



Code of Practice for Implementing and Maintaining Key Metrics

Acknowledgments

Authors:

Anass Maayouchi Edward Ray Forrest Foster Jon Christopherson Matt Cooper Max Pritikin Mosi Platt Raj Krishnamurthy Sambit Misra Willibert Fabritius

CSA Staff:

John DiMaria Pete Chronis





Key metrics¹ should always be closely tied to your primary objectives. The key point is to choose metrics that clearly indicate where you are now in relation to your goals and your expected targets. To qualify as a metric, a measurement must be based on a deep understanding of process and connect with an objective management intended.

Key metrics should be improved. Key metrics measure progress, which means there needs to be room for improvement. For example, increasing your uptime by 3%. If you're already at 100%, your team will be focused on maintaining that level instead of improving it.

Key metrics should inspire action. When your metrics are important and can be improved, it will be the pulse of the company and your team will immediately know what to do or what questions to ask in order to determine possible root causes and work to resolve them in a timely fashion. Key metrics are ever fluctuating. If they are static and not providing a measure of effectiveness (or lack thereof) they are not key metrics.

- **Strategic and Aligned.** To create effective key metrics, you must start at the endpoint with the goals, strategic objectives or outcomes you want to achieve. It's important that performance metrics are aligned with corporate objectives. To align metrics, you need to devise them together in the context of an entire ecosystem designed to drive certain behaviors.
- **Simple.** Key metrics must be understandable. Stakeholders should be trained to know what is being measured, how it is calculated, what are data sources, what the targets are, how incentives work, and, more importantly, what they can do to affect the outcome in a positive direction.
- **Establish RACI (Responsible, Accountable, Consulted and Informed).** Every performance metric needs an owner who is held accountable for its outcome. Without accountability, metrics are meaningless. Additionally, recipients of every metric must be identified, different levels/details can be defined depending on the destination of the metric result (Management, Ops, Customers, ...)
- 4 Actionable. Metrics should be actionable. That is, if a metric trends downward, employees should know the corrective action process to facilitate the decision on what corrective actions to take to improve performance. To achieve that, metrics must have a defined objective (Target), and a defined threshold, when the metric is on its threshold, an action plan becomes mandatory in order to identify the root cause and define adapted measures.
- **Frequency (Hourly, Daily).** Actionable metrics require timely data. Performance metrics must be updated frequently enough so the accountable individual or team can intervene to improve performance before it is too late. If needed for the same metric, different frequencies can be considered depending of the destination (Management, Ops, customers ...)

© Copyright 2021, Cloud Security Alliance. All rights reserved.

¹ A key metric is also known as a key performance indicator, or KPI. A key metric is a statistic which, by its value gives a measure of an organization's, department's or processes overall health and performance.





- **6 Referenceable and Relevant.** For users to trust a performance metric, they must understand its origins. Why did we choose this metric? Also important to remember that a performance metric has a natural shelf-life. When first introduced, the performance metric energizes the stakeholders to improve. Over time, the metric loses its impact as you reach your goal and processes and technology must be refreshed, or revised to stay relevant.
- Accurate and Correlated. It is difficult to create performance metrics that accurately measure an activity. The measurement system delivering the metric needs to be Repeatable and Reliable. It is easy to choose metrics that do not accurately measure the intended objective. A good assessment should be reliable, valid, and free of bias, i.e; stable and consistent results. Periodic statistical evaluations should be performed to test the accuracy. Additionally performance metrics are designed to drive desired outcomes and/or achieve specific targets. When you choose metrics you must calculate the degree to which they influence the behaviors or expected outcomes. Companies must continually refresh performance metrics to ensure they correlate and drive the desired outcomes.
- **Tamper-proof.** Organizations need to test all performance metrics to ensure that they can't be circumvented. The process needs to be consistent. Data needs to be consistently collected from the same source and data submitted the same way, same schedule and using the same process. If the process is changed, it should be noted at that point in time so as not to confuse the analysis.

The metrics catalog containing the above elements should be formalized per indicator/Metric as an "indicator identity card".

© Copyright 2021, Cloud Security Alliance. All rights reserved.

² https://www.leansixsigmadefinition.com/glossary/gage-rr/