Secure, Compliant & Resilient Management System (SCRMS) Principles

A Plan, Do, Check & Act (PCDA) Approach To Being Secure, Compliance & Resilient

version 2026.1

The Security, Compliance & Resilience Management System (SCRMS) takes a comprehensive view towards governing a cybersecurity and data privacy program. Without an overarching concept of operations for the broader Governance, Risk & Compliance (GRC) function, organizations will often find that their governance, risk, compliance and privacy teams are siloed in how they think and operate. These siloed functions and unclear roles often stem from a lack of a strategic understanding of how these specific functions come together to build a symbiotic working relationship between the individual teams that enables quality control over people, processes and technology. The SCRMS principles utilize the Deming Cycle, or a Plan, Do, Check & Act (PCDA) approach, that is a logical way to design a governance structure:

- Plan. The overall GRC process begins with planning. This planning will define the policies, standards and controls for the organization. It will also directly influence the tools and services that an organization purchases, since technology purchases should address needs that are defined by policies and standards.
- **Do**. Arguably, this is the most important section for cybersecurity and privacy practitioners. Controls are the "security glue" that make processes, applications, systems and services secure and compliant. Procedures (also referred to as control activities) are the processes how the controls are actually implemented and performed. The Secure Controls Framework (SCF) can be an excellent starting point for a control set if your organization lacks a comprehensive set of cybersecurity and privacy controls.
- **Check**. In simple terms, this is situational awareness. Situational awareness is only achieved through reporting through metrics and reviewing the results of audits/assessments.
- **Act**. This is essentially risk management, which is an encompassing area that deals with addressing two main concepts (1) real deficiencies that currently exist and (2) possible threats to the organization.