the following information:

- A timestamp that reflects the time at which the metric result was computed by the metric.
- A link to administrative information about the job associated with this invocation of the metric. Metrics run as jobs within the network. The metrics network collects and saves information about all jobs that run and persists this information in a collection of tables within the metric results database.
- One or more links to business entities such as location, business unit, business service, and employee status, as examples. The entities to which a metric is linked will vary depending upon the metric. For example, metrics about vulnerabilities will be linked to operating system type while metrics about identity management will be linked to employee status. Both of these types of metrics can be meaningfully mapped to entities such as location.
- Measured and/or computed values of the metric. These values can be quantitative or qualitative. An example is the WeakPWD metric that might be defined to track both the number of accounts that could be cracked in under 1 minute, 1-5 minutes, 5-15 minutes, 15-60 minutes, and over 60 minutes while also assigning a color coded status of red, orange, blue, yellow, or green to each of these intervals based upon the number of accounts cracked within that timeframe.

**COMMUNICATION PHASE**

The final lifecycle phase is the communication of metric results to authorized recipients. Delivery can be initiated by either the end user or by the metrics network.

Metrics network-managed delivery is based upon subscriptions and notification policies that an end user can define. Examples include:

- Issue an email when new results are available.
- Issue an email when newly available results meet pre-specified criteria.
- Issue an email at regular intervals, such as at 8:00 a.m. every Monday morning.

User managed delivery is based upon on-demand requests issued by a user directly to the metric results database or indirectly via a Web site or report designer. The integration of a report designer that is capable of delivering metric reports or scorecards in the form of Web pages, PDF files and graphics images is recommended.
SUMMARY
A well-planned metrics initiative delivers on governance and compliance requirements by delivering the hard facts and data that verify the existence and efficacy of controls. By moving beyond self-assessments and surveys, IT organizations can confidently evaluate IT and security investments within the context of the enterprise, enable better decision making, and safeguard information assets more effectively.

ABOUT CLEARPOINT METRICS
ClearPoint Metrics solutions enable IT and Security executives and their teams to consistently and reliably measure, monitor and communicate the state, business impact and effectiveness of their IT governance, risk and compliance initiatives. As both regulatory and best practice frameworks mandate the use of metrics, ClearPoint delivers the hard facts and data that evidence the existence and efficacy of internal controls and the executive views and scorecards that enable evaluation of performance and alignment with business objectives. CIOs and CISOs of leading Global 2000 companies rely on ClearPoint Metrics software and best practice know-how to quickly and cost effectively implement a successful metrics initiative supporting their strategic imperatives and establishing a foundation for constant improvement in safeguarding their organization’s information assets. www.clearpointmetrics.com.