External vs Internal Documentation

External Frameworks

Industry frameworks are often referred to as a standard. In reality, most frameworks are merely a repository of specific controls that are organized by control families (e.g., NIST CSF, ISO 27002, NIST SP 800-171, NIST SP 800-53, etc.). For example, while **NIST SP 800-53 R5** is called a "standard" it is made up of 1,189 controls that are organized into 20 control families (e.g., Access Control (AC), Program Management (PM), etc.). These controls are what make up NIST SP 800-53 as a "framework" that an organization can use as a guide to develop its internal policies and standards that allow it to align with those expected practices.

Internal Cybersecurity & Privacy Documentation

An organization is expected to identify cybersecurity and privacy principles (e.g., industry framework) that it wants to align its cybersecurity and privacy program with, so that its practices follow reasonably-expected controls. For example, to help make an organization's alignment with its NIST SP 800-53 R5 more straightforward and efficient:

- A policy that corresponds to each of the control families that defines executive leadership's statement of management intent for that specific area of focus (e.g., access control, compliance, physical security, etc.).
- Control objectives provide a 1-1 mapping to address a specific control (e.g., AC-3, AC-7, etc.). For each control, there should be a control objective.
- Granular standards addresses the particulars necessary to accomplish the objective of the control (hence the name "control objective").
- Guidelines may or may not be needed to provided additional details about the standard.
- Procedures (e.g., Standardized Operating Procedures (**SOP**)) describes how the standard is operationalized to meet the intent of the control.