Executive Metrics Reporting For Situational Awareness & Oversight

The ComplianceForge Security Metrics Reporting Model™ (SMRM) 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?" 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 SMRM 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 SMRM 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 SMRM 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?" question can be both tracked to display trending and drilled down into KPXs, or individual metrics, to identify why the score changed.

Organized into five (5) categories, the KPX help answer specific aspects of the "Are we secure?" 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 five (5) NIST CSF functions (e.g., 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.

NIST CYBERSECURITY FRAMEWORK — IDENTIFY · PROTECT · DETECT · RESPOND · RECOVER
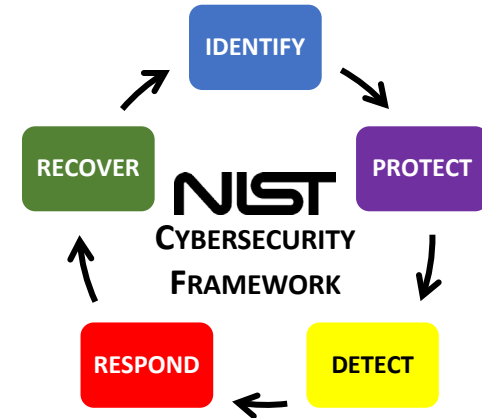
What does a CISO/CIO/CEO/Board wants to know?

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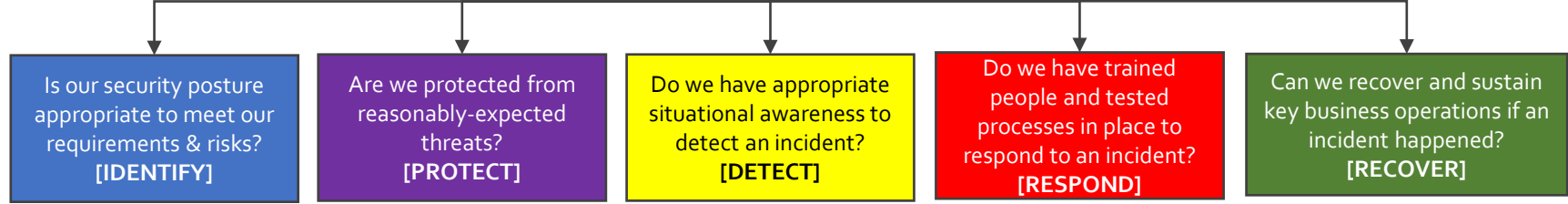
Key Performance Indexes (KPX) combine function-specific and weighted metrics to answer the "Are we secure?" question.

KPXs are grouped to align with the NIST Cybersecurity Framework.

Is our security posture appropriate to meet our requirements & risks? **[IDENTIFY]**	Are we protected from reasonably-expected threats? **[PROTECT]**	Do we have appropriate situational awareness to detect an incident? **[DETECT]**	Do we have trained people and tested processes in place to respond to an incident? **[RESPOND]**	Can we recover and sustain key business operations if an incident happened? **[RECOVER]**

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.

[IDENTIFY]
AST-A-01, AST-A-09, NET-A-02
AST-A-02, AST-A-10, RSK-A-01
AST-A-03, AST-A-11, RSK-A-02
AST-A-04, BCD-A-01, RSK-A-03
AST-A-05, BCD-A-02, RSK-A-04
AST-A-06, BCD-A-03, RSK-A-05
AST-A-07, CPL-A-01, TPM-A-01
AST-A-08, NET-A-01, TPM-A-02

[PROTECT]
AST-A-15, MDM-A-01
BCD-A-07, MDM-A-02
BCD-A-08, SAT-A-01
BCD-A-09, SAT-A-02
CHG-A-01, SAT-A-03
CFG-A-01, VPM-A-01
CFG-A-02, VPM-A-02
DCH-A-01, VPM-A-03
HRS-A-01

[DETECT]
MON-A-01
HRS-A-05
VPM-A-07
VPM-A-08
VPM-A-09

[RESPOND]
IRO-A-01
IRO-A-02
IRO-A-03
PES-A-01

[RECOVER]
BCD-A-13
IRO-A-07

KPI
KRI

Metrics vs Analytics Discussion

It is important to point out that metrics are discrete, "point in time" measurements. The SMRM 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.
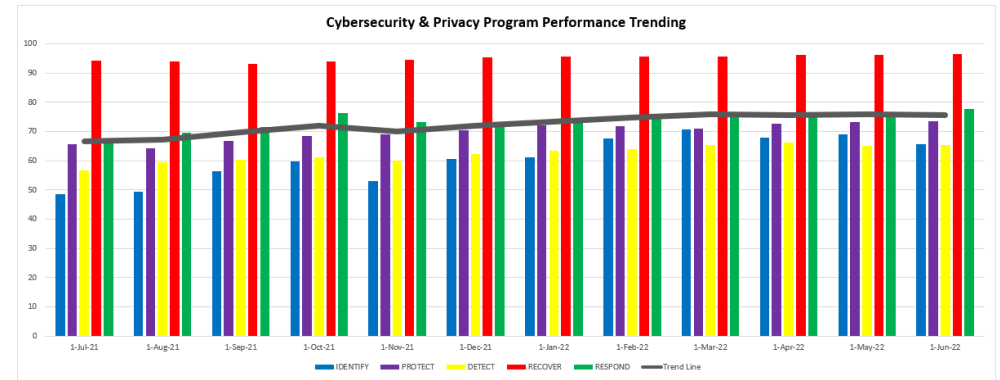
Analytics are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance related data. Therefore the KPX utilize these analytics to generate reporting numbers that are based on relative weighting, based on the organization's risk profile.

Cybersecurity & Privacy Program Performance Trending

(Secure / Minor Issues / Significant Deficiencies / Not Secure)

Legend: IDENTIFY · PROTECT · DETECT · RECOVER · RESPOND · Trend Line