Executive Reporting For Situational Awareness & Oversight

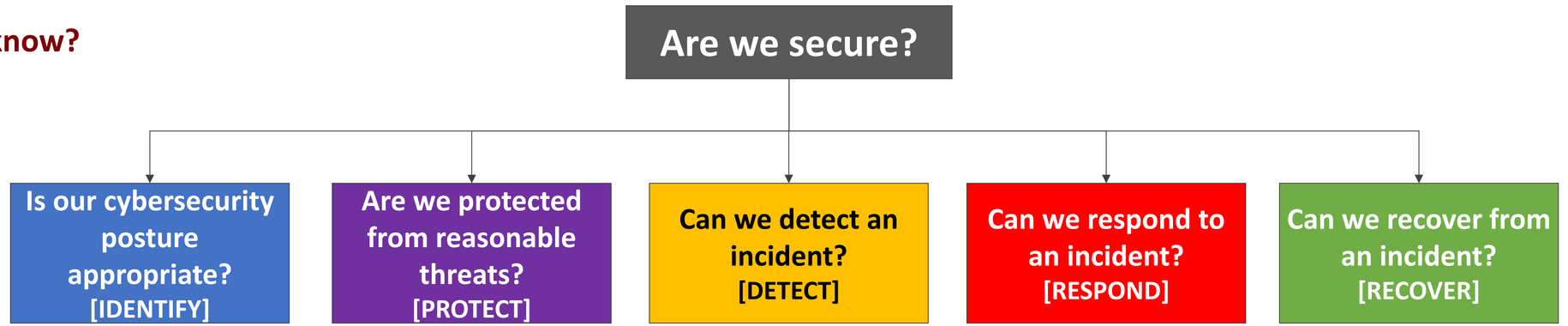
version 2019.2

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. Through automating the SMRM in a **Governance, Risk & Compliance (GRC)** platform, the "*Are we secure?*" question can be both tracked to display trending and can be 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. Since many BoD are now wanting reporting in terms of the NIST Cybersecurity Framework (NIST CSF), the KPX are also aligned with the NIST CSF for added functionality (e.g., Identify, Protect, Detect, Respond & Recover). The KPX is designed to encompass Key Performance Index (KPI) and Key Risk Index (KRI) metrics. The metrics shown in this model are included in the ComplianceForge Digital Security Program (DSP).

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



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.

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.

KPI

KRI

AST-M-01	DCH-M-04	RSK-M-07	AST-M-17	END-M-02	PRM-M-05	END-M-01	MON-M-10	IRO-M-07	BCD-M-03
AST-M-02	GOV-M-01	RSK-M-08	BCD-M-01	END-M-03	TDA-M-01	END-M-04	MON-M-11	IRO-M-08	BCD-M-08
AST-M-03	GOV-M-02	RSK-M-09	BCD-M-04	GOV-M-03	SAT-M-01	HRS-M-04	MON-M-12	IRO-M-09	BCD-M-09
AST-M-04	HRS-M-03	RSK-M-10	BCD-M-05	HRS-M-01	SAT-M-02	IRO-M-03	PES-M-03	IRO-M-10	IRO-M-22
AST-M-05	HRS-M-05	RSK-M-11	BCD-M-06	HRS-M-02	SAT-M-03	IRO-M-04	VPM-M-16	IRO-M-12	IRO-M-23
AST-M-06	NET-M-03	RSK-M-12	BCD-M-07	IAC-M-01	SAT-M-04	IRO-M-05	VPM-M-17	IRO-M-14	IRO-M-24
AST-M-07	NET-M-04	RSK-M-13	BCD-M-10	IAC-M-02	SAT-M-05	IRO-M-11	VPM-M-18	IRO-M-25	
AST-M-08	NET-M-05	RSK-M-14	BCD-M-11	IAC-M-03	SEA-M-01	IRO-M-13	VPM-M-19	IRO-M-26	
AST-M-10	NET-M-06	RSK-M-15	CAP-M-01	IRO-M-01	VPM-M-01	MON-M-04	VPM-M-20	IRO-M-27	
BCD-M-02	NET-M-07	THR-M-01	CFG-M-01	IRO-M-15	VPM-M-02	MON-M-05	VPM-M-21	IRO-M-28	
BCD-M-12	PRM-M-01	THR-M-02	CFG-M-02	IRO-M-16	VPM-M-03	MON-M-07	VPM-M-22	IRO-M-31	
BCD-M-13	PRM-M-02	TPM-M-01	CFG-M-03	IRO-M-21	VPM-M-04	MON-M-08	VPM-M-23	IRO-M-32	
CLD-M-01	PRM-M-03	TPM-M-02	CHG-M-01	MNT-M-01	VPM-M-05	MON-M-09	VPM-M-26	MON-M-06	
CPL-M-01	PRM-M-04	TPM-M-03	CHG-M-02	MNT-M-02	VPM-M-06			VPM-M-15	
CPL-M-02	RSK-M-01	TPM-M-04	CHG-M-03	MNT-M-03	VPM-M-07				
CPL-M-03	RSK-M-02	TPM-M-05	CHG-M-04	MON-M-01	VPM-M-08				
CPL-M-04	RSK-M-03	TPM-M-06	CHG-M-05	MON-M-02	VPM-M-09				
DCH-M-01	RSK-M-04	TPM-M-07	CPL-M-05	MON-M-03	VPM-M-10				
DCH-M-02	RSK-M-05	TPM-M-08	CRY-M-01	NET-M-01	VPM-M-11				
DCH-M-03	RSK-M-06	TPM-M-09	CRY-M-02	NET-M-02	VPM-M-12				
			CRY-M-03	NET-M-08	VPM-M-13				
			MDM-M-01	PES-M-01	VPM-M-14				
			DCH-M-05	PES-M-02					
			DCH-M-06	PES-M-04