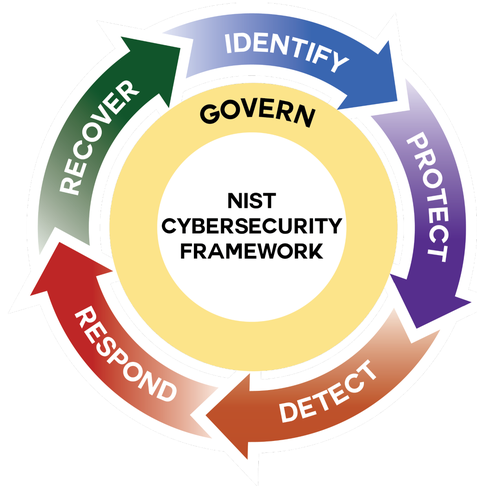
Cybersecurity Metrics Reporting Model (CMRM)

Version 2024.1

The ComplianceForge Cybersecurity Metrics Reporting Model (CMRM) takes a practical view towards implementing a sustainable metrics reporting capability. At the end of the day, executive management (e.g., CIO, CEO, Board of Directors (BoD), etc.) wants an answer to a relatively-straightforward question: ***"Are we secure and compliant?"*** In order for a CISO to honestly provide an answer, it requires a way for the CISO to measure and quantify an "apples and oranges" landscape where processes and technologies lack both uniform risk weighting and abilities to capture metrics. The CMRM solves this aspect of dissimilarity by utilizing a weighted approach to metrics that generate Key Performance Indexes (KPXs) as a way to logically-organize and report individual metrics. Using KPX enables the CMRM to provide a reasonable and defendable answer.

The "Are we secure?" question is best answered as a numerical score. This quantifiable score is used to visualize the score against a numerical spectrum to provides context, based on the risk profile of the organization. The numerical score would land between "not secure" and "secure" on the spectrum, according to a baseline score definition that would be specific to the organization. This can provide long-term trending to evaluate the direct impact of certain security initiatives. The CMRM can be automated in a Governance, Risk & Compliance (GRC) or Integrated Risk Management (IRM) platform, but it comes as a Microsoft Excel spreadsheet as part of ComplianceForge's Digital Security Program (DSP). The "Are we secure and compliant?" question can be tracked to display trending, as well as drilled down into Key Performance Indexes (KPXs), or individual metrics, to identify why the score changed.

Organized into six (6) categories, the KPX help answer specific aspects of the "Are we secure and compliant?" question. It is increasingly common for BoD to want reporting in terms of the NIST Cybersecurity Framework (NIST CSF) so KPX are aligned with the NIST CSF 2.0 functions (e.g., Govern, Identify, Protect, Detect, Respond & Recover). The KPX are designed to encompass Key Performance Index (KPI) and Key Risk Index (KRI). The metrics/analytics shown in this model are included in the ComplianceForge DSP.



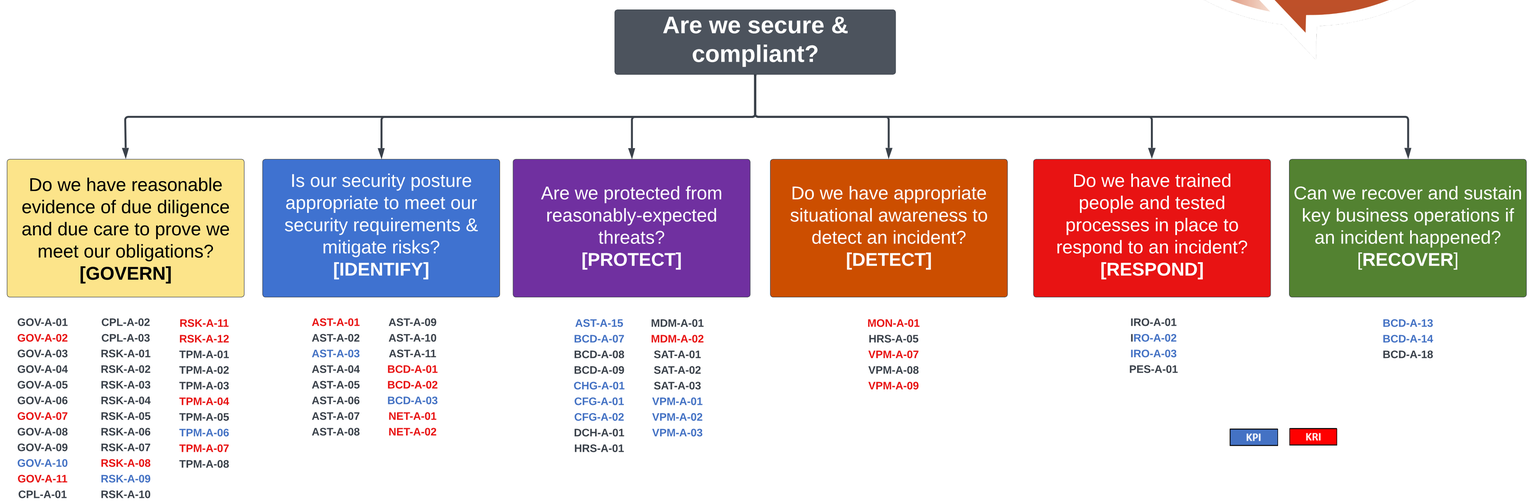
What does a CISO/CIO/CEO/Board wants to know?

Key Performance Indexes (KPX) combine function-specific and weighted metrics to answer the "Are we secure and compliant?" question.

KPXs are grouped to align with the NIST Cybersecurity Framework 2.0.

Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) exist within the metrics that make up the KPX.

KRIs and KPIs provide insights into a specific area being measured to help identify trending that is of specific importance to management



Metrics vs Analytics Discussion

It is important to point out that metrics are discrete, "point in time" measurements. The CMRM utilizes metrics to develop analytics. Analytics are generated from the analysis of metrics and that is generally what executive management expects when they improperly ask for "metrics" when the intent is to have analytics.

Analytics are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance related data. Therefore the KPX utilize these analytics to generate reporting numbers that are based on relative weighting, based on the organization's risk profile.

Trending

Once you start collecting metrics from your environment and you've defined the analytics you want to report on, it is possible to use this model to provide a historical trend. This is something that is feasible to generate reporting in tools as common as Microsoft Excel or it can be captured in a custom-designed tool.

Where this is useful is that historical trending can be used to identify what is and what is not working. This increased situational awareness can help in risk management decisions and budget expenditures.