Operationalizing Cybersecurity Business Plans

version 2019.1

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 in the planning and implementing processes. Where the rubber meets the road, Individual Contributors (ICs) need to know (1) how they fit into business planning, (2) what their priorities are and (3) what is expected from them in their duties. When looking at it from an auditability perspective, the evidence of due diligence and due care should match what the cybersecurity business plan is attempting to achieve.

The central focus of any cybersecurity business plan should be a Capability Maturity Model (CMM) target that provides quantifiable expectations for People, Processes and Technologies (PPT), since this helps prevent a "moving target" by establishing an attainable expectation for "what right looks like" in terms of PPT. Generally, cybersecurity business plans take a phased, multi-year approach to meet these CMM-based cybersecurity objectives. Those objectives, in conjunction with the business plan, demonstrate evidence of due diligence on behalf of the CISO and his/her leadership team. The objectives prioritize the organization's service catalog through influencing procedures at the IC-level for how PPT are implemented at the tactical level. Those Standardized Operating Procedures (SOPs) not only direct the workflow of ICs, but the output from procedures provide evidence of due care.