KPIs vs. KRIs: Measuring the Program You Have and the Risk You're Taking

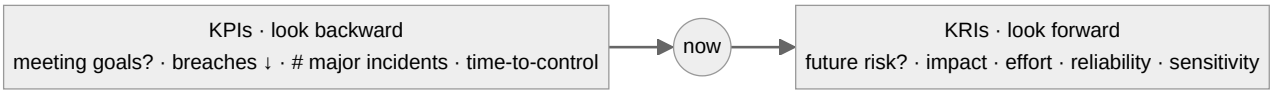
Fri, Aug 28, 6:00 PM EDT · https://scottslab.io/posts/kpis-and-kris-security-metrics

TL;DR

KPIs look backward: are we hitting our security goals? (ITIL lists example KPIs: % decrease in breaches, number of major incidents, time from spotting a threat to shipping a control.) KRIs look forward: what risk could jeopardize us next? (ISACA says pick them by business impact, implementation effort, reliability, and sensitivity.) The rule that makes either one honest: define the metric before you measure, so nobody cherry-picks the number that flatters them.

Security metrics come in two directions, and mixing them up is how leadership ends up reassured about the wrong thing.

Key Performance Indicators look backward. They measure whether the security program actually met the goals you set: a report card on what already happened. ITIL offers a set of example KPIs worth stealing, among them the percentage decrease in breaches, the number of major incidents, and the time between identifying a threat and getting a control in place for it. That last one is my favorite, because it measures the thing that actually determines your exposure: not whether you eventually fixed it, but how long you sat in the window before you did.



KPIs vs. KRIs: Measuring the Program You Have and the Risk You're Taking

Key Risk Indicators look forward. Instead of grading past performance, they quantify risk that could jeopardize your security going forward: early-warning gauges rather than a rear-view mirror. Because you could track an infinite number of them, ISACA gives you selection criteria so you pick the ones that earn their place: business impact (does this risk actually matter?), implementation effort (can we realistically measure it?), reliability (is the signal trustworthy?), and sensitivity (does it move early enough to warn you?). A KRI that only spikes after you're already breached is just a slow KPI.

The rule that keeps both honest is the same, and it's the whole point: define your metrics in advance. If you decide what "good" looks like *after* the numbers are in, you'll unconsciously (or consciously) pick the framing that makes the program look best. That's cherry-picking dressed up as reporting. Metrics chosen before the measurement are accountability; metrics chosen after are marketing. Write down what you'll track and what target counts as success, then let the numbers land where they land.

Written by Scott S. — Contact: scott@scottschlangen.com — scottslab.io — https://scottslab.io/posts/kpis-and-kris-security-metrics