Understanding Basic Cybersecurity & Data Protection Documentation Components

It is imperative that cybersecurity and privacy documentation be scalable and flexible, so it can adjust to changes in technology, evolving risk and changes within an organization. The modern approach to cybersecurity and privacy documentation is being modular, where it is best to link to or reference other documentation, rather than replicated content throughout multiple policy or standard documents. Not only is "traditional model of cybersecurity documentation" inefficient, but it can also be confusing and lead to errors. Additionally, when it comes to audits/assessments, it is true that "time is money" where inefficient, cumbersome documentation has a very real financial cost associated with the amount of time it takes an auditor/assessor to parse through the documentation. Concise, efficient documentation can pay for itself in the cost-savings from a single audit/assessment. Additionally, having good cybersecurity documentation can be “half the battle” when preparing for an audit, since it shows that effort went into the program and key requirements can be easily found.

A good example of documentation that is scalable, modular and hierarchical is in the diagram below: