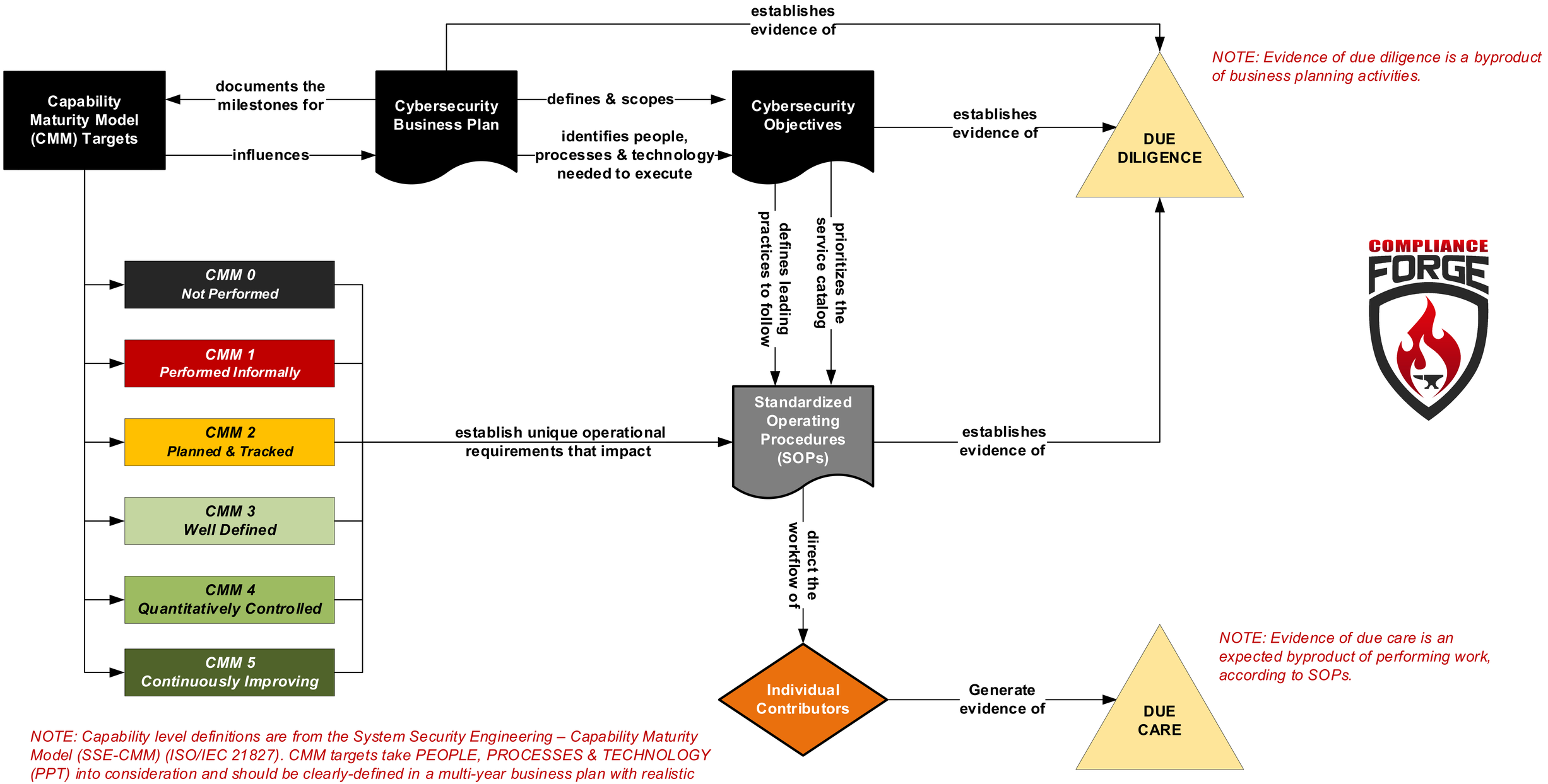
Operationalizing Cybersecurity Business Plans

version 2020.2

The **ComplianceForge** Operationalizing Cybersecurity Planning Model™ (OCPM) takes a practical view towards implementing cybersecurity business plans. CISOs are often not at a loss for a plan, but executing these plans often fall short due to disconnects between strategic, operational and tactical components of the planning process. At the end of the day, Individual Contributors (ICs) need to know how they fit into business planning, what their priorities are, and what is expected from them in their duties.

The nexus of any business plan should be a Capability Maturity Model (CMM) target that provides quantifiable expectations for People, Processes and Technologies (PPT). Likely, there is a phased, multi-year roadmap to meet these CMM-based cybersecurity objectives. Those documented objectives, in conjunction with the business plan, provide evidence of due diligence. The objectives define the operational needs and prioritization of PPT and those include standardized procedures, for how these technologies and processes are implemented at a tactical level. Those Standardized Operating Procedures (SOPs) both direct the workflow of ICs, but the output of the SOPs provides evidence of due care.



NOTE: Evidence of due diligence is a byproduct of business planning activities.

NOTE: Capability level definitions are from the System Security Engineering – Capability Maturity Model (SSE-CMM) (ISO/IEC 21827). CMM targets take PEOPLE, PROCESSES & TECHNOLOGY (PPT) into consideration and should be clearly-defined in a multi-year business plan with realistic milestones to mark CMM progress.

NOTE: Evidence of due care is an expected byproduct of performing work, according to SOPs.