Solaris Consulting Group

Policy and Process Development (P&PD)

- **Purpose:** Its purpose is to establish the organizational policies and processes that govern cybersecurity across the enterprise. These documents are foundational. Without them, there is no basis for assigning responsibility, holding organizational members (staff, partners) accountable, no ability to meet compliance and no basis for developing the supporting technical systems. As an example, each family of security controls in NIST 800-53 and the same for the ISO 27000 series begins with policy and process. The technical security controls follow from determining the organization's policies and processes. Lastly to emphasize this point, the first thing the auditor will ask for is the documented and approved policies and processes that lead to the run-books.
- **Level of Effort:** The LOE is determined by a project scope worked out with the client. It is dependent on the size and complexity of the organization. This is generally considered to be the fourth element of any cybersecurity activity. A yearly review and refresh is required to correct for the drift that may occur with changes in the organization and its supporting
- **Owner:** The owner of the deliverables is typically the CISO or the equivalent role.
- **Completing the P&PD:** Solaris Consulting Group (SCG) conducts a template-driven development of the P&PD starting with an Information System Security Plan (ISSP). The ISSP is one of the documents that defines the target information system, what it should be on completion of the roadmap. Other documents in the series establish authorized use policies. However, the P&PD is not alone sufficient to operate. Operations requires "run-books" that are detailed. These run-books are not part of this effort, rather would be developed as part of the implementation projects. Cybersecurity is a cost to the organization. SCG's methodology will assure aid in budget formation, that the cost of the cybersecurity operations is efficient and effective and based on the foundations of what is necessary for the organization to operate securely within its threat / risk profile.
- **Key Elements:**
  - Templates: SCG uses templates to develop the documents that provide the basic structure, then tailored to meet the specific organization's situation. It includes the privacy documents that establish use and control of personal identifiable information.
  - Architecture: It starts with identifying the business structure that allows an architectural understanding for how the information system is constructed, ideally a close match between major business function and the supporting system. Segregation into enclaves of operation (logical / physical isolation) is expected.
  - Systems of Record: Defining the Systems of Record (SOR) provides the authorizing mechanism to control the operation. All aspects of this are considered and make up part of how SCG develops the P&PD.
- **The Solution Package:** The list of deliverables for this service offering includes:
  - Deliverable 1: A package of documents that establish the organizational cybersecurity policy and processes aligned to the tailored set of security controls, the business and cybersecurity architecture, the risk mitigation priorities, gap analysis and roadmap.
  - Deliverable 2: An Information System Security Plan that defines the target system for implementation to baseline cybersecurity
  - Deliverable 3: A protected library of the completed documents in electronic folders

Features of P&PD

- A library of the required P&PD documents
- Template driven for efficiency and consistency
- Architecture-based
- Business-Aligned
- NIST CSF guided strategy

Benefits of P&PD

- Defines the target state
- Documents the authorized system by establishing SORs
- Foundation for operation including the creation of the Run Books at implementation
- Useful in developing a cybersecurity operating budget