The "ComplianceForge Reference Model" for writing documentation is entirely based on industry-recognized "best practices" according to terminology definitions from NIST, ISO, ISACA and AICPA. This approach is designed to encourage clear communication by clearly defining cybersecurity and privacy documentation components and how those are linked. This comprehensive view identifies the primary documentation components that are necessary to demonstrate evidence of due diligence and due care. It addresses the inter-connectivity of policies, control objectives, standards, guidelines, controls, risks, procedures & metrics. The Secure Controls Framework (**SCF**) fits into this model by providing the necessary cybersecurity and privacy controls an organization needs to implement to stay both secure and compliant. ComplianceForge simplified the concept of the hierarchical nature of cybersecurity and privacy documentation that visualizes the unique nature of these components, as well as the dependencies that exist.

To demonstrate that bold claim, we wrote the "START HERE: A guide to understanding cybersecurity and data protection documentation". This follows the schema shown above (the Hierarchical Cybersecurity Governance Framework (HCGF)) that demonstrates the linkages from policies all the way through metrics. The following guide is designed to demonstrate "what right looks like" for cybersecurity and privacy documentation, so that it is at the same time scalable, concise and provides comprehensive coverage. You can jump straight to the definitions on page 6 if you are curious.