

Operationalizing Cybersecurity Business Plans – CMMC Specific

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 clear target that provides quantifiable expectations for People, Processes and Technologies (PPT). In the case of Cybersecurity Maturity Model Certification (CMMC), that compliance framework provides a specific target and minimum expectations are provided in NIST 800-171A. For most organizations, compliance efforts are a phased, multi-year roadmap to meet these cybersecurity objectives. Those documented objectives, in conjunction with the business plan and the organization's documented policies and standards, 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**.

