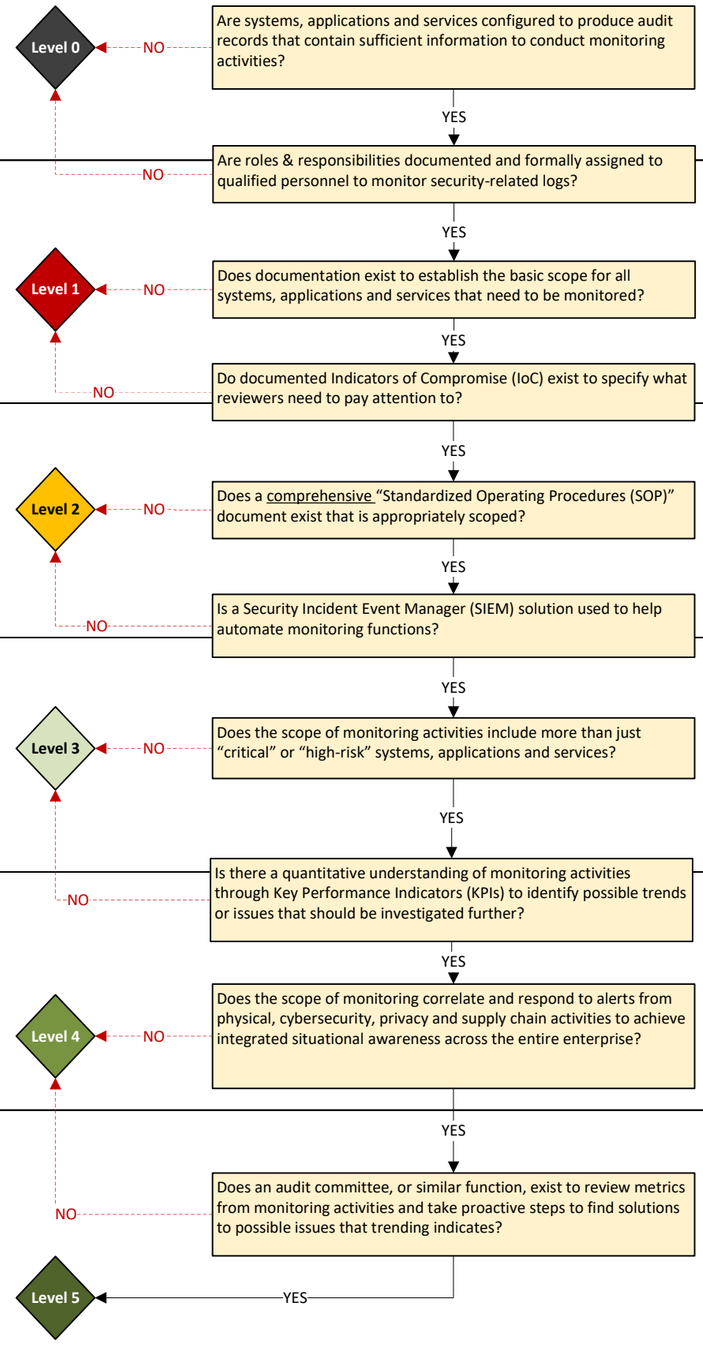
Cybersecurity Program Maturity – Holistic View of People, Processes & Technology (PPT)

ISO/IEC 21827:2008 Systems Security Engineering – Capability Maturity Model (SSE-CMM)		Example Assessment of Cybersecurity Program Maturity – SCF Control # MON-01 (*Continuous Monitoring*)
Level 0 Not Performed	There is general failure to attain the purpose of the process. There are few or no easily identifiable work products or outputs of the process.	NEGLIGENT
Level 1 Performed Informally	Base practices of the process area are generally performed. The performance of these base practices may not be rigorously planned and tracked. Performance depends on individual knowledge and effort. Work products of the process area testify to their performance. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for the process.	AD HOC OPERATIONS
Level 2 Planned & Tracked	Performance of the base practices in the process area is planned and tracked. Performance according to specified procedures is verified. Work products conform to specified standards and requirements. Measurement is used to track process area performance, thus enabling the organization to manage its activities based on actual performance. The primary distinction from Level 1, Performed Informally, is that the performance of the process is planned and managed.	REQUIREMENT-DRIVEN OPERATIONS
Level 3 Well Defined	Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes. The primary distinction from Level 2, Planned and Tracked, is that the process is planned and managed using an organization-wide standard process.	ENTERPRISE-WIDE OPERATIONS
Level 4 Quantitatively Controlled	Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed, and the quality of work products is quantitatively known. The primary distinction from the Well Defined level is that the defined process is quantitatively understood and controlled.	METRICS-DRIVEN OPERATIONS
Level 5 Continuously Improving	Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization. Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies. The primary distinction from the quantitatively controlled level is that the defined process and the standard process undergo continuous refinement and improvement, based on a quantitative understanding of the impact of changes to these processes.	WORLD-CLASS OPERATIONS

SCF Control #: MON-01
Control Description: Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.



Courtesy of: www.complianceforge.com

Reasonably-expected technologies or documentation for CMM1:
- Policies & standards that require monitoring functions.
- System configurations support the collection of audit logs in sufficient detail to conduct monitoring.
- Assigned roles & responsibilities to one or more individuals.

Reasonably-expected technologies or documentation for CMM2:
- Centralized log aggregator exists that provides 8x5x5 (weekday) situational awareness of security logs from critical systems, applications and services.
- Documented asset inventory that provides a basic view of systems, applications and services that require monitoring.
- Documented Indicators of Compromise (IoC).
- Some form of daily, weekly or monthly activity reporting to management.

Reasonably-expected technologies or documentation for CMM3:
- Security Incident Event Manager (SIEM) solution exists that provides 24x7x365 situational awareness of security logs from critical systems, applications and services.
- Documented Standardized Operating Procedures (SOP) exists to govern how monitoring activities are performed that ensure standardized processes are maintained.

Reasonably-expected technologies or documentation for CMM4:
- Scope of logging is more than just critical systems, applications and services and includes less-critical assets.
- Key Performance Indicators (KPIs) are developed and reported against.
- Logs from Host-based Intrusion Protection System (HIPS)
- Logs from Network-based Intrusion Protection System (NIPS)
- Logs from File Integrity Monitoring (FIM)

Reasonably-expected technologies or documentation for CMM5:
- Executive-staffed audit committee, or similar function, that is tasked with governing enterprise-level monitoring operations.
- Documented process that is permanently staffed by a project manager who is tasked with continuous refinement and improvement of processes, based on monitoring metrics.